DISSECTING THE HACK

The Forb1dd3n Network

Jayson E. Street
Kent Nabors

Dissecting the Hack

This page intentionally left blank

Dissecting the Hack
The F0rb1dd3n Network

Jayson E. Street

Kent Nabors

AMSTERDAM • BOSTON • HEIDELBERG • LONDON
NEW YORK • OXFORD • PARIS • SAN DIEGO
SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO
Syngress is an imprint of Elsevier

SYNGRESS®

Syngress is an imprint of Elsevier
30 Corporate Drive, Suite 400, Burlington, MA 01803, USA
Linacre House, Jordan Hill, Oxford OX2 8DP, UK

Dissecting the Hack: The F0rb1dd3n Network

Notices
Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding, changes in research methods, professional practices, or medical treatment may become necessary.
Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information, methods, compounds, or experiments described herein. In using such information or methods, they should be mindful of their own safety and the safety of others, including parties for whom they have a professional responsibility.
To the fullest extent of the law, neither the Publisher nor the authors, contributors, or editors assume any liability for any injury or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions, or ideas contained in the material herein.

Library of Congress Cataloging-in-Publication Data
Application submitted

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library.

ISBN: 978-1-59749-478-6

Printed in the United States of America

09 10 11 12 13 10 9 8 7 6 5 4 3 2 1

Typeset by: diacriTech, Chennai, India

Publisher: Laura Colantoni
Acquisitions Editor: Rachel Roumeliotis
Assistant Editor: David Bevans
Project Manager: Julie Ochs

To Earl L. Street
All that I am and part of what my children will become is because of who you were. Thank you and I miss and think of you everyday.

To Dee Drake and Aliera
For all the love you give me thank you. Also for putting up with me when I am there and missing me when I am away.

This page intentionally left blank

Contents

Foreword

The world of hacking is a world of pain and frustration. Frustration for the hacker as he tries to figure out how to break the latest and greatest security device, and pain for the manufacturer or corporate that made or was relying on that device.

At least, that is the layman's view – the hacker is the "bad guy," set on doing evil and causing pain to those he comes up against, and interested only in one thing: destroying the security of the systems in front of him, and the manufacturer is the innocent victim, trying to go about its business, but suffering unprovoked attacks. But it's not as simple as that. Hackers come in all shapes and sizes, some good and some bad, and they hack for all kinds of reasons, some benign and some selfish. Manufacturers also come in all shapes and sizes, and of course, the pain and frustration definitely comes in all shapes and sizes:

- The frustration of not getting your message across – trying and failing to make people understand not only what is wrong with their product but why it's important that they get it right.
- The pain of seeing your research buried under threats of lawsuits, even though you are right and the issue you've uncovered is there to be exploited.
- The frustration of dealing with manufacturers or commercial businesses that put profit or expedience over end-user safety and security.
- The pain of losing data or suffering an intrusion through an unpatched system...

The list goes on.

When I met Jayson, he didn't know it then, but he was going to experience pain and frustration in spades. He had come up with a brilliant scheme for overcoming all these obstacles, and it should have been a "no-brainer." Not only that, but he was enthusiastic, intelligent, personable, committed, and, most importantly, *on the right side*. He was one of us, one of the good guys, with something that was going to help solve the everlasting problem of how you get those with the power to make things change understand not only *what* needs to happen but *why* it needs to happen. In other words, how to engage them. Talk to me about marketing and my eyes will glaze over and I'll be a million miles away in a world of my own. Talk to most management about technical or security problems, and you'll have the same effect – they are off with the fairies and your wise words are going in one ear and out of the other...

However, Jayson had a plan. What do people like better than technical manuals and lectures on threat management or risk assessments? Stories, of course. Thrillers! Action! Secret agents taking on the forces of evil and winning!

Jayson and I meet about once a year in, of all places, Las Vegas. We both go there for the world's largest "hacker" conference, DEFCON. When I first met him, Jayson was excited. He had a book. This book. As soon as he explained the concept to me, I was sold. The idea that you could read a good book that not only entertained you but

could then be flipped into a technical reference that showed you exactly how each of those neat hacks worked was a sure winner. Maybe this would be the way to get the "suits" to understand that this is not the stuff of fiction. This is real and it's happening to them, *right now*.

When I met him again the following year, he was still excited. Ideas were flowing, research was pouring in, and his book was progressing. He was now looking for a publisher. Things were looking good.

The year after that, he was still excited, but he was feeling the pain of rejection, and frustration as finding a publisher wasn't as easy as he'd first thought. But he was upbeat. He was a man on a mission. He had loads of new ideas so that just meant the book would be even better by the time it came out, so no problem... soldier on!

Three years on, and here he is again – still smiling and determined, but still frustrated and in pain. They just don't get it. The book gets better and better, but he's hitting a brick wall.

It could have ended there, but Jayson is no quitter. The other thing that impressed me about him when we first met was his determination to follow things through. He's never made me a promise that he hasn't kept (and we all know those are ten a penny at conferences..."Sure, I'll send you that stuff as soon as I get home..."), and he's always looking out for something he can do to benefit those around him. This book is all about sharing and learning, and that encapsulates the hacker ethos and, in particular, the DEFCON ethos. If you know something, share it. If you learn something, learn more. When you really know your stuff, teach it.

The publication of this book was a hard-won victory, and I hope you learn as much from it as Jayson did researching it, but most of all, I hope you enjoy it as much as I have and as much as it deserves to be enjoyed.

Adam Laurie
Dorset, UK, June 2009.

Acknowledgments

Thanks to Haki Berkeri for the pizza, Pepsi, and the good advice that kept me going when nothing else was.

I also owe thanks to Weldon for Wednesday, Dee for all the days in between. Rudy for the rides and for sticking with Hanzo. David Letterman for letting me be on his show (and for Stephen Colbert, I hope). Del Rhea and Lee for their love of rodents who hang out at the mall. Rafe for his patience and tolerance of a wild and loud crazy roommate. Laura (she knows why). Pam for leaving. For Crystal, Jason, and Sean for being good students. Marco for the experience in warehouse living. Leslie's mom for giving me Jackie (I'm taking good care of her). Capt. Tom Johnson for the loan of the gun (I was glad to give it back). Mrs. F. Collins, the only teacher who encouraged me in learning and poetry. For Sherry, Andrea, and Kris for all the help in the background with the book. Of course to Rachel for taking a chance on some geek on Twitter ☺. Also to Syngress for making my dream a reality. Stay tuned – more to follow. To my family, who's fault it is I am such a creative and unique individual. Oh yeah, and to that person for that thing (yeah, you know who I'm talking about) – that was great.

Last and not least the INFOSEC (especially Tim Smith) and Hacking communities who have made my life a lot more interesting than it would have been if I had become a lawyer.

Jayson

Lisa, Christina, and Margaret – thank you for giving me the time and inspiration to write. Mrs. Coffin, thank you for teaching me brevity.

Kent

This page intentionally left blank

H0w t0 R34d Dissecting the Hack: The F0rb1dd3n Network

Both sections of this book tell a single story. The adventures of Bob and Leon are more than just a fun read. They illustrate many very real threats to individuals, businesses, organizations, and even countries. The networked world is so interconnected; many don't realize how valuable a target they really are. The best and worst of humanity connected with the speed and power of modern technology comes together in a world of our own making that we do not yet understand.

"The F0rb1dd3n Network" tells the story of two kids caught up in an adventure they did not expect. Bob and Leon are most comfortable in a digital world but soon find that digital actions have physical consequences. Throughout their fictional story are real-world lessons.

"The Security Threats Are Real" or STAR focuses on those real-world lessons. The hacks and tools in the fictional story are very real. STAR provides the details, sources, and references to learn more about the threats, defensive techniques, attacker techniques, and even cool toys of the fictional story.

"The F0rb1dd3n Network" can be read by itself as a story. It can also be read as an illustration of the issues described in STAR. Throughout "The F0rb1dd3n Network", you will find links that point to specific references in STAR where you can get more information about key concepts. Or if you read STAR, you will find links to "The F0rb1dd3n Network" where the story illustrates a scenario where very real tools and techniques are applied. Each section leans on the other. How you read them is entirely up to you.

For the more adventurous reader, "The F0rb1dd3n Network" contains "Easter Eggs" as well. Woven throughout are references, hints, phrases, and more that will lead you to significant or trivial insights into hacker culture. Again, STAR will help you find out more about the "Easter Eggs." But not all the answers are given away. There must be some unsolved mystery to make hacking worth the time.

So read "The F0rb1dd3n Network" as a story. Read STAR as a reference work. Dig for "Easter Eggs" in "The F0rb1dd3n Network". Or put it all together to learn more about the very real threats of the digital world we all live in.

Dissecting the Hack: "The F0rb1dd3n Network" can happen IRL.

This page intentionally left blank

Author Biographies

Jayson E. Street Jayson is well versed in the 10 domains of Information Systems security defined by the International Information Systems Security Certification Consortium ([ISC]2). He specializes in intrusion detection response, penetration testing, and auditing. He also has a working knowledge of the implementation and administration of major firewalls, vulnerability scanners, and intrusion detection systems.

He has created and conducted security awareness training for a major Internet bank and has created security policies and procedures currently used by several companies. He also created and taught a three-day training course on intrusion detection systems for an undisclosed government agency in Washington D.C. He has also created and taught a workshop on ethical pen-testing with Backtrack 3 for ISSA. He also taught a two-day class for Backtrack 4 for ISACA.

His consultation with the FBI and Secret Service on attempted network breaches resulted in the capture and successful prosecution of the criminals involved. In 2007, he consulted with the Secret Service on the Wi-Fi security posture at the White House.

He has also spoken from Belgium to Brazil and at several other colleges and organizations on a variety of Information Security subjects.

He has attended XCon 2008 in Beijing, the 25th CCC in Berlin, SYSCAN '09 in Shanghai as well as PH-Neutral 0x7d9 plus; he is a regular attendee at Black Hat and DEFCON.

Forbes and Scientific American interviewed him regarding his research on the issue of cyber-warfare as it relates to China and their preparedness for an online war. He was an expert witness in two cases involving the RIAA. His declaration was on Slashdot and other Web sites and is currently being taught as source material at a University in Massachusetts.

He is on the SANS GIAC Advisory Board as well as a mentor for SANS. He is also a current member on the board of directors for the Oklahoma INFRAGARD. He is also a Vice President for ISSA OKC and a member of the OSVDB. Jayson is also a longtime member of the SNOsoft research team.

On a humorous note, he was chosen as one of Time's persons of the year for 2006.

Kent Nabors Kent Nabors serves as a Vice President of Information Security for a multibillion dollar financial institution. He has significant experience in both the banking and the IT industries. He has worked in bank examinations with the Federal Deposit Insurance Corporation and the Federal Reserve Bank.

Kent's background includes security policy development, systems implementation, incident response, and training development.

Kent is a graduate of the University of Oklahoma and Southern Nazarene University.

When he isn't thinking about locking down bits and bytes, he is usually trying to keep up with his wife and two daughters. Quiet time usually involves power tools or an eclectic reading list.

Dustin L. Fritz Dustin L. Fritz [BSISS; E|CSA] is owner and Chief Executive Officer of The Computer Network Defense Group LLC in Owings Mills, Maryland providing executive-level strategic and tactical cybersecurity consulting services. He specializes in Information Operations Conditions, Information Assurance Vulnerability Management, risk and vulnerability assessments, certification-n-accreditation, security awareness and planning, configuration management, and incident response team development.

Dustin has over 10 years of Information Assurance and Computer Network Defense (CND) experience, with core foundations in creating enterprise-wide CND strategies for the HYPERLINK "http://www.navy.mil/swf/index.asp" \t "_blank" Department of the Navy, realigning incident response throughout the HYPERLINK "http://www.cpf.navy.mil/" \t "_blank" United States Pacific Fleet, and implementing the first-ever "http://en.wikipedia.org/wiki/INFOCON" \t "_blank" Information Operations Condition response team (IRT). Dustin's contributions and outstanding achievements in cybersecurity have been consistently recognized over the years by the United States Navy and the Secretary of the Navy; most recently in November 2007 for his actions in attaining 100 percent readiness for all Forward Deployed Naval Forces. Dustin holds a Bachelor of Science in Information Systems Security (BSISS) from Westwood College out of Denver, Colorado and is a EC-Council | Certified Security Analyst (E|CSA). He is an active member of Institute of Electrical and Electronics Engineers, Association of Information Technology Professionals, the Cyber Warfare Forum Initiative and can always be found speaking in public about cybersecurity and providing professional mentoring. Along with being the technical editor for Dissecting the Hack: The F0rb1dd3n Network, Dustin has also contributed to Syngress' CompTIA Network+ Certification Study Guide (2009) (ISBN-10: 1597494291; ISBN-13: 978-1597494298) as a technical editor and author.

He expresses his thanks to his father and mother, without you nothing would be possible!; his wife for her continuous love and support; to Jayson E. Street for his steadfast pursuit to change the security community; to Joseph McCray for being a good friend and mentor; and Rachel Roumeliotis of Syngress; all whose help and support have made his contribution to this book possible.

PART

F0rb1dd3n

1

This page intentionally left blank

Pr010gu3

A NEW ASSIGNMENT

Thursday, 9:24 a.m.

Stepan Senn looked up at the clear, blue sky of a fall morning. He could hear the crunch of dry grass beneath him as he turned his head slightly. The cool air on his face felt sharp against the hot blood that trickled from the corner of his mouth that was quickly swelling. He tried to sit up, but his body wouldn't obey. There was a sharp sound of metal on metal. The sound was familiar, but his mind wasn't working fast enough to recognize his situation. He craned his neck as he struggled to look above him. He saw legs, a hard face looking down at him, and a gun. The shape of the gun seemed to grow large enough to fill all he could see.

Everything began to spin in his mind. He closed his eyes hard against the image.

◖◗◖◗◖◗

"Sir? Excuse me, sir?" A hand touched Stepan on the shoulder and he jolted awake. "I'm sorry, I didn't mean to startle you."

"No problem." Stepan replied automatically as he picked up the briefcase he had just kicked over. He hadn't realized how tired he was after staying up late the last couple of nights.

"Sir, I believe your flight is boarding."

Stepan looked blearily at the Aeroflot gate agent. As his brain came back into focus, he stood.

"Thank you," he replied as he gathered his briefcase and coat. He made his way down the gangway and onto the plane in a mental fog. His clouded mind began to clear as it processed the surroundings he had awakened to find.

Stepan Senn's job had taken him all over the world. He had flown in many types of aircraft, but the Russian Tupolev 154 was not his favorite. He had flown on Aeroflot a couple of years after the collapse of the U.S.S.R. He remembered back then all the staff put on a good show, but the aircraft itself had looked tired. The exterior paint was faded and chipped. The interior was worn. Seats were dirty. Even the crew's

uniforms looked threadbare. Stepan hadn't been convinced then that the plane should have been in service.

Stepan also remembered when he was in Barcelona on business not that long ago and an Aeroflot pilot landed this same type of aircraft 250 meters to the right of the runway. Aeroflot just wasn't good enough for Stepan.

As he took his seat, this aircraft didn't improve his impression of the airline. The cabin was more cramped than similar-sized Boeing and Airbus planes Stepan had flown in. Its oval shape and low ceiling made sitting in a window seat particularly unpleasant. He was thankful that he wouldn't be repeating this journey.

But what should I expect when I'm flying to the second-poorest country in Europe? he thought to himself.

After they reached cruising altitude, Stepan relaxed again and closed his eyes. He began to think back to how he had ended up on this flight. He had been in Moscow. October trips to the Russian capital weren't a problem for a man from Switzerland. A Russian autumn was a nice change of pace, and his employer made sure he traveled well. Or that's what he had believed until now.

Stepan had been sent to hand-deliver a package to the office of one of his employer's partners. He didn't know the full story of what he had been carrying, but not knowing was a major part of his job. He had handed the envelope to the receptionist. Once she had sent an e-mail to his boss confirming delivery, Stepan left the office with his Moscow business complete. He knew better than to ask questions or, even worse, try to see what was on the disk he had guessed had been in the envelope.

It was a clear, cold day, so Stepan decided to walk back to the hotel. It only took about 25 minutes for the walk to the Rossiya Hotel. He even took the time to go past the east side of the Kremlin, turning at the Spasskaya Tower and on to the Rossiya. Once he entered his room, Stepan turned on his laptop and connected it to the hotel network. He typed in his overly long password, all the while wishing for some painful end for the skinny technician back at the office that insisted everyone had to memorize such nonsense just to gain access to their laptops.

Stepan pulled out his access token and typed in the six-digit random number from the token and the four-digit PIN he had memorized. Soon he had established an encrypted connection to the office back in Zurich, Switzerland (⋆pp. 212, 243). He opened his e-mail software and found the message waiting for him:

```
Your contact is waiting in Chisinau, Moldova. Your flight
arrangements have been made. You leave at 7:00 a.m. local time
tomorrow on Aeroflot. You are booked in the Hotel Dedeman Grand
Chisinau. There is a package for you at the front desk that you
need to deliver.

You will meet Simon Torgova at the outdoor café across from the
Central Garden on Columna Street the day you arrive at 3:00 p.m.
local time. Tell him his password is the same as your project
name. Report back here when an agreement is obtained.
```

This was Stepan's first project where he had been "let in" on more of the story. He had grown tired of the desk time he spent as a researcher for an international oil brokerage firm headquartered in his hometown. He had come up with an idea that could give his employer a huge advantage in the international trading game. In fact, he believed he had created a new product line for their brokerage activities: information. He had identified the target company and even found someone that might be easily influenced to assist them. When Stepan turned in all his research, he was told to do some courier jobs while preparations were made. It had been two months before this e-mail message from his boss told him it was time for action.

Stepan's boss had taken care of identifying an appropriate operative. Stepan didn't have any contacts that could help him with that part of the project. But this project started with his idea. He would be able to move out of research and maybe have a chance to be in on some of his employer's deals. But why Moldova, and where was that, anyway?

Stepan opened Google and typed in "Moldova." He thought he had seen a lot of the world, especially in the last two months of fieldwork, but backwater former Soviet territories had not been on any previous itinerary. *Land-locked*, *near the Black Sea*, *south of Ukraine and east of Romania*. *Why would anyone want to operate out of such a place?* he thought to himself.

◖◖◖

With a jolt, Stepan opened his eyes. He had fallen asleep again. As the plane's speed dissipated, over the bumpy runway in Chisinau, Stepan blinked his eyes and looked around. He made a promise to himself to either drink more coffee or sleep better on his next trip. It was time to begin his work in Moldova. He pulled his briefcase out from under the seat in front of him and waited for the plane to stop at the gate.

Stepan looked out the window of the aircraft. The side of the airport facing the tarmac was neglected and dingy. The plane finally stopped short of the terminal and stairs were rolled to the door. Stepan and his fellow travelers had to walk down the stairs, across the tarmac and into the airport. No covered automatic walkways with protection from the weather.

"Why Moldova?" Stepan mumbled to himself as he walked through the airport, his poor opinion of the little country now confirmed. The inside of the airport was a relic of past glory, although glory was hardly the word to describe it. The faces of the people sitting and waiting for flights seemed much happier than those of the arriving passengers. Stepan's countenance matched his fellow travelers as he waited for his one suitcase.

Once outside the airport, Stepan turned and looked at the front of the building. Its blue windows and bright red front entrance were a clean, modern-looking contrast to the run-down Cold War relic he had seen from the other side. Stepan shook his head as he was suddenly even more grateful for living in Switzerland. He soon found a taxi to take him to the Dedeman. The weather was warmer than Moscow, but still brisk.

"Welcome to the Dedeman, sir, how long will you be staying with us?"

"One night."

"All right, if you will fill out this information, I'll get a room for you."

The clerk passed a form and pen to Stepan. As Stepan completed the form, he asked, "Do you have a concierge?"

"Yes sir. His name is Viktor. He is right over there." The clerk pointed to an average-sized young man standing at a counter on the other side of the lobby.

"Thank you."

"And sir, I believe this is for you." The clerk turned and pulled a small, bulging envelope from a desk behind the counter and handed it to Stepan. Stepan collected the envelope and the key card for his room and walked across the lobby to Viktor.

"Welcome sir, what can I do for you?"

"I will be checking out in the morning. I'm in room 330. Please make sure I have a taxi ready at 8:00 a.m. for the airport."

"No problem, sir. Anything else?"

"Yes. Is that the Central Garden across the street?" Stepan asked as he pointed to the front of the hotel.

"Yes sir. It's not so pretty in the fall, but it is still a good place to start if you would like to take a walk around town."

As Stepan walked away, Viktor typed a note in the hotel's new guest information system so he would get a reminder in the morning to have the cab ready for Mr. Senn, room 330.

Stepan made his way to his room, set his suitcase and briefcase on the bed, and checked his watch. He was hungry and he had several hours before his meeting. He checked his pockets.

Envelope. Room key. Wallet. Phone. Okay, *time for food*, he told himself as the door closed behind him. He left the elevator, made his way through the lobby to the hotel restaurant. He was soon seated by an attractive, overeager hostess with bright eyes and a quick smile.

Okay, *perhaps there are a few redeeming qualities to this country*, he thought as he took the menu and returned the smile from the hostess.

Stepan took his time making a selection and then settled into a decent meal. Sitting still and eating was a pleasure compared to his flight.

Viktor watched from across the lobby as Stepan began to eat. He had worked as a concierge for the hotel for almost a year. It gave him an opportunity to practice his language skills and make the Lei needed to pay for school. The phone call Viktor was about to make would get him the Euros he needed for pocket money.

"I think your guest has arrived."

"Are you sure?"

"You said there would be a business man traveling alone; he would arrive this afternoon and only stay for one night. We've only had one man check in by himself today and he's scheduled to check out in the morning."

"Good job. We will be there shortly. Pay attention and let me know if he leaves the hotel."

Stepan finished his meal, charged it to his room account, and then walked out onto the street. Moldova wasn't much, but he would at least have a look while he had the time. He didn't notice how carefully Viktor watched his movement and noted the time as he left.

Two men entered the lobby a few minutes later. Vlad was middle-aged and tall, with cold, gray eyes and dark brown hair cut tight on the sides but just long enough on top to show a natural wave he brushed back as they came out of the breeze. He moved with the ease of an athlete but was dressed like a well-traveled businessman with a black open-collared shirt and silk sport coat. Pavel was younger and shorter. He had dirty blonde hair that was pulled into a short ponytail and a rather dingy backpack slung over one shoulder. He stooped under the weight of the load as they made their way across the lobby to the concierge.

Viktor was nervous as Vlad approached, but the presence of Pavel, Viktor's older brother helped him stay in control.

"Hello, Viktor. Thanks for the call."

"Sir, here is the room key you misplaced," Viktor said a little too loudly.

"Thank you. I always liked the service at this hotel. Your brother here is doing good work for me. Keep up your studies at university and maybe I'll have a job for you as well."

"Yes, sir. Your associate left just five minutes ago."

Vlad took the room key card and together with Pavel, made his way to Stepan's room. Inside, they found what they were looking for—a briefcase with a new IBM Thinkpad computer inside. It was one of those ultralight computers that doubled as an executive toy.

"Pavel, start with the laptop while I have a look around," Vlad ordered.

While Vlad walked around room, looking in drawers and sorting through Stepan's suitcase, Pavel lifted the computer deftly as someone who was comfortable with any device connected to a keyboard. He turned on the power and hit the default key combination to modify the boot settings. No power-on password. Pavel could always count on business types to not think of the basics. They always thought that spying was only targeted at governments (★p. 213).

Pavel enabled the laptop for booting from a USB device. He pulled out his keychain and plugged the tiny storage device into the port on the right of the laptop case. Instead of the normal start-up screen that Stepan saw everyday, Pavel was greeted with a black screen with a few simple command options. This was a handy tool Pavel had picked up from a security Web site. It allowed him to reset any password on a Windows system as long as he could control how the system started. Pavel didn't bother giving the administrator account a new password. He set it to a blank password, disconnected his USB device, and rebooted the machine (★p. 179). Soon the Windows XP "splash" screen appeared. He typed in "administrator" for the ID and no password and pressed the "Enter" key. He was in. Pavel turned the computer on the small desk and stood to give Vlad room to sit down.

"This is too easy. I wish he had used another hotel," Pavel said as Vlad sat in front of the now unlocked computer. "At least then it would have been a challenge."

"What challenge would you want?" asked Vlad.

"Viktor getting us into the room means that we got the laptop information, but now I don't need to do the Hotel Hack."

"The what?"

"At DEFCON, Major Malfunction presented a hack using a Linux box to break into hotel information systems through the TV set in a room. You can grab reservation information, TV movies they've watched, and sometimes even credit card information or read their e-mails" (⋆p. 299).

"Who is Major Malfunction?"

"What? You don't know? He's the guy who wrote the hack!"

"Never heard of him," Vlad responded.

"You should really keep up with what the über-leet guys are—"

Pavel saw a subtle firmness appear in Vlad's expression and he stopped himself.

"That's right, you were busy recruiting virus writers for one of your jobs. You missed out on some of the really skilled hackers." Pavel was pushing his luck with the way he talked to Vlad. But he knew he was right. If Vlad kept bringing in work like this, Pavel knew he needed to practice a variety of skills.

Vlad seemed to have had enough of the conversation. He removed a Swiss Army knife from his pocket. He opened a small connector from the knife, which fit neatly into the USB port on Stepan's laptop. Soon he was copying the "My Documents" folder from Stepan's laptop to his "pocket knife" (⋆p. 269).

"Only 10 megabytes. He must have another computer at his office or he keeps everything in e-mail," Pavel said as he looked over Vlad's shoulder.

A quick look from Vlad reminded Pavel that he was already getting on his employer's nerves. Pavel shut up and walked across the room and picked up the remote to the TV set.

Vlad ignored Pavel and kept his attention on the laptop. He looked in the default folder and quickly found the file he wanted. He copied the "outlook.pst" file to the pocket knife. This would give him a copy of all the e-mails Stepan had stored locally. With the e-mail secured, he looked up at Pavel (⋆p. 215).

"What are you doing?"

Pavel was looking at what appeared to be Stepan's room bill displayed on the TV.

"This guy hasn't had any time to pick out a movie and didn't use the Internet e-mail system offered by the hotel. But, he's got a request for a taxi at 8:00 a.m. tomorrow, and he paid for everything with an American Express card. Here's the number. I can't believe they didn't set this thing up to mask the digits on the display!"

"This could be useful," Vlad replied with a slight smile. Pavel was a resourceful young man to keep around, Vlad reminded himself, even if he was annoying at times.

"Now that you're done playing with the television, finish up on this laptop for me," Vlad ordered.

Pavel took Stepan's laptop from Vlad and blanked the three Windows event log files. Next, he changed the "last logged in user" registry key so that it would appear that Stepan's account was the last one used (⋆p. 193).

"Do you want me to reset the administrator password?" Pavel asked.

"No. You've done enough. This one won't ever know what he lost," Vlad answered as he walked toward the door.

Pavel powered down the computer, returned it to where he found it and followed his boss.

Vlad and Pavel strolled through the lobby without speaking. Vlad led the way as he walked across the street and into a small café. They took a table near the window where Vlad had a clear view of the hotel entrance in case Stepan returned.

"Set up your laptop. I want to see what we found," Vlad ordered.

Pavel complied and pulled his own sticker-covered laptop from his backpack and set it on the table between them. He logged in and took the pocketknife Vlad offered and connected it to a USB port.

Vlad took Pavel's laptop and looked over the list of files they had just acquired from Stepan's laptop. He didn't have much time, so he sorted the files by "Last Modified Date" and scanned the list. One file caught his eye immediately. It was called "Odysseus.doc" and was last updated just one day before (⋆p. 378).

"That would be too obvious," he said mostly to himself as he double-clicked on the file name.

After a quick scan of the first page, he said, "I've got what I need Pavel. You can take the rest of the day off. I'll call later if something comes up from the meeting. In the mean time, I'm going to be borrowing your laptop."

Pavel paused. He wasn't one to part with his laptop. He had too many tools there that he had spent months "acquiring." But he also knew that Vlad was not one to be disobeyed.

"Be careful with the laptop. I've been working on a potential new IE vulnerability and all my notes are stored there. Let me give you an account, so you can get to the tools you need without messing with all of my shortcuts."

Pavel took the laptop back from Vlad and created a new user account. He then did a "change user" command, typed "boss" for the user ID, and pushed the laptop back across the table.

"Your password is 'penguin.' Just call me and I'll come pick it up when you're done." Pavel stood from the table and walked away. At least Vlad was going to have to pay for his meal.

As Pavel left the hotel restaurant, Vlad began typing his password.

That kid never stops, he thought to himself as he finished typing the not-too-subtle reminder from Pavel that Vlad didn't really know how to use Linux even though he insisted on using it as his main operating system. Vlad found the document he had been reviewing and continued reading. It looked like Stepan had been given a research project by his employer. Stepan had filled this document with notes and information pulled from Web sites. He had started with a company called Data Mining, Inc. based in Raleigh-Durham, North Carolina. He had some information about a small firm in Houston, Texas called 3DNF, Inc. that had been acquired by Data Mining within the last six months (⋆pp. 137, 377). Vlad found some links from the U.S. Securities and Exchange Commission's Web site and the text from a press release about the acquisition (⋆p. 137).

Then Stepan had listed some names and e-mail addresses that belonged to the 3dnf.com domain. Vlad could only guess that Stepan had "googled" the domain name to harvest the addresses. If so, Stepan was a fairly resourceful researcher (*p. 138).

One of the names was in a red font instead of black like all the others. Michael Resol was someone of interest to Stepan. There were links to what appeared to be blog pages by Michael. There were even links to gambling sites. Then, there were some notes by Stepan:

> Michael Resol is the best target. He is a network admin that has worked at 3DNF for five years **(*p. 380).** He has been passed over for promotions and he talks too much about his employer on his blog site. Both his blog and Facebook sites reference his favorite online gambling pages. I think he has some financial problems - see link below.
>
> Michael's tech position, length of time with 3DNF and money problems make him a good candidate for deployment of our application.

"Interesting, but what is the 'application'?" Vlad muttered to himself. He had an idea based on the name of the file he was reading. Vlad looked at his watch. He needed to move along. He would have to fill in the gaps during his meeting with Stepan, and there were other files yet to read from Stepan's laptop.

Vlad shut down the laptop and stood to leave. He was in a good mood because of the progress so far. He left a large tip and paid for his and Pavel's meal. Outside, Vlad walked across Puskin Street and into the central garden at the middle of the town. He made his way down the tree-lined walk to the central fountain. On the far side of the fountain, he turned to his right and made his way to Columna Street. A left turn and one more block, and he could see the outdoor café.

As Vlad approached, he could see a small man in his thirties sitting alone at one of the four outdoor tables. He had blonde hair cut short, glasses, and sharp facial features. There was something about the way he moved that suggested to Vlad that whatever was around the next corner was sure to surprise this man. As Vlad approached, he saw that he was making a bad show of reading a newspaper.

"Impressive. You don't look like someone who can read Romanian," Vlad said in perfect English. In fact, every word Vlad said sounded as if it had been given individual consideration before it was spoken. He knew his baritone voice was a tool he could wield effectively.

"I can't," Stepan admitted nervously. "But I thought I should at least take a look and see if I could learn a little about the city." Stepan's Swiss accent was obvious to Vlad at once. He sat down in the empty chair across from Stepan. "Are you Simon?" Stepan asked.

"Yes," Vlad lied. As sloppy as Stepan had been securing his laptop, Vlad knew he would have exposed too much about his activities. *That's why you never use your real name*, he thought to himself.

"You must be Stepan."

"My employer tells me you come highly recommended."

"I finish my jobs efficiently if that is what you mean," Vlad responded.

"Uh, yes."

Stepan was obviously new at this business.

"What consultation does your firm require?" Vlad asked.

"We need someone who can install a certain program on a computer inside a company located in Houston, Texas, USA."

"What type of program, and what type of company?" Vlad responded.

"A rootkit to answer your first question, and a database consulting firm to answer your second." Stepan responded.

"That hardly seems like a task worth the cost of my skills," Vlad answered.

"We need to be certain that the program is installed on a particular system and we are willing to pay to ensure that it functions as designed. We need this to be done discretely and efficiently," Stepan answered.

"I can get that done. Is that all?"

"There are a few other steps to help ensure the information we need is accessible. The details are documented for you."

"Are you aware of my fees?" Vlad asked.

"Yes," Stepan answered.

Vlad took a pen and small piece of paper from his coat pocket and wrote "Volksbank, 111-8-18-1-13-15-27-1" from memory (★p. 378). "Have the first half of the payment deposited here. I'll start as soon as I have confirmed the funds, and by the way, don't complain if you see any extra charges on your American Express card. I'll expect you to cover some of my travel costs."

"Certainly. Do you have the necessary account information?"

Stepan's confused look was a pleasure to Vlad.

"I took the liberty of acquiring some financial information about you. Just a demonstration of the skills you are retaining," Vlad told him. *You're too inept to be doing this*, he thought to himself as he met Stepan's surprised gaze.

"Yes, well, of course, we will cover whatever expenses are required to complete the job." Stepan took an envelope out of his coat and slid it across the table. "My employer has also provided some background information on the job that you will find useful."

Vlad opened the sealed envelope. It contained a pen.

"What is the pen for?"

"It's a data storage device. If you pull the top off, you will see a USB connector for your computer. Inside is an encrypted file that details the instructions for your team, as well as the application we need installed on the target system (★p. 269). To access the files, you'll need the password—Odysseus."

Vlad allowed himself a small smile at that last piece of information.

"As I said, I'll begin when I have confirmed payment."

Stepan obviously wasn't sure what to do next. He began to gather up his newspaper and then paused.

"I have to ask—I understand you operate in many countries, so why Moldova? Are you from here?"

Vlad let out an honest laugh.

"No, I'm not from Moldova. But I do have some family ties here. I have found the legal environment of this country to be accommodating to my line of work. Local talent, although sometimes hard to find, is quite affordable. People from here are anxious to find work that gets them out of the country, and for the right skills, I can offer that."

"Oh, well, that does make sense. I'll make sure everything is in order." Stepan stood and walked away.

Vlad ordered a cup of coffee and then turned on Pavel's computer that he was still carrying. He logged in with the "boss" account Pavel had setup for him and connected the pen. He opened a window to review the files on the pen. Sure enough—two files. One was called "instructions.exe" and the other "files.exe." Vlad double-clicked on the file called "instructions.exe" and was greeted with an error message.

"Everyone assumes the whole world runs Windows," he muttered. Vlad looked through the program list on Pavel's Linux laptop. Sure enough—VMWare (*p. 271). Vlad launched the program and found that Pavel had several different Windows operating system images available. He clicked on the one Pavel had named "Surfing Win2K" and waited for it to boot. Vlad smiled—Pavel had modified that splash screen to show a penguin instead of the normal "Windows" welcome. It didn't require a password to open either. Vlad tried again to open the file. This time a window appeared asking for a password. He typed in "Odysseus." The program built a directory called "Transfer" on the desktop. Vlad opened the directory and inside were the files he expected. Vlad opened the one called "instructions.doc" and began to read.

Thirty minutes later, he was walking through town. It looked like he had to start his job a little sooner than expected. The last page of the file included instructions that he was to eliminate anyone who had complete knowledge of his activities—beginning with the individual who had delivered the instructions. At least there would be an extra payment for this service. He pulled out his cell phone and dialed a programmed number.

"Da?" The course voice sounded half asleep.

Vlad sighed disapprovingly as he answered in Russian, "Andrei, I need you to pick someone up tomorrow morning at 8:00 a.m. at the Dedeman Hotel in a taxi."

◖◗◖◗◖◗

Stepan was feeling pretty good the next morning. He had completed his first real "field assignment" without any problems. He also had finally put in motion an idea he had been working on for months. If Simon succeeded in setting up a reliable back door to the American company, he would be able to show his bosses a new revenue stream. Arbitrage of commodities had been lucrative to his firm for years, but it was old school. Arbitrage of information was how Stepan would become a partner.

Stepan knew a former partner of Mark Richardson had started his firm. The American had fled his home country after some questionable business dealings and

set up an international trading company in Switzerland. Their new practice had been successful because of a willingness to deal with anyone. Stepan's plan would fit in just fine with such a firm.

Stepan finished packing and went down to the lobby. He walked over to Viktor at the concierge desk.

"Do you have that taxi ready for me?"

"Excuse me, sir, what room?"

"330."

"Oh yes. He is waiting for you just outside. Do you need help with your bag?"

"No." Stepan was ready to start making progress home. He walked out the door and met his ride.

"Good morning. I need to go to the airport."

"Yes, sir," was the response from the cabbie with a thick Russian accent. The cabbie took Stepan's suitcase and placed it in the trunk. Stepan got in the back seat and settled in for the brief ride back to the airport.

The day was clear and crisp. There was a slight breeze, but everyone on the street seemed to appreciate the sunshine. Stepan noticed more of the city as they drove than he had on the way in the day before. This time his attitude wasn't as gray and he was able to enjoy what he saw. He saw mostly old, Russian-made cars on the streets. He noticed the small shops that were starting to open for the day. The park he had walked through the afternoon before was mostly empty. A few people were walking through, probably on their way to work.

The traffic wasn't bad this morning. The drive down Bucuresti Street went quickly, and soon the city fell away and Stepan could see more of the landscape. Modest homes gradually yielded to countryside. The landscape seemed hard because of the coming winter, but the brightness of the day brought warmth in through the cab window. Suddenly Stepan's senses sharpened and he leaned forward in his seat.

"Is this the way to the airport?"

"Yes, sir," was the quick answer.

"This doesn't look like the way I came yesterday."

"Yes, sir."

"Do you speak English?" Stepan asked with growing concern.

"Yes sir."

That answer didn't convince Stepan. He leaned back in his seat and began to realize his problem. He was alone in a country he didn't know. His suitcase was in the trunk. He couldn't communicate with his driver. But the driver obviously had a destination planned. He thought about jumping out of the car. But that didn't make sense either. He would be abandoning his things, and he wouldn't know how to get back to the city or the airport.

The cabbie turned off the road suddenly. They pulled down a gravel road, turned right past some trees, and came to a stop beyond a little rise in the ground. Stepan looked around. He couldn't see the road. The cabbie turned off the car and got out. Stepan was too scared to even speak. His heart began to pound in his chest and his hands started shaking.

Andrei opened Stepan's door and caught him hard in the mouth with his fist. Stepan slumped. He wasn't unconscious—at least not quite. The shock of the act had the desired effect. Stepan stumbled as Andrei dragged him from the car and tossed him to the ground outside the car.

Stepan Senn looked up at the clear, blue sky of a fall morning. He could hear the crunch of dry grass beneath him as he turned his head slightly. The cool air on his face felt sharp against the hot blood that trickled from the corner of his mouth that was quickly swelling. He tried to sit up, but his body wouldn't obey. There was a sharp sound of metal on metal. The sound was familiar, but his mind wasn't working fast enough to recognize his situation. He craned his neck as he struggled to look above him. He saw legs, a hard face looking down at him, and a gun. The shape of the gun seemed to grow large enough to fill all he could see.

Andrei pulled the trigger and walked back to his car. He would collect his payment from Vlad that afternoon for another completed job. Vlad had been keeping Andrei busy lately.

CHAPTER

0N3

PROBLEM SOLVED

Monday, 10:11 a.m.

"Yes! We've got the bastard!"

Mark pushed his chair back from the table and punched at the air. He had just spent the last four hours searching through piles of papers and books taken from Randolf Jamison's house the day before.

Randolf was sitting in a cell at the Houston federal prisoner transfer facility. He had been arrested on suspicion of trafficking in child pornography. Mark was the FBI agent from the Houston Computer Crime Task Force assigned to go through all of the hard drives taken from Randolf's three computers.

Unfortunately, Mark had hit a wall immediately. Most of the information on the computers looked normal, but on two of them, two-thirds of the storage space was filled with an encrypted volume. There would be no way to read the data, and what they had found in his house was not sufficient to keep him in custody. This case wasn't big enough to task some of the Bureau's special resources for such problems, so Mark had to find another way into these encrypted files.

"Try telling that to the little kids this pervert used to make his money!" Mark had snapped back at his supervisor when told he would have to find another way. Mark knew the math. There was no way he would be able to break into these drives—unless Randolf Jamison was stupid.

"If they were smart they wouldn't be doing this stuff in the first place," he told himself as he began. Mark went through every piece of paper they could find in his house. Sure enough, it was late-afternoon on his first day when Mark found it. Mark had been digging through magazines, bills, letters, books, and even saved junk mail trying to find a clue. For a pervert, Jamison kept a pretty plain-looking collection. They had only found a few pictures—just enough to confirm the statement they had from a probable victim's mother. But Mark finally noticed something that didn't belong. A Gideon Bible—obviously stolen from a hotel—stood out because it didn't fit the pattern of other material. There was a single piece of paper left inside the back cover. What Mark found there was the key to putting Jamison away.

"Thank God criminals can be so sloppy!" Mark exclaimed to the empty conference room. "If you record an encryption key, someone can always find it!"

Mark stood up from the table and started walking around the room. His body was moving on its own accord while his mind began to process what he had just found. Agent Jackson knew that he needed to start cataloging the contents of the once-encrypted drive he had been pounding on. But he had too much energy to be still. He started marching down the hall to get some coffee. Maybe he would run into someone on the Cyber-Crimes team he could talk to. After all, what's the use in solving a puzzle when you can't brag about it?

◖◗◖◗◖◗

"There he goes now," Special Agent Thompson said as he pointed at the glass wall of the conference room. The cluttered room had a large table running down the middle with two glass walls and hallways on either side. Mark was on his mission for hot caffeine on the opposite side when his boss noticed him. Agent Battle hardly had time to get a look at the blur as Mark disappeared down the hall.

"You'll find that Agent Jackson is a little…intense."

"Is he good?"

"One of the best investigators we have on the Cyber Crimes Task Force."

Special Agent Fredrick Thompson had been with the Bureau for nearly 20 years. After five years of fieldwork, he had shown the mental flexibility to adapt to technology better than most. That led to particular case assignments, the Houston Field office and, eventually, a command with orders to establish the Cyber Crimes Task Force for the South-Central United States.

For several years most of their work had been on drug cases. The Columbian and Mexican organizations bringing in drugs were constantly looking for an edge—and often that meant sophisticated communications gear and computers to track their business. But since 9/11, everyone in the Bureau was spending more time on anti-terror activities. And his team was no different. Agent Jackson's current case was almost a throwback with an old-fashioned pervert trafficking material across state lines. The only thing new was the technology used to hide the activity.

Thompson had a reputation in the Bureau for bringing together a strong team of more traditional FBI agents and technical talent he had personally recruited from the Air Force (★p. 379).

"Agent Jackson was one of my finds from the San Antonio Air Force Base 'Tiger Team.' They're an elite group of warrior-geeks who specialize in breaking into military networks and facilities to test security."

"That explains why he's so skinny. Does he know what to do with a gun?" Agent Battle asked with obvious skepticism.

"He's qualified for field work, but that's not his specialty. That's why you're here. Let me show you around some more. We'll catch up with your new partner in a while."

◖◗◖◗◖◗

"So have you met Battle yet?"

"No. Have you?" Agent Jackson replied as he sipped on his coffee.

"Yeah. Impressive. Marines, then NYPD. Battle's even spent some time on anti-terror work with our NYC office before Thompson decided we needed more muscle."

Mark was standing outside a cubicle talking to Agent Frank Adams, another member of the Cyber Crimes Task Force. Mark had just finished his tale of how he had found the encryption key that was going to send another pervert to jail. Frank hadn't been impressed. In fact, Frank had looked like he was holding something back as he listened to Mark. As soon as Mark had finished his story, Frank had cut him off to ask about Agent Battle. Mark even thought he saw a slight tension in Frank's face—kind of like a kid who had a secret.

"So what kind of name is 'Battle' anyway? Could there be any more testosterone than a Marine named 'Battle'?" Mark asked.

Frank smiled. "Probably not," he replied and started to turn back to his work with a slight shake of his shoulders. Mark wasn't done yet.

"More muscle is the last thing I need. I had my fill of jarheads when I was on the Tiger Team in San Antonio. I bet all Agent Battle could do with a hard drive is use it for target practice."

"I think I'll take that bet, Jackson," Frank replied, careful not to look at Mark.

Mark turned to see his boss standing next to his new partner. As his brain tried to process what he saw, he could hear Frank suppressing a laugh as he shrank further into his cube. Standing next to Special Agent Thompson was a tall, athletically built woman. She stared slightly down at Mark as they measured each other with an intense stare. Agent Chris Battle clearly won as she had the element of surprise. Mark broke the eye-lock as Special Agent Thompson interrupted the slightly too-long silence.

"Agent Jackson, this is Agent Chris Battle. She is going to be joining the Cyber Crimes Task Force and will be your partner. Why don't you start bringing Battle up to speed by giving us a briefing on your progress on the Randolf Jamison case."

"Uh, yes sir. I was just heading back to the conference room. If we go back there I can show you what I found. I think we will have everything we need on Jamison before the end of the day."

As Mark led the way to the conference room he heard snickers from several cubes. He allowed himself one thought as his boss spoke. *Oh, this is going to be a long day.*

"Really? Is that why I saw you shooting out of the room so fast a while ago?" Thompson asked his subordinate.

"Yes sir. Well, I needed some coffee, actually. I just figured out the encryption key for Jamison's computers." Mark said as the three of them walked into the conference room.

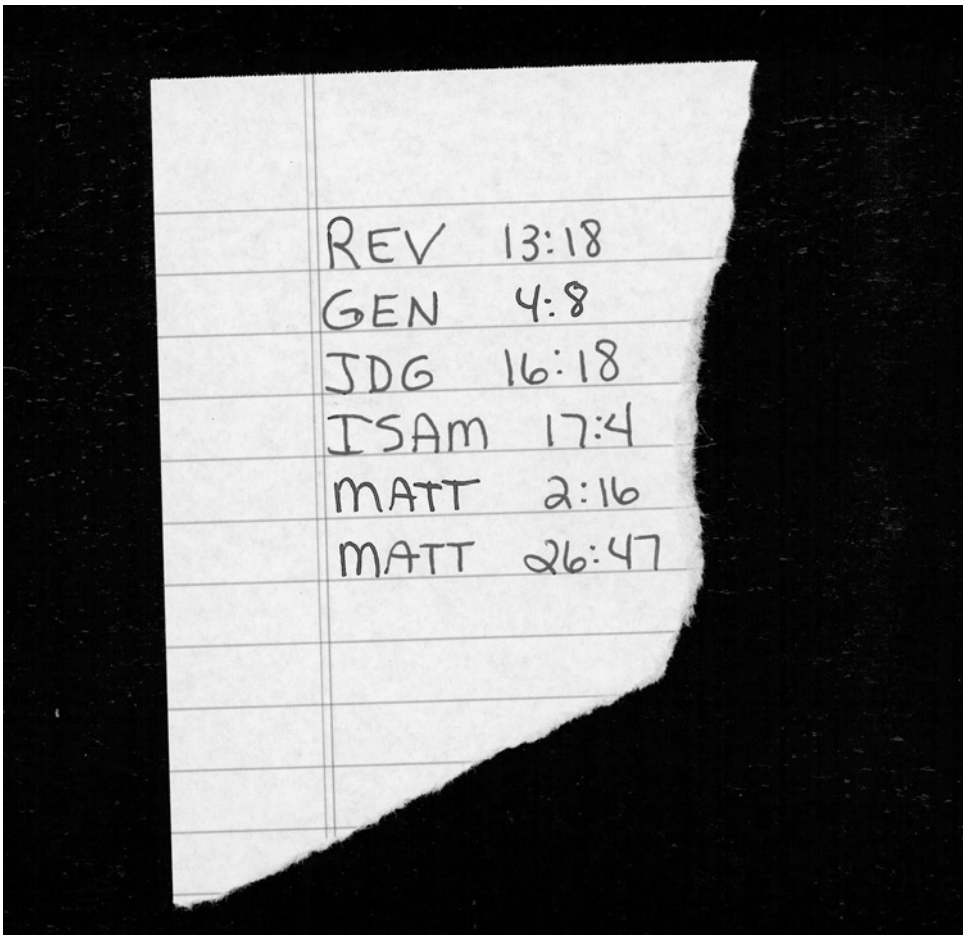
"Good. Maybe the rest of us will get this room back, Jackson. How did you find it? This morning you told me we didn't have the tools to get to the data."

"We don't, sir. I spread all of this stuff out in the conference room to get a better perspective on what Jamison had in his house. An encryption key is the only way into the drives, and Jamison didn't strike me as very cautious. I made an assumption that

he wrote down his key somewhere, just in case. Agent Battle, do you want to take a shot at this pile and see if you can find anything interesting?"

While Jackson had been talking, Battle had already started lifting magazines and books from the table. "Sure," she responded. As Agent Battle made it to the end of the table, she turned and asked, "I thought I heard you say earlier that Jamison was a pedophile. I don't see anything here but an average, boring single guy. What led you to him in the first place?"

"We got a tip from Perverted Justice. They're today's online version of the Guardian Angels from the 1970s. They got into a discussion with this pervert in a chat room. He claimed he had some "content" that he had personally created, and they talked him into giving a sample. When they got that, they called us. Jamison had given Perverted Justice a Yahoo! e-mail account (*p. 389). The Bureau checked it out and found that



account was last accessed from here in town. That's when I got the case. We sent an e-mail back to the account with a hidden embedded link to a Web page we controlled. When Jamison opened the e-mail, it forced his computer to hit our Web page and we were able to log his IP address. From that, we were able to track him down through his Internet Service Provider. Jamison had a DSL line under his own name. For all of his precautions on the encryption software, he didn't think about us tracing him back through his e-mail."

"What about this?" Chris cut off Mark's story as she picked up the Gideon Bible.

"Not bad, Agent Battle." Mark said with a smile. "Why that?"

"If we are dealing with a pedophile, then this is the one book that doesn't belong here."

"You're close. But how do you find a pass phrase in there?" Mark asked.

"Agent Jackson, we're impressed you figured it out. Just tell us what you found so I can get back to work." Special Agent Thompson said impatiently.

"Yes, sir." Mark took the Bible from Chris and opened it. "My first clue was what Chris noticed. The Bible didn't belong here. And look. There was a handwritten list of verses folded and tucked in the back."

"So, every one of those verses makes up the encryption key? That doesn't make sense—it would be too much to remember or type, and most criminals are lazy." Agent Battle pointed out.

"You're right. I looked up all of the verses in the list and wrote them down. Here, look at the list." Mark handed Chris a sheet from a legal pad with a list of handwritten Bible verses. Throughout the verses were circled words, numbers, and lists of names scratched in the margin.

"So where is the secret in all of this?"

"The first thing I noticed was that the verses weren't in the order they come in the Bible. They looked random. That made me think there had to be something that they all had in common. I played with the numbers of the verses and chapters, but that didn't work. I highlighted all of the names and then noticed that all the verses had a 'bad guy' from a Bible story. In fact, Jamison had taken the time to put the verses in alphabetical order by the name of the bad guy. So I took all of the names and typed them in. I got it on my second try—he didn't use any capitalization for the names, and no spaces between. So his pass phrase was 'beastcaindelilahgoliathherodjudas'."

"Clever Jackson. You and Agent Battle can clean up the mess you made of my conference room and then start going through the data Jamison was nice enough to save for us."

As their boss walked out of the room, the new partners looked at each other for a moment then they turned to opposite ends of the room and started stacking up the papers, magazines, books that Jackson had spread around the room.

"Do you always make this much of a mess?" Battle asked.

"I didn't think it was a mess. I was just trying to see if I could find a pattern."

"I can't think with clutter. I thought an Air Force guy would be a little more organized."

"I am organized, but that doesn't mean I'd pass inspection in a Marine barracks."

"No, you wouldn't. So where do we take all of this?"

"Back to the Cyber Crimes area. Come on, I'll show you where we work."

The two agents each made a couple of trips carrying boxes back to a large room. The space was filled with cubicles, all just high enough to give some privacy when seated.

"So what's with all of this junk on everyone's desks?" Battle asked.

"What do you mean?"

"This." Battle said as she picked up a can of Diet Pepsi wrapped in an R2-D2-shaped plastic holder.

"That's not junk, that's ambiance. I don't like this place to look too government-issue."

"Looks like none of you in this area are government-issue," Battle commented as she held the R2-D2 holder with one hand and pointed to a black T-shirt pinned to the inside of Jackson's cubicle just above the desk.

"What does 'I am the Fed' mean?" Battle asked as Jackson reclaimed his drink and took a swallow of the now-warm Pepsi.

"I was 'spotted' at DEFCON this summer" (*p. 330).

"You let your cover be blown?"

"I didn't have a 'cover.' I'm not a field agent, at least not in Las Vegas." Jackson sat down in his chair and looked at Battle. "So do you have a PC at home?"

"Yes."

"Figures. What operating system do you use?"

"Okay, I know where this is going. You want to know if I'm 'geek' enough to work here. I'll give you 10 questions, and then I'm done. But first, I want to ask you just two questions."

"I can handle that. What's your question?" Agent Jackson responded.

"Have you ever had to fire your sidearm in the field?"

"No."

Battle allowed her face to show her disappointment at the first answer. She also realized she didn't start at the beginning. "Have you even had to draw your sidearm in the field?"

"No."

With a roll of her eyes, Battle walked over and sat in the extra chair in Jackson's work area. "You're just what I expected. And if you want to ask, my answer to both of those would be 'Yes'—and both in my first week."

They stared at each other for a moment. Then Jackson broke the silence.

"How about if we just go get some pizza for lunch? I'll skip the geek questions."

GETTING STARTED

Tuesday, 3:30 p.m.

Pavel sat down at the desk in his room at the Houston JW Marriot. He knew this job was a big deal for Vlad because of the nice hotel room and the complicated logistics. Vlad had him fly to Houston by way of New York, then a day in Chicago just waiting

in another hotel room. Now he was supposed to get settled in Houston and wait for Vlad to come pick him up the next day. Vlad had told him they would have a couple of others working with them on this job. Pavel's only other U.S. trip with Vlad had been DEFCON in Las Vegas. That was a simple, but long flight with no side trips.

Pavel knew that this was the continuation of the work they had done back in Chisinau a couple of weeks before. He didn't know what else Vlad had learned after he left him at the hotel that day. He also didn't know exactly what Vlad wanted him to do in Houston.

He was just told to bring whatever technical tools he needed for a network penetration. Pavel had an idea how to figure out some of the details.

Pavel reached into his backpack and pulled out an IBM Thinkpad. He pressed the power button and started fishing through his backpack while he waited to see what kind of operating system was loaded.

"Windows—typical," he mumbled to himself when the familiar splash screen appeared. He pulled out his CD case and started looking for his Ubuntu install disk. As he flipped through the case, his mind drifted. When Pavel left the hotel in Chisinau, he had to leave his laptop with Vlad. The next day they met at a coffee shop and Vlad returned his laptop, along with this Thinkpad.

"Consider this payment for the help in the hotel room," Vlad had told him. "Stepan won't be needing it."

Pavel knew what that meant as soon as he heard it. But now the reality started to settle in. Pavel was a hacker for Vlad. That meant writing custom Trojan code and root kits for Vlad's "projects." Pavel had even broken into several networks in the last couple of years. The trip to Las Vegas for DEFCON had been part payment from Vlad and part new assignment. Pavel had played tech-interpreter for his boss. Vlad could speak flawless English, but he couldn't last more than a few minutes talking "tech" with a true hacker.

So now I'm working for higher stakes, he said to himself. As soon as he said it he asked the next question. *How high are the stakes if people are dying?* This was the first job he worked on that he knew left people dead. Ever since Vlad recruited him, Pavel knew his employer was tough. Now he knew that he would kill. Pavel couldn't decide if he was excited, scared, or both by the rules of this game.

He blinked a few times and realized that he hadn't moved while his mind wandered. He turned his attention back to the laptop. He brought his hands to the keyboard and became aware of his heart beginning to beat harder in his chest. Just the idea of digging into Vlad's plan made him nervous. Actually beginning to do it had created an involuntary response in heart rate. He pushed on and fished through his backpack for his BackTrack 4 CD (*p. 272). As he worked, his hands began to sweat. After a few more keystrokes he paused again.

If I learn something and then let the wrong information slip in a conversation, *I'm gone*, he thought to himself. *I would be a 'loose end' for Vlad.* Vlad had trusted him more lately. The fact that he was sitting in the hotel room pointed to his greater confidence. *But is it worth the risk?*

Pavel chose caution. He ejected the BackTrack 4 CD and powered down the laptop. As he sat in the chair staring blankly at the wall, he could feel his heart rate

slow and the nervous energy dissipate. "At least I should know some more about this place before we get started," he said aloud to himself. Pavel returned the CD to his backpack and pulled out his own laptop. Soon he was connected to the hotel Wi-Fi and doing Google searches for local television stations and newspapers. He spent the next hour trolling through local news stories, blog sites, and Twitter entries about Houston.

THE ACQUISITION

Wednesday, 12:05 p.m.

As Michael Resol approached his turn off the 610 loop, he gave a half-hearted shoulder check and then reached for his right turn indicator. His gaze came back to the front of the car, and he startled as his windshield wipers made a loud, dry rubbing sound in front of him. He brought his focus from the car in front of him to the motion of the wipers he had mistakenly turned on. Just then he saw the brake lights and telltale rise in the bumper of the car immediately in front of him as it quickly slowed. Michael slammed on his brakes and held on as his ABS took over and slowed him down. The sound of screeching tires from behind told him he was about to be hit. Michael watched as the nose of an old GMC pickup lurched down in his rear view mirror. And then—they all stopped. Michael put his head on his steering wheel as his wipers continued to count out a loud, dry, rubbing beat.

"Come on, pull yourself together Resol!" Michael said aloud. He turned off the wipers and started to slowly make his way off the highway.

Michael walked into the Starbucks at the appointed time. The efforts of an army of retail specialists to create a comfortable coffee shop were lost on him. He nervously scanned the patrons as he walked past the product displays and approached the counter. He noted a group of college-age kids gathered around an assortment of iPods, cell phones, and a laptop spread across a table in one corner. Nearby, two ladies were sipping their drinks and talking rather loudly about a movie they had just seen. In another corner was a man alone reading a newspaper. There was a cup of coffee and a book sitting on the table in front of him.

Was that the one? he thought. Staring wasn't an option. He'd check again as soon as he—

"What can I get for you today?"

"What? Oh…uh…just a coffee."

"Which one sir?"

"Uh…just your coffee of the day."

"Which one? We have three."

"The strongest you make."

"What size?"

"Right…large, no Venti, I guess."

"Room for cream?"

"No. Just coffee. Thanks." Michael tried to control himself and even managed a half-smile as he concluded the complicated $2 transaction. He was too nervous to even

order a plain coffee. He fumbled with the cash as he paid, took his drink and turned to approach the man in the corner by himself.

There it is—'Takedown', Michael confirmed for himself as he drew closer and could read the cover of the book on the table.

"That looks like an interesting book."

Vlad lowered the newspaper and smiled slightly. "It is a very interesting book. Have you heard of it before?"

"No," Michael answered as he pulled up a chair.

Vlad folded the newspaper neatly and placed it in an empty chair to his left. He slid the book slightly toward Michael. "It's a true story about a hacker who gets caught. Personally, I think the author embellishes too much. But it is still instructive. In fact, I have an idea for a variation on the hack used in the story."

"What do you mean?" Michael responded, concentrating carefully as he put his coffee on the table, trying to control the shaking in his hands.

"In the book, the hacker finds a program running on a computer. He used that program to connect to and manipulate the system. In fact, the computer he broke into was one owned by the man who eventually wrote the book. I want you to help me do something like that with your employer."

"That's going to be hard," Michael protested. "We got some kind of government contract last year and ever since then they've been installing firewalls, scanning our e-mail, and watching where we surf on the Internet. I even got in trouble for hitting a personal site on my lunch hour."

"That is not a problem. When someone installs strong defenses, the best method of attack is to just avoid them," Vlad answered confidently. He tapped the book lightly. "Look inside the book later. There are detailed instructions you will need. You will also find the first part of the agreed payment. I need you to use some of the payment to buy a wireless router. You will install it in your office building on the side closest to the parking lot. Just find an empty cubical and plug it into the network and hide it under the desk. Don't worry about any encryption settings. Be sure to change the SID from the default and don't allow it to broadcast. Like I said, just read the details I've left for you in there." Vlad explained with a casual wave of his hand toward the book.

"Next, you'll need this." Vlad reached in his sport coat pocket and pulled out a pen.

"There is a USB drive inside this pen—just pull the cap off and connect it to your boss's PC and run the program called 'svchost.exe'."

Michael's face screwed up in a nervous convulsion at the order. "There's no way I can run a program on my boss's computer! How am I supposed to get access to it?"

"That's your problem. Don't worry about his antivirus software. This is a custom-built Trojan that was made for this job—it's never been used in the wild."

Michael took the pen and the book. The pen went into his shirt pocket. He opened the book and found an envelope inside. He shoved it roughly into the back pocket of his blue jeans and stared at the cover of the book while he screwed up the courage for another question.

"I really don't know how to get this onto my boss's computer. What if I get caught?"

"Getting caught is your problem. Getting the job done is what you are paid for," Vlad responded.

Michael didn't have the sense to know that he shouldn't persist. "But they could trace this to me." Then he pressed just a little farther. "Wouldn't that lead back to you?"

Vlad's face was like stone. "It will lead back to no one." Vlad stared straight at Michael. Michael didn't perceive the danger in that response. Vlad then decided this one needed some help or the work would not get done.

"You know your boss's habits and temperament. Just watch and you will find an opportunity. The part you want to be careful about is installing the access point. You'll want to do that after hours. Tell me how you access your office."

"Access, uh, oh, how I get in?" Michael was trying to keep it together. "I have a badge. Here, I can show you." Michael pulled a credit card sized plastic badge out of his pocket and handed it to Vlad.

Vlad looked at the picture of Michael with his name at the bottom and the words "Network Support" at the top. He flipped the card over and then returned it to Michael.

"So you have a proximity access system?"

"Yeah, I just wave it at the sensor at each door."

"Is there a guard?"

"No. We have a receptionist at the front desk," Michael answered.

"Does anyone read the logs from your proximity card system?" Vlad continued.

"I think the security company might, I've never checked."

"So who is in charge of building security?"

"I think they outsource it," Michael answered.

"Since your company was recently acquired, have there been any new contractors working there?"

"How did you know about the acqui—uh, never mind. Yeah we've brought in some new techs lately. We've been getting rid of a bunch of our computers and installing new systems. They want us to match the big corporate standard."

"Can you get a badge for a contractor?" Vlad was getting weary of leading Michael along.

Michael sat for a moment and stared. "I think so. When they work late, they return them at the front desk. I might be able to get one after the receptionist leaves for the day."

"Use a contractor badge when you go in to make this change. That way if there is any suspicion, it will go back to the contracting firm" (*p. 217).

"Okay. I'll try that," Michael answered with no sound of confidence in his voice.

"Don't try it. Do it," Vlad corrected. "When you are done, we can meet here again in a week and I'll give you the rest of the payment."

"How will I know if I did everything right?" Michael asked.

"If I'm here next week at the same time, then you'll know you did everything right."

"And if you're not here, that means something didn't work?"

"If something doesn't work, I'll find you. But you don't want that to happen."

"What if I need to contact you?" Michael asked.

"There are instructions in that envelope. There is a number to call and a phrase to say. Then I'll call you. Write your cell phone number down." With that Vlad pushed a slip of paper toward Michael. He quickly complied.

Vlad picked up the paper and put it in his shirt pocket. "One other interesting point about your new book—the hacker gets caught in the end. Don't make that mistake, Michael."

With that, Vlad stood, picked up his newspaper and neatly returned the chair to its place at the table.

"By the way, make sure you don't leave any finger prints on the access point. That's the first thing they check."

Michael looked down, briefly trying to decide if paying off his gambling debt would be worth dealing with whoever "they" turned out to be. He looked up in time to see Vlad walk out the door of the coffee shop. Michael sat there staring at the now cold coffee he had bought, but not touched.

This page intentionally left blank

CHAPTER

TWO

JUST ANOTHER DAY

Friday, 5:00 p.m.

For the uninitiated, Bob Falken's bedroom looked like part-NASA control room and part high-tech junkyard. To Bob, it was both lab and sanctuary—the one place where he was in control of his world (*p. 380).

There was a constant hum from the combined sounds of cooling fans in nearly a dozen computers. There were various pieces of networking gear, cables, computer parts, and tools spread in even distribution across nearly all available space. Where there was an occasional gap, dirty clothes and DVD movie cases filled the void.

It was warmer in this room than in any other part of the house, and it smelled like a college dorm. For Bob, there was no better place to be. From here he could become anyone he wanted. He could travel anywhere in the world. For that matter, he could travel anywhere in a number of virtual worlds as well.

Outside of this room people ignored him, at best. More often they harassed him. In this space, he had power to control and remake himself.

Very few people were trusted to enter this part of Bob's world. In fact, only his dad and Leon were regular visitors. Bob's dad, George, was a retired engineer. He and his son lived in a middle-class neighborhood in Houston, Texas. Their neighborhood hadn't looked new since the 1970s when they moved there after George got his job. George had spent the majority of his life working on a variety of obscure pieces of the space program. Some of his designs had even orbited the earth in the forms of door components and panel covers. Nothing he designed had ever failed. If only his family had worked out as well.

He didn't know much about his son's activities. In fact, he was pretty sure that he didn't want to know all that happened in Bob's room. Since his wife had died when Bob was only 12, George had done all he could to encourage his son's interests.

Bob's natural affinity for anything digital pulled him farther into his own world. Only his friend Leon could bring Bob out into the "real" world as George called it. But to Bob, any time out of his room was just a distraction from his favorite reality. Bob carried scars from the loss of his mother. He and his dad were both very lonely,

and neither knew how to help the other deal with the loss. That failure created other losses as they both drew into their own worlds. One world had been a plodding career that was really a self-sacrifice for the son. The other was a search for a connection and feeling of completeness that was stolen when he was too young.

The world Bob embraced was full of computers, networks, hacking, and the personas he created. For George, the closest he came to peace was when Bob was at home. His son was safe and appeared satisfied. *At least he's not running with more dangerous kids*, he had thought to himself on many an evening as he listened to the hum of computers and the clicking of a keyboard. George had spent quite a bit on computers for Bob over the years. But most of his spare cash flow for the last year and half had gone to Rice University where Bob was a sophomore. George knew that there was more gear in that room than what he had paid for. His son was supplementing his income somewhere, and it certainly wasn't from a regular job.

Drip…drip…drip…

The living room was silent except for the sound of the leaky kitchen faucet George kept meaning to fix. George sat in his favorite chair. His wife had bought the chair for him years ago as a Father's Day present. It was worn and dirty, but George would never replace it. He could sit in that chair and instantly remember the happier days when his wife was alive and his son was a little boy.

George turned the page of the year-old issue of *Popular Mechanics* he was perusing and then reached up to adjust his near-terminal combover. Right as his mouth opened in a yawn…

Slam! George startled and tore the page from the magazine at the sound of Bob's bedroom door closing.

"Gotta go, Dad—I'm late to meet Leon."

There was a blur as Bob rushed through the house and out the front door. George looked about, never quite catching up with the image that flew past him while his mind was still processing the sound from down the hall. His mouth opened to dispense some fatherly advice about being safe. But then it closed—no use talking to an already empty house. George held up the now-torn magazine page to finish the article as he heard his old car start.

Bob backed the 1986 Buick Electra Estate station wagon out of the driveway and started down the street. The white paint on the car had long ago acquired a dull, chalky patina. The faux-wood sides were peeling and rust created a kind of south Texas lace around all the edges of the car. For Bob, the beast of a machine was perfect. He had plenty of room for his pack-rat habits, including installing all manner of portable computer equipment in the car over the last couple of years. As he drove, he barely looked down the road while he turned on his old Toshiba Libretto laptop that was bolted to the dash of the car. Bob had a habit of wardriving whenever he could. He was constantly on the lookout for open wireless networks, and today was a good day to try out the new antenna he had installed the night before. Bob turned out onto Kirby Drive and drove down the street to the local Anime store. When he arrived, he suspended the laptop and made sure he locked the car.

Inside he met up with his best friend, Leon. They had relied on each other since high school. Both were equally bright, constantly testing themselves with anything they could hack. Leon had better people skills—to Bob's frustration since it meant he did better social hacks. Bob could hold his own on anything with a keyboard. The Anime store was the appointed meeting place for the day. Bob was a paranoid young man. His time online had taught him how easy it was to be traced. He didn't like leaving a trail in either the digital world or the physical one.

"Hey, did you drive yourself in circles over here?" Leon asked as he spotted Bob walking in the front door.

"You know I'm not going to let anyone follow me."

"Dude, no one is going to follow you just because they'd have to keep looking at the butt-ugly car you drive."

"Hey, the price was right! It was a freebie from my dad, and it's got plenty of room for my gear. Come on. I got that new directional antenna installed last night. I want to see if it works better than the Pringles can (★p. 277)." Bob started walking back to the front door. Leon followed after. They were soon crawling through Houston traffic on their way to the Galleria.

"So do you have the riddles worked out for 'Capture the Flag'?" Leon asked. "I've got some, but I need help to finish. I think it's going to take us a while to come up with 20 of them."

"No, I haven't got any done since yesterday," Bob responded as he drove and watched the Libretto screen. "We'll dream up the rest after we find eight more open access points. I've got 11 good ones we haven't used before already."

"That's only 19 access points. You just said there were 20 riddles. Aren't we going to plant 20 flags?" Leon asked.

"We're planting 20 flags. One of them is going to be at my house."

Leon turned with a surprised look. "Why would you want to have all of the 2600 hackers pounding on your network? Are you setting up a honeypot to track someone?"

"No. I need plausible deniability," Bob responded. "And don't you ever tell anyone I said that" (★p. 246).

"You need plausible deniability for what?"

"I want to try a hack on Groom Lake. Remember when Gary McKinnon was busted for breaking into U.S. government computers from London? (★pp. 331, 333, 381). I think he got a lot more information than what was told. I think he found a link between the NASA computers he hacked and the Groom Lake facility. I want to take a shot at the Groom Lake network, but I don't want it to be traceable to me and get Dad in trouble. By putting a flag at my house, I'll have a default system that's been hacked by 20-plus hackers from around town. Any one of them could have been the source!"

"Your plan sounds too clever," Leon answered. "I think you'd do better jacking into one of the country club houses with an open network."

"I'll try that as soon as I have a car that looks like it belongs in a country club," retorted Bob.

Leon turned quickly and looked behind them. "Hey, I think that's the second time I've seen that PT Cruiser since we left the store." Leon didn't care about who was near them, but he knew he could tweak his friend by playing on his paranoia.

"Don't start with me. We've had three PT Cruisers near us since we left—and no repeats." Bob answered. "Don't laugh." Bob pointed a finger at his friend. "There are people out there watching for people with skills like ours. If you don't start paying attention, you're going to find yourself in a room with no windows and a couple of NSA guys 'recruiting' you for a job."

"Bob, it's a scary enough world without your paranoia."

"It's not paranoia when they really are out to get you."

Leon knew there was no hope. This conversation was an old one. From there they went on mostly in silence. Bob drove, spending more time watching the cars behind him than the ones in front. Leon spent his time watching the number of unsecured wireless access points increment up on Bob's laptop.

They pulled into the Galleria parking garage and found a place to park. To Leon's continuing frustration, the space was in the opposite corner of the garage from the entrance to the mall. He knew that it wasn't worth asking Bob to find a closer space. This gave him a clear line-of-site to his car and gave him room to meander through the garage watching for eyes that might be tracking him. Bob was a good friend. Putting up with paranoia was the price Leon had to pay for that friendship.

Soon they were inside and making their way down to the food court. As they approached Ninfa Express, they could see that the usual crowd was supplemented with extra people this time. This was the monthly 2600 Club meeting. Leon and Bob were regular attendees. Today, they were leading the prep for the first Capture the Flag war drive put on by the Houston chapter (★p. 331).

Leon sat down at an empty table. Bob walked to the center of their group of acquaintances (there weren't any real "friends" in this club). Leon always marveled that in this one setting Bob didn't have any problem talking to people. Leon looked around at the eclectic group of about 30 people. There were a couple of Goths, a Preppie, some geeky-looking teenagers, and even a Kicker. That was unique. Leon had spotted the thin guy in the cowboy hat at a couple of previous meetings. Leon got out of his chair and walked over and found him pounding on a Mac Power book with a DEFCON sticker on the top.

"How's it going'?" Leon asked as he sat down in the empty chair.

"Fine. Name's Jeb," he said while extending a hand. "I've seen you at all of the sessions I've been to."

"Yeah. Bob and I are regulars." Leon pointed to Bob at the table near the center of the group. "What brings you here?"

"I've been hacking on computers since my dad bought a PC to keep the books on our farm near Conroe," Jeb answered. "I don't want to be in the family business, so I've been trying to learn all I can so I can get a tech job."

"How'd you get the DEFCON sticker? Did you go this year?"

"No—I wish I could. I just picked it up from a guy I met at one of these meetings."

Leon started to comment on the Mac, but was interrupted by Bob who had now stood up.

"Hey everybody! Looks like we've got a pretty good crew. Today we're going to set the rules for Capture the Flag," Bob started. Slowly the talking stopped and everyone looked up from many different sticker-covered laptops to watch Bob (⋆p. 332).

"It looks like word got out since our last meeting. I don't recognize quite a few faces. If anyone here spots a Fed in the group, speak up" (⋆p. 330).

There was a moment of silence followed by a few snickers as everyone looked around and tried to take the measure of each other. Bob noted a couple of faces that he didn't recognize. One of them was Jeb. *Since when does a hacker wear a cowboy hat?* he thought to himself.

"All right. There are going to be 20 flags for the contest. The flag is a CyberBob icon file."

"What's a CyberBob?" came a rather meek question from the side of the gathering. There were a few more snickers as most of the crowd quickly noted the "newbie" in the group.

Bob was quick to respond. "It's another piece of the Hollywood conspiracy against me." This brought some eye rolls from a few "old timers" who knew Bob's reputation.

"Really, first they used my full name for the professor in *War Games*. Then they used my first name for this chat icon in *The Net*. And don't think I didn't get the message when they killed—" At that point Leon stood up.

"Like Bob said, it's an icon from the movie *The Net*. Just Google it, and don't worry about any conspiracies targeting our fearless leader here. I'll keep an eye on him."

Leon sat down, smiled and shook his head. Bob didn't seem to know he probably should have been embarrassed. He just kept going with the instructions.

"Leon is going to help me set up the contest and serve as the judge." Bob pointed at Leon as everyone in the meeting gave him one more look.

Bob continued. "Here are the rules. No damaging systems you find open. No dropping Trojans or using Trojans that you find already installed. We will only put the icon files in system folders, so don't go poking around where you don't belong. Don't hack into systems—we will only drop the files on boxes that have netbios running. They deserve to be used if they haven't at least locked that down. Finally, pull off the icon files you find. Don't leave a copy for someone who comes after you. There will only be 20 files out there, and the one who comes back here with the most wins.

"You will get 20 riddles to solve. Each one will give you a clue about the location of the unsecured access point. All flags will be located in Houston proper, so don't worry about suburbs. You can use whatever equipment you think you need. I suggest a good GPS, a good external antenna, and a copy of *Net Stumbler*."

Leon stood up again to add a little more. "Don't try to be clever and bring your own copy of the icon files. We're going to give each its own MD5 hash, so I will know if you have the genuine file."

"And no hacking the judge's PC for the MD5 hash files, or trying to work out a collision on your PS3," Bob added (*p. 300). "The contest will begin next Friday at 5:00 p.m. Meet here at noon next Saturday with the files you find. Leon and I have some more flags to drop still. We'll post the riddles on the Web site at the start time. But I'll give you one now to get you started."

Bob passed out a piece of paper to everyone at the meeting. A single sentence was printed on each:

Look for the first flag between the sheriff and the Merry Men's leader.

"And don't try to find the file for this clue now. We won't drop the file at this location until Friday," Bob added before sitting back down.

With that, the meeting broke up into a dozen small conversations. An outsider would have seen only an odd group of people clustered around different tables. However, there was actually a self-organizing structure to the groups. The more stickers and the newer the laptop a person had, the more people seemed to be drawn to them. Bob and Leon spent some more time talking to people and looking at the new gear some had brought. Soon it was getting close to 8:00 p.m. and they still had work to do. They made their way back to the parking garage. Leon humored Bob and walked down and back one wing of the mall first, to make sure no one was following them.

"Can you do some more war-driving tonight?" Bob asked as he started the car.

"Sure. I'm good for a couple of hours."

At the end of the evening they had enough open access points in their list. They parked outside the Anime store where the day started and worked on riddles for an hour. Progress wasn't as fast as they liked.

"Let's knock off and try again tomorrow," Leon suggested. "I want to get back and put in some Halo time. How about I stop by tomorrow?"

"Sure, we can also get some more drive time in to see if we can find more open systems. Maybe we'll find some that are easier to write riddles to match," Bob agreed.

THE INSTALLATION

Saturday, 10:00 a.m.

Michael Resol walked out of the Wal-Mart with a new wireless access point. He had read through the instructions his contact had given him enough times in the last two days to memorize them. He had already spent most of the $25,000 that was in the envelope Vlad passed him in the coffee shop. He knew that he should have used more than just half of it to pay down his debts from gambling. "I can take care of the rest of my debt with the second installment next weekend," he told himself as he put the access point—and the new 30-inch HD flat screen monitor into the trunk of his car.

As Michael drove to the office, he thought about how lucky he had been the day before. He had spent all afternoon watching for an opportunity. At 3:45 p.m. he saw his chance. His boss got a call Michael guessed was from his wife. He heard

something about a teacher conference at the school, a suspension and then the rush of wind as his boss stormed out of his office and out of the building. Michael waited for about five minutes, and then took some papers into his boss's office to leave on his desk. Sure enough—he hadn't locked his workstation. Michael made sure that no one was watching and sat down at the desk. He right-clicked on the desktop and selected "Properties." His boss had a password-protected screen saver set to go off after 20 minutes—just like company policy. Michael disabled the screensaver and turned off the monitor, then quickly walked out (★p. 219). He would take care of the Trojan on Saturday when there were fewer people in the office.

Michael pulled into the parking lot to find only a few cars there and a couple of motorcycles. As he walked to the front door, he pulled out the contractor badge he had found on Thursday afternoon. In fact, it had surprised Michael how easy it was to get. He had never noticed it before. The receptionist kept a box at the front desk with a slot in the top. Next to it was a sign for visitors who stayed after she left for the day that read "Please return badges here." A quick check by Michael revealed there was no lock on the box. He had found several visitor badges and two contractor badges (★p. 217).

His pulse quickened slightly as the door beeped and the light turned green when he swiped the badge. Michael first made his way to the break room for a soda, and then on to his desk. He tried to act as normal as he could as he walked to his part of the building.

On the way, he counted three people, all with heads-down, pounding on their keyboards. Michael did the same for a while.

After about half an hour with no one moving around the building, he got up quietly and walked into his boss's office. He slid into the chair and turned the monitor on. There it was—an open desktop. He pulled the pen out of his shirt pocket and removed the cap. The USB connector slid easily into the front of the PC. Soon a window popped up on the monitor with the contents of the new drive.

A sudden sound was enough to make him dive for the floor. Michael froze and listened…just someone at the copier down the hall. He took a deep breath, got slowly back into the chair, and scanned the cubicles around him. Nothing. "Where is Sydney Bristow when you need her? (★p. 383)" he muttered to himself as he looked back to the monitor.

He double-clicked on the "svchost.exe" icon and waited. Nothing happened. *I hope that's what was supposed to happen*, he thought to himself. Next Michael had to cover up his change from the day before. He right-clicked on the desktop again and selected "Properties." He made sure to select the same screensaver that his boss had been running and re-enabled the password lockout at 20 minutes. He started to get up, and then remembered the papers he had placed on his boss's desk yesterday as a cover for his presence in the office. He gathered up the papers and walked out of the office. *It won't be smart to leave evidence that I was in here after he left*, he thought.

Michael went back to his desk and picked up his backpack. All was still pretty quiet in the office. He walked to the row of empty cubicles in his section. In the third one he checked, he found a spare network patch cord connected to the jack, but

no PC. He set his backpack down and pulled out the access point, some duct tape, a rag, and his laptop. He powered on the laptop and connected it to the access point with the patch cord he had found. While he waited for his PC to boot, he connected the power cord to the outlet in the cubicle and powered up the access point. After his laptop was up, he opened his browser and logged into the access point with the default password. Out of his pocket he pulled the crumpled instructions that had been in the envelope he got on Thursday.

He followed the instructions, disabling the SID broadcast, changing the admin password to "penguin" and renaming the SID to "f0rb1dd3n." He made sure that logging was turned "off" on the access point. He then disconnected his laptop and plugged the access point into the empty network jack with the patch cord. Michael looked around—no movement, and he could hear some music coming from one of the programmer's cubicles. He crawled under the desk and wiped down the access point with the rag. He duct-taped the access point to the underside of the work surface and then took the time to wipe down the network cable as well.

Michael went back to his desk and worked for another hour. He had a hard time getting any real work done. His hands shook slightly as he typed. He was too excited thinking about how he was about to frame his boss, and make an easy $50,000.

CHAPTER

THR33

IN COUNTRY

Saturday, 10:45 p.m.

As he stood outside the hotel waiting for Vlad, Pavel shifted restlessly under the weight of his backpack. He had only been there for five minutes and already he was sweating. The Houston night was humid and the temperature was still close to ninety degrees.

"Why do people want to live in a place like this?" Pavel muttered to himself as he tossed the last of a cigarette to the ground.

A blue, late-model van with no side or rear windows pulled through the circular hotel drive and stopped not far from where Pavel stood. Pavel walked casually across the drive and climbed in the side door after an unseen occupant opened it for him. As Pavel took his seat, he surveyed the occupants. Vlad was sitting in the seat next to him. Pavel recognized the driver—it was Andrei—whom he had little use for. As Pavel turned to the passenger in the front, Vlad started introductions in English.

"You know Andrei. This is Haki. He lives in the States and does occasional work for me. He was kind enough to arrange for our transportation and equipment on this job."

Haki turned in his seat to look at Pavel. Pavel's and Haki's eyes met and they both nodded a slight acknowledgement of the other. Pavel ignored Andrei, turned to Vlad and said in English, "Why did you bring the gorilla on this trip?"

"You better be careful. He's been studying English," Vlad answered with a slight smile. "You don't know what words he already understands."

Pavel looked at Andrei and saw no reaction.

"I know he can use a gun, but I don't see language skills in his future."

Vlad ignored Pavel, turned to Andrei and ordered in Russian, "Let's get started. We have a schedule to follow."

Andrei put the van in gear and pulled out of the drive as Haki punched in an address on a hand-held GPS.

Pavel turned to look at the back of the van. Behind him was a small work surface extending from one side of the van. An empty bucket was turned over and looked like it would serve as a chair.

"I thought you had a bigger budget for this job," Pavel commented.

"I do. The van will serve its purpose, and I want to make sure that we can abandon it quickly if necessary and not leave any gear behind."

Pavel continued his survey of the van as they drove, noticing that Vlad had a large duffle bag at his feet.

"How do I do this, on site?" Pavel asked.

"No, you'll need your wireless gear. You brought your antenna?" Vlad's question had the sound of an order.

"Always do," Pavel answered (★p. 248).

"Ding Ding. Prepare for a—right turn—in—point seven miles."

"So, if you've done so many field operations, why the GPS besides the pure geek factor?" Pavel asked.

"None of us have been in Houston before. Haki is based out of Dallas now. A little storm chased him out of New Orleans."

"That was no little storm. It was nothing like wha—" Haki tried to protest before Vlad allowed a slight grin and continued explaining to Pavel.

"We don't want to be wandering around town. A vehicle that is driving in circles will attract attention we don't need."

Pavel appeared to accept the explanation. But he knew Vlad liked high-tech toys enough to find an excuse to use gadgets like a GPS whenever he could. They rode along in silence for a few minutes. Haki and Andrei spoke briefly in Russian. Pavel listened quietly as Haki translated directions to Andrei as they drove.

After about 15 more minutes of driving, they turned into the parking lot of a small office park. The lot was surrounded by trees and nicely landscaped. There were a few cars clustered close to a couple of the low, white buildings, but for the most part, the lot was empty.

Andrei parked the van in the corner of the lot at the edge of the office park. They had a direct line of sight to the office where Michael had installed the wireless router just the day before. Near the roof at the corner of the building was a simple sign that read "3DNF, Inc."

Vlad began snapping orders in Russian, "Time to start. Andrei, Haki, I want you outside. Keep an eye on our perimeter, but don't draw any attention."

Vlad reached into his duffle bag and pulled out three small radios and gave one each to Andrei and Haki.

"Channel seven," Vlad noted as he adjusted his own radio.

Andrei and Haki did the same. Then, Haki opened the glove box in front of him and pulled out two Glock 19 pistols. He handed one to Andrei. They both checked the action of their firearms. Pavel noted that Andrei was quicker and moved with greater confidence.

After they both had left, Pavel pulled his backpack up from the floor in front of him. Several key chains, a small flashlight, and a broken USB thumb drive jangled

on their lanyard clips hanging from the well-worn bag. Pavel pulled out his laptop. This was no ordinary laptop. An executive dashing through an airport would be left gasping for air in half a concourse if forced to carry this brick. Pavel had bought the custom-built machine after his first job with Vlad two years ago. It had two processors, two optical drives (one to burn CD's while the other played a DVD), more memory than most servers, and an odd collection of stickers.

Pavel maneuvered to the little work surface in the back of the van and sat down on the overturned bucket. As he waited for his laptop to boot, he dug around in his bag for a cable. He pulled out a small cable attached to a wide, flat piece of plastic about the size of a pocketknife. He connected the cable to a round jack on a card inside one of the accessory slots on the computer.

"Here—Can you get this near a window?" Pavel asked as he handed the other end of the cable to Vlad.

"Your cable isn't going to reach to a window," Vlad answered as he took the cable. He balanced the end on the back of the seat that Pavel had been sitting in and pointed it toward the front of the van—and the office building.

Pavel logged into his laptop and turned to Vlad. "You never answered my question about the gorilla. But first I want to know why we are here."

"You were there when we tossed Stepan Senn's room in Chisinau. The information we got off your new spare laptop, plus the instructions I got from Stepan were clear. This job requires a hands-on visit to ensure success."

"But I thought all we are doing is dropping a Trojan on a computer so we can remote in and steal some information. You've had me do that three times for different jobs just since we were in Stepan's hotel room. Why did we have to come all the way to Houston?"

Vlad drew a slow breath and looked at Pavel carefully. He was taking the measure of his young lieutenant. He wasn't ready to trust him—at least as much as Vlad was capable of trusting anyone.

"Stepan was working on a project for his employer to gain access to information that 3DNF is working on. 3DNF specializes in querying large sets of unstructured data."

"They were just bought by Kimeron, a large U.S. defense contractor (★p. 384). Kimeron wants them to get the brain power 3DNF has built up recently. Think about it—the U.S. government has the world's largest sets of unstructured data from all of their electronic eavesdropping. We are here because 3DNF is a doorway to that data. It's too risky to break into a U.S. government network. But 3DNF is a new acquisition for a defense contractor. The defense contractor is a trusted network—and that makes 3DNF the doorway we are going to use." Vlad could have continued, but Pavel cut him off.

"That doesn't sound like something worth a visit," Pavel noted.

Vlad was sharp in his response. "It is worth a visit. But your job isn't to decide what it is worth. Your job is to deal with the technical variables we will find. I need a reliable way into this network when we are done. That way in has to be undetected, and allow us to pull down a lot of data."

Vlad gave him a moment to be sure the point was understood, and then he continued. "Our front door is a wireless router and some duct tape under a desk. We will

use that to jump from 3DNF to Kimeron. Once inside, we install a reliable back door that won't set off alarms."

"When we are done, there will be a nice payoff from Stepan's employer."

Pavel paused to be sure Vlad was done. Then he asked, "Is there anything else I need to know before I begin?"

"No. I'll make sure that you know what you need to as we go along," Vlad responded.

"What about my first question?" Pavel couldn't help himself.

"Andrei? I would think the answer to that one is obvious. Remember who the target is. I need backup with more skills than just a keyboard. Haki is good, but we need Andrei's talent…and temperament," Vlad added with a slight smile.

With that Pavel turned his attention to his laptop. He set his wireless connection to the settings Vlad had given him and waited for an IP address assignment.

"How long do you want to sit here?" Pavel asked.

Vlad understood the meaning behind Pavel's question to know he was asking if he wanted an aggressive and quick, or quiet and slow scan of the network.

"We won't have to sit here long. Don't run any kind of network scan," Vlad explained as he produced the familiar pocketknife from his sport coat pocket. Pavel could see the USB connector at one end.

"There are two files on this. Copy them both to your computer, and then run the one called 'Achilles.'

Pavel followed instructions and was greeted with a window that had a simple blank box and a 'Connect' button.

"Now what?" Pavel asked as his hands paused over the keyboard.

Vlad tossed a small, folded piece of paper onto the keyboard of Pavel's computer. "Enter the IP address on that," he ordered.

Pavel unfolded the paper and leaned it against the bottom corner of the laptop display. He typed in the address.

```
10.24.53.192
```

A black box filled most of the screen and then a Windows desktop appeared. Pavel turned to Vlad. "I'm sure this is a question I'm not supposed to ask, but how do you know where I should start?"

"Stepan wasn't the only resource on this project. I have other contacts that his firm is paying me to use," Vlad responded.

Pavel looked at Vlad for a moment and quickly saw he had used up his allowance of background questions.

"What do I do next?" Pavel asked as he turned his attention back to the computer he was remote controlling.

"Use the remote computer to pull the other file from your system. Then you will need to start carefully checking out the network for me," Vlad answered.

Pavel knew he was being sloppy, but no one was watching. He enabled the Windows server service on the remote computer, created a share of the root directory, and

then went back to the desktop of his own laptop. From there he simply mapped a drive to the new shared folder that had appeared under the name of the target computer.

Bob took a quick right and pulled into a small, twenty-four-hour convenience store.

"I need some more Diet Pepsi, and it looks like there is an office park over there." Bob pointed with one hand while he maneuvered the wagon into a space on the edge of parking lot. The car shuddered to a stop and Bob turned his attention to the Libretto bolted to the dash. They had been driving around for the last hour looking for more wireless networks for the scavenger hunt the next weekend. They had plenty of networks, but Leon was the one being difficult this time. He didn't think they had enough "interesting" targets, as he kept explaining with each new find.

Bob and Leon watched as several wireless networks appeared on the screen of the Libretto.

"Will any of these work?" Bob almost complained as he pointed to the Netstumbler display.

"I don't know yet. Let me look with Kismet (★p. 149). You don't see as much when you run just Netstumbler."

"Let me know what you find. I'm going to go get a drink." The door creaked as Bob got out. Leon pressed the power button on his laptop and waited through the Ubuntu boot sequence. He clicked on his Kismet shortcut and waited for the application to load. He looked up from the laptop and scanned the parking lot. He saw only the usual traffic around a convenience store. Inside he could see Bob making his way to the back near the soft drinks.

Bob pulled two one-liter bottles of his favorite caffeine source from the cooler and walked over to the candy isle. He gave a quick scan of the sugar sources and selected a box of mints. He finished up his purchase and walked back to the wagon.

"Dude! We have our target!" Leon said too loudly as Bob climbed back in the car. Bob half-listened as he threw yet another empty Diet Pepsi bottle in the back seat and replaced it with one of the two he had just bought.

"What did you find?" Bob asked as he leaned over to see what was on Leon's screen. There were seven networks displayed. Four of them matched what Bob had detected on his computer. Three were not set to broadcast so Bob couldn't detect them. Of the new networks, one was not encrypted, and the name was "F0RB1DD3N."

"This one hadn't showed up because we were just running the scan with the Windows box. Kismet catches the ones that aren't broadcasting," Leon noted.

Bob had his chin down and was looking at Leon almost through his eyebrows with a "you don't need to tell me that" look. But instead of saying what he was really thinking, he just observed, "That's not a corporate network name."

"It's not a corporate name, but that doesn't mean it doesn't belong," Leon responded. "This place is full of little tech companies. There are plenty of nerds that work here that would set up something like that."

"Yeah, but why isn't it encrypted?"

"Let's find out," Leon answered as he changed his network settings to receive an IP address from the "F0RB1DD3N" network.

"Load Wireshark. I want to see what else is running on this network," Bob suggested as he reached in the back seat and grabbed his backpack with his main laptop inside (★p. 278). Bob and Leon quickly settled into a zone of typing and reading. The only sounds were from the people in the parking lot walking in and out of the convenience store.

Leon made more progress at first since he had a head start on Bob. Leon followed Bob's suggestion and had Wireshark running. This program would give him an idea of the traffic running on the local wireless network he and Bob were investigating. Leon quickly saw that they were not alone on the network. Someone was transferring a large binary file. He didn't say anything at first. Instead, he changed the settings for Wireshark to do a packet capture so he would have a copy of what was flowing through the network.

Bob didn't like the silence. His fingers began to fly across his keyboard. The sound of his typing was the nerd-equivalent of machine gun fire.

"What are you doing? You can't type that fast!" Leon squawked at Bob.

"Sorry, every hacker movie I've ever seen has the lead nerd pounding on his keyboard like that. I just wanted my scene for the movie."

"Like anyone would want to watch a couple of unemployed nerds drop CyberBob icons," Leon mumbled as he turned back to his monitor.

Bob shrugged and began to browse through his list of utility programs. He was about to click on the "T00Lz" folder when Leon spoke.

"Hey, I see a file transfer. Someone is working late tonight."

"What d'you see?" Bob asked as he leaned over to look at Leon's monitor.

"There's a computer on the wireless network with us. See, he's got a 192.168.1.2 address. I'm 192.168.1.3. He's transferring some kind of binary file to a box at 10.24.53.192. The ten network must be the corporate network."

"Are you doing a packet capture?" Bob asked. Leon looked at him with a 'do you think I'm an idiot' look and said, "Of course."

Bob went back to his "T00Lz" folder and clicked on the SuperScan icon (★p. 152). If someone was transferring a file to the .200 box, then there must be other interesting things in that network. This would be a good bonus site for the CyberBob icon. Once the program loaded, Bob started the scan to explore the 10.24.53.x network and see what he could find (★p. 383).

"What are you doing now?!" Leon yelled at Bob.

"What? I'm just running a network scan," Bob retorted.

"You're being sloppy! Dude, you lit up the subnet. Just because they leave the gate open doesn't mean you have to drive in with a bulldozer."

"If they're dumb enough to have an open Access Point, then they won't watch a SuperScan," Bob responded.

"Fine. I'll filter out your IP so we can see something besides your noise." Leon focused on his laptop. There was a brief quiet in the old Buick while each of them stared at their respective screens.

Bob's wrists looked like they were glued to the front of his laptop as he typed. His skin was so white from years indoors that it nearly glowed in the low light of his monitor. His fingers looked like two spiders reaching for prey as he typed. It took Bob only a few moments to produce a list of computers on the network he was scanning. He left the scan to run and opened a new window from his "Run" box at the bottom of the screen. He typed the first name of a computer that looked like a server followed by the default root path \\3D-FS1\C$ (*p. 248).

He was quickly rewarded with a listing of files and folders. He wasted no time in dragging a copy of the CyberBob icon from his desktop to this new window (*p. 383). He then confirmed with an updated file listing that now contained the bonus flag for their upcoming contest. Bob decided not to tell Leon yet. He wanted to look around a little more so he pulled the SuperScan window back on top to watch the results.

Andrei and Haki had each walked in the opposite direction when they got out of the van. It didn't take long to see that the office park was mostly quiet. The few people there were not paying attention to their surroundings. They were on a mission to get to their offices or cars and on with their tasks.

Vlad's two "hired muscle" soon met up next to a grouping of small trees that stood in a landscaped island near the edge of the parking lot.

"Do you really think Vlad needs the protection on this job?" Haki asked in Russian.

"I've learned that when he calls me in on a job, I generally have work." Andrei answered.

"Watch for a while. I'm going to go get some smokes." Andrei pointed to a small store near the office park and started walking along the shadowed edge of the parking lot. Haki stayed in the shadow of the trees where he could see their van and the majority of the parking lot.

Andrei walked into the small store and up to the clerk at the counter.

"Marlboro," he said with a thick accent and held up two fingers. This was one American word he had learned a long time ago.

The clerk turned and retrieved two packs of the requested cigarettes from behind the counter.

"Thirteen seventy-three."

Andrei didn't really understand the clerk, but he fished a twenty-dollar bill out of his wallet from the allotment Vlad had given him earlier that day and slid it across the counter. The clerk gave him his change and Andrei walked out of the store. Andrei paused outside the door and opened the pack. He lit a cigarette and surveyed his surroundings while he took a first drag. There were two cars and a truck at the front of the store. The truck had a woman asleep in the passenger's seat. Both cars were empty, their owners wandering inside the store Andrei had just left. In the corner of the parking lot was an old, beat-up station wagon with two kids and a strange blue glow lighting their faces. Andrei had seen the same glow before when Vlad or Pavel were staring at a laptop screen in the dark. He pulled out a piece of paper and pen and wrote down the license plate number. Then he started back along the edge of the parking lot to where he had left Haki.

In just over a minute Andrei had covered half the distance with a determined gait. He didn't like that even this small exertion brought a few beads of sweat to his forehead in the sticky southern night. He took another drag on his cigarette causing a tiny dot of amber light to appear. Haki took note of the return and watched as Andrei approached.

"We need to talk to Vlad," Andrei announced as he approached.

"We just got here. I don't think it's smart to bother him."

"I'll take that chance."

Andrei didn't wait for a response. He changed his course back towards the van. Haki paused for a moment and then decided to follow behind Andrei. When Andrei reached the van, he gave a light knock on the side and then opened the driver's side door and sat down closing the door behind him. Haki was a couple of beats behind when he sat down and shut the passenger's door. Andrei was already talking.

"There is an old car parked at a small store just north of this lot," Andrei began as he pointed out the front of the window toward where they had just been. "There are two kids inside and they each have laptops running. They look like an American version of your little one," he said with a glance toward Pavel.

Vlad turned to Pavel. Vlad didn't need to say anything. Pavel gave just a moment to meet Andrei's look and then turned his attention back to his own computer. A few quick clicks and he had browsed through a menu and launched his copy of Nmap (⋆p. 154). He typed in the 192.168.1.x wireless subnet he was using to connect to the 3DNF network and began a scan.

Three seconds after the scan started, there were two other computers listed on the display that should not have been there.

◖◖◖

"Dude, now what are you doing?!" Bob yelled.

"What?" Leon answered as he turned toward Bob.

"Look!" Bob pointed to the flashing alert on his computer. His Comodo Firewall had popped a window in front of his SuperScan (⋆p. 280).

"Someone just scanned me!" Bob pulled his hands quickly off the keyboard as if he had been shocked.

"It wasn't me. I've just been looking at the ten-twenty-four corporate network," Leon answered.

◖◖◖

"We are not the only ones on the network," Pavel said as he turned the laptop around so Vlad could see the Nmap result.

"What can they see?" Vlad asked.

"If they are paying attention, who knows?" Pavel answered.

"Is the file transfer done?"

"I've got about 25% to go."

"Stop it," Vlad ordered.

Pavel shut down the transfer and killed his scan.

"It stopped," Bob and Leon said in near unison. Bob had seen the network scan drop first, then Leon watched the screen stop scrolling on the packet capture.

"I've got a lot of data, but I don't think they were finished. It was all going to something that looks like a PC called 3M5763," Leon said.

"What now?" Bob asked.

"Let's just wait."

Leon and Bob sat quietly, each glancing from their respective computer displays to their surroundings. Two minutes crawled by filled with only the sound of quickened breathing from both of them.

"Look!" Bob almost squealed as parking lights on a van came on in the parking lot about 200 yards from their position. "That's got to be where this traffic came from!"

Leon and Bob watched, but there was no other activity from the van.

"Relax," Leon said. "There are several cars over there. That doesn't mean they were the ones."

"That has 'Fed' all over it! What if they were watching us, or maybe they were tracking something inside one of these offices?"

"We've got enough access points for the game. I'm going to pull out." Bob cranked up the old engine and put the car in gear. He didn't turn the headlights on, but slowly turned the car in the parking lot. As soon as they reached the street, the headlights of the van came on.

"I told you that's who we were watching!" Bob insisted.

"I don't think they're following us." Leon responded as he turned in his seat to see the van pull out onto the same street, now about a 100 yards back. He didn't sound quite convinced of his own words.

"Of course they are! There's no way the stuff we saw was from anywhere but that van!

They came up to a left-turn lane on Kirby Avenue. Bob finally turned on his headlights as they pulled up to the green protected left signal. Instead of going through, Bob stopped.

"What are you doing?" Leon asked as he looked back. Three cars separated them from the van. All were in the same turn lane.

"Proving that they are following us."

Horns started honking as Bob watched the light turn to yellow. As soon as it turned red, the cars on the perpendicular road got a green light for a protected left turn. Before the first car could take the turn, Bob punched the accelerator. The old V-8 engine roared and they lurched into the intersection. More horns blared as Bob cut off the surprised driver and led him across the intersection, continuing down Kirby.

"What are they doing?" Bob asked.

Leon watched behind them, bracing himself from the sudden motion.

"Oh my…you're right!" Leon watched as the van turned into the on-coming traffic lane and forced its way through the intersection. Horns blared again as the van cut off two cars that were trying to take their turn at the protected left.

"It's time for counter measures!" Bob yelled as he continued to accelerate past 50 miles per hour.

"That won't work," Leon complained. He had given his friend grief for the last year as he had watched him trick out the old wagon with more and more gadgets. 'Counter measures' was just his latest addition of weirdness from a paranoid mind.

"Shut up and hit the red button when I tell you to!" was Bob's reply.

Leon opened the glove box that revealed a piece of plywood mounted with three buttons crudely wired to cables extending into the dashboard through the back of the glove box. Two buttons were red and one was green.

"Which red button!?"

"The left one! Now wait for it! And whatever you do, don't hit the green button!" They continued down the road as the van swerved trying to make up the ground between them. Bob went through the next intersection on a green light—the van made it as well.

"They're gaining!" Leon shrieked. He had been pulled all the way into Bob's world.

"I told you it's not paranoia when they are trying to get you!"

Ahead Bob saw a Lexus RX350 SUV coming at them with its right-turn signal flashing. Bob accelerated and turned left across traffic onto the small side street lined with cars on each side, in front of the SUV.

"Now!"

Leon mashed the red button. He turned around to watch as the tailgate of the station wagon fell open. Four cans of white paint that had been rigged to fall came crashing out the back. Just as designed, each bounced once on the pavement, arced back into the air and emptied their contents onto the street in mid-flight.

Leon could see the lady driving the SUV toss her cell phone and grab the steering wheel with both hands. She gave the wheel a hard jerk and swung the SUV sideways as she slammed her breaks. Leon next saw several little league uniforms bounce around the back as the chaos faded into the distance. The nose of the SUV was now pointed askew to the direction of the street—neatly blocking any way around.

◖◖◖

Andrei nearly stood on the brake peddle of the van. The sound of screeching tires and a flood of heated words in three different languages filled the van as Andrei managed to stop just inches from the back of the SUV. Andrei threw the van in reverse and mashed the accelerator, skillfully driving backwards to the intersection where he threw the wheel hard to the right and spun the van completely around. Pavel grabbed at his backpack to protect the contents from taking flight across the back of the van.

◖◖◖

"Did you see that!?" Bob was hardly able to keep driving as he was so filled with adrenaline. His hands started shaking as he realized that his virtual world had just intersected with the real world. "I didn't think that would really work," he mumbled to himself.

Leon wasn't doing much better. "We are so screwed," he gasped.

"One of you might be able to figure out where we should go next with this," Andrei said as he pulled the piece of paper from his shirt pocket. He handed Bob's license plate number to Vlad.

"What is this?" Vlad asked as he looked at the number.

"I wrote down the number to the car when I first spotted it. You and your little friend might have a way to find them with that number."

Vlad wasn't happy, but the information took some of the sting of failure away. Before Vlad could bark an order, Pavel slipped a data card into his laptop and hit the 'connect' icon to bring up a mobile Internet connection.

"Give me a few minutes," Pavel stated as his fingers flashed on the keyboard.

This page intentionally left blank

CHAPTER

FOUR

IN REAL LIFE

Saturday, 11:53 p.m.

Bob pulled the car into an empty space at Wal-Mart. He turned off the engine and shared a collective expression of glazed disbelief with Leon. They knew that they had stepped across a line, but neither was ready to believe it. Even Bob, who had talked such a good story of paranoia, couldn't quite square the reality of a car chase with the imagined threats he had always seen around the next corner. Even so, Bob spoke first.

"I don't want to go home yet. We need to get some more information."

"Like what?"

"If they followed us, then they saw the license plate number. If they're Feds, then they probably will have someone sitting outside my house! Crap! Dad!" Bob realized the next step their pursuers would take.

"My dad is at home, or he was when I left!"

"It's only been a few minutes—just call him." Leon was trying to keep his friend calm, not realizing the volume he was using in his own response.

"And say what? 'Hey Dad, how's it goin'? By the way, has a van full of goons pulled up front yet? If so, it wasn't my fault. Oh, and whatever you do, don't let them in my lab.'"

"We've got some time," Leon said. He was starting to calm down and his brain was clearing a little.

"Let's assume the worst case scenario that they're Feds. We have to assume they know where you live from the car. That means we…"

"No!"

"What now?"

"My lab! It's going to end up in some evidence room with a bunch of bureaucratic nerds going through my data!"

"So do we go home now and see if we can beat them there?"

"Dude, you can't outrun a radio! The last time I checked the speed of light beats a Buick!"

Leon was getting frustrated as Bob became more agitated.

"Okay, calm down. Let's start over. We have to find a way to warn your dad. We can't protect all of your data—there's just no way to get back to the house safely."

Bob cut him off. "First we have to get rid of this car. We're a target as long as we are in this thing."

"How are we going to g—"

"Rudy!"

"What about him?"

"I bet he'd let us swap cars for a while. We don't need to tell him why; we just need a different set of wheels. We can give it back when this blows over, and if he gets stopped, he can't be linked to any of this. Give me your cell phone!"

Leon had no better suggestion so he just fished through his pockets for his cell. He handed it to Bob who started punching in the number.

"You have his number memorized?" Leon asked while Bob stared forward.

"Yeah, don't know why. It just stuck in my head after we worked on the last LAN party—Rudy! It's Bob…Yeah, we're about done with the Capture the Flag work. It's going to be great…Dude, I've got a favor to ask. We want to do some wardriving over in the River Oaks edition and my wagon will stick out for obvious reasons. Are you at work?...Cool. Can we stop by and swap cars for the night?...Yeah, Leon's with me… Okay, I promise he'll do the driving…Sheesh, I'm not that bad… I said yes I promise he'll drive…half an hour, sure. Thanks."

"Not bad—social engineer a hacker." Leon complimented Bob.

Bob didn't say anything, but he couldn't contain a self-congratulatory grin that spread across his face as he started the car and put it in gear.

"So what about warning your dad or saving your data?" Leon asked as he swayed with the rolling shocks of the old Buick that Bob was tossing around corners.

"Dude. I got nothin' okay?" Bob snapped.

Leon had no answer either. They drove in silence the rest of the way to the House of Pies twenty-four-hour diner. They did manage to calm down by the time Bob parked the car near the back of the parking lot close to the trash bins.

Inside, Bob and Leon had just gotten their drinks when Rudy walked up.

"So how many flags do you have left to plant?"

"Hey—how's it goin'?" Leon said as he slid over in the booth to make room for Rudy.

"Same old. I just finished working on a new boot screen for my PSP. Sousanator released a new prx you can use to make a custom startup."

"Cool—bring it to the next 2600. I'd like to see how you do that," Leon replied (*p. 336).

"We've got enough flags already, but we thought we ought to plant at least one in a country club. Most of the people playing will have cars as bad as mine, so this will make it a little more interesting."

"I understand. And thanks—that means I know at least one place to find a flag. I still haven't figured out your Merry Men clue."

"The clue wasn't about Merry Men. It's about the Merry Men's leader. Think about it, you'll get it. We need to get started if we are going to get this done."

"Thanks for letting us use the Mini." Leon said as Rudy put the keys on the table. "I promise I'll keep Bob away from the wheel."

Bob only half-smiled as he passed the keys to the Buick to Rudy.

"Can we meet tomorrow afternoon around five o'clock?" Rudy asked.

"Sure. How about back here?" Leon responded.

"And don't mess with any buttons!" Bob warned as Rudy stood up to leave.

"I won't. I'm afraid to think what mods you'd do to a car after seeing the stuff you bring to the meetings."

After Rudy left, Bob and Leon sat still for a few minutes staring around the restaurant. Bob's eyes lingered mostly outside, tracking the cars in and out of the parking lot. Bob suddenly got up, throwing three dollars on the table for the drinks and picking up his backpack.

"We've got to go. I know how we can check on my dad. I should have remembered sooner."

"What?" Leon asked as he followed Bob through the restaurant.

"My webcam. I keep the one over my main screen on feeding a password-protected Web site". We just need to find someone's network to jack into. Then I can see if anything's going on in my lab.

Ten minutes later Bob and Leon were parked just inside the country club called River Oaks at the beginning of a cul-de-sac. The little Mini Cooper blended in with the occasional cars parked in driveways and on the street. The area was only partially lit with lights built into the brick mailboxes that lined both sides of the street.

Leon turned off the car and watched as Bob connected his laptop to an open wireless network from one of the houses around them.

"You'd think people would figure out to encrypt all of these older Linksys networks that everyone still uses". Leon commented as Bob waited for his browser to load the page from one of his Web servers.

"Something's wrong!" Bob exclaimed after a few seconds of tapping on the edges of his laptop.

"What?"

Bob rechecked a long URL he had just typed into his browser. "My Web server is down. I'm going to check my off-site box."

"What off-site box?"

"Uh, it's a server I found that I use to auto-FTP motion video clips from my room," Bob answered. "And besides, the professor at the university in Australia who runs the site teaches Medieval English Literature. It's not like he's ever noticed I've borrowed a gig. Or two."

Leon gave Bob a skeptical look.

"Okay, 30 gig, but he doesn't use the space they give him." Bob's fingers did their spider dance across the keyboard as Leon shook his head.

"Here it is," Bob said as he scanned the folder structure on the remote server. "I've got a file that was uploaded 20 minutes ago. That means someone was in my room." He clicked on the file name and his video player loaded. Leon looked close over his

shoulder as the choppy video started. They both saw the door to Bob's lab open. First Bob's dad walked in, but he was followed by four other men.

"Crap! Feds! I told you they would find my house!"

There was no audio with the webcam, but they could figure out what was going on. Bob's dad was pushed into the room and was obviously confused and scared. The toughest looking of the three had his gun on George Falken. The well-dressed one who appeared to be in charge was standing near the door, and the youngest was looking at the monitors.

◖◖◖

Twenty Minutes Earlier…

"What was your son doing tonight?" Vlad asked George. Vlad's voice was calm, but forceful.

"I don't know. He was out with his friend." George, like his son, thought he was dealing with federal agents. He didn't know what was going on, but was convinced that Bob had finally crossed a line somewhere.

"We were investigating a corporate network break-in and found your son in the parking lot. We think he was involved."

"Bob wouldn't do something like that. He's a good kid." George was so focused on Vlad's questioning he didn't pay attention as Pavel walked around the room.

"Smile. We're on camera," Pavel said as he leaned close to look just above the 24-inch LCD in the middle of Bob's lab.

◖◖◖

Bob and Leon watched as Pavel's face nearly filled the screen. Pavel pulled back out of view and Vlad's gaze turned right at the camera. Andrei turned to the camera and in a swift motion brought his Glock away from Bob's dad and level with the camera. Bob and Leon both jumped as the screen went blank.

"Dad!" Bob yelled.

"Quiet! We don't want anyone to call the cops on us!" Leon insisted.

◖◖◖

George had thought his "visitors" were agents until Andrei shot the camera. He knew in an instant that whatever Bob had done, it wasn't the government he had offended.

"Watch him!" Vlad ordered Andrei—careful to use no names even in Russian. He then turned to Pavel. "Tell me what you can learn from this place."

Pavel had been admiring the setup since the moment they walked into Bob's room. He sat at the main desk that supported the seven monitors in the lab. "Chair" wasn't the right word to describe the seating. It was a large inflated ball of thick rubber resting on a round base with wheels and a support shaped kind of like E.T.'s head that formed the back of the "chair." It was a treasure Bob had found at a garage sale the year before and it fit the college-geek-dorm look of the room perfectly. The big

flat screen was unharmed, but the camera that had been neatly mounted on the top was now little pieces of plastic spread on the bookshelf behind the monitors.

"This will take a lot of time. I see three different operating systems, a firewall console, an IDS console, and I think this is a wireless network detector," Pavel said as he pointed at the different displays.

He turned back to the main console. "This is a PGP passphrase screen—if he has anything valuable, it's going to be in this system, and we aren't going to get in" (*pp. 255, 279).

Vlad turned to George who had been standing quietly with Andrei's gun pointed at his chest. He grabbed George by the shoulders and pushed him down to the only other chair in the room.

"Let's start again. What was your son doing tonight? We saw him out with one other person near a company called 3DNF. We think they were trying to break into their network."

George's hands shook. He was scared enough when he thought he had federal agents in his house. Now he knew he was in as much trouble as Bob and Leon.

"I don't know who Bob was out with tonight. He told me he had a date."

"Thank you. Now I know what you look like when you're lying to me. This isn't the room of a young man who goes out on dates," Vlad replied calmly. He turned his back on George and began to walk around the room, inspecting the chaos of Bob's life. "He was in your car with another young man. We know they both had laptops with them, and we know they were connected to the company's network. This company was conducting special research for the government; we believe they were trying to steal information that would have been very valuable."

George leaned on the desk and put his head in his hands. Pavel was plugging in a USB drive to Bob's main computer next to him. Then George saw it. Spread among the clutter of Bob's desk, between science fiction action figures and spare computer parts was an Office Depot "Easy" button. He remembered when Bob had asked him for help modifying the marketing gimmick button to be a real electrical switch. Bob wouldn't tell his dad what he was going to do with it. Bob had just said that once it was hooked up, not to ever hit it if he ever came in the lab.

"I told you, Bob is a good kid. He wouldn't do anything illegal." As George talked, he shifted his weight slightly and leaned to his right, closer to the button.

"You don't expect me to believe you. I'm sure my assistant will find plenty of evidence of illegal activities in here. There is no way all of this gear came from a teenager with an innocent hobby."

George knew this was going to hurt, but he didn't know how else to protect his son. In a quick motion he brought the hand that had been supporting his forehead down on the button. Pavel saw the sudden motion and realized too late that George had a plan.

A female voice emanating from Bob's main computer filled the room.

"Sequence initiated."

A hum began to build.

Vlad grabbed George and threw him to the other side of the room.

"I told you to watch him!" he spat at Andrei.

Pavel pulled his USB drive out of the computer. He hit the "Easy" button, but nothing happened. The hum increased in intensity. Three of the seven displays flickered, and then showed a "no signal" message.

The female voice continued. "Sequence complete. Primary drives have been magnetically wiped. Sorry, Bob." A blue-white flash shot from the largest tower computer under the desk. The smell of burnt plastic filled the room.

Vlad took George by the arm, and then turned to Andrei. "Toss this room, then go break out a window in the back and make it look like a robbery."

Vlad forced George out of the room, through the house and out to the van. Pavel followed behind, looking around for anyone that might be watching them.

"Tie him up!" Vlad barked at Haki as he shoved George into the back of the van. Haki worked quickly to secure George while Vlad and Pavel got into the van. Andrei came along just shortly after.

"Done." Was all Andrei dared to say in Russian to Vlad.

George picked up on the language change. What had his son gotten involved in? Haki got back in the driver's seat and started the van.

"Start driving! Just get us away from here! Haki, do you have a place we can take our guest and not be disturbed?" Vlad asked in English.

"Yes. I have a place."

As they drove through the neighborhood, George sat quietly in the back, nursing the pain in his wrists where Haki had secured him to the side of the van. George made eye contact with Pavel. For a moment, he thought he detected remorse or doubt, or maybe just fear. But for George, his own fear filled his mind too much to allow him to fully process what he saw.

Vlad was watching Pavel. "We need to give our guest some time to think of a way to help us find his son and companion. On the off chance they were watching that camera, then they will be more difficult to find now."

Leon was driving just to be moving. They didn't know where to go next. Bob wasn't speaking yet. He was still trying to process what they had seen on his webcam. Leon didn't mind the quiet. His body had already processed more adrenalin in the last few hours than it had seen in the last year. He had to concentrate just to keep the car at the speed limit. Intersections seemed to be too much information for his mind to assimilate.

"We need some cash," Bob broke the silence.

"What?"

"We need cash. We can't go home, and we have to take this car back to Rudy soon. We need to be able to buy ourselves some time."

"Do you have any?"

"Are you kidding? Any cash I get always ends up in my lab," Bob responded.

"Does your dad have any?"

"No."

"So where do you get the money for the lab?" Leon asked.

"I sell vulnerabilities I find to iDefense."

"You do? I've been selling to TippingPoint's ZDI!" (*p. 337).

Bob shook his head. "Dude, you should go with iDefense. They throw better parties at DEFCON."

The half-grin Leon managed with his friend's comment quickly faded. They drove along in silence, still with no purpose other than constant movement. They both stared blankly at the road ahead, barely seeing the traffic as they tried to cope with their situation.

Suddenly Bob looked up and exclaimed, "Turn back around! We need to go back!"

"Did you see something?" Leon asked as he scanned the traffic behind them.

"No. I just figured out where we can get some cash. You won't like it, but I don't think we have any choice."

"What's your idea?"

"It's more like where is my idea," Bob responded. "I'm going to get your laptop started and hook it up to my Wi-Fi antenna. We need to practice our Capture the Flag skills."

Ten minutes later Leon and Bob were driving slowly through the River Oaks development again. The price of the homes was evident by the number of unneeded chimneys each house had reaching into the warm and humid Houston sky.

"We can jack into a network here again and scan for Trojans. There's got to be someone around here with more money than sense," Bob explained.

"You're right. I don't like it," Leon responded. "But I don't see many options right now. Anything we take we pay back, agreed?"

"Sure—if we live long enough."

Bob pulled up Kismet and watched the screen as Leon drove the Mini through the neighborhood; careful to avoid the section they had visited the first time. It didn't take long.

"I've got one," Bob said. "I think it's up ahead."

Leon drove past two more houses and turned off the headlights as he parked the car. The large Tudor-style house had no lights on inside. There were a few landscape lights, but no signs of activity.

"Okay, give me a minute," Bob said as he connected to the wireless network.

"I've got an IP—192.168.1.103. I love it when they leave everything as defaults. This is a twelve o'clock person."

"What?" Leon asked.

"Twelve o'clock. You know, someone who's VCR is always flashing twelve o'clock because they have no clue how to reset it."

Leon managed a grin as he watched Bob work.

Leon opened up Bob's laptop and launched SuperScan and ran a quick scan of the subnet.

"Okay, you get mad at me for using that and now you pull that tool out," Bob observed before Leon had even started.

"Just give me a minute. I'd worry about a sensor tracking me if it were your house, but not here." Leon got a quick hit on 192.168.1.102.

"Here it is. The home computer is a Windows box and even has the SubSeven Trojan running (⋆p. 180). I bet they have a teenage son who pulls down music on his dad's computer."

Leon opened the client application and connected to the IP address.

"Wow this version is old enough to have the 'not so secret' master password," Leon said (⋆p. 183).

"I know," was Bob's simple reply as he stopped what he was doing on Leon's computer and watched Leon work on his.

Leon quickly had a window open on Bob's computer that displayed the desktop of the computer in the target house. He browsed through several different directories and soon had a cached copy of the password used for an online brokerage account. A quick browser session confirmed that the password worked, and there was enough money in the account for their needs.

Next Leon opened an IRC session and was quickly logged into a carder site.

```
I need a quick cash out. $10K guaranteed 30/70 split. No rip-
pers. No Nigerians (⋆p. 392).
```

"This won't take long," Leon said as his fingers tapped on the side of the laptop. He and Bob watched as several posts came through over the next two minutes Bob leaned closer to Leon to see the posts.

"I'm going to check these out before I respond," Leon said as he typed.

"How did you learn about this channel?" Bob asked as Leon worked.

"I just picked up some chatter when I was trolling for some ideas on vulnerabilities that carders use to get their product—here's one we can use."

"What did you find?" Bob asked.

"Of the three responses, only one of these actually masked their IP address. I'd bet this one is the most professional. I'm going to do a PM," Leon said.

Leon opened a private message session on the IRC and started to make arrangements.

```
Can you do Western Union to Houston, TX?
Deal. Here is the account.
```

Leon swapped over to the browser window that was still logged into the online brokerage account. He ordered a transfer to the account requested by his new associate.

```
Done. Can you wire tomorrow?
If the funds clear, you can pick up your $7K tomorrow.
```

"That was too easy," Bob observed.

"Now for the hard part," Leon responded grimly.

Leon swapped back to the brokerage account and changed the password. He then went back to the desktop of the compromised computer. He opened up the word processing program and typed a message.

```
I'm sorry, but I needed to borrow $10,000 from your brokerage
account. I will arrange for repayment as soon as I can. I also
changed your password on the account to 's3cur1t33'. I suggest
you change it to something else as soon as you can. As soon
as you finish reading this, disconnect your computer from the
Internet and take it to a computer shop and have them restage it
for you. While you are there, have them tell you how to secure
your wireless network.
```

Leon then closed the connection to the compromised computer, leaving the message visible for the owner. He created a text file on Bob's desktop with the name and address of his "victim."

"That should scare him into being a little more careful," Bob observed as Leon started to pack up.

This page intentionally left blank

CHAPTER

F1V3

STATUS CHECK

Sunday, 9:32 a.m.

The South Texas rain fell heavily on the 1970s vintage house. The small structure wore its 30-plus years of tropical storms, sun, humidity, and general neglect no better than the rest of the neighborhood. The only distinctive attribute of the house was the lack of cast-off items in the front yard. In fact, the only extra object in front was the blue van Andrei had deftly tossed around Houston the night before.

Inside the nearly empty house were Vlad and Pavel sitting at a small table in the kitchen. In the front room were Andrei and Haki. In one of the two bedrooms was George. He was sitting on a small wooden chair with his wrists locked firmly in handcuffs behind his back. A sturdy chain was looped through the cuffs to an eye bolt screwed straight into the wooden floor.

George had spent the night in the chair and his body ached. He hadn't been particularly abused, but the fear alone of the last 12 hours was enough to leave him nearly desperate. He had spent too long with his body prepared for fight or flight and no chance to do either. As he began to stop dozing and felt hunger and thirst build, he also started thinking a little more clearly. Bob was in trouble but not with any law enforcement agency. Bob must have been hacking into something he shouldn't have.

"I thought he was a good kid," George muttered quietly. He stared at the blank wall and the resolve of a father began to build.

"He is a good kid," he said a little more clearly.

◖◗◖◗◖◗

"So what did we get from our target last night?" Vlad asked as he sipped at a cup of coffee.

"Nothing yet. Your contact had good information. I got through the tunnel on the first PC and saw traffic from the government network."

"I want to go back today," Vlad said quietly.

"I don't think that would be a good idea," Pavel replied carefully. He surprised himself at the daring to disagree with Vlad. "We crossed into another network. We need to see if that tripped any alarms. We also don't know what those two others did on the network. They may have just been watching us, or they may have been tripping alarms."

"So…Michael isn't as disposable as I had planned. At least not yet," Vlad allowed the first smile Pavel had seen since they got to Houston. It was a smile that brought no comfort to Pavel. "We can just stay here for the day and give the father a chance to help us find those kids."

"What if they go to the police?" Pavel asked.

"After seeing how they acted last night, they won't go to the police." Vlad stared at Pavel while he thought through the next steps. Pavel shifted nervously under the gaze.

"I'll go talk to the father," Vlad announced. He picked up the coffee cup and tossed back the last of the drink as he stood. He set the cup down with a firm rap on the table.

Pavel let out a barely-audible sound. He wanted to speak, but thought better of it.

"What?" Vlad turned and held Pavel in his gaze again.

"Do we have to hurt him?"

Vlad smiled broadly this time. "Pain doesn't usually work that well, especially when family is involved. He just has to believe he can be hurt. Besides, the last thing we need is a bunch of screaming in a small house like this."

Pavel looked relieved, but didn't say anything as he watched Vlad.

"You wouldn't want to clean up the mess any way," Vlad said casually as he walked from the room.

Pavel's face lost a little color as he stared at his own cup of coffee.

"Andrei! With me." Vlad barked in Russian.

"…four…five…six…seven…eight…nine…seven thousand. Is there anything else we can do for you?"

"No thank you," Leon replied as he gathered up the stack of bills and placed them quickly in his front pocket. He walked out of the Western Union office and got into the Mini Cooper where Bob was waiting.

"How can being evil be this easy?" Leon asked as he started the engine. "I could never make this kind of bank with a real job."

"You aren't crossing over are you?" Bob asked as he eyed his friend.

"No. I just see how much needs to be fixed so it's not that easy to be so bad. We need a place to stay. I'm not sleeping in a Mini and I'm tired of jacking into Wi-Fi networks."

Bob ignored the sleep comment—he could go longer than Leon without sleep. "I've been looking at the code from the stuff we captured last night. This stuff is over my head. We need to talk to Max St341.

"I don't remember that name," Leon responded. He drove aimlessly just working to obey every speed limit sign and not draw any attention in their direction.

"I used him to help on some code on one of my exploits from last year," Bob responded.

Leon drove quietly for a block. "Those guys sure didn't seem like Feds to me. Shouldn't we go to the cops or someone?"

"I am not taking that chance! For all I know my dad is in Bagram Air Force Base right now. You don't know what a Fed looks like any more. They can be harder to spot in the real world than in Vegas."

There was another too long silence as they both considered what to do next. Bob spoke first.

"Let's get to a hotel that's got Wi-Fi. You can crash for a while and I can contact Max."

The cubicle at 3DNF sat empty. It was too early for the employees who kept normal hours and too late for the programmers. There were four computers whirring and six monitors glowing with no one to watch. The desk was cluttered with scribbled IP addresses, discarded meeting agendas, and an empty Mountain Dew bottle.

The middle and largest monitor was unlocked. It displayed the aggregated data from the few network intrusion detection sensors deployed in the company network. Near the top of the screen, the oldest entries sat unread. Steadily, new entries appeared at the top of the list. In the middle, a grouping of entries in red slipped a little lower. Chance would determine how far down the list, or even off the screen, they would be by morning on Monday when the analyst came in.

"How do we find your son?"

Nothing in George's history prepared him for this. The face that stared back at him was strong and intense. George hadn't been abused, at least beyond being yanked from his house, tossed in the back of a van, and chained to the floor in a small, dark room. During the lonely hours he had just spent with the handcuffs cutting into his wrists, George had prepared himself for resisting. But in the moment of looking into his questioner's eyes, he chose differently. He knew he wouldn't last long. His son's best hope wasn't in how long George could take a beating. Bob was smart and George had to trust that.

"He doesn't carry a cell phone."

"What about his friends?" Vlad asked with a steady tone that told George he had chosen right.

"No. He never told me their numbers. You have to wait for him to call me."

"And how would he know to call you?" Vlad asked.

"I bet he knows his computers have been destroyed. He'll want to know what happened at the house."

"But how will he contact you then?" Vlad asked, as he grew impatient and leaned in over George's face.

"He—he doesn't carry a cell phone. But back at the house, Bob keeps a cell phone in a drawer. The battery isn't in it. Whenever Bob stays out real late with his friends, I would put the battery in the phone and turn it on. Bob would call and let me know he was okay."

"We detected your son connected to a wireless network he shouldn't have. What was he doing?"

"Bob usually doesn't tell me what he is up to."

"I didn't ask what he usually does. What was he doing?"

"I don't know. I…well, it could have been Capture the Flag."

"What?" Vlad was getting impatient and his body language changed from confident control to in-your-face threat.

"C-capture the—it's a game I think—at least that's what I heard him talking about last week."

"Continue," Vlad said as George tried to shift his weight in the chair and Vlad drew even closer.

George quickly brought his eyes back to his questioner. He had allowed himself a quick glance at the quiet man who looked even more menacing and was standing guard at the door. "They plant an icon file inside networks and then leave clues for their friends to find them."

"What icon file?"

"I never saw it. But I heard him mention something called 'Cyber Bob' once when he was doing a video chat with a friend."

"One more thing—where is the cell phone?"

"In the kitchen. There is a drawer near the…"

George didn't get a chance to finish as Vlad spun on his heal and walked out of the room. He could soon hear his questioner's voice in another language through the walls.

Is that Russian? He doesn't sound happy, George thought to himself.

George allowed himself a snicker at the thought. Bob has always had the gift of being able to get under someone's skin quickly but he had outdone himself this time. He went still, though, realizing the consequences of it this time.

"Andrei!" Vlad snapped as soon as he shut the door to the little bedroom where George was chained.

"Go back to the house. Be careful. I don't want you walking into the police. In a drawer in the kitchen is a cell phone. Bring me that phone. And make sure you get the battery; it will be in the same drawer. And don't draw any attention to yourself. That van is already at risk because of the way you were driving last night."

Andrei's only response was to turn and walk to the door. He knew better than to ask questions when Vlad was barking orders as fast as he could think of them.

"Don't put the battery in the phone—just bring it to me!" Vlad called as Andrei started to close the door behind him. Andrei paused and looked back, giving a nod of acknowledgement before leaving.

◖◖◖

Leon tried to doze for a while but sleep wouldn't come. Part of it was the stress, part of it the noise from Bob that kept pulling him back from sleep. Bob sat at the little desk in the hotel room illuminated by the glow of a monitor. He was working on "the Beast"—the name he had given his oversized, sticker-covered laptop. He had just finishing setting it up and getting it connected to the hotel Internet service. Leon got off the bed and walked over to Bob. He looked over his shoulder and watched as Bob loaded World of Warcraft. Soon his character was running down a stone road in the middle of a dark forest. There was no one around, but occasionally there was movement off to either side. Bob ignored the motion and kept running like he was on a mission.

"I thought we came here so you could get some help from Max," Leon asked as he pulled a chair up next to Bob.

"We did, and that's exactly what I'm about to do."

"It looks to me like you're playing a game when you ought to be making a phone call."

Bob didn't take his eyes off the laptop. "There's no way I'd call him. This has to be done out of band" (*p. 394).

Bob hit a function key and checked his friends list. "Look, he's on," he said as he pointed to the fourth name down the list. "Just let me do a whisper."

```
I need to meet in the place. We need to talk. Code Alpha 9!
Again with the codes! Is Alpha 9 an emergency or did you finally
get a girlfriend?
```

"I like this guy already!" Leon said. "He knows you pretty well, too." Bob ignored Leon and just kept typing.

```
Just meet me!
I'm dropping out of a group to do this, so it better be good. OMW.
```

Bob didn't run anymore. Instead, he teleported and was now standing inside an Inn in Stormwind city.

"If you could have done that all along, why were you running?" Leon asked.

"I wanted to get away from the area where I had finished my last session just to make sure I was alone," Bob responded.

He ran through the streets, ignoring guards and other players. He crossed over a bridge and ran along a canal. After a few turns, he crossed a bridge again and continued to follow the water.

"Dude, are you running in circles?" Leon asked.

"Just a minute—I always get lost here." Bob tapped a key and a map appeared on the screen. He leaned in toward the monitor and mumbled something.

"There it is," Bob said clearly as he leaned back in his chair and changed the display back to Stormwind City. Bob crossed the canal one more time and then ran more deliberately. "This is the trade district..." Bob continued to run, ignoring less powerful characters around him. "Now the Mage Quarter…" Bob turned right after another bridge. "That's the Meeting Stone." The area grew darker as he passed into

a room. "And this is the Stockade." Bob ran downstairs and came to an opening surrounded by a spinning blue light. He walked through the portal and a "loading…" screen appeared.

"Now we are in our own instance," Bob explained.

"Our own what?" Leon asked.

"Instance. We just entered an area where we can chat with Max on an instance server," Bob said as he tapped a few keys. "I'm going to do a shadow meld."

"So what did you do that for if this is private?" Leon asked.

"I still have trust issues," Bob replied with a smile.

They stared at the screen for only a few moments before another character appeared through the portal. "That's Max," Bob observed as he typed another command.

```
Shadowmeld. Really? Show off :-P.
```

Bob moved his character and it became solid. He turned and faced Max.

```
Better?
Why do you always want to meet here?
It's as private as we can get without a Vent server. Why don't
you just get on the Vent server?
```

"What's a Vent server?" Leon asked.

"Man you need to game more," Bob sighed. "It's like an IP telephone. You can use the speakers and microphone on your computer to talk to other players in a dedicated channel. No eavesdropping and you can communicate faster than typing. I don't know why but Max will never get on one."

```
What do you need?
I need help looking at some code. It's too hot for the Net. Need
to meet in person.
I told you before. I know we live in the same city, but I don't
meet IRL.
```

"What's IRL?" Leon asked.

Bob looked at him like he was an idiot. "In Real Life. You should really game more. You are missing out on an entire subset of our culture."

"Hacker Speak is easier than your WOW slang," Leon responded.

```
I'll give you $500 cash if you will just look at the code.
What makes this code so special?
I picked it up on a wireless sniff. I don't know what it is but
it was something being pushed into a network not pulled out.
```

There was a pause. Max was thinking about the offer and the challenge.

```
Where do you want to meet?
```

```
   In front of Brother's Pizza in the Greenspoint Mall. How do I
recognize you?
   Look for the one wearing the iDefense shirt. I'm Hearthing back
to the Outlands. Time?
   Tomorrow at noon.
```

The hands on Max's character began to glow green. There was a flash of white light, and Bob's character was alone. Leon walked across the room and sat down on the bed.

"So tell me how all of that was 'out of band.' None of that conversation was encrypted," Leon demanded.

"Sometimes obscurity is good enough security. Tell me what Fed would be able to convince his boss to let him play World of Warcraft on the government clock until he had a player that would know how to get around the world like this. Besides, terrorists would think this is a depravity of the West. They wouldn't use it so that means the Feds wouldn't care to look into it."

Leon accepted the logic of Bob's reasoning. For all of his paranoia, he had a smart and unique way of thinking outside the box.

"I'm going to get some sleep," Leon said as he fell back on the bed.

"I'll do the same in a few. I want to look around Stormwind City a bit and make sure we were really alone." With that Bob turned back to the monitor of his laptop. Leon sighed.

"How can you tell if anyone was watching you? Can't they just transport out just like you could?"

Leon watched as Bob's character climbed up the stairs and walked back out towards the canal. Bob ignored Leon's comment.

LOG REVIEW

Monday, 9:37 a.m.

Jonathan Tao sat his Mountain Dew on the work surface of his cubical and sat heavily into the chair. Jonathan hated Mondays. Monday mornings never brought good news. Most of his attitude was from self-inflicted sleep deprivation each weekend mixed with an over-application of caffeine. He opened up the laptop backpack and pulled out his main work computer. He alternated between unlocking the monitoring stations on his desk and connecting the cables to his laptop. The dance was an amusing ritual of imbibing caffeine, typing passwords, reading logs, and rubbing tired eyes. Eventually, Jonathan's attention turned to the large display at the middle of his set of monitors. He kept this screen on and logged in all the time. It was used mostly to display logs from the firewall and the few network sensors recently deployed at 3DNF.

Jonathan took a couple more swigs of his carbonated breakfast as he scanned the entries on the Snort console (*pp. 253, 257). He was rarely fully awake for this

weekly ritual, but he performed it faithfully. Usually, if he found anything of interest, it only merited a call to the network support team because a server went down. Jonathan squinted his eyes as he scanned through Friday evening then into Saturday. His expression didn't change except for the breaks for additional swallows of breakfast. Suddenly at 11:06 p.m. on Saturday, there was a string of alerts. Someone had run a network scan from inside the company. He nearly missed the desk as he sat up abruptly and slammed down his drink.

"What the frack is this?" he asked aloud to himself. None of the caffeine he had consumed could bring about the same level alertness as what was just done with a few lines of log entries. His eyes tracked through the rows of text until 11:09 p.m. when the entries stopped. Jonathan got up and trotted off to the receptionist.

"Hey Susan, who can check the logs from our badges?"

"We can get those from the building management company. I can call and ask for you. What do you need?" she responded efficiently.

"I need to know everyone who was in the building Saturday." Jonathan's hand tapped out an impatient rhythm on the counter between them.

"I can have them send it to you," Susan volunteered.

Jonathan quickly responded, "Oh, I can just wait for it."

Susan turned, looking a little annoyed. She looked through the contact list on her computer and then dialed a number on the phone.

"Yes, this is Susan at 3DNF…Yes Alice, the weekend was nice, and yours?"

Jonathan's tapping on the counter approached a drumbeat as he watched Susan listen to Alice's response.

"Uh, Alice, I'm sorry to be quick, but can we get a copy of the building access logs from Saturday?...Just e-mail it to me when you get it…Thanks for the help. Oh, and tell your sister I got the catalog she sent me—" thump—thump—thump. "I'll talk to you later. Thanks."

"Thanks, Susan, I really appreciate it." Jonathan didn't wait for a response as he started to walk away. "Just forward the e-mail you get from Alice, as soon as you can—it's important," he said as he disappeared behind the door out of the lobby.

"Hey Jonathan, why the hurry?" Michael asked as Jonathan scurried past his work area and into the general manager's office. Michael didn't get an answer. He sat there trying not to stare, but wondering what was going on. There were very few offices at 3DNF. Since their product was software, they had mostly cubicles for the developers. There were a couple of conference rooms and a few offices. All these had at least one wall of glass opening into the common area. The company had built its reputation on the creative power of some very smart people. Closed offices didn't fit the culture. Neither did the closed door to Alex Henderson's office where Jonathan sat behind a glass wall talking. Michael could see the expression on his boss's face change and his posture go from a relaxed slouch to a stiffened upright, then to standing. Michael looked down as the door opened.

"Michael, come here," Alex ordered.

"Sure," Michael responded as he locked his workstation and walked to his boss's office. He was suddenly 13 years old again and on his way to the principle's office

after getting caught committing some prank. Michael sat gingerly in the chair next to Jonathan as Alex closed the door behind him.

"Jonathan, why don't you start by explaining to Michael what you just told me?"

Michael listened and tried to produce an appropriately surprised expression as Jonathan described the log entries he had reviewed. Thoughts came to mind too fast to answer. *Am I busted? Is this from what I did? I thought they didn't want to get caught? Am I supposed to say something?* Michael suddenly realized both Alex and Jonathan were waiting for his response.

"How do you know it came from inside the network?" Michael started.

"The IP address was internal, and the firewall didn't show any strange activity," Jonathan explained.

"Was it just a programmer doing an experiment?" Michael offered.

"It didn't look like an experiment to me. It was a noisy scan," Jonathan responded.

"Could this be related to the buyout?" Alex asked looking at Michael.

"What do you mean sir?" he responded.

"We just about wrapped the sale and I know people are nervous. Everything I've been told is we are going to all keep our jobs, and probably make out pretty well. But if someone has doubts, they might be looking around for ways to make Kimeron back out. Guys—do some homework on this. I want to know what's going on, but I don't want to raise any suspicions. If this is someone inside, then we need to keep everything quiet. We don't want to be the ones that screw up this deal. Give me a report tomorrow morning on what you learn."

Michael and Jonathan looked at each other briefly and both stood. They knew they had been dismissed. Alex turned his attention to the papers on his desk. The two walked out quickly.

Jonathan started talking as soon as they cleared the door to the office. "I want to look over some logs. I'll stop by later and we can talk."

Michael was grateful for the answer. He walked straight for his cube and did his best Invisible Man impersonation.

Jonathan was soon pouring over all the logs he could.

"I knew we should have put more money into the sensors than this," he complained to himself as he read. He moved his focus from screen to screen. Anyone watching would not have been able to discern any pattern. To Jonathan, he was checking off each sensor and control point until he had a clear picture of what he knew and what he didn't. He rummaged through his desk drawer and pulled out a business card. "He said they wanted to build relationships with the community," Jonathan mumbled as he picked up the phone and dialed the number on the card.

"Houston FBI, may I help you?"

"Huh, yes. Agent Mark Jackson please."

There was no acknowledgement as the line went silent for a moment.

"This is Mark."

"Hey, uh hello. This is Jonathan Tao at 3DNF. We met at the InfraGard meeting a couple of weeks ago" (⋆p. 399).

"Yes, I remember."

"You said in your presentation that the FBI was looking for ways to build relationship with infrastructure companies," Jonathan tried to get started.

"Yes."

"I know we are just a software company, but I have an issue here at the office that you might be interested in."

"Try me."

Wow—very concise—can this guy be any more Fed? Jonathan thought.

"I detected a noisy network scan that originated from inside our network over the weekend. We are about to be bought out by Kimeron."

"The defense contractor?" Mark asked.

Okay, now he's a little interested, Jonathan guessed to himself.

"Yeah. My boss is suspicious that there may be an employee who is trying to disrupt the purchase. He asked me to look into it further. I've been digging through our logs and I can't get a clear picture of what was done. Do you have anyone that could help me take a look?"

"Just a minute, let me check something on my calendar."

The line went silent for less than half a minute.

Mark came back on the line. "Can I stop by this afternoon?"

"Sure, that would be great." Jonathan responded. *I hope I'm doing the right thing*, he thought.

Chris Battle looked up from her paperwork with a poker face as Agent Jackson hung up the phone.

"Chris, I've got a project for us."

"What?"

"One of the contacts I made at the last Infragard meeting has some suspicious activity on their network and they want some help looking at it," Mark explained.

"What is Infragard?"

"It's a program the FBI set up several years ago to build contacts with organizations that control national infrastructure. Banks, utilities, local government agencies, even food producers participate in the program. They get together once a month for presentations and to get to know each other. It's better if something bad happens that people don't have to waste time swapping business cards."

"So this contact—have they had a loss?" Chris asked.

"He hasn't found one yet. He works for a software company that is being acquired by a national defense contractor. That definitely qualifies them as "infrastructure," Mark answered.

"I thought there had to be at least $30,000 in loss before it qualified for our involvement on business issues," Chris continued her questioning.

"It does. But this is building contacts. You never know who knows who in this business. This is how I build our network. We're probably just going to calm down an administrator at a software company. Some guy sitting in the corner who sees the FBI walk in will suddenly realize they shouldn't poke around the network. And we can get out of the office for a couple of hours."

"It sounds like a waste of time, but you're the one doing the training. What time?"

"About 1300. Let's get some lunch on the way," Mark answered as he filed the last of the papers he had spread on his desk and then stood.

◖◗◖◗◖◗

"Hey Michael, I got some help for us." Jonathan had startled Michael as he tried to look like he was working. Michael took a slow breath, turned to face Jonathan, and leaned back slightly in his chair.

"What do you mean?"

"Remember I told you I went to that Infragard meeting last month?" Michael asked as he set his now warm Mountain Dew bottle on Michael's desk.

"Sort of—wasn't it something about pandemic flu?"

"Well, that was the main presentation. They have different topics every month from public and private organizations," Jonathan explained.

"Is that all? I would think the FBI has some other reasons," Michael asked.

"Oh I'm sure they do. I bet they are better at asking questions than telling what they know. Anyway, I just got off the phone with one of their agents."

Michael was pretty sure he felt a heart palpitation. "What did they say?"

"He's going to be here this afternoon to help us look over the logs. If we have to give Alex an answer tomorrow, maybe he can give us some ideas about how to figure this out," Jonathan answered.

"Let's not tell Alex," Michael volunteered. He was going to lose control of this situation soon.

"Okay, why?" Jonathan asked.

"You heard what he said. We better not be the ones who mess up the merger! That's why he's so nervous about this network scan. Anything that could mess up the deal will look bad on him and cost him a pile of money." Michael was making this up as fast as he could.

"Makes sense," Jonathan agreed. "We still have to give him a report tomorrow, and by then maybe the FBI will have some ideas."

"Cool. Uh, I think I better wrap up the new Dev server install, so I'll have some time to help." Michael hoped this would get him some quiet time to make a phone call.

"Sure. I'll come get you when he gets here." Jonathan picked up his drink and wandered off.

Michael was fairly successful in keeping his movements to a near-normal speed as he reached for a desk drawer and pulled out a now-crumpled manila envelope. He looked over the instructions again and then dialed a number.

"Pizza Hut, may I help you?"

"Sorry, wrong number," Michael responded and quickly hung up.

"This is way over my head! Though the money is good and I no longer have any other options."

Michael sat with his head down near his knees and took a few deep breaths. He jerked back up at the sudden ring of his cell phone. He mashed the "talk" button and brought the phone to his ear.

"What do you need?" Vlad started abruptly. Michael gave a quick summary of the morning as quietly as he could. There was a moment of silence as Vlad processed the information.

"This will work out well," Vlad answered. Michael couldn't think of any way this would work out in his favor.

Vlad continued."I have your Lee Harvey Oswald."

"What?" Michael didn't see any connection between an assassin and his hacking problems.

On the other end of the conversation,Vlad smiled as he started to explain.

CHAPTER

S1X

THE MEETING

Monday, 11:47 a.m.

Leon and Bob walked into the Greenspoint Mall. They had covered little distance when Bob turned to the arcade at their right and pulled Leon in with him.

"I thought we were going to the pizza place?" Leon protested as Bob walked to the change machine.

"We are. But I want to look around first." Bob pulled a few crumpled bills from his jeans pocket and walked over to the token machine while Leon loitered near the front and failed a feeble attempt to look inconspicuous. Bob quickly returned and passed a handful of tokens to Leon.

"You play a game here near the entrance. I want to see if anyone is tailing us."

Leon had stopped joking about his friend's paranoia. Now he was thankful for it. He dutifully slipped a token into one of the games and played while Bob leaned next to the machine and watched. He didn't see anyone showing any interest in them as he scanned the entrance to the arcade or the main hallway of the mall. After a few minutes, he was satisfied.

"We will be late. Let's go," Bob said as he started to walk. Leon left the game running and followed Bob. As they walked through the food court, Bob stayed to the right so he could survey the open space.

"I don't see the T-shirt yet," Leon observed.

"Keep looking," Bob responded as he looked.

Leon was first. "Your Max friend is cold. He's got his sister to be a decoy for him."

"What do you mean? Where?" Bob asked. He followed Leon's nod toward a table on the far side of the food court. A thin, college-age brunette sat with her back to them. He couldn't see a face, but her shape was nothing like the nerd acquaintances Bob knew.

"How do you know she's his sister?" Bob asked.

"She's hot. No geek would have a girlfriend that looked like that," Leon observed.

"Good point."

"Do we take the bait?" Leon asked.

"Do we have a choice? Just watch out for pepper spray. You go left, I'll take right." Bob started walking. Leon followed the lead and headed around the food court in the opposite direction. They both reached the round table at the same time and sat down in unison. The girl didn't startle at all.

Bob started. "Your brother should have told you not to sit with your back to the crowd."

"Then how would you have seen the iDefense T-shirt?" she responded. The logic caught Bob off guard, but Leon quickly smiled at their new acquaintance.

"Beside the point," Bob recovered. "Where is your brother?"

The girl flipped her hair out of her eyes—succeeding in revealing only one striking brown eye that contrasted with the shock of dyed, bright blue hair that covered the other one. Her attractive, vaguely Asian features were enough to cause Leon pause, and keep Bob off balance.

"Why are you asking me about a brother? I don't have a brother. You wanted to meet me."

Bob wasn't convinced. "Sure. Where is Max? Do we have to go somewhere to meet him? We don't have much time."

"I'm Max."

"Right. We need help fast. Where do we find him?" Bob continued. Leon just sat with a half-grin watching the parlay.

"You find him right here. What do you want?"

"Okay, how do I know you're Max?" Bob challenged.

"In WOW, you have a pet Scorpion you named 'Snookums'."

Leon chuckled as Bob answered exasperated. "That's pretty good, but anyone who plays WOW could know that."

"Okay, I'm the one that showed you how to pop the sled on that buffer for the browser bug you were working on about a month ago. Since I didn't get any credit in the shout out, I know you didn't tell anyone how I helped," Max responded.

Leon laughed and turned to Bob. "Dude, you are so busted. You told me you came up with that bug on your own!"

Bob's mouth hung open like a flytrap for a moment before he recovered. "That's beside the point!" he protested to Max. "Dude, you're not a dude!"

Max was quick. "Get over it. It's the Internet! The guys are guys. The girls are guys. And the 14-year-olds are FBI agents! What do you expect?"

Leon looked straight at Bob. "I am starting to like her," he confessed and then turned to Max. "Okay, we need some help. Let's delete the awkward introduction. Bob's a little harder to deal with IRL."

"You're paying, so what's the job?" Max asked.

Bob finally started to get his footing. "We need you to go back to our hotel."

"Whatever, what do you think I am?" Max protested.

"I thought you were a dude with enough candle power to help! Here, I'll show you some of it." Bob reached down and opened his ever-present backpack. He pulled out his older machine and booted it. While it was coming up, Leon pulled a USB thumb

drive from his pocket and slipped it into the side of the computer. Bob typed for a moment and then turned the laptop to face Max.

"Here is a Wireshark capture we did when we were planting icons for a wireless Capture the Flag game. We saw this code and we think it has something to do with the Feds. What do you see?"

"Max looked for less than a minute. "This is serious. Whoever was planting, this was deliberate. Your capture doesn't show any scan from the source of the code. They knew what their target was."

Bob looked at Leon. "Why didn't you see that?"

Max looked at Bob. "I'll go look at what else you have, but I've got pepper spray."

Leon just smiled as Bob took the laptop and handed the thumb drive back to Leon. The three got up and Bob led the way they came toward the arcade. Max assumed they were walking toward the exit when Bob took a quick turn to the right and opened an unmarked door where there was no shop. Max gave Leon a questioning look but he just followed along without hesitation. Max did likewise. They were walking along a maintenance hall behind the food court restaurants. They came to a branch that went to a door marked "Exit" but Bob continued straight ahead.

"Have you been here before?" Max asked as they walked.

"I wouldn't have suggested a meeting here if I hadn't," Bob answered as he led them to another door. He opened it and they were back in another main hallway of the mall. It wasn't crowded, but there were enough people there for them to quickly blend in. Bob marched across the hallway, past a Sears, and opened another unmarked door on the other side. Leon and Max just kept pace as they went down the brick-walled space. They came to another branch, and this time, Bob veered left. He pushed open the door into the daylight of the parking lot.

As they approached the Mini, Leon pulled out his keys. Max looked at the car and quickly spoke up, "I'm not getting in a stolen car with you two."

Bob turned. "Why do you think it's stolen?"

"I wasn't sure until you just answered that way," Max responded. "You two don't look like you could afford a real car."

Leon took this one. "It's not stolen. We borrowed it from a friend."

"Borrowed doesn't sound too safe," Max responded as she looked at the line of police cars parked near them at the Houston PD Mall substation. "For a car of questionable source and two guys scared of Feds, why are you parking by so many cops?"

"The closer to danger, the farther from harm," responded Leon smugly.

"Huh—Tolkien fan," Max observed. "Shotgun!"

Leon smiled as he watched Bob acquiesce and fold himself into the back seat. As Leon turned the key in the ignition, Max turned back to look at Bob.

"And one more thing—IRL my name is Hannah."

Bob didn't have a response. He just gave a sigh. Leon watched his face in the rear view mirror and then turned to his passenger. "Nice to meet you, Hannah. Thanks for helping us." Leon pulled out of their parking space and patiently made his way out of the mall parking lot. Bob processed his online acquaintance's real-life identity in silence.

FIRST LEAD

Monday, 1:01 p.m.

"Good afternoon, how may I help you?" Susan asked as a man and woman walked in the door at 3DNF.

"I am Agent Jackson and this is Agent Battle. We have an appointment with Jonathan Tao," Mark responded dryly as he and Chris both displayed their badges.

Their identification could have come from a cereal box. Susan was so taken aback when she saw the letters "FBI" that she saw nothing else. She said nothing more and quickly turned to the phone in front of her and dialed Jonathan's number.

"This is Jonathan."

"You have a couple of visitors from the FBI," Susan reported with a halting voice as she looked up at the two standing in front of her.

"Great, I'll be right there." Susan heard the click and set the phone down. "He'll be with you in just a moment," she reported as she continued to stare. She had never seen FBI agents at the office. Most of their visitors were strangely dressed programmers, some rumpled academics, and vendors. Lately, there had been an influx of lawyers with the buyout. *They look more like lawyers than agents*, she thought as the shock wore off and they turned and surveyed the entrance behind them.

Very shortly, the door to the office opened and Jonathan appeared. "Great. Agent Jackson, I'm Jonathan," he said as he extended a hand.

"Call me Mark. And this is my partner Chris," Mark responded as he finished the handshake.

Agent Battle didn't look too pleased with her partner as she shook Jonathan's hand as well.

"Let's start at my desk," Jonathan led the way through the door and past the rows of cluttered desks and large monitors.

"This looks like your kind of place," Chris commented to Mark as they walked. She muttered, "There probably hasn't been talk of a date around here since this place opened for business."

Mark allowed a couple of steps worth of space to open between him and Jonathan as he responded. "Just because we're bright doesn't mean we don't mate."

"Great now I won't get that image out of my head," Chris responded as they walked.

Jonathan pulled a couple of chairs over to his work area and tossed an empty Mountain Dew bottle in the trash. Chris gave a quick glance around the area before she sat down. She noted one set of eyes that marked her movement. Michael quickly leaned forward in his chair out of their line of sight. Jonathan was already talking and Mark was listening intently when Chris turned her attention to the monitors in the work area.

"So what I don't get is why they were doing such an obvious scan," Jonathan was stating. "I looked at our main servers and didn't find anything out of the ordinary. But then I found this." Jonathan's right hand was driving a mouse and clicking quickly

as windows appeared on the main screen. He pointed to a server called 3D-FS1 and double-clicked. Another flurry of clicks and soon, a window appeared listing the contents of directories.

"Here in the root of one of our file servers is an icon file called 'CyberBoB'." It doesn't tie to any executables. The time stamp shows that the file was placed here right in the middle of the scan traffic that started all of this."

Mark leaned forward and stared intently at the screen for a moment. "Can I have a printout of this listing?" he asked.

"Sure." Jonathan clicked some more. "It will be on the main printer." He started to get up before Mark interrupted.

"Do you have a wireless network here?"

"No. We used to do subcontract work for a defense contractor and now that they are buying us, they don't want any wireless. I have to run a check every couple of weeks just to make sure."

"How do you do that?" Mark asked.

"Let me show you." Jonathan opened up the wireless options window on his Windows XP system and clicked the "scan for available networks" options. The three of them watched as it returned a blank window. "Nothing. I'm kind of surprised, I haven't picked up anything lately from some of the other businesses around here either." Jonathan stood up. "I'll get that printout for you." He left Mark and Chris in the cubicle.

"What are you thinking?" Chris asked.

"Not yet." Mark answered and turned as Jonathan reappeared quickly with a sheet of paper.

"Jonathan, have you had any staff turn over lately? You mentioned a buyout," Mark questioned.

"No, we haven't. If the deal goes through, I think most of us will make out pretty well. They are buying the company for the brainpower anyway."

"Have you had any temps around? I noticed a lot of new computer boxes piled up as we walked in," Mark continued.

"Yeah a couple of kids. We've been getting new equipment. Alex, my boss, said we are supposed to have everything matching the new company's standards. He had Michael bring in help."

"Who is Michael?"

"Oh—Michael Resol. He runs our infrastructure. He had to get some help for the equipment staging work," Jonathan explained.

"Did they come from an agency?"

"No. I think they were friends or relatives of one of our programmers."

"Did you do background checks on them?" Mark continued.

"I don't know. Hey Michael!" Jonathan called across the hall. Michael looked like a prairie dog popping out of his hole as he jumped a little too fast at the mention of his name.

"Yeah?" came the reply with a voice that cracked on the single word.

"Do you remember the names of the temps you had in to do the PC installs?"

Michael walked over to the group. "Uh, there was John Aggarwal and Robert something. I think it was Focker. No, Falken."

Michael's eyes met Agent Battle and he instantly looked away. Mark followed up. "Do you have any paperwork on these people?"

"No. I should have, but they were friends of friends. They were just kids and it was just for a few hours. I paid them with old gear we were going to get rid of anyway."

Mark made some notes on a pad he carried. "Do you have a way to reach them?"

"Do you think they did the scan?" Michael asked.

Mark looked at Jonathan expectantly. "It's okay, Michael and I are the ones who are supposed to be looking into this," Jonathan volunteered.

Mark looked back at Michael. "I don't have a theory. I just want to make sure I get the facts."

"Sure. I don't have anything for John, but the Robert guy gave me an address and phone number. Just a sec." Michael went back to his desk and pulled a Post-It note off the top of a pad. He had just written down the info that morning from Vlad.

"Here you go." Michael handed the note to Mark. Chris noted a slight tremor in Michael's hand at the exchange.

"One of the days they were here Robert was wearing some kind of geek or hacking shirt," Michael volunteered.

"Interesting. Thanks for the help." Mark stood and Chris followed the lead. "We need to check a couple of things out. Can I call you tomorrow?" Mark asked Jonathan.

"Sure. If you have any ideas, let me know. We're supposed to report to our boss in the afternoon," Jonathan responded.

"No problem." Mark started to turn for the entrance.

"Do you need to look through the server logs or anything else?" Jonathan asked.

"I've got what I think I need for now," Mark answered. I might have some follow-up questions, but first I want to check a couple of ideas and we'll be in touch.

"I don't trust that Michael guy," Chris observed as soon as they closed the doors to the car.

"He's scared, but it could just be because we were there," Mark observed.

"What's your theory? You knew something with that icon thing," Chris asked.

"I think they have some sloppy network security and just got used for a hacking game."

"A game? They are about to get bought by a major defense contractor, and some strange network scan happens and your theory is a game?"

"Yeah. I don't have enough to get a warrant, but it's worth our time to go for a drive."

"A drive? Where to?"

"I think I know who this Robert is. If I'm right, then I can use this defense contractor connection as a reason to look at a network I've been wanting to see for several months."

"What network?" Chris was not following any of this.

"There is a group of local hackers that I've been trying to build a relationship with. One of the brightest is named Bob, and I think this looks like something he would

have done. I don't think he did anything malicious here, but he might have just given me a way to get a look inside his home network. I'm betting we will find some leads on other things that will be interesting," Mark explained.

"Home network?" Chris asked.

"Sure. Guys like him have some pretty impressive networks that they use to do research."

"And do you have one?" Chris asked.

"Of course. It's not too big. Just a few servers, two laptops, my main PC, and of course the gaming machine. You should come over some time and—"

"You did not just invite me over."

Mark gave Chris a confused look. "What?"

"You did not just invite me to your place," Chris clarified for her slow partner.

Mark shook his head as he turned his eyes back the road.

"No. I invited you over to see my lab." Mark curtly replied clearly put off. "It's just as well—it would be lost on you."

THE DISCOVERY

Monday, 5:32 p.m.

"What do you think we can do without a warrant? Are you going to just ask him to show you his network?" Chris asked as they drove through the dreary neighborhood to the Falken house.

"I don't know yet," Mark answered as he finished the turn and started scanning for house numbers. He started to slow the car and eased toward the curb as he approached. "Right now I just want to talk to him and see what he can tell me. It might lead us to," Mark's voice dropped off as he set the car in "park."

He pointed down the left side of the house. "The gate to the backyard is wide open. Let's do this together," Mark said as he gave a quick look up and down the street and pulled out his revolver. Chris was already ahead of him and had her door open first. Mark wanted to take the lead, but Chris was around the front of the car and making her way up the driveway before Mark could gather himself.

"Front door looks normal," Chris noted as she walked past the left corner of the attached garage and started to walk through the gate. Mark followed along the house, watching down the street before following into the backyard. No one noted the visitors.

There were no windows along the side of the house as they reached the back corner. Chris gave a pause for Mark to catch up. She gave a quick look around the small rectangle of overgrown Bermuda and a lone spindly tree in the backyard. The first window was about shoulder-high. Chris glanced in the corner. She didn't say anything, but Mark noticed she bent down quickly and her hands flexed on the grip of her gun. A few steps and she paused at a glass patio door that was standing pushed open with a bent handle. The matching door frame that once held the lock was bent.

Mark noted a crowbar tossed on the patio before he caught Chris's eyes as she got ready to go in.

"Hello? FBI! Anyone home?" Mark announced. Chris swept the room from right to left and saw no movement. She moved across the cluttered family room to her left toward a hallway as Mark came in behind and gave another look to the kitchen to the right. It had obviously been tossed. This was what Chris must have seen through the window. Mark turned to his left and saw Chris paused at the hallway waiting for him. He covered the distance in three quick steps and Chris then turned into the hallway and held her gun straight ahead of her.

"Clear!"

Mark moved behind Chris and checked a small front foyer and living room. It was neat and unoccupied.

"Clear!" Mark responded as he turned back to find Chris proceeding down the hallway. Mark followed with his gun held low. Chris checked a bathroom to the right while Mark checked a small neat room to the left. The room was too neat compared to the house they had seen so far. Mark's gaze took in a sewing machine, a cutting table, perfect curtains in the window and—

"Something burned in here!" Chris noted as she positioned herself by a closed door at the end of the hall. Instead of going in, she looked to her right at the open door to George's bedroom. Mark took Chris's place in the hall as she proceeded into the room and did a quick sweep of the bedroom and small bathroom. Chris came back as Mark opened the door to Bob's bedroom/lab. It was hard to see if anything was out of place or the mess was a normal state. Mark noted the acrid smell of burnt electronics as he holstered his gun and scanned the room.

"Is this how you people live?" Chris asked. "I'm going to go see why the kitchen was tossed." Chris was only one step down the hall when Mark stopped her.

"This might be part of it." Chris turned back as Mark held up the largest piece of a shattered webcam and then pointed at the top of the largest of the many monitors arrayed at the makeshift desk. Chris followed Mark's gaze and then saw the hole in the wall.

"So why did someone break into this geek's house, shoot a camera, and toss a kitchen?" Chris asked. This makes no sense. And what is that smell?

"Something fried the electronics in here," Mark said as he tapped a couple of keyboards with the tip of a pen he had pulled out of his pocket. Nothing is working in here. I bet the kid wiped everything.

"Your kid wasn't here when this happened," Chris answered.

"How do you know that?"

"That kitchen was tossed like someone was searching for something," Chris explained as she walked around the room. "I don't see why they would shoot the camera, but whoever came in didn't think anyone was home. They would have made too much noise with the crowbar and the patio door."

"I don't know," Mark doubted as he walked over and checked the two small windows in Bob's room. "They're both locked. He didn't get out this way."

"Let's see what the kitchen has to say," Chris said as she walked down the hallway.

"Why would the kitchen be so interesting?" Chris asked as they surveyed the mess. Most of the cabinet doors were still closed, but every drawer starting from the right side of the room was tossed on the floor with its contents spread evenly about. About a third of the way around the room, the mess stopped. "Whoever it was found what they were looking for in this drawer," Chris observed as she stood over the last tossed drawer.

Mark surveyed the dumped contents on the floor. Most looked like typical kitchen contents with silverware, measuring cups, and other utensils. But the pile of stuff at the center under the last open drawer was different. There were an unusual amount of batteries, small nails, spare change, pieces of paper, coupons, pens, and even a tossed deck of cards.

"Whatever they were looking for was in the kitchen junk drawer," Mark observed.

"I've never seen a house without one of those," Chris noted. That just means we can't figure out what they were looking for from here. It could have been anything."

Mark pulled out his phone and hit the speed dial for the office. He gave a sigh thinking about the time he was going to be spending trying to get some data off of those cooked hard disks in Bob's lab.

An hour later, Chris and Mark were getting back in their car.

"So am I going to have to sit at the office tomorrow and watch you do your geek thing with all those computers the guys are back there tagging?" Chris asked.

"Probably not. I do that work alone, and I bet it won't reveal much. Bob is a bright guy and if he wanted information wiped, then it's wiped."

Mark pulled out of the neighborhood and headed for the highway.

"Where are you going? I thought the office was north of here," Chris asked as Mark made the turn onto the entrance ramp.

"I'm not done with this. There are three guys who hang out with Bob at the 2600 meetings. I know where two of them work, so I want to go ask some questions."

◖◖◖

Twenty minutes later, Mark parked the car outside of a Bellaire strip center in front of a store called LightSpeedSystems.

"Just let me talk," Mark cautioned as they got out of the car.

"Of course—like I even speak the language," Chris answered as she held the door open for Mark.

Chris was just inside the door behind Mark when a large unkempt guy with dark eyes and sloppy red hair called out.

"Hey Jeb, if that really is your name, why are you bringing a Fed with you?"

"Sorry, my name is Mark Jackson and this is—"

"I know who you are. You are the kicker who calls himself 'Jeb' at the 2600 meetings. You clean up pretty good. She's a Fed, so I'm betting you are, too."

Mark gave up. "Chris, this is Dobbs. He's a friend of Bob from the 2600 meetings."

"I knew it!" Dobbs exclaimed. "You guys and your Patriot Act are watching all of us!"

Mark revealed a look of exasperation and annoyance as he raised both his hands slightly towards Dobbs. "I'm just a tech who has learned it's best not to tell everyone where I work."

"That's crap! I bet you are part of a whole program made just to watch people like us. You just need to put some faces with all the data you've been scraping with Echelon!" (*p. 303)

"I'm not going to convince you. I just need a few answers." Mark said almost pleading.

Chris suppressed a laugh as she surveyed the store and watched Mark blow his own cover.

"Like I'm going to give you guys answers. You don't need answers anyway. I bet you've been using your wire taps on—"

"Dobbs, give it a rest. I just want to know if you can help me find Bob," Mark interrupted now losing patience playing "good cop."

Dobbs stopped talking and looked down at his shorter visitors for a moment. "Okay, I'll confess." Dobbs sighed. "Bob and I have been building a small nuclear device. We had to scrape the glowy stuff off of about 1700 watch faces we found at flea markets to get enough fissile material."

Mark leaned on the counter with both hands and just bowed his head slightly. "Dobbs, you need to understand I think Bob is in trouble and I want to help."

Mark held Dobbs' gaze for a three-count and then Dobbs looked away.

"I haven't talked to him since the meeting. You know as much as I do. He was still working on the Capture the Flag setup.

"Can you get in touch with him?" Mark asked.

"He's the only person I know who's more careful than me," Dobbs responded reluctantly. "I don't even have an e-mail address."

Mark reached in his pocket and pulled out a business card. Dobbs gave a flinch at the motion before he saw the white paper.

"Here is my card. If you hear from him, call me."

Dobbs looked at the card and saw "Federal Bureau of Investigation." "Why would I need to call you? If I hear from Bob, you'll probably have it all on tape…"

"Dobbs, the last thing we have time for or care about is tapping your lines," Mark interrupted him as he turned to walk out.

"Why not? All I need is a detonator and my watch-bomb could take out half the Gulf!"

Mark paused at the door. "And what would you have to hack then?" Mark gave a grin and walked out before there was a reply. Usually, no one got the last word on Dobbs at the 2600 meetings.

"So that is what we work so hard to protect from terrorists?" Chris asked with disgust as they got back in the car. "That must be what happens when Dan Haggerty goes geek."

"Dobbs is one of the smartest ones at the 2600 meetings. I swear if you put a keyboard on a '57 Chevy he could write a Perl script to improve the gas mileage."

"What's a pearl script?" Chris asked (*p. 285).

Mark just gave a sigh and started the car. "We have one more visit to make."

◖◖◖

"House of Pies?" Chris asked as they turned into the parking lot. "If these guys are so smart, why don't they have better jobs?"

"A lot of them work just to feed their computer habit," Mark answered. They walked in and paused at the "Please Wait to Be Seated" sign. A young, African–American man approached with two menus. He wore the same polyester slacks and polo as the rest of the staff, but Chris saw the flash of a Tag Heuer watch. She also noted some very nice looking black D&G rimless glasses.

"Would you two agents like a booth or table?" he asked.

Chris gave an annoyed look to Mark.

"What do you mean?" Mark asked.

"You talk to one hacker, you talk to all. Information wants to be free. And you two look just like Dobbs described." Mark noticed the iPhone secured to the waiters' belt.

"I just want to ask if you know where Bob is."

"I haven't seen him or Leon since they left the 2600 meeting to do more wardriving. I thought with all your spying at our meetings, you would be able to find him if you want." Rudy gave his best angry look, but it wasn't as convincing as Dobbs had been.

"So there were two of them." Mark saw an opportunity. He reached out with his left hand and placed it on Rudy's shoulder and gently guided him to the closest booth. Rudy sat down and Mark slid into the booth beside him and Chris took a seat across from them.

"Listen, if you were paying attention at all of those meetings, I'm just as much a propeller-head as you guys. Bob never seemed like someone who would go bad. I just know he's in trouble and he needs help. Please, tell me what you know." Mark responded earnestly.

Chris wouldn't admit it, but she was impressed. Mark had picked the right technique at the right time. She saw Rudy's expression ease just enough as he took in a long breath.

"Bob was here with Leon last night," Rudy started.

Mark gave a slight knowing glance toward Chris, and then turned back to Rudy. "What did they tell you?"

"Not much." Rudy looked at Mark, then across at Chris. He didn't trust her, so he turned back to Mark.

"Anything you have will help," Mark encouraged. Mark and Chris waited for Rudy to fill the silence.

"They needed a car."

"I thought Bob had a car."

"It's not that. They needed a car for the wardriving. They wanted to scope out some places in a country club. Bob said he wanted to find a spot that a regular hacker wouldn't fit in," Rudy explained.

Chris allowed herself a nod of agreement at the logic.

"So what car do they have right now?" Mark asked.

"They took mine. I've got Bob's wagon parked in the back. He and Leon have my Mini Cooper."

"That's a pretty good ride for a waiter," Chris observed. "That watch doesn't look like it belongs here either." She said inquisitively.

Rudy and Mark both gave Chris a look.

"My dad agreed to pay for my college and car as long as I keep an hourly-wage job. He said everyone should respect hard work," Rudy responded in a somewhat haughty tone, and then looked back to Mark who gave a slight helpless shrug of his shoulders.

"Can you give me the license number?" Mark asked as he handed Rudy a piece of paper and a pen. Rudy just nodded and started writing.

"I hope you didn't let Bob drive your car," Mark added as he collected the paper and pen from Rudy trying to lighten the mood.

Rudy seemed to perk up at the comment. "No way—I made Leon promise he would drive."

"Rudy, you did good. We want to help Bob, too," Mark said as he got out of the booth. Mark looked to the front of the restaurant and then at Rudy. "You've got customers. We will be in touch." He shook hands and presented his card in hopes of possibly more information in the future from Rudy.

It wasn't until Mark reached to turn the ignition in the car that Chris spoke.

"You did good."

Mark paused and turned to look at Chris. "You sound surprised."

"I am."

"The best hacks are human, not technical. Rudy needed to tell someone. I just gave him the right 'someone' so he could help his friend."

"So do you have any other leads—or do we get to call it a day?"

"You can call in the bolo on the Mini." Mark handed the slip of paper to Chris. "Tomorrow I'll see if there is anything left on the gear from Bob's house. Right now that's the only path I see."

CHAPTER

S3V3N

CODE REVIEW

Tuesday, 3:19 a.m.

Leon wanted to stay awake. He had enjoyed watching Hannah work as she parsed through the code they had captured from 3DNF. He sat in an uncomfortable hotel chair between Bob and Hannah as they worked. Hannah's hands moved across the keyboard with the flair of a pianist. After each command was completed, there was a certain virtuoso quality to the way she finished off the strike on the "Enter" key. As Leon watched his two companions, every blink of his eyes took a little longer to open. His breathing slowed and his body relaxed slightly. One deep breath and—

"What!?" Bob had punched Leon on the shoulder.

"I told you they were Feds!"

"What?" Leon still couldn't command any more words.

"I told you they were Feds!" Bob tried again.

"We don't know that," Leon responded and then yawned. "That's just what Dobbs said in his Twitter (*p. 287). Did you find anything in the code?"

Hannah jumped in. "Whatever you guys caught, it wasn't amateur. I found references to IPs that tie back to Germany, Russia, Switzerland, and China. There's no way to know where the command and control for this is. I tried looking at these IPs and they are all black holes. They either don't exist or they have some good source filtering".

"What does the code do?" Leon asked.

"We can't tell. But there is more about where the code was going when you caught this copy. You guys were too quick looking at the packet capture. Here," Hannah pointed at the display on her laptop. "—the file was going to 10.24.53.192."

"Yeah, we knew that," Leon said. He turned to Bob and wondered aloud to Bob brooding in his chair, "Since when are you so quiet?"

"But did you see this?" Hannah continued scrolling down a couple of screens worth of captured data and pointed again. "Whoever was on the wireless network with you was also talking to 10.43.84.143."

"Okay, so they hopped to another private network," Bob responded. Leon noted the slight annoyance in Bob's tone.

"What were they doing?" Leon turned back to Hannah.

"Well, it's a different subnet. So I'd sure like to know if it just hopped through a switch, or if it is going through a router to an internal segment, or DMZ, or out to another extranet. We just can't tell if this is in the same general network or not. Since the person you were eavesdropping on went straight to the first IP, they knew what they wanted." Hannah turned to Bob. "You didn't see any scanning before you started this capture, did you?"

"No—this is the only interesting part of the traffic we saw," Bob responded.

Hannah continued, "I bet if they are good guys or bad, they were placing some kind of command and control on at least one box, maybe two."

"Feds!" Bob loudly concluded.

"We don't know that," Leon pointed out trying to break Bob out of his funk.

"They've got my dad!" Bob responded, his voice close to cracking.

"What?" Hannah turned to Leon. "That's more than the code review I signed on for."

Leon didn't want to lose the new help. "Listen, we think—but we don't know—the people who were on the network were Feds."

"Of course, they were—you guys saw Dobbs's DM when they went to his shop." Bob was getting his voice back. He turned to Hannah. "Max, I had a camera in my lab. It was tied to a motion sensor and sent a video file to a remote server I use. We pulled down the file and saw three people in my lab with my dad. They had a gun on him and one of them shot out my camera. None of my stuff is live on the web anymore."

"That doesn't sound like the Feds," Hannah responded.

Bob looked almost wounded with her answer, but he didn't stop. "Dobbs. He's from 2600, he—wait a minute—you were lurking at the meeting last month, weren't you!"

"I was watching," Hannah confessed defiantly.

"Where?" Leon jumped in.

"I was hanging out close enough to listen to what was going on. I knew if I sat down and started talking, I'd probably get pulled in and then I'd have to come up with some complicated real-world story."

Bob shook his head, a little mad at himself for not connecting the dots before now. "Anyway, two Feds showed up at Dobbs's shop yesterday. They were asking about me!"

Hannah started to ask a question, but Bob cut her off.

"And get this—one of the Feds has been going to 2600!"

"Who?" Hannah asked.

"Jeb—the kicker. He was in a suit at Dobbs's place. They've been watching us all along!"

"Listen, if they are Feds, they won't get you for anything more than listening to an unsecured wireless. I've looked at the logs and you don't have anything other than a radio broadcast someone was dumb enough to not encrypt properly. But, if these guys are bad—you don't know how far they will go. If they have your dad, I say go to the Feds now and take your chances."

Bob was shaking his head in disagreement before Hannah even finished. Leon was a little slower to come to a conclusion. Everyone had exhausted his or her arguments. They sat in silence with each looking at a different random object in the room. After a few sighs and shifts in a seat, Leon tentatively broke the silence.

"I think Hannah's right. We need someone on our side and I think it's worth taking the chance." Leon paused, expecting the push back from Bob, but it didn't come. Instead, he just looked expectantly at Leon to see if he had more. Leon continued his thought.

"If Jeb—or whatever his name is—has been watching us, then at least he knows we aren't that bad. If he's been paying attention in the 2600 meetings, we don't teach people to do evil." Leon paused for a breath and Bob let him continue.

"Let's set up a meet at some neutral place. Maybe they can help."

Bob sat and considered the idea. He knew his friends were right, he just had to break the momentum of his own distrust of anyone in a position of authority.

"Okay, let's send a text to Jeb. I've got his cell number from Dobbs."

"Don't use your phone," Hannah volunteered.

Bob gave her an incredulous look. "Of course, not. I don't carry a phone—and I'm not going to use Leon's and give them a way to trace us. I'll use a VMware browser appliance through TOR to a Web site that sends texts" (⋆p. 305). Bob turned and reached for his laptop, balanced it on his knees, and started typing.

Hannah looked a little embarrassed at the answer and leaned back in her chair while Bob worked. Leon leaned over Bob's shoulder as he typed.

```
I hear you are asking around about us. Meet at Galleria parking
garage, where we exit from 2600 meetings at 17:30 today. Don't
bring goons. Bob.
```

"I don't think 'goons' is a way to make a friend," Leon suggested.

"Tough. I don't want any extras," Bob answered still agitated with no tangible target to lash out at, then he clicked the "Send" button on the screen. "Now, we need a different car. The Mini works for wardriving, but we may need to blend into the crowd now. Max, do you have a car?"

"Uh, yeah. But I don't want every cop on the street looking for it." Max said taken aback at the abrupt transition.

"What do you have?" Bob asked, ignoring Hannah's concern.

"It's a Ford Taurus my dad gave me after he wore it out driving to work for years."

"Perfect. We'll need you to drive to the meet by yourself and be our way out. We will need to ditch the Mini. If the Feds have been talking to Rudy, then they probably know we have his car," Bob deduced.

"I'm not sure. I don't think Rudy would tell them," Leon suggested.

"We can't take that chance—Rudy has more to lose than we do. We've got to assume the Mini isn't safe. Besides, we left the wagon in the parking lot, remember?"

Leon nodded in agreement, but Hannah wasn't satisfied with her part.

"I just said I don't want to have cops looking for—"

"Max, we don't have a choice. We need to get out of there and you are the only way," Bob responded. "Besides, we won't be followed. They won't ever see us get into your car—that's why we picked the location."

Hannah still wasn't convinced. She looked at Bob and started to speak. Just as she took a breath, Leon cut her off.

"Hannah, please," was all he said quietly. She looked at Leon and her expression softened just slightly.

"We arrive at different times, and I don't park anywhere near you."

"Deal," was all Bob said.

Leon smiled slightly at Hannah and nodded his head. "Okay, now we are a team." He turned back to Bob. "So what do we need for the meet?"

"Let's see…" Bob leaned back in his chair and stared at the ceiling with his hands behind his head. "We'll need my iPaq to check for heat, my laptop with the code, and, uh, and that's probably it." I don't want to take more and risk losing it."

Two hours later, Leon and Bob pulled into the Galleria parking garage slowly. Leon started up the ramp while watching the environment for threats. Bob had his iPaq running WiFiFoFum. The software gave him a radar-like display of wireless access points in the area.

"We're clear so far—no cops in this part of the garage." Bob leaned over and showed the display to Leon. A single dot appeared near the edge of the screen.

Leon understood. The display showed sources of wireless network signals and estimated their distance. The Houston police department, like a few others around the country, had begun using wireless signals between their squad cars and repeater stations set on traffic signals. The resulting network gave them a high-speed data link back to their headquarters, so they could retrieve datalike lookups on license plates or pull up videos on certain public area surveillance cameras. The problem with the system was that they hadn't considered how easy it was to detect the wireless signal. Even though it was encrypted, it still warned of their presence. Even when they went on silent runs, they were emitting a Wi-Fi networking signal (★pp. 400–401).

Leon turned back to watching the cars slowly pass as they drove up the ramp. Just as they made the turn passed the second-level stairwell entrance, neither of them noticed the man step out of the door. As Leon and Bob proceeded up the ramp, Andrei strode calmly across the ramp and over to an older-model sedan. He needed something that wouldn't have an alarm. The well-practice move was only visible to someone directly in front of Andrei. He slipped the tool between the window and the rubber gasket of the door and with a deft move, caught the lock and pulled. The door was open and Andrei quickly went to work on the ignition.

Mark and Chris were already standing by their car on the third level. As agreed, in the texts they received, they were positioned on the opposite end of the level from the stairwell. Neither spoke as they watched the full parking lot. There was a lull in foot traffic, but they could hear the sound of cars and people on the other levels. Chris caught the motion first and tapped Mark's arm as she turned.

Leon pulled the Mini Cooper up the ramp and continued around up to the fourth level. Chris followed the movement of the car while Mark watched where it came from.

"Is that our contact?" Chris asked as she tracked the movement.

"Yeah. Watch for them to walk in. They'll either come from behind us or that stairwell," Mark motioned across the parking garage to the metal door that had no window. They stood scanning the area for only a couple of quiet minutes before the door to the stairwell opened slowly. Two college-age kids walked out. The shorter leaned forward slightly to compensate for the weight of the backpack he carried.

"We don't need to worry about them running," Chris noted.

Leon paused for a moment, but Bob never broke stride. Both of them were scanning the area. Bob went straight to the first space between a parked car behind him and an SUV in front. Leon was close behind. From their position, they could see the door to the stairwell, were a few paces from the ramp up to the next level, and had a clear line of sight to the two "Feds" who were the objective of the day. The hood of the SUV gave more protection from their biggest threat.

"Dobbs was right—that's Jeb from the 2600 meetings," Bob observed. He could see both of Mark's hands, but the lady stood with her side facing them. Her left hand was visible resting on the hood of a car, but her right arm was held close to her side, hiding her hand. "I think she has a gun," Bob noted while trying to deny the reality at the same time. Leon nodded half in agreement but didn't speak.

"Bob. What were you guys doing at 3DNF Saturday night?" Mark started the conversation.

Bob didn't give Leon a chance to speak. "I'd rather know what you guys were doing there!"

"Bob, we weren't there. We got a call that they found a CyberBob icon file on one of their servers. That sounds like you were planting stuff for the Capture the Flag."

"You were there!" Bob retorted without answering Mark's question. "We were minding our own business at a convenience store and detected you guys planting a Trojan on their network!" Bob yelled accusingly.

Leon winced and gave Bob a look since he had just confessed to eavesdropping on a network to a federal agent. However, "Dude, shut up!" was all that came out.

"Bob, I don't know what you are talking about. We weren't there."

"We have proof you were dropping files on a private company's network!" Bob took a breath and decided to play his only card. "I'll give all that up if you will just let my dad go! He had nothing to do with it and didn't know where I was!"

There was a pause while Mark and Chris exchanged confused looks.

"Bob, let's go somewhere to finish this conversation in private. I think you don't understand—"

Mark stopped talking as a car pulled behind Bob and Leon's position. It was coming up from the lower level and passed in front of the stairwell entrance. Leon caught the motion and turned. Chris saw the car, and then saw the taller of the two kids move rather quickly.

In the same moment, Andrei pulled behind Bob and Leon. He smoothly raised his gun up from the passenger's seat, where it was laying with his hand on the grip.

Leon felt the first shot more than he heard it. The sound of a gunshot inside the parking garage reverberated and then a ringing sound began to grow inside his head.

Before he could decide if he was hit, he saw Bob go down. The bullet hit Bob directly in the middle of his backpack. The impact slammed him forward and his face caught the passenger's side mirror on a Chevy Tahoe as he fell. For a half-count, Leon saw Bob hit the ground and saw the back of his backpack stained a dark color, looking like it was wet. Leon yelled for his friend and ducked low at the side of the SUV and tried to get to Bob.

From there, the experiences of the two friends diverged. For Leon, he was suddenly amazed to find Bob struggling to get back up and begin barking orders at him. For Bob, the gunshot impact, the face-plant into the SUV, and Leon's shouting blurred into a surreal world of soldiers and gunfire.

"What are you looking at?!" Bob barked with a voice of authority. Before Leon could process the fact that his friend was standing, more orders followed.

"Cover my left while I find where they're coming from!" Bob crouched down, opened the Velcro cover on the case attached to his belt and pulled out his PDA. Leon saw Bob's WiFiFoFum wireless scanner. But it was clear that Bob saw something different.

By now, Andrei had continued in the car up the ramp to the next level. As soon as his first shot hit, he tried two more that Leon never heard. Both shots missed. They traveled passed Bob and Leon towards Mark and Chris. From Chris's position, the fire appeared to come from the kids. Mark was down behind the engine block of their car while Chris stayed up just high enough to return fire. She did little more than inflict even more damage on the Tahoe protecting Bob and Leon.

"What are you doing!?" Mark yelled at Chris.

"One of your geeks is shooting at us!"

"That's not them—do you think they know anything about—" Mark stopped talking as he followed the motion of Andrei's car around the curve to the next level. Andrei had kept his gun pointed out the driver's side window as he pulled away from Bob and Leon. As he saw Chris duck first, he fired again. Andrei needed to keep them pinned down as he drove by. Mark wasn't as quick to react. He had his weapon out by this time, but he hadn't fired. The moment of decision had already passed and he had not acted. Chris was already moving. As she went down behind the car, she reached with her left hand and grabbed Mark's jacket. Her momentum pulled Mark down in just enough time for Andrei's shots to miss.

"I've been here for less than a week and you already owe me!" Chris yelled as she turned to follow the motion of Andrei's car up the ramp. There was no angle for a shot.

"We've got two in the area, but we should make it to the LZ. Cover the left and stay low!" Bob was just starting to get his feet under him when Leon grabbed his backpack. Bob jerked back with the sudden hindrance and spun at Leon.

"Dude, you follow an order when—" Leon's open hand met Bob's left cheek with a smart pop.

"Bob! Shut up!"

Bob's eyes went glassy for a moment as if the landscape around him was changing.

"This isn't a game, it's a parking garage and you just got shot!"

Bob's voice was shaky this time. "I—I'm okay."

"We've got to get to the car and stop the bleeding!" Leon barked.

"Stop the what?"

"Just stay low!" Leon grabbed Bob and began to drag him toward the stairwell.

Mark stood and looked up the ramp in the direction Andrei had gone. Chris lowered her weapon and turned her attention from Mark to Bob and Leon. She looked just in time to see Leon nearly toss Bob into the open stairwell door and follow him in. They ran two levels down and came out at the ground floor. Bob stumbled more than ran as the adrenalin was wearing off, and he found he had less control over his arms and legs. They made it across a corner of the garage over a sidewalk and into the stairwell of the adjacent garage. Bob was convinced the stairs were steeper here. He was getting weaker and had to force his body up to the third level behind Leon's lead. By the time they reached the car, the outline of a Chevy Tahoe mirror was obvious on Bob's face.

By now, Andrei was strolling through the mall. He had already jumped out of the car with it still in gear. The car had continued into a grey Mazda Miata, leaving a knot of metal and the wail of a car alarm. Andrei had left the chaos and walked calmly through the door to the stairwell. He paused at the sound of footsteps. He hadn't realized he was nearly close enough for another shot at Bob and Leon, who were dashing down to the first level. As the sound faded, Andrei had moved steadily down, but at the second landing turned instead for the mall entrance. He was clear before Bob, Leon, Mark, and Chris had a chance to conclude who had been doing the shooting. As far as Andrei knew, he had taken out one of his two targets. That should be enough for now. It wasn't worth the risk of staying around to finish the work. There would be another chance.

"What happened?" Hannah asked when they opened the two passenger doors on the old Ford Taurus. Hannah couldn't understand the answer because Bob and Leon were both yelling. She heard a "Go!" in the torrent of words and hit the accelerator as they both pulled the doors closed.

"No! Not here! Take the other exit!" Bob yelled and Hannah gave the wheel a quick right flick and all of them crumpled to the left with the force of the turn. Hannah was on the accelerator again and the engine responded as best as it could. On the turn, there was just enough force to break the tires loose from the concrete parking garage surface. They squealed and fishtailed before Hannah hit the breaks hard for the next right. Bob hit the back of the seat in front of him and groaned in pain while Leon was greeted with the dash since neither had a chance to put on a seat belt. Another lunge to the left as the car squealed right and then there was daylight.

"Slow down!" Bob ordered as he pulled himself upright. Still trying to process what happened to him "We need to blend in. Just get on the highway!"

Leon turned in his seat to look at Bob. "Why are you alive? I saw you get hit!"

Leon hung over the seat and reached for Bob's backpack. "Just lay down while I see the damage."

Bob complied as best he could while Hannah began to drive slowly and submerged into the Houston traffic. Leon managed to get the backpack off and raised Bob's shirt to find the beginning of a massive bruise—and nothing else.

Leon started to laugh. With a mix of shock and relief he said, "Dude, you're gonna have the biggest bruise I've ever seen!"

"What?" Bob managed as he started to sit back up. He reached for his backpack and some quick rummaging was followed by "Damn it! They killed the Beast!" Bob started to pull his Toughbook from his backpack, but only got it part way out before he exclaimed. "Ow!"

"What?" Leon watched as the Toughbook landed on the seat beside Bob.

They both watched as the laptop hissed and smoked. Bob wiped his now wet and stinging hand on his pants.

"I think it hit the battery. That was a lot of heat." He bent his arm around and felt his back. "And I think he popped my Pepsi bottle too. Bob looked in his backpack. "Yeah, I think some of the other stuff in my bag must have slowed it down enough so it didn't go all the way through. I'm glad I didn't bring Beauty on this one."

◖◖◖

George's body was beginning to stiffen and ache from the hours spent tied in the same position. He shifted as much as he could to vary the pressure on his back against the unpadded chair. It had been a while since he had heard any voices in the house. He wasn't sure who was left there to guard him. Then it hit him—maybe it had been too quiet. Was anyone actually left? He had to test before he started making some real noise for help.

"Hey, can I get some water?" …Nothing.

"Come on, it's been hours. Just a drink!" he exclaimed a little louder with more defiance.

The pause was long enough for George to think there was no one left. He took a breath and hopped his chair as far in the direction of the window that the chain would allow. On his second try to stretch a little further, he heard a chair leg scrape on the floor in the other room. It was followed by footsteps, then the sound of water from the tap. George was motionless and held his breath. He still had company. Now to see who it was.

Pavel opened the door carrying a plastic cup with water.

"I suggest you don't ask for things when the boss gets back," Pavel said as he brought the cup to George's mouth. George took a long drink, leaving about half the water down the front of his shirt.

"Thanks for the drink, and thanks for the advice. He didn't seem like a very helpful type."

Pavel managed a slight smirk as he turned and began to leave the room.

"You seem like a smart, young man." *Will be talk?* George asked himself.

Pavel paused and turned to look at George but said nothing.

"So why don't you tell me about your retirement plan?" George had already concluded that Pavel was the best of the group to target for making a personal connection. If he could find a way to get the young man to relate to him, then George would have a better chance of surviving this ordeal.

"My skills are my retirement plan," Pavel responded with false bravado pointing at his laptop that could be seen on the table through the open door.

"Those skills will serve you well as long as you get a chance to live long enough," George countered.

"I don't have any reason to think I won't," Pavel answered. He didn't seem as confident as his answer.

"You are putting a lot of faith in the good will of you partner."

"He's not my partner—I just work for him."

"So how long do you think you will work for him?" *Set the hook*.

"I haven't thought about it much," Pavel answered as he shifted in his chair and looked directly at George for the first time in this conversation.

"I used to not think about retirement," George leaned forward slightly as he answered. "The problem is, life seems to go faster the older you get. You will be surprised how it sneaks up on you. And you will look around and realize a lot of little decisions you made without thinking have woven themselves into a rope you can't break."

"What do you mean?" Pavel asked.

Don't jerk too hard on the line… "It makes sense to work for someone like your boss right now. You're smart, I assume the pay is good, and I bet you get lots of time off."

"It's been worth it so far," Pavel confessed.

"But I bet he doesn't like his secrets to be out of his control," George responded.

"I've proven myself to him." Pavel countered a lot less confident.

Almost there… "So you know things he probably wouldn't trust to be shared?" George asked.

"I guess so." Pavel slowly responded as he saw where this conversation was going.

"So what happens if you decide to do something a little less risky?"

Pavel paused, and then took a breath to respond. The sound of a car door outside ended the moment. He didn't say another word but turned quickly and walked out of the room, quietly closing the door.

Damn. A few more minutes and I might have had a chance, George thought.

Pavel returned to his chair in the kitchen in front of his laptop. He slouched slightly and rested his chin on one hand and began randomly surfing on some hacking sites. He didn't want Vlad to walk into the house and find him talking to their "guest." Pavel tried to look relaxed. After only a few minutes of feinted interest in browsing, he realized that the car door wasn't Vlad.

It must have been someone next door, he thought to himself after he began to relax again. Pavel sat and stared blankly at the wall. He processed the conversation he had just had with George. He thought about what he had done at 3DNF, about Stepan's laptop that Vlad had given him… "The laptop," he said aloud as he nearly jumped from his chair. Pavel went into the front room where he had left his backpack. He dug around the big main compartment and pulled out the Lenovo ThinkPad. Pavel had hardly touched the laptop since Vlad had given it to him. That one time in the hotel, he had almost gone through the drive to see what other information about

his current job was still there. This time he would go through with the forensics. He was determined to see what Vlad wasn't telling him about their work.

Pavel fished through a couple of pockets in his backpack and came out with a handful of CD cases. He shuffled through the pile and settled on a disk that had the words "BackTrack 4" handwritten on it (⋆p. 272).

"Let's see what Vlad left behind on this laptop," Pavel mumbled as he waited for the box to boot. He was soon greeted with a Windows login screen. He hit the "Enter" key since the last time he had worked on the laptop, he had reset the administrator account to have a blank password. He was logged in.

"Wait, this is different," he observed. Vlad had apparently reinstalled Windows on top of the image Stepan had used. Pavel saw that Stepan's custom wallpaper was gone and had been replaced with the default Windows "grassy hill" screen. He browsed the Programs menu and found that everything was default.

"Okay, so I have to work for this," he observed as he slid the BT4 disk into the laptop and hit the power button. Soon Pavel was in a zone of file fragments and remnants of e-mails. His mind was trying to process the global reach of what he was working on. This was bigger than anything Vlad had ever given him before. This information cost Stepan his life. Would Pavel have to pay a price too? What would it be?

After an hour, he heard the car door, but it took a couple beats before he realized that sound was most likely Vlad. He didn't have time to shut everything down properly. He just hit the power button on the ThinkPad and shoved it into his backpack along with his pile of CDs and a portable USB hard drive he had been using for file images. He just managed to turn back to his other laptop and pull up the SANS Internet Storm Center page before he heard the front door open (⋆p. 239).

"Has it been quiet?" Vlad asked.

"Yeah. Just doing some surfing," Pavel offered as he sat up straighter and stretched.

"Good. Andrei and Haki should be back soon. Andrei can handle all manner of situations, but he will need Haki to survive this Houston traffic and not create an incident for us."

Vlad poured himself a cup of coffee and sat down opposite Pavel.

"Since we have some quiet, we need to talk about what you will be doing at our next visit to 3DNF."

CHAPTER

E1GHT

BATTLE PLANS

Wednesday, 11:37 a.m.

Bob, Leon, and Hannah walked into the front of the bookstore. Leon turned to go to the coffee area but Bob snagged his sleeve.

"Perimeter," was all he said and turned to his left. Leon understood and this time with no eye roll, dutifully changed his path to go past the coffee and toward the back of the store. Hannah lingered at the "Newly Published" table and watched the entrance while Bob and Leon finished their sweep. As they made their way back, Hannah drifted toward the barista and ordered an espresso.

"That will be $2.76."

"Thank you," Hannah said as she gathered the drink. "He will pay for it," she answered and gave a nod and a wink to Leon. Hannah walked to a table and took the chair with her back to the wall.

"What can I get you?" the barista asked Bob. Bob was off his game again as he watched Hannah take his chair.

"Uh…just a bottle of water," Bob mumbled and walked off without claiming his drink.

"Coffee." Leon was still smiling from the wink he just received as he pulled out the money to pay and gathered his cup and Bob's bottle of water. Leon arrived at the table to find Bob shifting his chair back against the wall, leaving Leon to put his faith in his friends.

"You know if the Feds are really after you, you shouldn't sit there with your face on that camera," Hannah nodded to the security camera dome in the ceiling. Bob started to look in the direction of her glance, then thought better and pivoted his chair to face Hannah.

"So who do we trust now?" Hannah asked. Her voice was less confident now.

"No one," Bob responded with a dismissive wave of his hand. He leaned back and held his hands to his head. He looked like he was trying to keep something from leaking from his ears.

"We can't fix this ourselves," Leon stated. "We never got to finish talking to the FB—er, Jeb," Leon corrected as he leaned forward and lowered his voice.

"Of course not—we were getting SHOT," Bob countered with the loudest whisper he dared.

"We don't know who was shooting," Leon answered. "If we have to trust someone, I say we pick someone we know has to follow the rules."

"Rules," Bob scoffed. "Since when does the government follow rules?"

Leon looked straight at Bob. "I'm not saying Jeb is a Senator—he's an agent. I'd trust an agent over whoever it was in that van Saturday night—or the shooter today!"

Bob turned to Hannah, trying to find an ally. "Max, you've got to see we are in this alone."

"I'm not sure I'm quite as much a 'we' as you want. I think Leon has a point."

Bob was cut. He leaned forward and was more careful to keep his voice down. "Look, let's assume we need to trust the Feds. Even if we go to them now, we don't have enough to buy our freedom. All we have is the partial code we captured, a wild story about a car chase, and my missing dad." He paused, but there were no protests from his companions as they processed the observation. "We need the rest of the code that the guys in the van were pushing into 3DNF. And we don't have much time. For all we know, they could have already gone back and finished the job!"

Leon was starting to agree, but he wasn't ready to give in. "So now what, we camp out at 3DNF?"

"Yes! But we need some help," Bob answered.

"So now you want to trust someone else? That doesn't make sense," Hannah observed.

Bob looked at Leon but answered Hannah's question. "The 2600 LAN party crew. If I would trust them on my home network, then I trust them to help us. And besides, they don't need to know what they are helping us do. We just need their labor and some of their gear."

Hannah looked at her watch and then changed the subject. "I've been off the grid too long. I need to make a few calls before people start to look for me." She looked at Bob. "Don't worry, I won't tell anyone what I'm really doing." She got up from the table and took her drink to another table next to theirs and pulled out her cell phone.

Leon watched as Bob reached into his backpack and pulled out "Beauty"—his small EeePC—and fished out a power cord. "So how do we get the help?"

"That's what I'm doing now." I'm going to check a few things, and then I'm going to send some DMs on Twitter. I don't want to do a tweet in case the Feds—or whoever is chasing us—is listening (⋆p. 287).

Leon sat in relative peace for a few minutes. He shifted his attention from sweeps of the bookstore to futile attempts to eavesdrop on Hannah's quiet phone conversations. "Who is she talking to?" he thought. He finally spoke to Bob. "So who do you think will help?"

"I thought I'd start with 0hm and M00d1mus. They've been working on a Yagi rifle that we can use for a distant wireless hookup" (⋆p. 306).

"Did they finally get that working? The last time I heard it was still giving them problems."

Bob didn't look up from his typing. "Yeah, it's working. At least that's what 0hm bragged about last week."

"Anyone else?" Leon asked.

"Yeah. R10t and Rudy have been doing some cool stuff with Bluetooth we might be able to use. I figure we can do a meet up at Dobbs's place".

"But the Feds know about Rudy and Dobbs. They've even been to Dobbs's shop." This time Leon thought he was the cautious one.

"That's the point. They've already been there. We will only be there for a few hours and the Feds will be looking for the next place to check, not where they've already been." Bob leaned in a little closer to Leon. With a nod of his head toward Hannah, he said in part command and part plea, "Make sure she doesn't say anything to Rudy about his car."

◖◗◖◗◖◗

Vlad and Pavel were again sitting at the small kitchen table. He took another sip of his coffee while Pavel continued to surf aimlessly. Then Pavel decided to use the moment to get a little more information.

"Where are the other two?" Pavel asked.

"Wetwork," was all Vlad offered with a quieter voice than usual.

Pavel's face tightened slightly. "So do we go back to that company tonight?"

"Yes. We need to get this finished. You need to be sure you know what your steps are when we get there. We are going to be quick and efficient. No wasted time at the location."

"All right. Is there anything besides the file I was dropping the last time?" Pavel asked.

"Yes. 3DNF is just a front door. We are creating a way further inside. The file I need you to drop is on a target another hop in on a government system.

"So what do I do?" Pavel asked.

"Do you still have the target IP I gave you?"

"Yes."

"Good, that will be what you target as soon as we arrive. Next, we need a more standard malware that we can drop on a couple of systems inside 3DNF."

"Won't this just set off alarms?" Pavel protested.

"I just want a couple, and they will be enough to make it look like they were sloppy with their surfing habits—which I'm sure they are. That way they won't be looking for external activity."

"All right. I've got a copy of the gh0stRAT," Pavel offered.

"Good—everyone loves to blame the Chinese. The Americans will spend their time looking in the wrong place," Vlad agreed (★p. 309). "It is usually easy to make them look for the wrong enemy."

◖◗◖◗◖◗

The back of Dobbs's computer shop looked like it once was a place of order. There was no window. A door led into the room from the shop, another led to a small bathroom, and a third to the alley in the back. The walls were lined with shelves filled with computers and related gear in various stages of repair. There were a few pegboards covered with so many different parts and cables that only Dobbs could make sense of the clutter. In the middle of the room was a large table. Lunch from that day and the day before had been shoved to the side and replaced with a pile of gear. The owners of the pile looked on in pride at their work—a pride only they would understand since it looked like a flea market display.

Dobbs, R10t, 0hm, and M00d1mus had just started going through their inventory when the front door chimed. Dobbs looked toward the front of the shop and saw Leon and Hannah walking in the door. Bob lingered outside a moment and then came in as well. As Bob walked in the shop, Dobbs got a good look at Bob's face. He immediately walked over to Bob.

"Dude, you get the license plate of the car that hit you?" Dobbs asked.

Bob didn't say a word. Leon smirked and said, "Actually it was an SUV."

Dobbs looked at Bob expecting more of a story, but Bob ignored him and scanned the shop before leading the way to the back.

"Where's Rudy?" Bob finally asked when he walked into the work area and saw the rest of the crew.

"I don't know, he called and said he had car problems and wouldn't make it," M00d1mus answered.

Bob and Leon just gave each other a quick glance but said nothing.

"So what are you guys up to?" Dobbs asked in the general direction of Leon while never taking his eyes off Hannah. Bob plopped his backpack on the table and started pulling out equipment of his own to add to the pile.

"We have a project that requires your skills," Bob cut in.

"Hi, I'm Dobbs," Dobbs extended his hand with a flourish to Hannah.

"Hi, I'm Max," she responded.

"You're cute for a Max."

"Careful—she could own you seven ways before you had a chance to patch," Leon said a little too defensively.

"Wait, are you Max St3ɛ1?" R10t asked.

"Yeah, that's me."

"Dude!" was all that 0hm could manage before Bob cut him off.

"We need some help with surveillance. Is this Yagi rifle working?" Bob asked as he picked up a blend of Old West and Buck Rogers. The device was the stock from an old shotgun. The barrel had been replaced with a length of handle from an old broom. Mounted to the contraption was a mass of wires and what appeared to be a small antenna at the end of the "barrel".

"Yup, we've been playing with it for the last week. We can connect to a wireless network from a quarter mile just like we were inside," 0hm answered. "What do you need it for?"

"We need to connect to a network from about a quarter mile away," Bob answered with a half-grin.

"What network?" M00d1mus asked.

"You don't want to know," Leon jumped in. "We just need some help getting ready and we'll bring your gear back when we are done tomorrow."

"This thing is pretty touchy, I think you'll need some help."

"You don't want to go there," Hannah cut in. She started to say something else but Bob cut her off.

"R10t, did you bring the Bluetooth gear?"

"Sure. It's working fine," R10t responded as he turned the small EeePC toward Bob. R10t picked up a small dongle cabled to the laptop. "With this and the Bluesnarf software we configured, you can use this either to detect a Bluetooth device in the area, or to even jack in on some of the older models" (★p. 292).

"Very nice," Bob answered intrigued as he looked at the display. "Show me how it works."

Bob and R10t descended into a conversation about the laptop. Hannah started walking around the room, looking at the gear and quietly continuing to assess the talent at the table. Leon picked up the yagi rifle.

"So show me how this works," Leon said to M00d1mus.

Soon the room was filled with an even buzz of tech-speak and keyboarding. In half an hour, the two groups were done. Bob had mastered the yagi rifle and Leon had even managed to listen in on a phone conversation from outside the shop by an unsuspecting passerby.

Hannah used the lull in the discussions to point at a monitor that displayed four black-and-white video feeds of the store.

"Dobbs, what cameras do you use for this?" she asked.

Dobbs almost jumped in response to the question and attention from "Max."

"It's just cheap stuff," he said as he pointed to the camera mounted near the ceiling pointing at the back door. "I do have a cool set of wireless cameras that actually run on a 9 volt," he volunteered as he began rummaging around one of the shelves.

Bob put down the yagi rifle he had been holding and turned. "Dude, we need those! That's perfect," Bob looked at Leon. Hannah shook her head as she caught Leon's eye. Bob just kept going as he caught up with Hannah's idea. "We can use those to establish a perimeter! What's the range on these things?"

"A few hundred feet," Dobbs offered. Why do you need a perimeter?"

"Again, don't ask," Leon responded starting to tire of questions he couldn't answer.

Soon Bob was finishing packing the extra gear in his backpack. Leon picked up the yagi rifle.

"Dobbs, thanks for the help," Leon offered as the trio got ready to leave.

"No problem. Does this mean we get a head start in the Capture the Flag?"

Bob let out a weak laugh. "This means you might be running the Capture the Flag if you don't hear from us tomorrow."

Dobbs gave a laugh that was cut short when he realized that Leon and Max didn't see the humor. "Be careful," Dobbs then offered.

"As long as you guys did the hacks on this gear right, we'll be fine," Bob answered and turned for the door. Bob, Leon, and Hannah left the shop with Bob leading the way, scanning for faces or cars that they should avoid. The rest

of the crew made their way back into the public part of the shop and lingered around the counter.

"Max was cute, but she hardly said anything. Why do you think she was with them?" Dobbs asked.

"I've seen some of Max—uh, her work on Milw0rm.com," R10t volunteered. If she's the same one, I can see why Bob is putting up with her—she has skills" (*p. 184).

"Yeah, but she still looks too good to be hanging around with either one of them," 0hm observed.

DATA COLLECTION

Wednesday, 11:46 p.m.

"Don't go straight to the 3DNF parking lot," Bob directed from the back seat of Hannah's car. He hadn't even looked up as he was going through all the gear they had packed into duffle bags a few hours earlier at Dobbs's shop.

"Why not?" Hannah asked. "I think we can set up far enough away with the—"

"I have another idea," Bob cut her off. "Turn just before the convenience store. There is another office building on this side of the parking lot that I think is empty. I bet we can get inside and use it for cover."

Hannah complied and turned right off of the access road just before the small shop where Bob and Leon had sat just a couple of days before dropping a CyberBob icon for a game. She drove down the street and pulled to the front of an empty three-story office building. It was dark outside, so once she turned off the headlights, they were well obscured by shadows (*p. 383).

"At least whoever owns this building didn't pay the electricity bill," Leon observed. He pointed at the lights for this section of the parking lot—they were all turned off. Leon looked toward Bob in the back seat. "Hand me one of the bags."

"Not yet," Bob answered as he scanned the area. "We need to give it a few minutes to make sure there isn't any movement around here. Bob pulled out his wireless scanner and watched the screen while Leon and Hannah looked for any motion around them or signs of activity in the building.

"Okay," Bob said as he returned the PDA to the holster on his belt. "No cops around and no other obvious wireless activity. I think we walk the perimeter and see if we can find an open door or some landscaping place that gives us cover and line-of-site to 3DNF on the other side."

The three gathered up their gear and got out of the car quickly. If anyone were paying attention, they would have seen the brief, dim dome light in the car flash on as they piled out and then three muffled door closings as they all tried to be as stealthy as possible. Bob led the way to the corner of the building.

"Aren't you at least going to try the front door?" Hannah asked as they walked.

"No. That's the only one that would be locked," Bob answered as he approached the side of the building. "Besides, it's harder to pick the lock on a glass door. They are secured from the inside."

The surface of the building was grey stucco that gave a soft glow in the low ambient light of the area. Halfway down the side of the building was a metal door. Bob gave the door a try and was rewarded with an unlocked doorknob—but the door was held fast with a deadbolt lock. "Okay, I can work with this. Watch out for me."

Bob knelt on one knee and began to rummage through his backpack. "I've been playing with bumping locks and I'm getting pretty good at it" (★p. 403).

"I hope 'pretty good' means we can get inside before we're spotted," Hannah responded. Bob ignored the comment while he began to work on the deadbolt. "Leon, hold the doorknob for me while I do this." Leon held the doorknob turned all the way open while Bob squeezed in beside him to work on bumping the deadbolt lock. It was a little awkward, as Bob had to have both hands working on the lock at the same time Leon held the doorknob turned.

Hannah stood back and watched. After just over a minute of unsuccessful tries and a little grunting she asked, "Do you think the bad guys or whoever they are would think to use this building too?"

Leon took a deep breath and turned back to Hannah. Bob gave one more hit and pressure on the lock and it finally yielded. "Yeah, they might. That's why we better hurry up," Bob said as he slipped into the dark hallway. Leon turned back to get a duffle bag while Hannah followed Bob inside. Leon gave one last scan of the area and began to close the door. Just then Bob came back down the hallway and squeezed past Leon.

"What?" was all Leon could get out before Bob cut him off.

"Just hold the door. If we are going to be inside, then we need to monitor the perimeter. Bob knelt down and fished through his backpack. He pulled out one of the wireless cameras from Dobbs's shop and switched it on.

"Watch the area for me," Bob whispered as he ducked back outside. He stopped at some shrubs and found a sturdy branch to balance the camera on. He checked to make sure he had set it with a good line of site to the door and went back inside. Leon pulled the door, too, and all three of them made their way down the hallway.

Once they reached the middle of the building, they came to an open atrium with a large stairway trimmed in glass and chrome that circled around the space to the second and then the third floor. They quickly and quietly went straight to the third floor. From there, they selected an office at the back of the building with a clear view of the target corner of 3DNF.

"Let me have that other camera," Leon asked Bob. "I'll set it down a hall on the second floor looking back at the stairs. That will give us one more warning if someone comes this way."

Bob pulled out the other camera and handed it to Leon. Leon started to walk out of the office while he flipped the camera on. Nothing happened. Leon stopped in the hallway and played with the switch. Nothing. He pulled open the back cover and found the batteries were corroded. "This one's worthless," he said as he turned back toward Bob and Hannah.

"I've got another option," Bob offered. "That's why I brought R10t's laptop as well." He was setting his laptop on a credenza near the window. "Remember, he had Bluesnarf on here. If anyone comes by with a Bluetooth headset, we'll see them coming."

"Yeah, but how do we know they are going to use a Bluetooth headset?" Hannah asked with a hint of doubt in her voice.

Bob didn't look up from his laptop. He just responded, "Because I saw at least two of the guys in my webcam video had them when they were in my room."

Hannah made eye contact with Leon. Leon just shook his head with a look of admiration for his friend. "You sure you're not related to A.C. Doyle somehow? You catch way too many details."

Bob still didn't turn from his laptop screen. He just mumbled, "Elementary."

◖◗◖◗◖◗

"Do not waste any time," Vlad directed his order at Pavel. You know what your steps are, we just need to get them done quickly."

Pavel didn't protest at being told the obvious. Vlad was in "commander" mode and had been barking orders through most of the drive from the safe house back to 3DNF.

"Andrei—you and Haki keep in touch. I need a good perimeter and eyes on anything that happens inside it," Vlad continued.

Haki nodded his head and turned to Andrei. The four were all still sitting in the same van, parked in nearly the same place as their last "visit." Haki's only comment to Andrei was "Let's go" in Russian before he opened the driver's door and began to walk back to the cover of the few trees at the edge of the parking lot. Andrei followed. Once they reached the cover, Haki finally spoke.

"It's not safe in there until the kid gets the work done on the computer. Until then, our safest place is out here. You take this side of the parking lot and watch the access road. I'll walk toward the back and make sure any area that has line-of-sight to their position is secured. Don't use the radio. If you need to talk to me, use the cell. We don't want to bother Vlad unless we have to." Andrei agreed and without a word turned and walked away toward the convenience store again to make sure that area was clear. Haki stood for a moment and just watched the area for activity. He didn't see any movement. There were a few lights on in the 3DNF building. The same odd collection of vehicles as before was in the parking lot. Haki pulled out a cigarette and lit it. He took a drag, creating a single red glow for just a moment. He then decided to begin walking slowly in the general direction of the building now occupied solely by Bob, Leon, and Hannah.

Pavel was soon situated at the back of the van again. His laptop was on the makeshift table. He was sitting on the overturned bucket. Vlad had pulled the cable for the external Wi-Fi antenna so that the end hung over the seat in front of Pavel.

As Pavel prepared to connect to the 3DNF network, Vlad pulled his laptop out from a bag he had brought. Pavel stopped and watched as Vlad brought the machine out of "sleep" mode and began to tweak the wireless settings. Vlad noticed Pavel watching and turned in his seat.

"You aren't the only one with a technical task on this part of the project," Vlad noted wryly.

"Is there something I can help with?" Pavel offered.

"No. I want you to proceed," Vlad responded. "I will need to verify that I can connect into the network myself once you are finished. "We have to have confirmation we can provide to the buyers that this connection works. It does not make sense for you to be the only one with the ability to get in on this connection from the outside." Vlad turned back in his seat and focused on the laptop display.

Pavel sat still for a moment while his mind raced. *If Vlad can get into the network by himself, then what does he need me for? Stepan stopped being useful and look what happened to him*. Pavel glanced down at his open backpack and noticed the black outline of Stepan's Thinkpad. He quickly added up the conversation with George, the information he had pulled from Stepan's laptop, and Vlad's comment. Pavel realized it was time to look out for himself.

Pavel made his connection to the 3DNF network. He was more cautious this time. He started by opening Wireshark, so he could watch any traffic on the same network segment as his connection, including Vlad's. He watched the screen and saw nothing.

"I know you told me to be quick, but I'd like to watch the network for a few minutes and make sure we are alone," Pavel offered.

Vlad sighed and turned in his seat to look at Pavel again. He held Pavel's look for a moment and then decided he was right. "Very well. Five minutes." Vlad sat his laptop on the floor of the van and turned back in his seat after checking his watch to mark the time.

Pavel turned back to his laptop and the now-open copy of Wireshark. He was immediately greeted with traffic on the network. It was directed at an IP address next to his on the subnet. He didn't say anything but just watched.

"Tell me if you see anything," Vlad said still sitting with his back to Pavel.

"I will. It's quiet right now," Pavel responded nonchalantly as he stared at the screen.

The office was dark except for the slight glow from two laptops—one for Bob and one for Leon. Leon was seated in front of his laptop. Bob and Hannah stood over his shoulders while he worked. Bob had run the antenna cable from the laptop to the yagi rifle, which now rested next to his own laptop on an empty credenza near the window. The end of the yagi rifle was balanced atop a couple of abandoned phone books Bob had found piled on the floor just outside the office. Occasionally, Bob and Hannah would look away from Leon's screen to inspect the single image on Bob's laptop showing the grainy picture of the side door. There was also a window showing Bluetooth activity in the area. Both indicated they were alone.

"So whose computer is this?" Leon asked as the three of them stared at the screen where he had just pointed.

"I think it's worth the risk to check," Hannah tentatively replied.

"Be careful," was all Bob offered.

Leon loaded nmap and began a profile scan of the single IP address. It didn't take long for the application to identify the target host as an unpatched installation of Fedora Core.

"Look, they've got SNMP running on the box," Leon again pointed triumphantly at the screen. Before Leon could get the mouse over to the folder to get his next tool, Bob pronounced "Use Metasploit" (*p. 185).

"Just a sec," Leon sounded mildly annoyed as he pulled up the app and directed an exploit at the target. It took just a few seconds for the remote shell to launch. Soon Leon was typing away as he explored the directory structure of the system.

"Look at this!" Leon said loud enough for Hannah to shush him. Leon just kept going, however. "This is as good as the 'F0RB1DD3N' network name."

"What?" Bob asked leaning in closer to see the window Leon was pointing at on the display.

"This folder under the home directory—it's called 'Odysseus.'" That's got to be some interesting reading. Leon pointed his cursor over the folder but Bob stopped him.

"Dude, just grab the whole home directory. You can read it later."

"You're right," Leon agreed. It took only a couple of minutes to begin copying back the home directory from the Fedora computer, bring along the interesting folder full of Open Office documents and a contacts file.

◐◐◐

"Have you seen anything yet?" Vlad asked.

"No, I think we're alone," Pavel lied as he minimized his Wireshark window, ensuring Vlad wouldn't be able to see the log of traffic he had just captured that included someone pulling data off of Vlad's laptop.

"Then it is time to get started," Vlad responded as he reached to the floor of the van and picked up his laptop. Pavel understood he couldn't delay any more and began to work on his target host.

◐◐◐

"I think this is one of the Feds!" Bob said a little too loudly for Hannah's comfort. She immediately "shushed" him.

"What? No one else is here," Bob observed pointing at his laptop.

"It just doesn't feel right is all," Hannah observed.

"I don't think we can tell who it is yet," Leon offered as he started browsing through the files he had copied. "Besides, I didn't think a fresh install of Fedora Core or Open Office is a standard issue for a three-letter agency."

◐◐◐

Haki and Andrei had continued to walk their assigned sections of the perimeter. The area was relatively quiet. The parking lot of the convenience store had a little traffic. Haki walked past the store along the edge of the office parking lot.

There were no cars in this area. An occasional tree planted along the property line provided sufficient shadows to hide his presence to all but the sharpest eyes. Haki wasn't being particularly careful. His occasional drags on the cigarette created a red glow to contrast with the occasional blue light from his cell phone headset.

As he walked along the edge of the abandoned office occupied by Bob, Leon, and Hannah, he noticed a slight glow from one of the office windows and an occasional moving shadow. *That is not right*, he thought. He looked back toward the van with Vlad and Pavel. The window above had a perfect view of their position. He continued along the back edge of the building and paused at the corner. He checked behind him, and then glanced around the corner of the building. It was clear. He could see the same door the kids had used a little while earlier. A few quick steps and he was in front of the door. He tried the knob—it was not locked.

Bob and Hannah were still watching over Leon's shoulders as he looked through the files he had just finished copying from Vlad's laptop. The display on Bob's laptop clearly showed both a Bluetooth device in the area, and the figure of someone at the side door. Hannah looked up just in time to see the door close.

"What was that!?" She nearly squealed.

"What?" "Quiet." Bob and Leon spoke over each other.

"Someone just came in the back door!" Hannah was pointing at Bob's laptop as Bob covered the space to his laptop with one large jump. Bob pointed at the display and where the Bluetooth headset signal was clearly visible.

"We aren't alone!"

Leon moved first. He grabbed the yagi rifle and yanked out the antenna cable. Bob and Hannah both scanned the room trying to decide where to go next.

"On the floor behind the desk," Leon ordered. He took up a position just behind the door that was slightly ajar. "And shut the lid on the laptops—we don't want any light in here."

Bob complied and closed both laptops and carried them with him to the far side of the desk where Hannah was already crouching. They didn't quite fit in the space but did their best.

Everything was suddenly quiet. Each could hear little more than their own heart beating out a quick beat that filled their ears. Leon thought he heard something and waved at the other two to get lower. There was some wiggling of a shadow, but they didn't succeed in shrinking down any further. Leon brought his finger to his lips and they all tried not to breathe.

There it was again. A footstep on the hard floor near the stairs. Someone was definitely coming. Leon's hands tightened around the stock of the yagi rifle. Now he wished it were good for its original design and not the tech mod they had been using.

Haki started to go past the door. He was trying to guess which office matched to the one that had a glow when he was standing outside. *What was that?* he thought.

Did something move? Haki brought his pistol up as he walked into the room. Andrei wouldn't have approved. Haki had led his way into the room with the pistol. Leon saw the shape and was ready. Haki's attention was on the desk and he walked straight to it before he realized there was a shape slightly behind and to his right. Leon brought the yagi rifle down and put the end right in the middle of Haki's back.

"Drop it!" Leon shouted and shoved the end of the yagi rifle hard into Haki's back. The quick bite of pain, noise, and surprise wasn't enough. Haki took a breath and tried to decide his next move. Because it was dark outside, the office window reflected what little light was in the office. He could see the rough shape of Leon and what appeared to be a rifle pointing at him. He couldn't move fast enough, so he complied and dropped the pistol.

Bob saw his chance and came out from behind the desk with what was left of his favorite laptop—"the Beast." He caught Haki in the forehead with the Toughbook and dropped him with one hit. Hannah started to come out from behind the desk.

"What did you do with my dad!? Where is he? What do you want from us!? That's what you get for shooting my best laptop!" With the last line, Bob brandished his Toughbook in the air one more time and then dropped it on the unconscious Haki's forehead.

Bob kept ranting, but Leon ignored him. He bent down and pulled out Haki's wallet. He looked through it and found a typical Texas driver's license, a couple of credit cards, and a little cash. Leon was so focused on looking at the documents he didn't notice as Bob stopped talking and bent down. He started to pick up Haki's gun. He managed to stand only part way up before he accidently fired the weapon. The bullet went through the side of Haki's left leg. Haki groaned at the pain and moved slightly, but he didn't come around.

"What are you doing!?" Leon jumped to his feet, checking himself for holes. Bob dropped the gun and Hannah jumped back behind the desk as it landed, this time with only a metallic clatter.

Leon looked at the weapon but didn't want to touch it. "Get the gear together now! We can't stay here—someone probably noticed we just shot somebody!" Leon directed the last two words at Bob who turned and started shoving laptops in his backpack. He even retrieved what was left of his favorite "Beast" that had been lying beside Haki's head.

Leon looked back at the gun and put his foot on the top of it and gave it a well-aimed shove down the hall. He was rewarded with the clatter of the gun bouncing down the first flight of stairs in the atrium outside the office.

"Come on!" Leon said as he turned back to see Bob and Hannah already packed up and heading towards him. As quickly as they could, they ran out of the office, down the stairs, through the hallway, and out the side door. They quickly piled into Hannah's car and drove away.

◖◖◖

The sound had been muffled, but Andrei knew what it was. He scanned the parking lot and could see no disturbance. He didn't want to use the radio yet. He pulled out

his cell and dialed Haki's number. Nothing. Now he had to tell Vlad. He pulled out the radio. "I'm coming your way. I think I heard something and now Haki is not answering."

Vlad didn't respond to Andrei's message. Instead, he immediately shut the top on his laptop and turned to Pavel.

"You keep working. I'm going to see what is going on. Stay here until you are finished. If I don't come back, use the GPS to get back to the house. You have to finish. That path into 3DNF and the target IP I gave you has to be working."

"How are you getting back?" Pavel asked.

"I can take care of myself," Vlad answered as he finished shoving his laptop into his bag and clipping the radio to his belt. "The question is, can you?" Vlad challenged. "Send me an e-mail when you're finished before you leave here. I need to know when the work is done. If you don't hear from me, stay at the house for no more than a day. After that, you are on your own." With that, Vlad climbed out of the van. He scanned the area and saw Andrei walking quickly in his direction.

Pavel crawled up to the passenger seat and carefully looked out the side window. He could see Vlad and Andrei walking slowly away from the van toward the convenience store.

"So how much am I worth to him after he gets that e-mail from me?" Pavel asked himself aloud. He moved back to his laptop and the first thing he did was save a copy of the Wireshark traffic capture he had of someone hacking Vlad's laptop. "I have an idea who was doing this, but I might need a copy, too." Pavel then opened a remote shell session on a box he controlled on a server at a local Houston university. He and Vlad had decided any local command and control testing should originate locally so that the true source of the activity would be hidden while they were in the country. A little more typing and soon, Pavel was rewarded with another shell, this time over an SSL session. He typed a single word.

```
patefacio
```

Soon he was rewarded with a rush of data across his screen. The data flow was so fast that he checked his network connection properties and realized it had saturated his connection. "Damn," Pavel muttered to himself. He paused his display occasionally and traced his finger down the screen as he read. He saw documents, spreadsheets, audio files, video clips, query strings. It went on and on while he scanned, losing track of his surroundings. "It works, but Vlad doesn't need to know quite yet," Pavel observed.

"I wonder if this is a concentrator of U.S. agency data. This must be what Vlad is going to sell access to. No wonder he wants to make sure he can get in by himself."

Pavel realized he wasn't tracking time. He looked around and made sure he was still alone. A quick look out the front and side windows confirmed no movement around him. He went back to his laptop and shut down all of his connections. If Vlad wasn't back by now, it was better to return to the safe house as ordered. Vlad and Andrei could take care of themselves. Pavel slid into the driver's seat and searched through the GPS. The safe house coordinates were there. He would take his time to make sure he didn't draw any attention.

This page intentionally left blank

CHAPTER

N1N3

DATA ANALYSIS

Thursday, 1:45 a.m.

Bob, Leon, and Hannah were gathered around the small desk in their hotel room. Leon was seated in front of his laptop, looking over the files they had pulled from the Fedora Core computer. The room was mostly quiet except for exclamations of disbelief when they finally came to the document containing Vlad's instructions. The file had traveled through three countries and four computers. It began as an opportunity for Stepan to improve his position in his company. Then it was an opportunity for his employer to add to their profits. Then, for Vlad, it was another job. Now for Bob, Leon, and Hannah they had a way to finally tell good guy from bad. They had their way to stop running.

"This is scary!" Hannah exclaimed as they all took some time to sit back and consider what they had just finished reading. "This means that these 'bad guys'—whoever they really are—have a way to spy on us without anyone knowing about it. They get to just sit back and let data pour into their collector."

"So what do they do with this information?" Leon asked.

"Any damn thing they want to!" Bob answered as he stood up. "It's bad enough our government is sucking up all of this information. For all we know data about us is in this 'Concentrator' thing. But I'd rather the 'bad guys' be the ones we know in our own country—not the ones we don't know in another." Bob was pacing around the room now. "If this kind of data is the target, then the rules are totally different. This would mean—DAD!"

Leon and Hannah didn't say anything. Leon had already reached the conclusion that Bob had tumbled to. "We'll figure something out," Leon offered.

"If this is what is at stake, then my dad is DEAD!" There were veins tracing their path along Bob's temples now.

"He's got to be okay for now," Leon answered as he stood and put both hands on Bob's shoulders trying to comfort and calm him down. "They must have grabbed your dad to find us. That means as long as we are still on the run, then they need him. They think your dad knows how to find us. When that van chased us, they didn't know what we knew—or didn't know at the time. We have to figure out what to do before they decide he can't help them."

Bob sat back down and put his head in his hands. He just worked at breathing.

"Bob, we can hack this," Hannah suggested. Both Bob and Leon looked over at Hannah. "Well, come on. You guys can social people, you can break systems. This is just a system and people. Bob, you've got Max to help, remember?" Bob managed a small grin. It was enough to pull him back to the puzzle they had to solve.

SHRINKING TEAM

Thursday, 8:03 a.m.

George's body was stiff and he ached everywhere. He had just enough slack in the chain that looped over the handcuffs and attached to the floor to almost stand. He was able to get out of the chair and lie on the floor just to put his body in a different position. But his hands were still behind his back, so no matter how he turned, eventually he would cut off the blood flow to one arm or the other and awake to prickling numbness.

Something was going on again. He had heard people returning the night before. He couldn't tell how many were in the house this time. With the daylight he saw only the young one he had spoken with earlier. Pavel had uncuffed George long enough for a visit to the bathroom, given him a few bites of a sandwich, and then returned him to his chair and chain. This time Pavel didn't speak at all. George concluded it wasn't safe to try since they were not alone in the house. George had tried to look around, but the voices he could hear came from a room he couldn't see.

Now George was alone again. He sat trying to move his legs and arms as best he could to relieve the pain. *How much longer is this going to last? Is Bob okay? What has he gotten himself into?* They were the same questions that tormented him in the dark hours when he couldn't sleep. There still were no answers.

Pavel was sitting at the kitchen table again when Vlad and Andrei walked into the room. Pavel looked up and watched them both while they took a seat. He hadn't heard what they had been discussing while he was taking care of their "guest."

"We have to assume this place is compromised," Vlad announced.

"So where is Haki?" Pavel asked. Their local contact had never returned from the trip to 3DNF. Pavel had come back in the van.

"I do not know," Vlad said curtly. "If he has decided to care for himself, then we can no longer trust any arrangements he made for us."

"Why did you let him go?" Pavel challenged Andrei in Russian. It was the first time Pavel had spoken directly to Andrei during the whole trip.

Andrei didn't respond with words. Instead, he was out of his chair so quickly that it flew back from where he had sat. Andrei reached across the table toward Pavel but Vlad caught his hand.

"Not now. Besides, he has a point." Vlad caught Andrei's gaze and held it for a moment. Andrei thought better of any more action if his boss was going to step in. But he couldn't let the little one be disrespectful.

"I told you, we split up to cover area. He disappeared and all I heard was a gun shot," Andrei protested.

"You think you heard," Pavel responded with a snort. He snapped back, even though he knew he would be dead if Vlad wasn't there.

"Enough!" Vlad ended it. "Pavel, I did not receive an e-mail from you last night. Since you are sitting here, I assume that you were successful with your assignment?"

"Yes. Of course." Pavel's voice had just the hint of a defiant attitude. Vlad assumed it was emotion left from the outburst Pavel had directed at Andrei. Since the conversation had changed to English, Andrei understood he wasn't needed. He walked over to the counter and got some coffee. He stood leaning against the kitchen counter testing himself to see how much of the conversation he could follow.

"Why did you not tell me when you confirmed it was working?" Vlad said in a relaxed tone that instantly put Pavel on his guard.

"I was worried about the attention we had drawn and wanted to get out of there as quickly as I could," Pavel lied.

Vlad appeared to accept the explanation. He leaned back in his chair. "You need to go pack up," he told Pavel. "I don't know where we will be going yet, but we will not stay here long."

"So where did the extra cars come from?" Pavel asked with a head nod toward the front of the house.

Vlad turned and looked at Andrei as he responded. "Andrei had to steal one to get back. You will be getting rid of that shortly." Andrei nodded an acknowledgement.

"The other is legitimate. I had a spare I had bought on my own in case I needed to make other travel arrangements."

Pavel looked at Vlad, wondering if he would have a part in those travel arrangements or not.

TENUOUS CONNECTIONS

Thursday, 8:20 a.m.

Bob's eyes were open, but it took a while for his brain to begin processing the large dark shape before them. *Where am I? What day is it? What is*—Bob remembered falling into bed sometime in the early hours of the morning. Hannah took the other bed in the hotel room, so Bob decided it was better to use just the edge of the bed where Leon was already snoring away. But now he awoke to find himself rolled over with his face next to Leon's back. Bob's brain engaged and he was instantly out of bed and making his way to his laptop that was sitting on the hotel desk.

The sudden movement woke Leon who rolled over and struggled to sit up. The water was running in the bathroom—Hannah was already up. Leon looked at his watch and pulled himself to the edge of the bed. After a few stretches he was ready to start the day…once the bathroom wasn't occupied.

"This could take a while," Leon mumbled and pointed at the bathroom. "Is it time yet?" he asked.

Bob didn't even turn from his laptop. "No. We have some time. I think Max woke me up when she got up."

Leon stared at the back of Bob's chair for a moment before he realized he had nothing to say. He made his way to the bathroom, paused, and then raised his hand to knock on the door. Instead of knocking, Leon swung lightly at air as Hannah opened the door and a small cloud of steam billowed toward him. She was obviously wide-awake and ready for the day. Her bright eyes, mischievous smile, and still-wet hair made her look like she had slept much longer than she actually had.

"Good morning," Hannah offered as she slipped past Leon.

Leon managed little better than a muffled sound that approximated "Eh uh huh." He began to process how vibrant she looked and what a mess he must be at that moment.

"You look terrible," Hannah grinned as she played off Leon's fogged facial expression. "Perhaps you need to keep better company at night."

Leon's jaw dropped slightly and his eyes opened just a little wider. "Uh, yeah."

"A girl could get jealous with the way you two cuddled up last night."

With that Leon retreated to the bathroom and shut the door before he had to look at Hannah—or let Hannah look at him—any more. "Idiot!" Leon mumbled to himself.

"What was that?" Hannah asked through the door.

Leon spun around to face the now-closed door. "Nothing!" Leon turned to look in the mirror. "So when did she get so hot?" he whispered to himself in the mirror. He looked at the door, but there was no voice from the other side this time.

Hannah went over to her bag and pulled out her laptop. She quietly sat back on the bed and started surfing and checking e-mail. She and Bob each went about their own digital business. The room was relatively quiet with only occasional clicking, typing, and the sound of Leon trying to get cleaned up in the bathroom. After 10 minutes of awkward silence, Bob and Hannah were relieved when Leon reappeared, looking marginally more awake.

◖◖◖

Agent Jackson arrived at his desk to find his partner already there. "Sorry I'm a little behind this morning. Are you ready to go?"

"Of course," Agent Battle responded. She opened her drawer and pulled out her sidearm. "How are we going to do this?"

"I think it will go better if they don't know we're coming." Mark picked up a small notebook from his desk and made sure he had his pen. "Okay, let's go."

◖◖◖

Jonathan picked up the phone on the second ring, giving him time to put down the half-empty bottle of Mountain Dew.

"Hello?" Jonathan managed after swallowing his last gulp of breakfast.

"Hi Jonathan—this is Susan. Do you know where Michael is?"

"He's here somewhere. He's probably just getting coffee. What's up?"

"He has a couple of visitors up here—the same two agents who stopped by on Monday." Susan dropped her voice for the second part of her statement and turned away from Mark and Chris who were standing near her desk.

"Really? Okay, I'll see if I can find him and come up front. Thanks." Jonathan got up and took two steps before turning around and going back to his desk to leave the drink behind. He stopped at the break room first. He was right.

"Hey Michael—we have company again."

"Who?" Michael asked as he turned around from the coffee machine.

"The two FBI agents who stopped by on Monday. Susan just called me and said they were up front."

"Did you call them?" Michael asked.

"No. I was going to ask if you did. I haven't heard anything from them since they called on Wednesday with those follow-up questions. You gave them everything they asked for, right?"

"Of course," Michael offered almost offended, sloshing some of his coffee as he motioned with the same hand holding his cup.

"How about you clean that up and I'll go get them," Jonathan offered, looking disapprovingly at the mess on the floor. "I'll just bring them back to our area."

Michael tossed out his coffee in the sink and made a weak attempt at wiping up what he had dumped on the floor. Jonathan disappeared down the hall toward the front door.

"What can I do for you today?" Jonathan asked when he met up with Mark and Chris. "Did you find out anything from the logs we gave you?"

"Not yet." Mark answered. "But we do have a few more questions. "Is Michael here today, too?"

"Sure. Is he in trouble?" Jonathan asked, wondering why the Network guy was getting so much interest and not him.

"No, it's not that," Mark assured him. "We just want to make sure we keep everyone on this up to speed."

"No problem. He's probably on his way back to his desk now. I just saw him in the break room. Come on back."

Michael was already at his desk when Jonathan and the visitors arrived. Michael had just finished a spell of controlled breathing trying to calm down.

"Hi Michael, how are you doing today?" Mark asked as he offered his hand. Michael stood quickly.

"Great. What can we do for you?"

"We wanted to check on that wireless sweep you were going to do yesterday. Did you find anything?"

"Oh sure. No. Uh, no we didn't find anything. We walked all through the building and outside like you suggested and never found anything new. There's one wireless signal from the company next door, but they've got the connection secured—I could see the little padlock on my laptop."

"Interesting," Mark offered sounding almost disinterested. "Based on the IP address information you gave us, that would have been a logical source. We could try—" RING—RING "…I'm sorry, excuse me for a moment." Mark pulled his cell phone off of his belt and turned slightly away from the other three to take the call.

"This is Mark…Yes, we are…Okay, just a sec." Mark wedged his cell phone between his chin and shoulder and pulled his notebook and pen out of his jacket pocket. "What kind of proof?…Okay, really? You'll have to prove that…, okay, I believe you, what was the name you saw on that?…Brad?…Oh, I'm sorry, Vlad. V-L-A-D right?… Listen, this is good info, but I need to see the evidence.…We need to meet…Yes, yes we will help you find your dad. Here, I've got an idea, let's meet at the Arboretum at…" Mark checked his watch. "…5:00 p.m.…Yeah, I know about the traffic, that's the point. It'll be safer for you. Mark gave Chris a questioning look, and she nodded. Jonathan and Michael just watched, trying to figure out what the conversation was about. "Okay, good…The open area near the middle…Yeah it's been a while but I know where it is, sure…No, it will just be me and Agent Battle. I promise after last time we will make sure we are alone." Mark chuckled and looked over at Chris. "Yeah, that one. See ya' then."

"Who was that?" Michael asked as Mark pocketed his notebook and holstered his phone.

"Just someone we need to speak with." Mark knew he hadn't given enough information to satisfy Michael.

"Was that about our case?" Michael tried one more time.

"3DNF isn't really a case at this point," Chris suggested, giving a non-answer. She watched Michael—he didn't like the answer, but didn't have the nerve to follow it up.

"Well, we're done here," Mark noted affably. "We just wanted to see if the wireless angle worked out." He took a step away from Michael's cube. "We don't want to be a bother. You both know how to reach me or Agent Battle if you see any more strange traffic, right?"

"Sure," Jonathan offered. "Are you sure you don't want anything else?"

Chris noticed the quick, sideways glance Michael gave Jonathan at that question.

"No, I think we're good for now. Your defenses look good. You have some issues with temps—I think you just had someone looking around who shouldn't have. They'll probably stop with word getting out that we came by. Chris, anything else?"

"No. We're good," Chris offered dismissively as she started to walk away.

"Here, let me walk you guys out," Jonathan offered.

As soon as Jonathan and the agents were down the hall, Michael nearly dove for his phone. He picked up the handset and put it to his ear before he realized he didn't know the number. He wedged the handset between his ear and shoulder and started fishing through his pockets. He made a mess dumping empty candy wrappers, keys, change, and an ATM receipt on his desk before he found the number. He tapped it in and waited for the answer.

"Pizza Hut, may I help you?"

"Sorry, wrong number," Michael responded and nearly tossed the handset across his desk, missing the base when he tried to hang it up. He got the phone back in its right place and laid his head on his desk.

"Are you okay?" Jonathan asked as he returned from the front of the office. Michael sat up abruptly.

"Yeah, I think so. I'm gonn—" Michael's cell phone rang. Michael stood up quickly and swept the contents of his pockets that he had spread onto his desk back into his hand and shoved them back in his pocket. He raised a hand to waive at Jonathan as he started walking away and answered his phone.

"Hello?"

"Why did you call?" Vlad asked.

"We need to talk. I can't—well, not right now. Can you call me back in a sec?"

"No. Just walk out of your office, I'll wait."

"Okay," Michael answered as he made his way past Susan and then out the front door. "Okay. The FBI was just here."

"What did they want?"

"They said they wanted to know if the wireless checks we did found anything."

"What did you tell them?" Vlad asked.

"Exactly what you told me to. But that's not the point. While they were here, one of them got a phone call. I could hear half of the conversation and he said something about a person named 'Vlad' and a meeting today."

"Did they say who Vlad is?" Vlad asked, trying to remember if he had ever let Michael know his real name.

"They didn't say. But they did say something about a meeting today at 5:00 p.m. at the Arboretum."

"And why do you think you need to tell me all of this?" Vlad asked, trying to see just what Michael knew.

"I just think they were on to something. I asked if the call was about 3DNF, but they wouldn't say. I think they know something about what's going on." Michael's words were spewing out so fast his cell phone needed a good wipe down.

"Relax," Vlad instructed. "You have done better work than you realize. The access point was successful. I think we need to meet so I can pay you the rest of the money. In fact, I'll have a bonus for you. If you want, I can put you in touch with someone that can help you with travel documents if you feel like taking a trip for a while until things calm down." Vlad finished in a relaxed tone.

"Wow, that's great," Michael responded, starting to finally control his breathing. Responding to the assurances from Vlad. "Where do we meet?"

"Do you know where Sharpstown Mall is?" Vlad asked.

"Uh, yeah. Are you sure you want to meet there—it's kind of rough."

"It is a busy place—we need a crowd where we can talk," Vlad answered. "Can you be there in 30 minutes?"

"Well, they'll miss me at work," was the nervous response.

"I don't think you need to worry about that job. Your bonus will buy you some time to find something better."

"You're right. I'll be there. Where do we meet?" Michael asked.

"There is a large entrance sign at the southeast corner, near where they have the carnival set up in the parking lot. I'll be there waiting for you."

"Okay I—" CLICK. Vlad hung up the phone and Michael was talking to air. Michael looked around and realized he had been standing in the middle of an empty section of the parking lot—and nowhere near his car. He looked around and saw no one else. He quickly made his way to his car and drove off.

RING—"Hello?" Michael answered as he pulled out onto the highway.

"Hey, it's Jonathan. Are you okay?"

"Yeah, I'll be alright. I decided to go get a drink, but I don't feel too good. I'm going to go home and lay down for a while." Michael lied.

"All right. The boss wanted a briefing on our visitors. I'll let him know how it went. Do you want me to cover for you?"

"Sure. Thanks for the help. I'll see ya." Michael hung up quickly before his nerves failed completely and settled in for the drive to Sharpstown Mall.

LOOSE ENDS

Thursday, 12:11 p.m.

Michael made his way down Bellaire Boulevard and drove past the large south entrance to the mall parking lot. He turned into the Taco Cabana across the street and walked over to the intersection to cross the street. The crossing turned out to be the most dangerous part of his trip from 3DNF. A few car honks and a dash and Michael was standing in front of the large yellow arch-shaped sign for the mall. As promised, his contact from the Starbucks was standing to one side of the sign.

Michael walked toward Vlad. Vlad matched Michael's stride and said, "Let's just walk along the edge of the street carnival here. I like to stay where we can both see what is going on around us." Michael didn't answer, but obeyed.

After a few steps, Vlad began. "As I said earlier, you have done better work than you realize. By the time they find the access point, you won't care. And your boss will have some explaining to do because of what is now on his computer."

"Cool. Uh, so it all worked out and I can get paid then?" Michael asked as he walked beside Vlad, watching his own feet and paying no attention to the crowd around him.

"Oh yes. But there are a few questions I have for you first." Vlad stopped walking and turned to face Michael. "First, is there anything else about the phone call you have not already told me?"

Michael looked away for a moment, thinking through what he had heard. "The agent said something about finding a dad. That part didn't make any sense."

Vlad had to make a focused effort to keep his facial expression neutral. *That confirms it*, he thought. "Anything else about the call?"

This time Michael was a little quicker with his answer. "No, that was it."

"All right. Next question, what happened with the wireless scan the FBI asked you to do?"

"It worked just like you said. We ran the scan with just a Windows laptop and nothing showed up," Michael reported.

"Good. Did they ask you any more about the name I gave you?" Vlad continued. He also started walking again, this time back in the general direction of the entrance sign. They had to split up for a moment because of all the people walking along the sidewalk towards the carnival.

"They didn't say anything about that today. They just said it looked like we had some issues with our temp help. I don't know if they did any more checking on that."

Vlad paused from the walking and looked at Michael as if he were checking to make sure he was telling everything he knew. "Did they say anything else about their investigation?" Vlad asked more sternly.

"Well, when they were done with that phone call, I asked if it was about the 3DNF case. One of the agents said that 3DNF wasn't really a case. That might mean they don't think anything happened."

Vlad paused for a moment, deciding what he should do next. The extra long look from Vlad made Michael look away at the crowd. "Well, we should get to the part you care about. I didn't want to bring cash with me for this payment," Vlad said in a more casual and relaxed tone. He took a step closer and put his hand on Michael's shoulder and guided him over to a tree at the edge of the parking lot next to the carnival. "I will set up a bank account for you off shore. You will get an e-mail with all of the instructions to access the account. You can do it remotely, but I suggest you visit in person. It is much easier if you don't bring any of your profit back into the United States."

Michael's head was spinning. He couldn't believe it had worked out so well. He was going to be out of debt, travel a little bit, and his old boss was going to be in trouble.

"So did that name they mentioned—Vlad—mean anything? Do they have a lead back to us?" Michael asked.

"I have not heard of anyone named Vlad. I think that was not related to your assistance in any way. That had to be either another case, or a dead end." Vlad's assurance was enough for Michael. Vlad surveyed the edge of the carnival in the mall parking lot in front of them. People were milling around in every direction. "This is a good place to complete our business." Vlad pointed back to the main entrance sign where they had first met. He walked in that direction and Michael followed.

After a few quiet steps Vlad began again, "I need to leave, and it is best if we do not take the same route. I believe when you arrived you parked across the street."

"Yeah, that's right," Michael, confirmed.

"Then I want you to go ahead and cross over, but instead of going back to your car, sit at that bus stop," Vlad motioned with a nod.

"What for?" As soon as the words were out of Michael's mouth he realized he should probably just shut up and obey.

"You will sit at that bus stop for at least five minutes. We need to leave separately, and you need to pay attention and make sure you do not see anyone that may have been trying to follow you."

That way you will have the opportunity to watch the crowd and make sure no one took note of our meeting," Vlad stated like he was schooling a child on the need for table manners.

Michael was even more compliant after Vlad's firm instruction. "Sure. Uh, thanks for the job. Let me know if there is another chance like this in the future."

"I will know how to find you," Vlad assured him with just a hint of a smile and walked away.

Michael looked up and down the street and saw no one that would make eye contact with him. He could see his car in the parking lot across the street. He followed instructions and crossed Bellaire and turned to his right. He walked over and sat on the bench of the bus stop and began to watch the people walking up and down the sidewalk.

Vlad turned north and walked straight across the parking lot, towards the mall entrance. The blue light of his active Bluetooth headset gave a soft glow. He had kept an open call going the whole time he was with Michael. One word was enough for the next step. "Da."

Andrei was stationed on the second level of the parking garage, northeast of Michael's bus stop. He was alone standing in front of the car he had stolen the night before. Through the scope of his rifle he could see Michael sitting and watching up and down the street. Andrei waited for a clear shot. "Breathe in, breathe out, hold, squeeze." There was a slight muzzle flash, but the silencer took care of most of the sound.

A man sitting next to Michael on the bench caught the unnatural movement next to him in his peripheral vision and turned. Michael gave a raspy grunt and slumped backwards. The small hole in his chest was much cleaner than the mess on his back where the bullet had begun to tumble as it exited his body. It had gone through the bench where Michael sat and continued in the direction of the abandoned Circuit City store behind them.

The man jumped up and began to look around. Nothing looked unusual. No one was running, no one stopped to look, no tires squealed. He looked down and saw he had blood splattered on his shirt. "Help! Hey, HELP!" People began to stop and then a few screamed. Some ran away, others hid their faces and just walked quickly by. No one ran toward Michael. The awkward position of Michael's lifeless body told the story.

◖◖◖

"Are you done?" Vlad strolled through the mall.

"Yes."

"Are you clear?"

"Not yet." Andrei had managed to disassemble his rifle and return it to its case before Vlad had asked for an update. The case was padded and looked more like a large sports bag. Andrei pulled a rag from his pocket and rubbed down the outside of the trunk and then walked to the driver's side door. He slipped back in the seat and wiped down the surfaces he had touched. He rolled down the window, covering the handle with the rag, and got out. He fished in his pocket, pulled out a couple of fifty-dollar bills and tossed them in the seat and began to walk away.

"On my way," Andrei spoke into his headset.

"Did you leave the bait?" Vlad asked as he exited the north side of the mall and made his way to his car.

"Yes. Whoever gets in to get the cash will leave their prints."

"Find another van. I'll meet you back at the house." Vlad hung up.

Andrei kept walking and gave a sigh and shake of his head. He scanned the area and looked for an older-model vehicle that met his boss's requirements.

EXPENDABLE ASSETS

2:11 p.m.

Pavel was sitting on the couch in the front room. He had his laptop balanced on his outstretched legs. He was looking at international flight options and trying to decide if he should fly out of Houston or rent a car and drive to New Orleans or Dallas. He had decided it was time to have his own contingency plan. The sound of a car door out front announced Vlad's return. Pavel surfed to the Black Hat conference site and then cleared his browser cache before Vlad walked in.

"Has it been quiet?" Vlad asked.

"Yes. How did it go?"

"Fine. We have one problem solved, but we are not yet done."

"I thought we had the file transfer process working, so we were ready to go now." Pavel put his laptop down and noticed Vlad checking the display to see what was open on the screen.

"We still have to find those kids that were at 3DNF. We have to make sure they don't pass anything to authorities. And we have to take care of our guest." Vlad answered with a nod to the back of the house where George still sat alone.

"We don't know if they have anything, and that connection we set up will be quiet as long as we want. Even if they scan their network traffic, it won't show up. It's just going to look like normal Web traffic on the way out."

Vlad's voice got louder than Pavel expected. "We cannot have anything left behind!"

"I understand, but we haven't left any—"

"You do NOT understand," Vlad pointed at Pavel. Pavel leaned back in his seat at the gesture. "We are not just working for Stepan's employer," Vlad stated impatiently.

Pavel gave Vlad a confused look and sat upright on the couch. "I don't understand."

"This data…This access is too valuable to just sell back once. The file I gave you to install was not what we received from Stepan. I had it customized," Vlad began.

"Why didn't you let me—"

Vlad just held a hand up for silence.

"This was custom work like you have never seen," Vlad started. He sat down on the chair next to the couch. "The volume of information processed through this feed is massive. Stepan's employer isn't the only one who is interested in this. I have others I answer to on this job.

Pavel wasn't catching on. "So who is in charge of this? I thought you were working as a contractor for Stepan's employer."

"I am. But that was just what led to the job. They are clients, but I have an employer. A more, um, exacting employer who is also interested. They do not tolerate failure well, and they are very—well, that is something for you to learn on your own. For now, you need to understand that I have to make a clean exit out of the country or I—we—all fail."

Pavel started to form another question but the door opened. It was Andrei. Vlad turned when he walked in the door, carrying his bag.

"Everything clear?"

"Yes."

"Good. Get your gear packed." Then Vlad turned to Pavel. "You too. We need to be ready to move, within the hour."

Hannah parked the car outside the IHOP and turned off the engine. "So is it time?" she asked.

Leon checked his watch. "Yeah, I think we should do it now." He turned to look at Bob in the back seat. "Are you going to be okay while I do this?"

"Yeah, whatever. You do the better non-geek social attacks anyway," Bob responded. He was slouched in the back seat leaning to one side on the pile of backpacks. Leon, Hannah, and Bob had tossed all their gear in the back after checking out of the hotel a couple of hours earlier.

"All right. Just keep quiet so I can concentrate." Leon pulled out his cell phone and scrolled down to the number he had saved into his contact list earlier that morning and hit "Send."

Andrei was in the back of the house packing up his gear as Vlad had instructed when his cell phone rang.

"Da—Haki?" Andrei had seen the local number and assumed Haki was finally making contact.

"Hello?" Leon wasn't sure he understood what the voice on the other end had said.

"Da?"

"Hey Andrei, listen, I just need to talk to Vlad."

Andrei's face revealed genuine surprise as he held the phone out from his ear and looked at the caller ID again. He walked into the kitchen where Vlad and Pavel were hunched over Pavel's laptop.

"I do not know who this is, but they know my name and yours and they speak English." Andrei handed the phone to Vlad.

Vlad slid his chair back from the table, took the phone, and walked into the front room. "Yes?"

"Hey, Vlad?" Leon asked.

"Who is this?"

"I'm one of the guys you chased Saturday night."

"How did you get this number?" Vlad was genuinely surprised at this development.

"I got it because you're sloppy. When you went back to the F0RB1DD3N network, your system got owned. Word of advice, if you go on a hostile network, don't use a Linux box that hasn't been patched in forever. I've got a copy of everything of interest on your laptop, including your contact list."

"Since you called me, what do you want?" Vlad asked, his voice sounding terse as he tried to gain control of the conversation.

"I want you to let George go free."

"I do not know who or what you are talking about," Vlad answered cooly. He needed to see what else this caller knew.

"I know you took George from his house. I know you trashed his house. And I have a video tape of you and your goons—"

Bob leaned forward from the back seat. "You let my dad go! You let him go NOW or we—"

Leon held the phone away from his ear and looked back at Bob, "Shut Up!"

"It sounds like you have a rather emotional associate," Vlad dryly observed.

"Yeah, but he has some skills you don't want turned against you. Now put George on the phone so I know he is alive!" Leon said with an edge creeping into his voice.

"And why would I do that?" Vlad asked unfazed by the boy's emotional state.

"If you don't, then I have no reason to make a deal with you, and my next call is to the FBI," Leon answered simply.

"Very well. One moment." Vlad walked back past Pavel and Andrei in the kitchen and down the hall to George's room. He threw the door open quickly and startled George. Vlad covered the phone with his free hand and leaned his face in right next to George's. "You will tell your son you are alive and nothing else. One more word and I do not have a reason to keep you." Vlad put the phone next to George's face. "Speak!"

"B-Bob, is that you? I'm okay. What di—"

Vlad pulled the phone away. He could hear the voice on the other end of the call speaking to someone—"He's alive."

"Now if I return George, how do I know I can trust you to not turn everything over to the government?" Vlad asked.

"You have my word."

"I do not know what your word is worth," Vlad countered with a low growl.

"Then I give you my word that you will have a bunch of Feds all over you before this day is finished. You don't have a choice but to trust me and let George go." Leon said.

Vlad didn't see much of an alternative. "So where do we meet?"

"The Arboretum today at 6:00 p.m. at the start of the Inner Loop Trail."

A grin spread across Vlad's face and he suppressed a chuckle. *That's how they think they are going to take me down*, he thought amazed at his good fortune.

"And if I bring George, what will you be bringing me?" Vlad asked.

"We will have the last copy of all of the data we collected on a USB drive," Leon answered.

"Not quite good enough. You bring your laptops with you. If you are as clever as you say, you might keep copies of the data."

Leon looked at Bob for a second in the back seat. "Agreed." The line went dead as Vlad hung up.

Bob looked at the pair in the front seat. "What? So you think I was a little over the top?" he said waiting to hear his review.

◖◗◖◗◖◗

Vlad walked back into the kitchen where Pavel and Andrei were sitting.

"Are you done packing?"

They both nodded in agreement.

"Good. We have had a development that will make our exit easier. The kids from the parking lot have overplayed their hand and they want to meet," Vlad started to explain.

"How did they get Andrei's number?" Pavel asked trying to act confused.

Vlad's face got a little harder as he turned to Pavel. "Apparently you are not giving me good advice on securing my laptop."

"What do you mean?" Pavel asked, feigning surprise.

"They got into my system and have a copy of the instruction documents for this job and my contacts file." Vlad answered. "They claim if we bring them our guest, they will delete everything."

"You didn't agree to that did you?" Pavel asked.

"Of course I did," Vlad answered. "I would have agreed to anything to get them to show up. Because, they want to meet at 6:00 p.m. at an arboretum, but Michael from 3DNF told me that he heard the FBI agents setting up a meeting with someone at the Arboretum at 5:00 p.m. These American kids think they can set us up." Vlad uttered the last sentence with contempt.

Pavel leaned back in his chair and put his hands over his face, trying to figure out if he was ever going to get home alive. Pavel put his hands back down and looked at Vlad. "How are we going to deal with the FBI and—"

"Relax. We have the advantage because we know where and when everyone is meeting. Everyone that is a threat to us is going to be conveniently in the same place an hour before our meeting. We just need to show up early for that first meeting and remove all threats." Vlad looked at Andrei with a satisfied smile. "I need your services one more time before we can go home."

"Understood."

CHAPTER

T3N

CHOOSING SIDES

Thursday, 4:05 p.m.

Vlad surveyed up and down the street as he threw the last of their bags into the trunk and closed the lid. There was no one watching. He turned to Andrei. "Go get our guest and put him in the van." Andrei took two steps before Vlad turned back to him. "And take off the cuffs. We do not want some neighbor calling the police because they see him restrained." Andrei nodded and returned to the house.

Pavel was already sitting in the passenger's seat of the van. Vlad got in his car and waited. Soon Andrei came out holding George Falken firmly by one arm. George was too tired to have any fight left in him. The deprivations and fears of the past days had made him compliant. He did his best to stumble along where Andrei led and fell into the van when Andrei gave him a light push. Andrei stepped in behind and locked the seatbelt across George.

Pavel turned to face George. He held his gaze for a moment and just before the driver's door opened, George saw a wink and the hint of a smile as Pavel turned around.

Andrei got into the driver's seat and tapped the Bluetooth headset to answer Vlad's call. "Just follow me and take your time," Vlad instructed. It took just over 40 minutes before they approached the turn off where Memorial Drive passed under a railroad bridge. At this point, Vlad called Andrei again. "Just pull over on the right before the tracks and have Pavel drive the rest of the way."

"Understood," Andrei answered. He gradually slowed the van and pulled off the road. He put the van in 'Park' and turned to Pavel. "Hand me that bag." Andrei growled and pointed at his bag at George's feet. Pavel struggled to pick it up and pass it to Andrei. "Keep track of the 'guest,'" Andrei instructed menacingly as he got out of the van.

Pavel didn't respond. Instead he slipped into the driver's seat and after a couple of tries, managed to merge back into the crowded and slow-moving traffic. He continued along the gentle curve of Memorial Drive until he reached the entrance of the arboretum.

Andrei hiked up the gentle embankment to the railroad tracks and followed them straight south along the eastern edge of the arboretum. Just as they had planned when they looked at the map on Pavel's laptop earlier that afternoon, there was a place

where the trees of the park thinned and there was a view of an opening that surrounded a small pond with a little tree-covered island in the middle. Andrei found a place under a tree and low brush at the edge of the arboretum grounds that gave him a clear view of the Inner Loop trail. He knelt down and pulled the parts of his rifle out of the bag.

He paused a moment as he lifted the stock. *The one thing Haki did right was getting this Blaser R93*, he thought to himself. He quickly assembled the weapon and began to attach the silencer at the end of the barrel. *It was a lot smoother this afternoon with the other American than my old Dragonov SVD.*

Vlad had followed the winding drive up to the main entrance ahead of Pavel. By the time Pavel got there, he could see Vlad's empty car. He parked the van and sat still, just staring toward the main building where Vlad must have gone in a couple minutes before.

George decided he had one more chance. "You know," his voice was raspy from lack of rest and food, "I think you could make it out of here now."

Pavel turned in his seat and looked at George, holding his gaze. "Yeah, I think you're almost right," Pavel agreed reassuringly. Pavel had been thinking about this since his first conversation with George. He didn't like his chances of getting out of the country if he stuck with Vlad's plan. Vlad would take care of himself, and so would Andrei. Pavel had to do the same. "I want to watch the area for a little while first. We have a few minutes."

Pavel turned back to George. In a genuinely concerned voice he asked, "If we have to get out and move, do you think you can make it?"

"I—I don't know." George was still using his hands to hold himself upright. "I'm sorry I think I would slow you down."

"I think we can stay in the van. I just wanted to be sure," Pavel answered as he turned his attention back to the situation around them. Since it was just at the end of the business day, the parking lot was not crowded. There were a few cars, the expected mix of SUVs, sedans, and one nice sports car. One mom was walking up to the main building with a couple of kids in tow. He spotted one sedan with a couple of people still sitting inside, talking. "It's time to get out of here and get some help," Pavel announced.

"What about my son? Aren't we here to meet him?" George perked up as the instinct of fatherhood overrode the one for self-preservation.

"The best way to help your son is to get out of here and contact the police," Pavel answered. He started the van and pulled out of the parking space. He hit the accelerator a little hard and the van lurched as he turned the steering wheel sharply to point the van back toward the entrance. George did his best not to fall over as the van leaned with each curve.

◖◖◖

"I see them," Andrei whispered to Vlad on the open call.

"Where are they?" Vlad asked sharply as he made his way along the wooded trail. The area was quiet as he continued along through the trees.

"They are on the north side of the pond facing away from my position. If you approach from the west trail, then that will turn them toward me."

"How many?" Vlad asked.

"There are five. I have seen four of them before, but the new one is just a girl. She looks like a civilian. The two adults are not."

"Anyone else around?" Vlad checked again to be sure.

"No. It looks clear." Andrei looked back behind his position to verify. As far as he could tell, he was alone.

"Good. Keep your aim on the agents. The kids are mine. Do not do anything until I tell you to."

"Understood."

Vlad reached the end of the tree-covered portion of the trail. He could see the people Andrei had described just ahead of him. He paused to check the surroundings. "Get ready for my word," he whispered to Andrei on the call. "I need to know what they know first."

Andrei shifted in his position and eased up to the scope on the rifle. He began to pan along the pond to cover his main target. The cross hairs rested dead center on Agent Battle.

Vlad walked out of the cover from the trees and approached the group, keeping a tactical separation and making sure that he did not get in Andrei's way. As soon as he was visible on the trail, the female agent tapped the shoulder of the other agent. He had kept his attention on the only other trail into the clearing. That motion was enough to cause the three kids to look back as he approached.

"I see you are the ones I should be dealing with instead of these children," Vlad began. He was certain he could see a weapon on each of the agents beneath their jackets. The kids showed no evidence of a threat.

Snap. A camouflaged figure, hidden in the shadows of some nearby trees shifted his weight slightly to watch Vlad's appearance in the clearing. The noise wasn't that loud, but it was enough. Andrei looked behind his position again and this time saw the movement of at least one figure. The rifle was too slow. In a smooth motion, Andrei dropped his rifle, rose out of his kneeling position and pulled out his Glock. As he began to pull the weapon level he heard someone from behind him yell "Gun!"

Seven rounds hit Andrei from unseen opponents before he even had a chance to respond. Andrei's lifeless body dropped to the ground. One camouflaged man ran to cover Andrei; two others broke their cover and moved into the clearing.

The sound of the gunfire surprised Vlad most of all. He expected to hear nothing from Andrei's silenced rifle when he chose to give the order to shoot. Instead, he pivoted around to the new threat and pulled his own weapon out in the same motion. Vlad squeezed off two rounds at the two agents moving into the clearing. Both shots missed, but the fire was enough to cause them to drop for cover. Their shots at Vlad were just as effective. He had already started to pivot, keeping his profile to his opponents as small as possible.

Mark and Chris both had their weapons out. Mark saw past Vlad and realized the agent checking Andrei's position was in his line. Chris saw only Vlad. Her shot caught his left arm. The force of the impact jerked Vlad awkwardly.

Vlad was hit and had counted at least four weapons with him in the middle. He had lost the initiative. Now it was just revenge. He turned back to those meddling kids that had shattered all of his careful planning.

At the first sound of gunfire, Hannah had dropped to her knees. Leon managed two steps in Hannah's direction, between her and Vlad. In the rush, he didn't see her duck. As he planted his foot for the next step, one of Vlad's next rounds hit Leon in the chest. The impact felt like someone had hit him with the full swing of a hammer. Leon had no control of his legs. He dropped hard, catching Hannah's shoulder in his back on the way down. His head snapped back and then found the packed gravel of the trail. His mouth filled with blood. All he could do was try to breath, but his lungs were not obeying. Everything went dark.

"LEON!" Hannah screamed.

Satisfied for the moment with two of the targets down, Vlad's next target was Chris. His left arm was hanging limp at his side, but the weapon in his right hand was still moving in a smooth motion. Chris's first shot was just to Vlad's right.

Vlad's movement had kept his profile to Chris small, but it left his chest uncovered to Mark who was a few feet right of Chris. Mark's shot hit center of mass. The impact jerked Vlad's arms out and his last shot went wildly high. Chris's next shot hit the side of Vlad's chest under his now-raised arm.

Vlad fell onto his back, disappearing into the grass just off the trail. With each attempt at a breath, he could hear a gurgling sound where air escaped his lungs from the holes in his chest.

Vlad looked up and saw the deep blue of the afternoon Houston sky through the trees. He could hear the crunch of dry grass beneath him as he turned his head slightly. The hot, humid air and sticky blood filling his mouth mingled to give a sensation of drowning. He tried to sit up, but his body wouldn't obey. There was a sharp sound of metal on metal. The sound was familiar, but his mind wasn't working fast enough to recognize his situation. He craned his neck as he struggled to look above him. He saw legs, a hard face looking down at him, and a gun. The shape of the gun seemed to grow large enough to fill all he could see—and then nothing.

Chris knelt down and checked for a pulse. "He's gone! How are the kids?!" She yelled over to Mark.

Hannah jerked Leon. "LEON!" She ripped open his shirt, tears clouding her vision as she fumbled with the straps of the bulletproof vest. Afraid of what she might find.

Leon took a couple of gasping breaths. "Gahh THAT HURT! And I busted my lip!"

"Well why'd you jump in front of me and take the bullet then!?" Hannah answered with fear and joy and relief all woven together.

Hannah began to pull off her own shirt, revealing a bulletproof vest.

"I thought that's what I was supposed to do!" Leon answered, not noticing the hint of tears in Hannah's eyes. He finished getting the vest off and wiped his bloody lip on the back of his hand.

"DAD!" Bob yelled. Somehow he was the only one of the five that remained standing through the whole shoot out. Even though he had had the most bullets fly past.

He was untouched. Once he realized everything was clear, he took off running down the trail towards the main building.

"Bob! Wait!" Mark did his best to keep up, but Bob had the greater motivation and stayed ahead of him.

Bob blew through the building and out into the parking lot. There he found a collection of police cars, an ambulance, some unmarked vans, and a large collection of people walking about in black jackets that had "FBI" on the back.

"DAD!" Bob yelled.

"Son, come over here." Special Agent Thompson was walking toward Bob. "I've got someone that wants to talk to you."

Bob paused, and then walked over to the tall man with salt-and-pepper hair combed straight back and black sunglasses.

"Bob, it's okay," Mark said between deep breaths as he caught up with Bob.

"Where's my dad!?"

"Right over here, son." Special Agent Thompson put his hand on Bob's shoulder and guided him over toward an ambulance. Bob ran ahead when he realized he was being led to the ambulance.

"Dad—are you al—"

George was sitting on the back bumper of the ambulance while an EMT checked his blood pressure. When George saw his son, he found strength he didn't think he had left and jumped up to wrap his son up in a hug. As soon as he did, his legs started to give. Bob and the EMT eased him back down on the bumper.

"Bob, you're okay. You're okay. I was so—" He couldn't stop the tears that started to fall. Bob tried to reassure his dad, but he couldn't form any words. He just held his dad. For the first time in too many years, they just held on to each other. Neither was alone any more.

Mark found an EMT without a patient. "We've got someone back there that needs to be checked out. He took a bullet in his vest."

"Who was hit?" Bob asked, starting to pull back and let his dad get some air.

"Leon, but he's goin—"

"What? Why didn't you tell me? Dad, I'll be back." And Bob was running back toward where he had just come from. The EMT picked up his bag and just let Bob lead the way. They only made it as far as the gift shop inside the main building when they came to Leon leaning on Hannah's shoulder.

"Are you okay?" Bob asked trying to hold back tears.

"Sure. How about your dad, is he—"

"He's fine. What happened?" Bob assured and asked in one breath.

"I don't know. I heard the shooting behind us, then in front of us and the next thing I knew I was on the ground and Oh THAT HURT!" Leon exclaimed.

"Oh man up," Hannah said as she continued to help Leon walk. Her concerned look not matching her words.

"I thought that's what I did when I took your bullet," Leon said with an added grimace of pain for effect.

"I didn't say I didn't appreciate the gesture," she said allowing a slight grin and squeezing him a little tighter.

Leon gasped slightly, not sure if it was from pleasure or pain.

"Sir, let's get you back to the ambulance. I want to get you checked out," the EMT instructed. Bob and Hannah made sure Leon made it the rest of the way.

Soon Leon was sitting at the back of the ambulance. George had found the strength to stand, helped by a candy bar and sports drink one of the agents brought from the gift shop.

"So where is the kid that helped me?" George asked Special Agent Thompson.

"We're holding him over near where we picked you two up at the entrance. He'll be going back to our office for some questioning."

"For what it's worth, I think he's a good kid who got in over his head. He was helping me escape when you stopped us. He didn't want to be with the other two."

"Sir, we will take your statement once these guys finish checking you out, and we will take that into consideration," Agent Thompson assured him.

Mark offered his hand to George. "Mr. Falken," he said as they began to shake hands, "you have one ingenious son. And he has a couple of very smart friends." All three of the kids smiled at each other.

George was feeling a little stronger as the sugar from the candy bar kicked in, and the feeling of being safe settled on him. "I still don't understand how everyone ended up here."

Leon and Bob started talking at once, then stopped. "You go ahead," Leon offered.

Bob took a breath. "Leon managed to hack into Vlad's laptop. He was the main guy who took you."

"Where is he?" George asked.

"Sir, he will not be a problem for anyone again," Mark said with conviction.

Bob continued. "Anyway, when we were at 3DNF Wednesday night, Leon hacked Vlad's laptop and got a copy of all of his contact information. We had to get more information to figure out who took you. We staked out the place across from 3DNF and tracked the bad guys when they came back. It got a little scary when I shot one of them."

"What!?" both George and Mark responded together.

"You didn't tell me about that part," Mark said.

Bob put his hands up. "I'll get to that in a second. We found out from the data on Vlad's laptop that he was trying to set up a back door into some U.S. government computers through their connection to 3DNF."

"Son, why don't you skip over that part," Special Agent Thompson advised. We can go over that back at the office in 'private.'"

Just a week ago Bob would have responded to the suggestion with as much attitude as Dobbs showed Mark and Chris when they visited. Instead, Bob understood now that some things were not for public disclosure.

"Vlad's laptop had a set of instructions, a contacts file, and," Bob looked at Thompson, "some stuff that could jeopardize a certain unnamed country on it. We got the phone numbers of people he was working with and used that to set him up."

Mark broke in. "So that's when you called me early this morning to set up that call while Chris and I were at 3DNF."

"That's right. Mark and I set up a call so Michael—he was also in the contact list as an employee of 3DNF—would overhear a conversation about a meeting today at 5:00 p.m."

"Who's Michael?" George asked.

"Michael was the employee who was helping Vlad," Mark answered quickly.

"What do you mean 'was'?" Leon asked but already dreading the answer.

"Michael called Vlad like we thought he would. They had a meeting today just after noon when we left 3DNF. We put a bolo on him, but we didn't have the time to put a tail on him. We got a call from the HPD that he was shot by a rifle."

"A rifle!?" Leon exclaimed. "These vests you gave us wouldn't have stopped a rifle!"

Mark continued, "We weren't counting on the vests to protect you from that shooter. We knew from our last meeting at the Galleria that there was someone else. We made sure to have people staking out his position. Remember, I picked the place. I knew there was only one clear shot into that area. We had a spotter across the railroad tracks and three other agents surrounding him in the arboretum area. The vests were to protect you from Vlad."

"But how did you get Vlad to bring me here?" George asked. This still doesn't make sense.

"I'm not finished yet, Dad," Bob continued, still euphoric from surviving the shootout. "There's more. Leon called Vlad. Well, he called the shooter—Andrei. We had his number from Vlad's contact list. Leon told him we would meet at 6:00 p.m. at the same place where Michael thought we were meeting the FBI at 5:00 p.m. Since Vlad and Michael would talk, we knew Vlad would think it was a setup and he would come early to trap us at 5:00 p.m. He didn't know we had a trap in his trap!"

George looked at the very self-satisfied expressions on everyone's faces. "I think I've got it. Bob, you'll probably need to tell me that again after I've slept for a day. And probably with diagrams."

Bob turned to Leon. A smile spread across his face as the enormity of the story he had just told sunk in. "Dude, do you know what we just did? We just saved the United States! That's bigger than saving the Internet! That means we're bigger than Dan Kaminsky! Or Tony Watson!"

Leon looked exasperated. "Bob, we aren't even up there with GOBBLES. Or n3td3v for that matter."

Bob's shoulders dropped a little and he asked almost plaintively, "Well then won't we at least get an interview with Stephen Colbert?"

"Sorry, Dude, I wouldn't be expecting a call even from Letterman," Leon responded with a satisfied smile as things got back to normal (*p. 344).

The EMT stepped in and broke up the conversation. "Mr. Falken, and you," he pointed at Leon. "Both of you need to leave now. You need to get checked out at the hospital."

"I'm going with him," Hannah chimed in. She hadn't let go of Leon since she had helped him get his vest off and walk back from the shooting.

"That's fine, but no one else in the rig," the EMT answered.

"I'll bring Bob and we'll catch up with you at the hospital," Mark offered. "Bob, let's talk for a second." Mark led Bob a few steps away from the ambulance as the EMT shut the doors. "You guys did some really clever work on this. You don't know, heck, I don't even know how many lives you saved today. I just want to throw this out. I think you and Leon could do good work with our unit."

"No way." Bob's head was shaking before Mark had finished. "There is no way I can work with you guys." He started counting off on his fingers, "I'd never pass a background check. I don't look like a Fed. I'll NEVER wear a suit. I won't even tuck in my shirt. And I'll never work on a computer where the only sticker is an asset tag for some bean counter to track a requisition."

Mark stopped him before he began on the other hand. "It's not that bad," Mark assured with a laugh. "Just think about it for a little bit. Once everything calms down you might consider it. Besides, you wouldn't be an agent. We have consultants and contractors who would be interested in your talents. And come on, you'd probably prefer walking in through the front door instead of an unmarked van just snatching you off the street some day to 'recruit' you."

"You wouldn't," Bob responded, partly as a statement and partly as a question.

Mark laughed again. "The FBI doesn't snatch citizens off the street." Then Mark added with a sly grin, "But I might know someone who would."

3P1L0GU3

END PROCESS

Friday, 2:00 p.m., St. Petersburg

RING…RING…

A woman reached her hand to answer the phone. Her hand paused over the receiver. She knew this line was never supposed to ring. "This is not going to end well," she said aloud just before she picked up the line.

This page intentionally left blank

PART

Security Threats Are Real (STAR)

2

This page intentionally left blank

Star Introduction

What follows is the product of a community. Information security practitioners of varying backgrounds have come together to produce this work. Bob, Leon, Hannah, Mark, and Chris are just the beginning. Their story is more than a fun diversion. Woven throughout are real-world examples of security threats. These are threats you should understand.

A corporate leader, a government official, or an individual trying to protect yourself and family—all can benefit from the lessons of the preceding story and the collective experience of the following reference material. This work adds context to the adventure of *Dissecting the Hack: The F0rb1dd3n Network*. It is the product of people who live and practice the craft of securing information, places, and people.

The only way to know if something is secure is to test it. It is in the application of real-world attacks that defenses are validated and improved. Over the years, I have developed what I call the Bush1d0 method of penetration testing. It is a five-step process that consists of recon, scanning, exploring, exploiting, and expunging. In the following, we will explore this approach and see how it was used in the story and IRL.

RECON

Search engines such as Google, Yahoo!, Bing, AltaVista, and others can be "weaponized." Web sites, individuals, and organizations "leak" valuable information that can be used to plan attacks. Search engines become the aggregation and parsing tools of these unintended disclosures. By asking the right questions, attackers can select targets and plan attacks. In fact, search engines can be used to begin attacks, but that is a later step.

SCANNING

This is the step when attackers begin to take risks of their own. They move from quiet observation of targets to actual probing for weaknesses. This is also the first opportunity a target has to identify the precursor of an attack. If done correctly,

an attacker can complete his or her probes without detection. If done correctly, a defender will make it very difficult for a probe to return accurate information.

EXPLORING

Now the action has truly begun. If an attacker reaches this stage, then the defender has lost the initiative. The attacker begins to create an attack profile with the primary data collection completed in the prior steps. Exploring is the stage of refinement as initial probing turns to validation of attack vectors.

EXPLOITING

The previous steps have led to the moment of execution. The attacker uses a variety of tools to transform vulnerabilities into open doors. For defenders, this is when the battle moves from the perimeter to interior assets. The frightening aspect of this stage in the process is the sheer number of easy to use tools available to the attacker. Specialization has led to a panoply of options for exploit. For the defender, the most concerning phrase is "point click root."

EXPUNGING

So just what is the fun in successfully identifying a system, attacking it, and then getting caught? Expunging is the step of removing evidence of the violation. If an attacker gets past this step, then you are no longer the owner of the system. In fact, you are just a service provider to the bad guy.

As you read these chapters, you will see that there is no clear delineation from one step to another. Instead, they are a descriptive for areas along a continuum of an attack. Both attacking and defending are part science, part art, and part intuition. Leaps of imagination and unusual combinations of techniques and practices are common characteristics of the best on either side of the game.

BLEEDING EDGE

This is the part that may be cool today and history tomorrow. Regardless, it provides important context to the hacking culture. Certain events have been pivotal in the creation of the "now" we currently experience. Here is where you can learn the "how" and "why."

HACKING CULTURE

This part of the story—for the real-world steps are as much a part of the story as the fiction of Bob and Leon—will also introduce you to the underlying hacking culture. Black Hat. White Hat. Gray Hat. No Hat. It's not Dr. Seuss. It is shorthand that has evolved to describe the types of characters that populate the world of security. The difficulty is discerning what color hat is resting on the head of the individual on the other side of a chat session, trade journal article, or firewall log. Today bad guys shoot bytes more than bullets.

… Connecting … the … dots: there is a narrative that flows between fiction and reference. The fiction illustrates how the reference could be applied. The reference gives context to the fiction. Both teach lessons you should learn. This part may not have shoot outs and car chases, but keep in mind that the tools here just might be running on your home computer or company network already. That just might be more exciting (and frightening).

This page intentionally left blank

CHAPTER

1 Recon

The biggest weapon in the arsenal of the attacker is also the biggest defense for the defender. Shorthand for reconnaissance, this is the information the attacker and the defender gather for the same reason—to find weakness though the attacker exploits it and the defender corrects it. Living in the information age is a double-edged sword. Back in olden times, the concern was the castle guards going to the local tavern and maybe saying too much about what was going on inside the castle or if there was a wall that needed to be repaired. This information could be used if there was a spy in their midst or if someone was bribed to relay the information. Nowadays, all you need to do is search Twitter and Facebook accounts to find out information that could be damaging to your employer, or by using the most powerful weapon for recon—Google—you could find the weaknesses (i.e., directly exposed databases, possible SQL injection points) to your Web sites, which could potentially be out on the Internet for anyone to peruse. The more information you gather about your target the more likely you are to succeed. If you conduct a recon scan on the Internet, you usually always find potential victim machines that can be exploited. Now, though, as more and more companies are shoring up their perimeters, attackers are starting to pick and specify their targets to more likely guarantee success. The Open Systems Interconnection (OSI) Model Layer 4 is no longer the main layer of attack; it is now Layer 7, the Application Layer, and Layer 8,[1] the Human Layer, where most attacks are succeeding. See below for details on the OSI model.

The OSI Reference Model or OSI Model is an abstract description for layered communications and computer network protocol design. See Figure 1.1 for a table of the Layer Model. It was developed as part of the OSI initiative.[2] In its most basic form, it divides network architecture into seven layers which, from top to bottom, are the Application, Presentation, Session, Transport, Network, Data-Link, and Physical Layers. It is therefore often referred to as the OSI seven-layer Model. A layer is a collection of conceptually similar functions that provide services to the layer above it and receives service from the layer below it. On each layer, an instance provides services to the instances at the layer above and requests service from the layer below. For example, a layer that provides error-free communications across a network provides the path

[1]http://searchnetworking.techtarget.com/tip/0,289483,sid7_gci1253302,00.html
[2]http://www.itu.int/rec/T-REC-X.200-199407-I/en

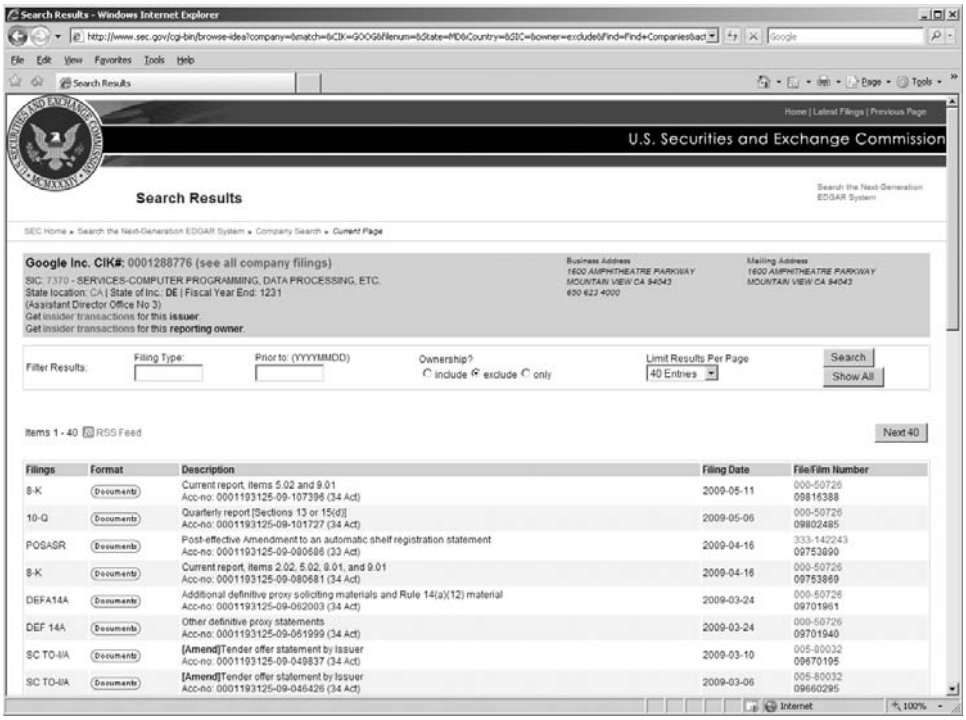


FIGURE 1.1

Google Inc. on sec.gov

Table 1.1 OSI Model

Data Unit	Layer	Function
Data	7. Application	Network process to application
	6. Presentation	Data representation and encryption
	5. Session	Interhost communication
Segment	4. Transport	End-to-end connections and reliability
Packet	3. Network	Path determination and logical addressing
Frame	2. Data Link	Physical addressing
Bit	1. Physical	Media, signal, and binary transmission

needed by applications above it, while it calls the next lower layer to send and receive packets that make up the contents of the path. Conceptually, two instances at one layer are connected by a horizontal protocol connection on that layer.

So let's go down through the scenario of what can take place when an attacker has chosen his target and starts the first methodology, which is recon. Let's review the first part of the scenario discussed in the prologue of the book. The target that was chosen is not the ultimate goal but a means to an end. When larger companies buy smaller companies, they tend to also assume the risk with those networks. Attackers are not always going to go through the front door of the victim company, especially when it is easier to find a back door created by acquiring a smaller company and creating a quick trust relationship with it.

So the first thing an attacker does after he identifies his target is to search all public filings and local newspaper articles that involve them. The sec.gov Web site and googling the local news sites are ideal for this. The company targeted is one going through layoffs or a merger with a bigger entity, or smaller one as in our scenario, by a major.gov contractor who has a well-defended perimeter but after acquiring a smaller specialized company exposes themselves to weakness by creating the extranet into their network. While this did help the business units make the transition more effective, it added unneeded risk into their environment. I am sure that in the real world the extranet would be better monitored and more restricted as to where and whom from the smaller company would be able to access data while connected to the contractor network. Now that we know of the new acquisition, it is time to start finding out about the people who work there. Doing a simple search in Google for "@3dnf.com" brings up all the places on the Internet that have been cached that contain e-mail addresses of employees who have posted or otherwise registered on a Web site with their work e-mail address. Other searches would be for the domain name and mail exchanger records to see where they are used as well. Another prime location to search is the company Web site's contact page and employment opportunities. This not only gives you some names and e-mails to work with, but if there are any IT jobs posted they may give an insight into what kind of internal environment they are running. Other types of tools to help with information gathering would be Web sites such as netcraft, Sam Spade, and dnsstuff.com. These Web sites help you find out what other domains or IP addresses might be useful to an attacker. Once again, when doing recon there is no such thing as enough information; the more information you discover, the more easy it is to find a way into your target.

FICTIONAL STORY DISSECTED: U.S. Securities and Exchange Commission

> He had some information about a small firm in Houston, Texas called 3DNF, Inc. that had been acquired by Data Mining within the last six months. Vlad found some links from the U.S. Securities and Exchange Commission's Web site and the text from a press release about the acquisition (p. 9).

FIGURE 1.2

Google Inc.'s address and phone number

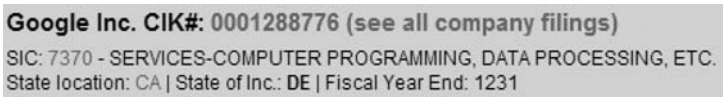


FIGURE 1.3

Google Inc.'s financial details

Stepan uses http://www.sec.gov to find out more information about 3DNF, Inc. by searching through the EDGAR system provided by the U.S. Securities and Exchange Commission's Web site. This site is a very powerful tool in researching public and private businesses who file their financials each quarter and each year. To demonstrate how easy it is to find certain information that can help collect information during the recon stage, Figure 1.1 shows Google Inc.'s information. In Figure 1.2, Google Inc.'s physical address and phone number are listed along with its mailing address. This information is very useful to someone like Vlad who can now fly to California and look for potential employees who work at Google to target one of them for more information. Vlad also has an upper hand through obtaining Google's phone number. He can start conducting social engineering probes by paying some college students from the local area to call Google's number and ask some more probing questions like, "What are the working hours for Google employees?" What if you had Google's CIK number? Well, with a CIK number you can find out many things, for example, who the stockholders and owners are of that company. In Figure 1.3 sec.gov provides the CIK number for Google and also other helpful facts. For instance, the kind of company Google is (SIC: 7370—Services-Computer Programming, Data Processing, etc.), the location (CA), where Google was incorporated (DE), and its fiscal year end (12-month calendar ending 31 December each year). With such information, you can arrive at what Figure 1.4 is showing, ownership data. Vlad did not do anything illegal when he found information on 3DNF's acquisition with Data Mining from sec.gov, but what he used the information for was illegal. The U.S. Securities and Exchange Commission's Web site is a very powerful tool in the art of recon.

FICTIONAL STORY DISSECTED: Harvesting Addresses

> Then Stepan had listed some names and e-mail addresses that belonged to the 3dnf.com domain. Vlad could only guess that Stepan had "googled" the domain name to harvest the addresses. If so, Stepan was a fairly resourceful researcher (p. 10).

Ownership Reports from: (Click on owner name to see other issuer holdings for the owner, or CIK for owner filings.)

Ownership Data	Filings	Type of Owner
AMERICA ONLINE INC	0000883780	10 percent owner
YAHOO INC	0001011006	other: See remarks
DOERR L JOHN	0001032455	director
TIME WARNER INC	0001105705	10 percent owner
REYES GEORGE	0001184217	officer: Chief Financial Officer
OTELLINI PAUL S	0001188930	director
HENNESSY JOHN L	0001198046	director
MORITZ MICHAEL J	0001201045	director
LEVINSON ARTHUR D	0001214128	director
SCHMIDT ERIC E	0001242463	director, officer: CEO, Chairman
MATHER ANN	0001244892	director
PICHETTE PATRICK	0001275968	officer: SVP & Chief Financial Officer
Kordestani Omid	0001294397	officer: SVP, World Wide Sales/Oper.
Rosenberg Jonathan J	0001295029	officer: VP Prod. Mgmt.
Drummond David C	0001295030	officer: VP, Gen. Counsel, Secty
Brown Shona L	0001295031	officer: VP Business Oper.
Brin Sergey	0001295032	director, 10 percent owner, officer: President, Tech, Asst. Secty
Shriram Kavitark Ram	0001295084	director
Rosing Wayne	0001295085	officer: VP Engineering
Page Lawrence	0001295231	director, 10 percent owner, officer: Pres, Products, Asst. Secty
Eustace Robert Alan	0001323010	officer: Vice President of Engineering
Tilghman Shirley M	0001340514	director

FIGURE 1.4

Google Inc.'s owners

Stepan is smart because he realizes that using a free service like Google can allow him to harvest millions of e-mail addresses, and then, if he wants, he can drill down even more specifically to certain e-mail addresses he might want to pay more attention to. How did he do it? Well, Stepan used a string of text in the Google search bar that might have looked like this: ***mail *3dnf.com filetype:xls**, as Figure 1.5 shows.

The first word "*mail" specifies that you are looking for mail with an asterisk (*) allowing that word to be proceeded by anything. The next word "*3dnf.com" tells Google what domain you want to find e-mail addresses in. And last, the "filetype:xls" only searches for files with an .xls extension, which means Microsoft Excel spreadsheet files. Figure 1.6 shows that Google has searched for e-mail addresses within the U.S. Department of Veterans Affairs (va.gov) domain. Figure 1.6 also shows that there are 15,700 results for spreadsheets within the va.gov domain. Figure 1.7 shows the contents of just one of the 15,700 spreadsheets. Over 80 e-mail addresses have been found by just one click of the mouse using Google. This is recon, and this is how people like Stepan find their targets.

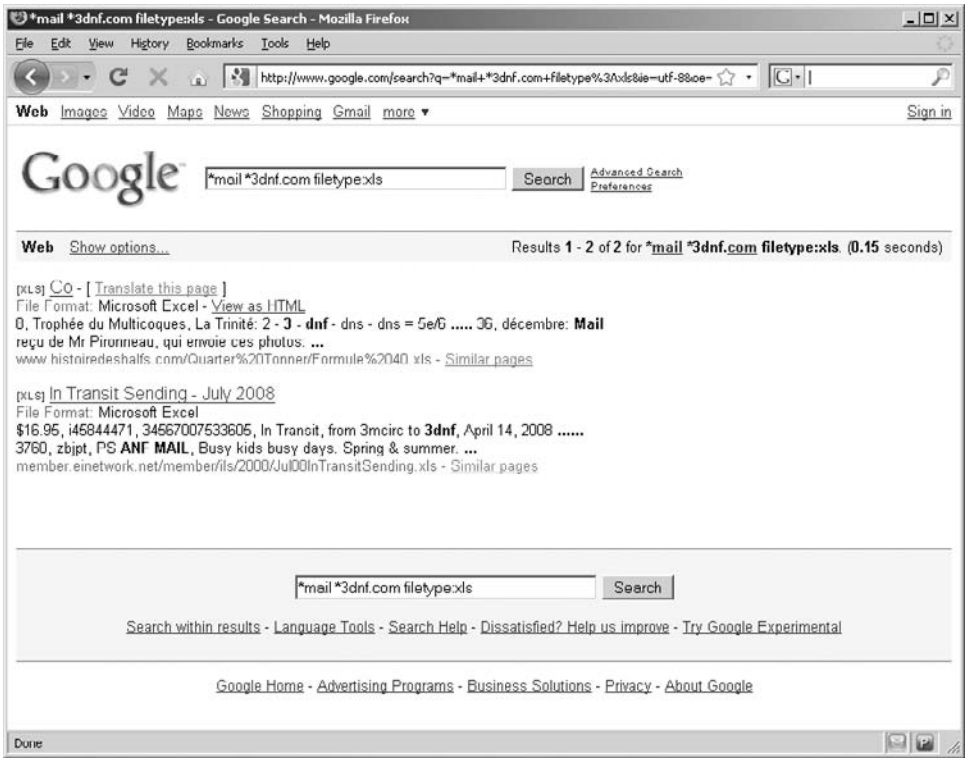


FIGURE 1.5

Stepan using Google to find 3DNF e-mail addresses

PUBLIC RECORD ON TAP: Real-Time E-mail Harvesting

Real-Time E-mail Harvesting on Twitter: Careless users unwillingly maintain an up-to-date list of e-mail addresses

By Lucian Constantin, Web News Editor, May 14, 2009, 10:21 GMT

Just one day after a method of harvesting e-mails from Twitter was exposed on WebProNews, a proof-of-concept Twitter e-mail grabber was released. The technique relies on using the service's real-time search function to exploit the carelessness of users who post their addresses in status updates.

There is nothing new about the fact that spammers and e-mail marketers are using automated tools to locate e-mail addresses through Google, Yahoo! and other search engines. Some are also employing their own custom-coded robots that crawl the web specifically for this purpose. Such programs are called e-mail harvesters or grabbers and the action e-mail harvesting.

So, why would Twitter be any different in this respect? As it turns out, it is and it isn't. It is, because someone posting their e-mail address within their messages automatically makes it

searchable, just like people posting it on their websites make it available on Google. This might seem obvious to many of you, but, judging by the feedback received on the issue, even knowledgeable users have overlooked this simple fact.

To read more visit: http://news.softpedia.com/news/Real-time-E-mail-Harvesting-on-Twitter-111609.shtml

MALTEGO

Maltego is an open source intelligence and forensics application. It allows for the mining and gathering of information as well as the representation of this information in a meaningful way. Maltego is also featured in BackTrack 4.[3] Figure 1.8 is a screen shot of this tool, and the Web site is http://www.paterva.com/maltego/.

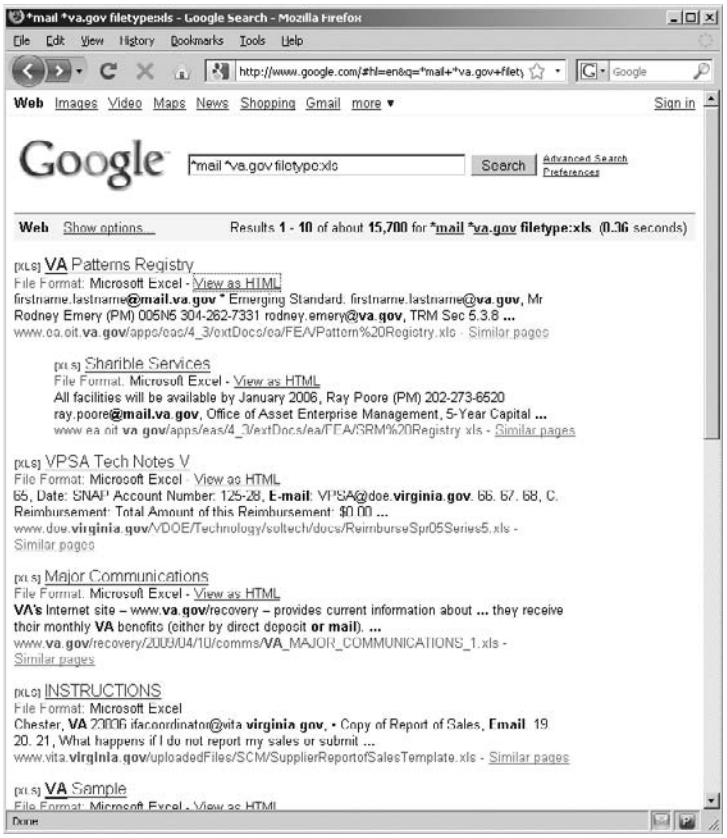


FIGURE 1.6

Google e-mail harvesting using "*mail *va.gov filetype:xls"

[3]http://www.remote-exploit.org/news.html

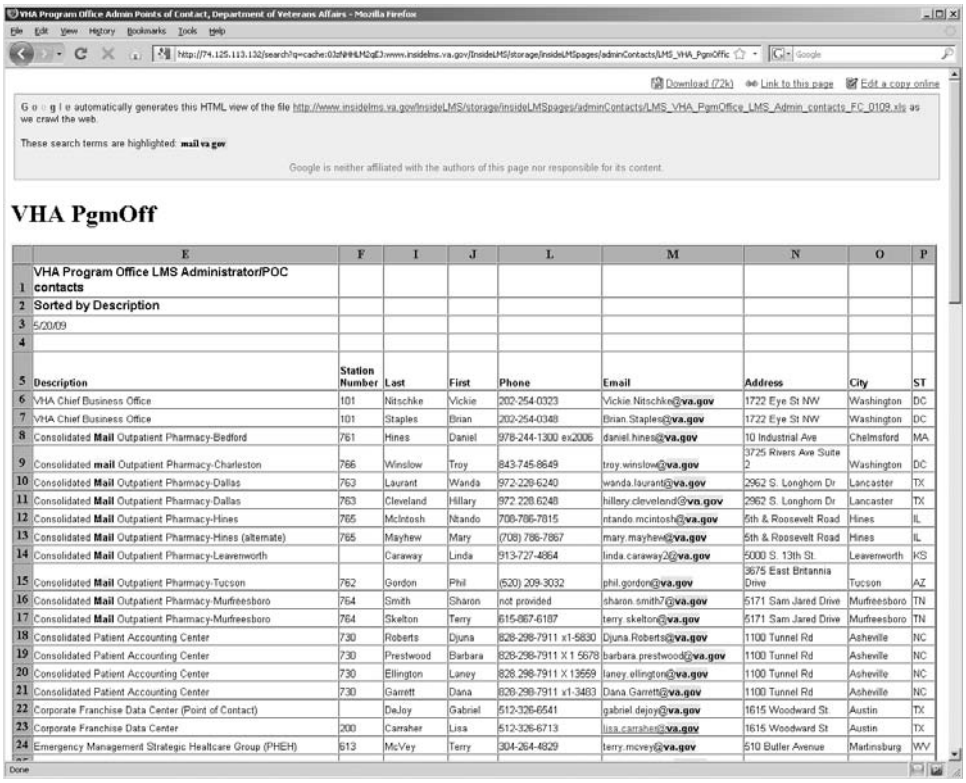


FIGURE 1.7

Spreadsheet with va.gov e-mail addresses and much more

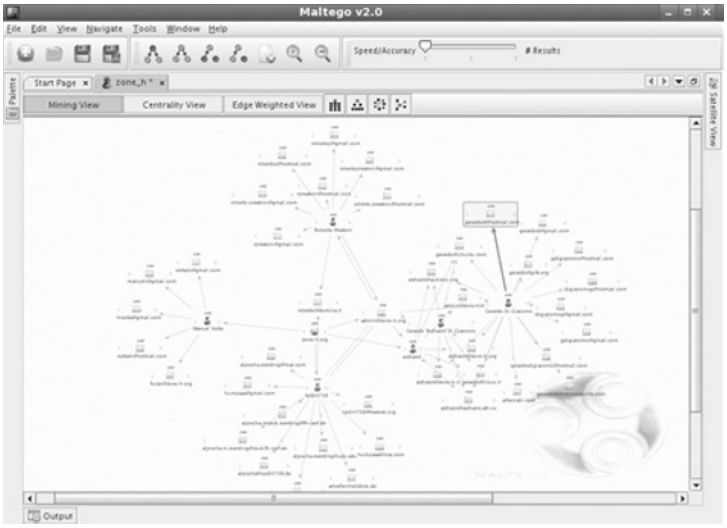


FIGURE 1.8

Maltego

GOOGLE

You can do Google search scripts from the command line with BackTrack,[4] a bootable operating system for penetration testing. You can also use the Google site for low-level scans where speed is not a necessity. This negates the need for an application programming interface (API). It also anonymizes your activity. This can't be defended or detected because you are relying on a third-party resource.

The Google search engine is fine, but just as MSN, Yahoo!, etc., it is a crawler or a automatic indexer, and "skimming" the web it returns search results based on popularity, etc.—point being, there are other or better search engines that would touch or query the actual servers and services that are "storing" the data; this is also known as the deep-web search or query. There is much publicly available information on the Internet, and a number of not very popular (in terms of public knowledge) deep-web query engines are available. One of these search engines is the http://www.pipl.com – you should see the difference in terms of company, entity, people, and e-mail address query results.

Also, another trick of the trade is this: ensure you have the right plug-ins for your browser of choice. In Google, once you've conducted a query, it will display multiple links in the search results page. At the "recon" stage, a potential attacker would never click on the actual link that would take him to the target. Instead, with java, active-x, and other executables disabled on his browser, the "cached" link would be selected to visit a cached page. It is critical at this stage to ensure all the executable options on the recon browser are disabled to completely "mask" the identity of who, what, and where the request is originating from. Although the page may be cached, any java or other executables (the coding) embedded on that cached page will reach out and grab the most current content to be displayed, i.e., exposing recon browser's identifying information.

NETCRAFT

Netcraft is an Internet services company based in Bath, England. Netcraft provides phishing and security, Internet data mining, Internet exploration, performance, and advertising services. One of its greatest services is something called "What's the site running?" This service allows anyone to type in a Web site and find out what the site is running along with other recon data like the last time the server was rebooted, the IP address, date the site was seen first on the Internet, who registered the domain, hosting history, and other various computer networking information. Figure 1.9 has an example of what this tool can provide using http://www.google.com as an example. To find out more, visit http://news.netcraft.com/.

[4]http://www.remote-exploit.org/backtrack.html

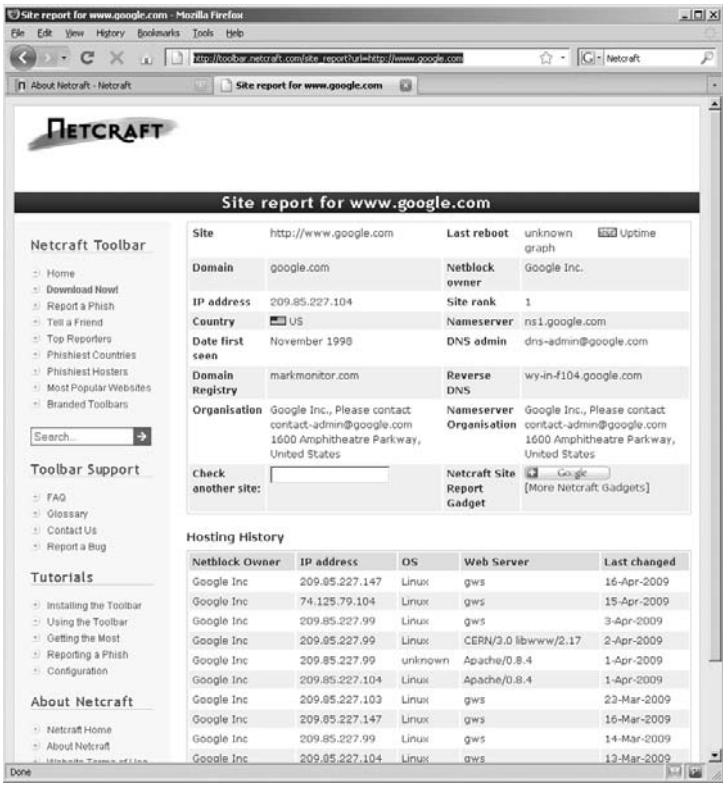


FIGURE 1.9

Netcrafting Google.com

SAM SPADE

Sam Spade is a network querying tool used to collect information on remote computers. Sam Spade provides the following features highlighted in the "Public Record on Tap." Figure 1.10 is a screen shot of this program.

PUBLIC RECORD ON TAP: Sam Spade

Sam Spade includes many different options. Below are some of those options.

Ping: Pings a network host to see if it's alive and to see how long it takes packets to get there and back.

Nslookup: Finds the IP address from a hostname, or vice-versa.

Whois: Asks a whois server who owns a domain name. Sam Spade will usually ask the right whois server automatically, or you can query a particular server. Whois queries for .com/.net/.org addresses are directed to the correct registrar automatically.

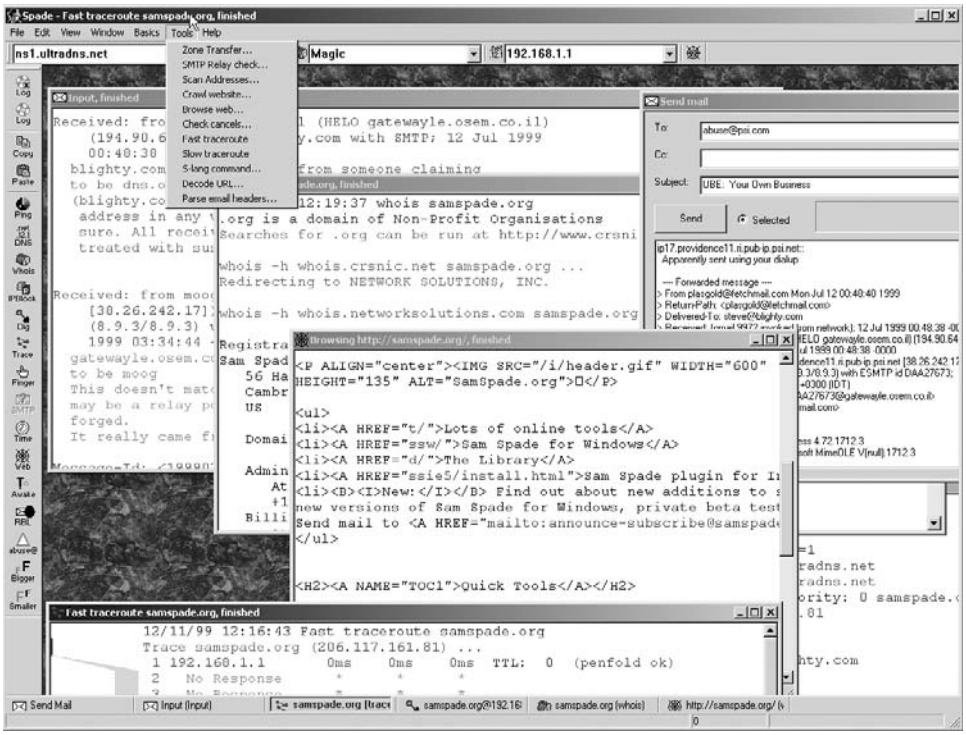


FIGURE 1.10

Sam Spade

IP block whois: Asks a whois server who owns a block of IP addresses.

Dig: A more advanced DNS query tool. Dig asks a DNS server for all the information it has about a host.

Traceroute: Finds the route packets take between you and a remote system. Both a slow, step-by-step mode and a fast parallel query mode are available.

Finger: Lookups user information on a remote Unix system.

SMTP VRFY: Asks a mail server whether an e-mail address is real and whether it's being forwarded to other addresses. Also attempt partial delivery to a range of addresses to discover whether a given address is valid or not.

Web browser: Browses the web, viewing the raw HTTP traffic rather than the rendered HTML. This lets you see the http headers and the raw HTML. Very handy for debugging CGI scripts.

It will not send any identifying information to the web server, and by not supporting file download, java, java script, cookies or anything else, it has far fewer security holes than real browsers. As it doesn't render the HTML, it makes attempts to hide information

(such as hidden form fields, white-on-white text, meta fields, etc.) obvious. These make it a useful tool for investigating malign Web sites.

Keep-alive: This sends http packets to your ISPs web server every minute or so, to keep a dial-up link active.

DNS zone transfer: This asks a DNS server for all the information it has about a domain. It automatically finds the authoritative servers for a domain and will query one or all of them.

SMTP relay check: This checks whether a mail server is secure. It attempts to send e-mail back to yourself via somebody else's e-mail server (one which you're not supposed to have access to). Hopefully, it'll fail, but if it doesn't the mail server is open to all sorts of abuse, and the administrator needs to secure it.

Usenet cancel check: This asks your local news server to look for cancelled messages in a set of groups.

Web site download: This will copy a Web site to disk.

Web site search: This searches a Web site for anything matching a list of patterns.

E-mail header analysis: This will check the received lines in an e-mail header for consistency. It can help in tracking down the true source of forged e-mail.

Blacklist lookups: This will check the Real-time Blackhole List, Dialup User List, and Relayed Spam Source List to see if any of a hosts addresses are listed.

Abuse.net query: This will identify the e-mail address responsible for abuse issues at a given domain using the database maintained by abuse.net.

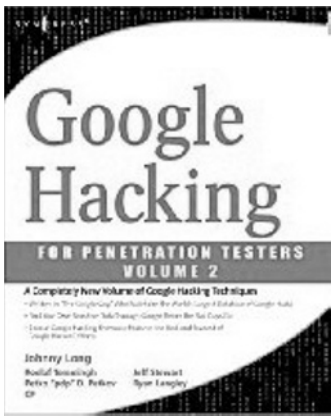
S-Lang scripting: Many features can be configured and scripted using the embedded S-Lang scripting language.

Time: This will query a remote host to see what time it thinks it is, via a range of protocols including SNTP. Optionally set the local systems time via SNTP at each application startup. To read more, visit http://preview.samSpade.org/ssw/.

DNSPREDICT

This PERL script, by Jimmy Neutron, is great for determining DNS names with Google. This tool, which is essential for network mapping, accepts two somewhat related words and a domain name as arguments. The two words are sent through Google sets which expand the words into a list of related words. For example, "Earth" and "Mars" would expand to Venus, Mercury, Jupiter, Saturn, Neptune, Uranus, and Pluto. If fed domain foo.com, dnspredict would then attempt to DNS resolve venus.foo.com, mercury.foo.com, etc. This Windows version is standalone, and requires nothing other than this executable. For more information, visit http://johnny.ihackstuff.com/downloads/task,cat_view/gid,16/limit,5/limitstart,0/order,name/dir,ASC/.

BOOKS



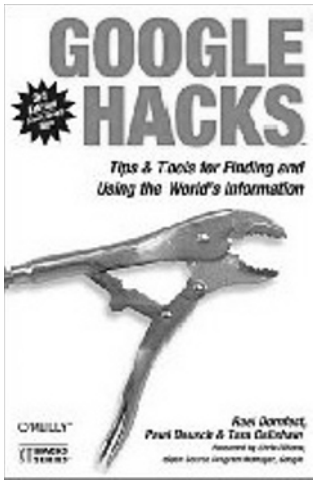
Google Hacking for Penetration Testers Vol. 2

By Johnny Long

Publisher: Syngress

ISBN-10: 1597491764

ISBN-13: 978-1597491761



Google Hacks: Tips & Tools for Finding and Using the World's Information

By Rael Dornfest, Paul Bausch, and Tara Calishai

Publisher: O'Reilly Media, Inc.

ISBN-10: 0596527063

ISBN-13: 978-0596527068

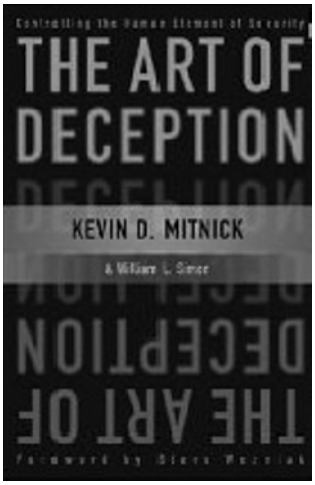
No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing

By Johnny Long, Jack Wiles, Scott Pinzon, and Kevin D. Mitnick.

Publisher: Syngress

ISBN-10: 1597492159

ISBN-13: 978-1597492157



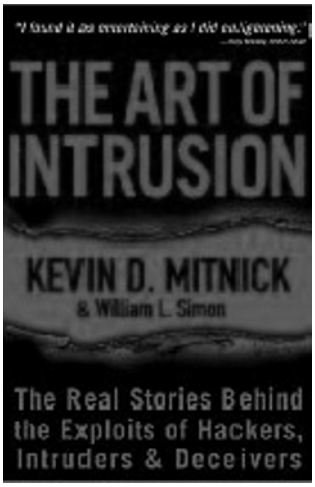
The Art of Deception: Controlling the Human Element of Security

By Kevin D. Mitnick, William L. Simon, and Steve Wozniak

Publisher: Wiley

ISBN-10: 076454280X

ISBN-13: 978-0764542800



The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers

By Kevin D. Mitnick and William L. Simon

Publisher: Wiley

ISBN-10: 0471782661

ISBN-13: 978-0471782667

CHAPTER

Scanning

2

In the first STAR chapter, we discussed recon, also known as reconnaissance or footprinting. In this chapter, we discuss the next stage in the hacker methodology: scanning. Collecting all the information in the recon stage will help Vlad and Pavel prepare to scan real targets to find out if they are alive.

Scanning is the step when attackers begin to take risks of their own. They move from quiet observation of targets to actual probing for weaknesses. This is also the first opportunity a target has to identify the precursor of an attack. If done correctly, an attacker can complete the probes without detection, and a defender will make it very difficult for a probe to return accurate information.

FICTIONAL STORY DISSECTED: Kismet

> I don't know yet. Let me look with Kismet (p. 39).

Bob and Leon are using two different programs to scan wireless network access points. These access points can be analyzed to determine if they are open to connecting to them from their laptops without using a password. Figure 2.1 shows a picture of what Kismet looks like after you have scanned a specific radio frequency looking for wireless access points. This figure also shows the name of the wireless network and how much traffic is passing through. Sometimes, Kismet will also figure out the Internet Protocol (IP) address associated with access points and even the access point's client(s).

Kismet is a network detector, packet sniffer, and intrusion detection system (IDS) for 802.11 wireless local area networks (LANs). Kismet will work with any wireless card that supports raw monitoring mode and can sniff 802.11a, 802.11b, and 802.11g traffic. The program runs under Linux, FreeBSD, NetBSD, OpenBSD, and Mac OS X. The client can also run on Windows, although, aside from external drones, there's only one supported wireless hardware device available as packet source. Distributed under the GNU General Public License,[1] Kismet is a free software.

[1] http://www.kismetwireless.net/documentation.shtml

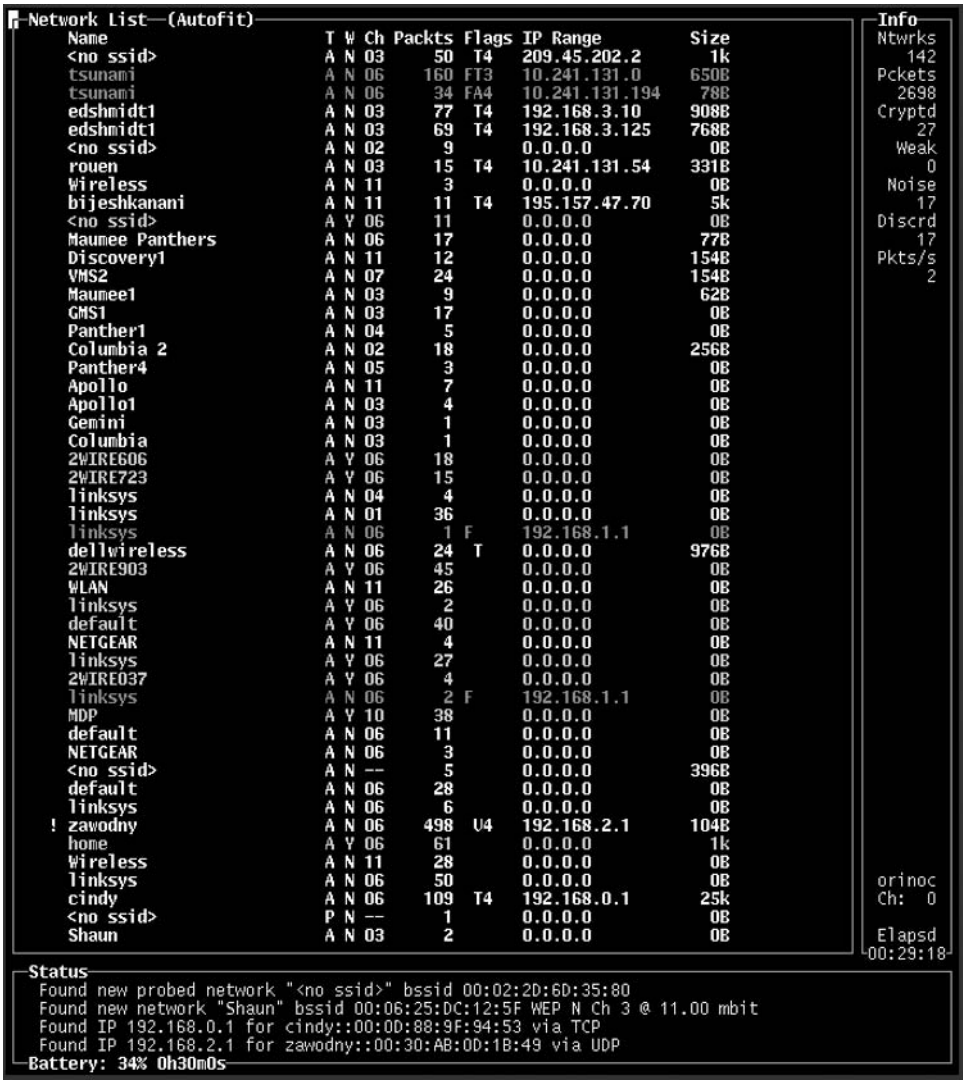


FIGURE 2.1

Kismet

Kismet is unlike most other wireless network detectors in that it works passively. This means that without sending any loggable packets, it is able to detect the presence of both wireless access points and wireless clients and associate them with each other.

Kismet also includes basic wireless IDS features such as detecting active wireless sniffing programs including NetStumbler, as well as a number of wireless network attacks. Kismet has the capability to log all sniffed packets and save them in a

tcpdump/Wireshark or Airsnort compatible file format. To find as many networks as possible, Kismet supports channel hopping. This means that it constantly changes from channel to channel nonsequentially, in a user-defined sequence with a default value that leaves big holes between channels (e.g., 1-6-11-2-7-12-3-8-13-4-9-14-5-10). The advantage with this method is that it will capture more packets because adjacent channels overlap. Kismet also supports logging of the geographical coordinates of the network if the input from a global positioning system (GPS) receiver is additionally available. See Figure 2.2 for a screen shot of this functionality.

NetStumbler, also known as Network Stumbler, is a tool for Windows that facilitates detection of wireless LANs (WLAN) using the 802.11b, 802.11a, and 802.11g WLAN standards. Figure 2.3 has a screen shot of this program after it detected some wireless devices. It runs on Microsoft Windows operating systems from Windows 2000 to Windows XP. A trimmed-down version called MiniStumbler is available for the handheld Windows CE operating system.

FIGURE 2.2

Kismet with GPS

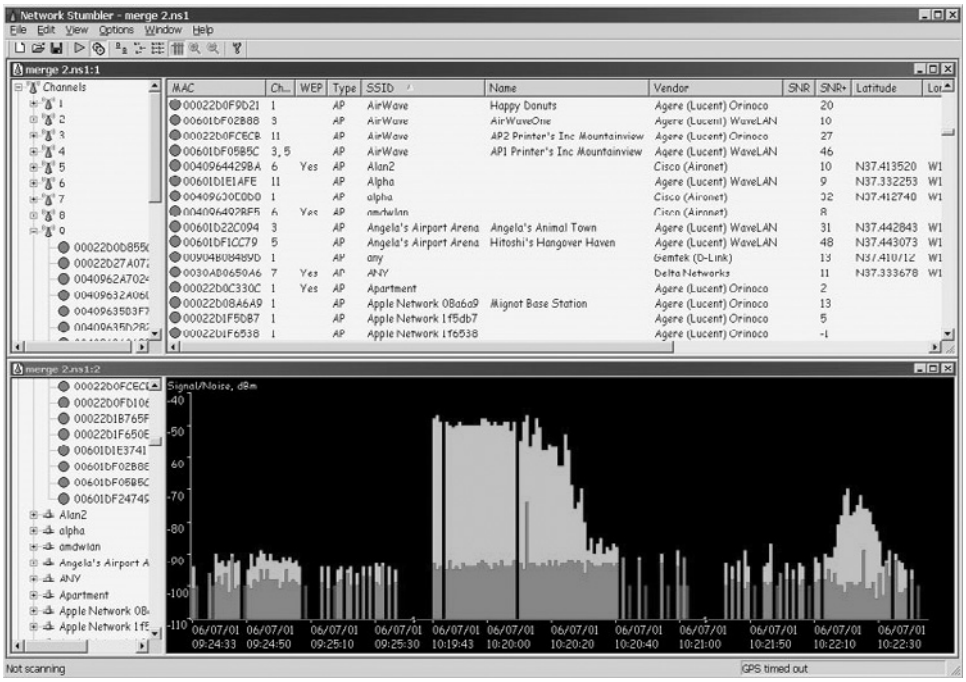


FIGURE 2.3

NetStumbler

NetStumbler is commonly used for wardriving, verifying network configurations, finding locations with poor coverage in a WLAN, detecting causes of wireless interference, detecting unauthorized ("rogue") access points, and aiming directional antennas for long-haul WLAN links. NetStumbler's author, Marius Milner, maintains the occasionally updated http://stumbler.net Web site where you can download the software. Another Web site, http://netstumbler.com, offers more frequently updated information and wireless news.

FICTIONAL STORY DISSECTED: SuperScan 4

> Bob went back to his "T00Lz" folder and clicked on the SuperScan icon (p. 40).

Here, Bob uses a scanning program to find out what kinds of services are running on the computers in the 3DNF network. SuperScan is a very easy-to-use tool for finding out computer's activities on a network. Bob and Leon both know that by scanning a network they are actively sending information into the 3DNF network which anyone who's looking in the right places can see. Soon Pavel and Vlad are tipped off by their scanning because they, too, are analyzing the network.

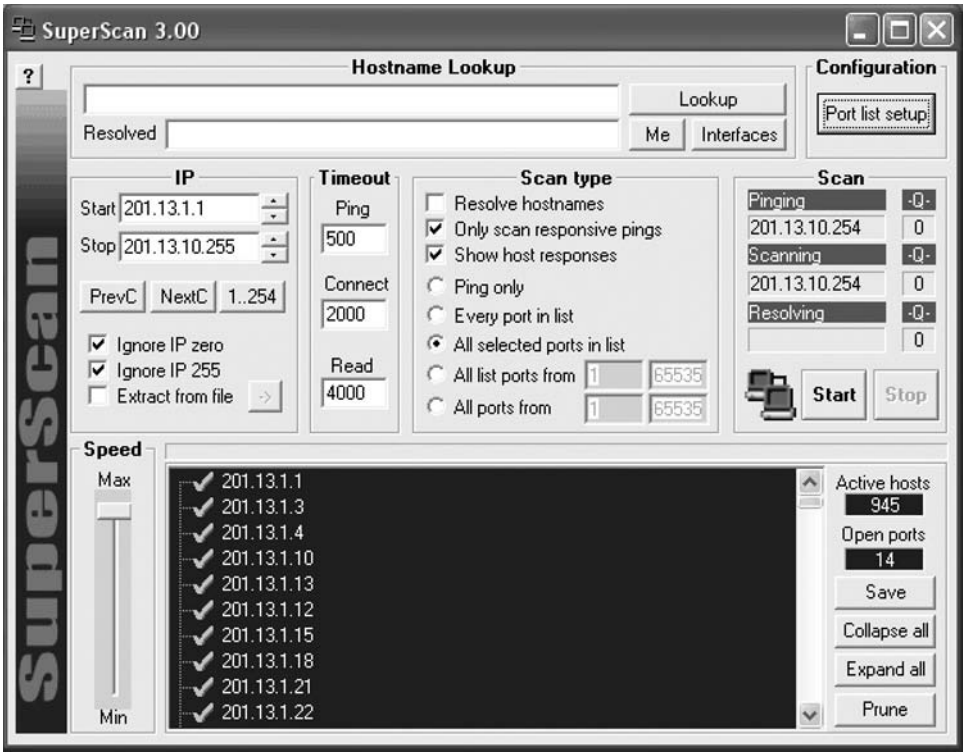


FIGURE 2.4

SuperScan 3

SuperScan is a free connect-based port scanning software designed to detect open Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports on a target computer, determine which services are running on those ports, and run queries such as whois, ping, Internet Control Message Protocol (ICMP) traceroute, and Hostname lookups.[2] SuperScan 4, which is a completely rewritten update of the software, features windows enumeration, which can list a variety of important information dealing with Microsoft Windows, such as NetBIOS information, user and group accounts, network shares, trusted domains, and services, which are either running or stopped. SuperScan is a tool used by system administrators, crackers (the malicious hacker with unlawful intentions), and script kiddies (also malicious, this is the derogative term for nonexpert-level hackers) to evaluate a computer's security. System administrators can use it to test for possible unauthorized open ports on their computer networks, whereas crackers use it to scan for a potentially insecure port to gain illegal access to a system. SuperScan is produced by Foundstone, a division of McAfee. Figure 2.4 is a screen shot for SuperScan 3 and Figure 2.5 is a screen shot of SuperScan 4.

[2]http://www.foundstone.com/us/resources/proddesc/superscan4.htm

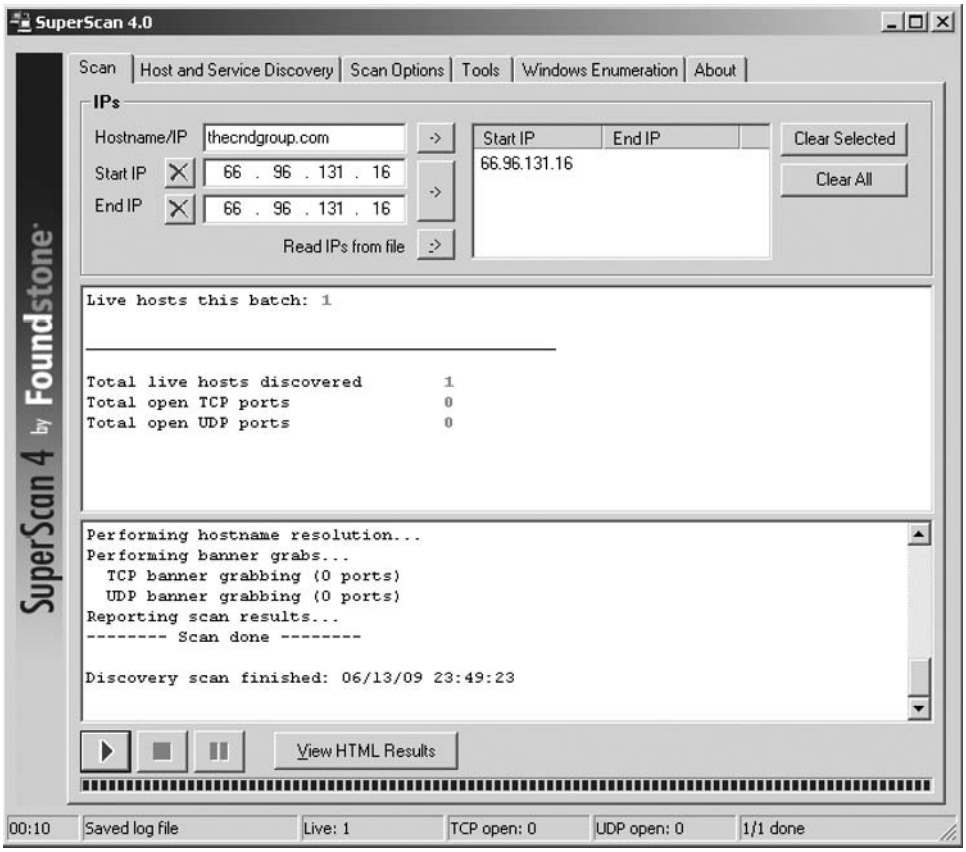


FIGURE 2.5

SuperScan 4

FICTIONAL STORY DISSECTED: Nmap

> A few quick clicks and he had browsed through a menu and launched his copy of Nmap (p. 42).

Nmap (Network Mapper) is a free security scanner originally written by Gordon Lyon (also known by his pseudonym Fyodor Vaskovich).[3] Nmap is a Network Mapper used to discover computers and services on a computer network, thus creating a "map" of the network. Just like many simple port scanners, Nmap is capable of discovering passive services on a network despite the fact that such services aren't advertising

[3]http://news.bbc.co.uk/2/hi/technology/3039329.stm

themselves with a service discovery protocol. In addition, Nmap may be able to determine various details about the remote computers. These include operating system, device type, uptime, software product used to run a service, exact version number of that product, presence of some firewall techniques and, on a LAN, even vendor of the remote network card. Nmap runs on Linux, Microsoft Windows, Solaris, and BSD (including Mac OS X), and also on AmigaOS.[4] Linux is the most popular Nmap platform and Windows the second most popular.[5]

PUBLIC RECORD ON TAP: The Matrix and Nmap

Matrix mixes life and hacking

Reloaded may be wooing some of its audience with its gung-ho gunplay and ferocious special effects, but one group of fans are impressed for entirely different reasons.

The web's hacking community has been impressed by the film's depiction of a hack attempt that uses future versions of tools and techniques widely used now. Net-based message boards have been buzzing with mentions of the realistic depiction and photos of the hacking scenes from the film are being passed around the web. The successful hack attack is carried out by Trinity, played by Carrie-Anne Moss, on a power company computer toward the end of the film.

To read more, visit http://news.bbc.co.uk/2/hi/technology/3039329.stm

PARATRACE

Paratrace traces the path between a client and a server, much like "traceroute," but with a major twist: rather than iterate the TTLs of UDP, ICMP, or even TCP SYN packets, paratrace attaches itself to an existing, stateful-firewall-approved TCP flow, statelessly releasing as many TCP Keepalive messages as the software estimates the remote host is hop-distant. The resultant ICMP Time Exceeded replies are analyzed, with their original hopcount "tattooed" in the IPID field copied into the returned packets by so many helpful routers. Through this process, paratrace can trace a route without modulating a single byte of TCP/Layer 4, and thus delivers fully valid (if occasionally redundant) segments at Layer 4. Visit their Web site to learn more: http://linux.die.net/man/1/paratrace.

[4] http://nmap.org/download.html
[5] http://nmap.org/install/inst-windows.html

SCANRAND

Scanrand is a proof of concept, investigating stateless manipulation of the TCP Finite State Machine. Figure 2.6 is a screen shot of this tool in action. It implements extremely fast and efficient port, host, and network trace scanning, and does so with two completely separate and disconnected processes; one that sends queries and the other that receives responses and reconstructs the original message from the returned content. Security is maintained, in the sense that false results are difficult to forge, by embedding a cryptographic signature in the outgoing requests that must be detected in any received response. HMAC-SHA1 (a keyed-Hash Message Authentication Code),[6] truncated to 32 bits, is used for this Inverse SYN Cookie. To learn more, visit http://linux.die.net/man/1/scanrand.

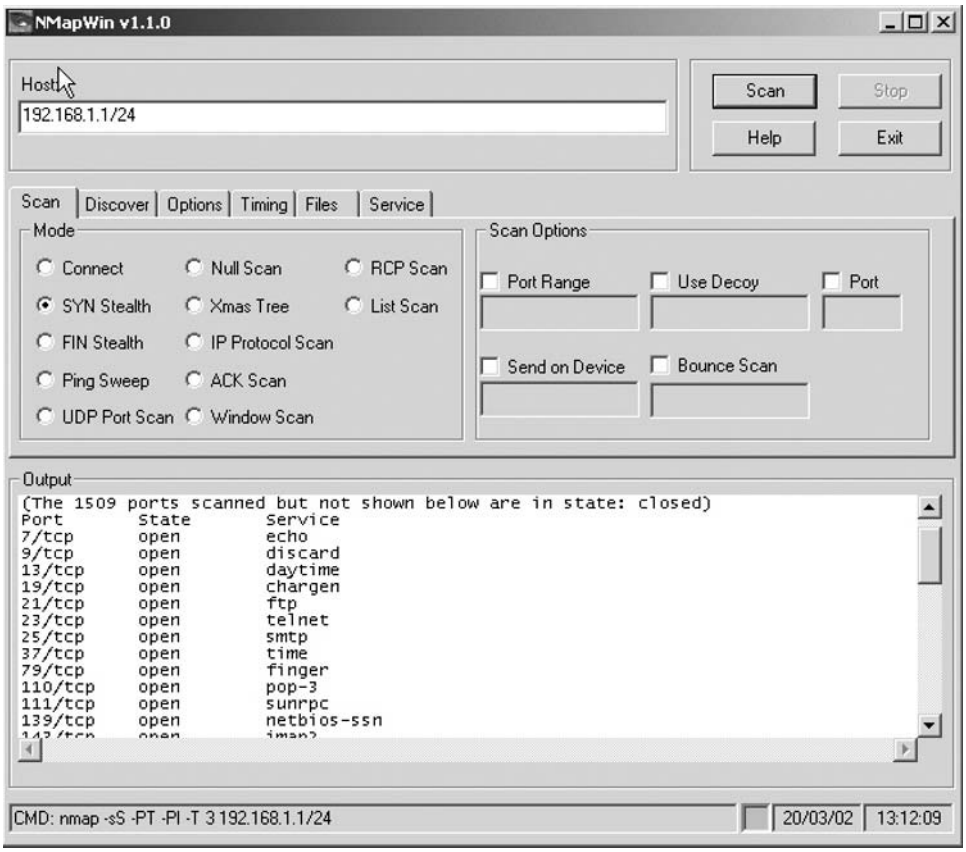


FIGURE 2.6

Nmap

[6]http://en.wikipedia.org/wiki/HMAC-SHA1

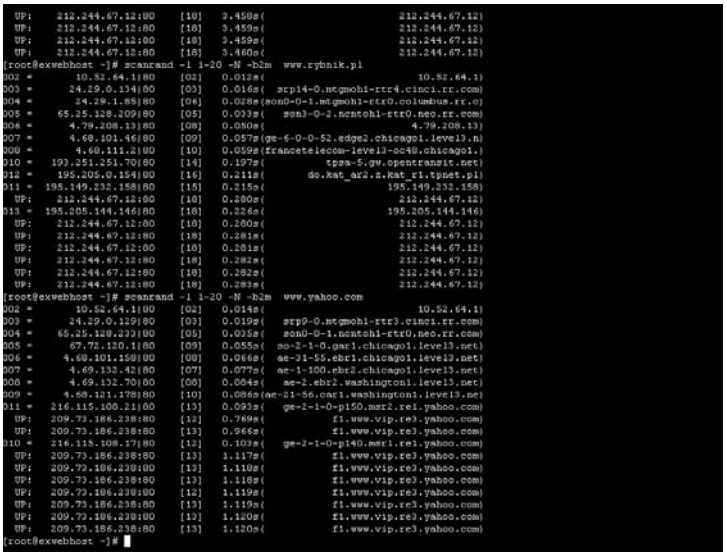


FIGURE 2.7

Scanrand

AMAP

Amap is a next-generation tool for assisting network penetration testing. It performs fast and reliable application protocol detection, independent of the TCP/UDP port they are being bound to. Visit Amap Web site to learn more: http://freeworld.thc.org/thc-amap/.

PUBLIC RECORD ON TAP: My Top 5 Fav Tools

This is a blog entry by Jimmy Ray Purser from the Network Sheriff Blog on The Cisco Learning Network, Posted May 14, 2009, 8:03:22 am

00×02. NMAP on Linux: Fyodor created a real gem here. Especially with the new and improved version 4.75. New OS detection sigs and graphic network mapping. NMAP is THE tool of choice for recon right behind observation. I love using NMAP in conjunction with AMAP. Hey, that is a perfect lead into to tool number three.

00×03. AMAP: This is a seriously awesome application mapper. AMAP uses the results from NMAP to mine for more info. This makes it nearly silent on the wire. To use AMAP correctly run NMAP with the following tag set:

nmap -sS -O oM target1rslts.nmap -oX target1rslts.xml -p l-65535 -v 172.16.4.88

(the -oX is a best practice and purely optional. It saves the results also in xml so I can use other xml tools to mine that data). Now just run AMAP with the following tag set:

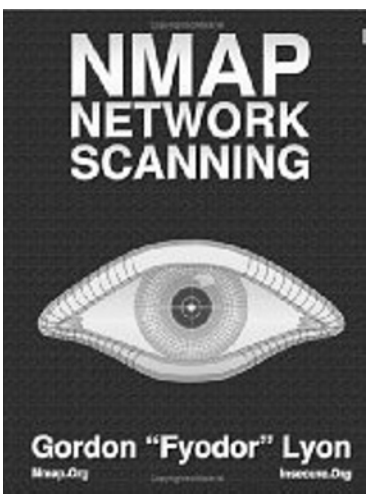
amap -i target1rslts.nmap -o target1rslts.amap -m

You will be amazed at what it finds!

00×04. Scanrand: All good target assessments start with a port scan. But where do you start? Scanning all 65535 ports will light off every IDS alarm from here to Madagascar plus it will seem longer then watching 8 mm home movies with your in laws. This is where scanrand comes in. This tool can scan all 65 K sockets with hits in around four seconds! scanrand is part of the Paketto Keiretsu tool set wrote by good ole Dan Kaminsky. Fantastic piece of code that works great! Inverse Syn Cookies rule!

00×05. ParaTrace: This is a toss up for me, but I have been using ParaTrace in my recon activities over the past few months. Nearly all networks have a firewall installed. How do I get beyond that and map the network behind it? ParaTrace is the answer! ParaTrace is what tracert dreams about becoming in it's sleep state. Basically, it listens for outbound connections leaving the network and quickly inserts a few TCP segments with an incrementing TTL value starting at 1, of course then all routers legally respond back along the path with ICMP TTL Exceeded…To read more, visit https://cisco.hosted.jivesoftware.com/blogs/network-sheriff/2009/05/14/my-top-5-fav-recon-tools.

BOOKS



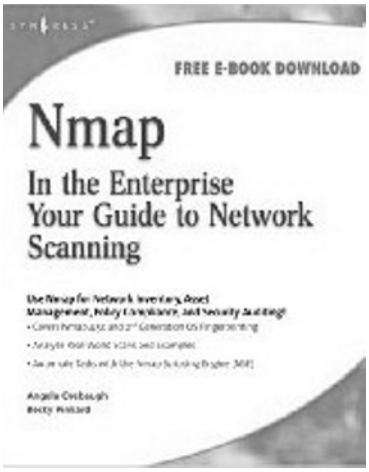
Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning

By Gordon "Fyodor" Lyon

Publisher: Nmap Project

ISBN-10: 0979958717

ISBN-13: 978-0979958717



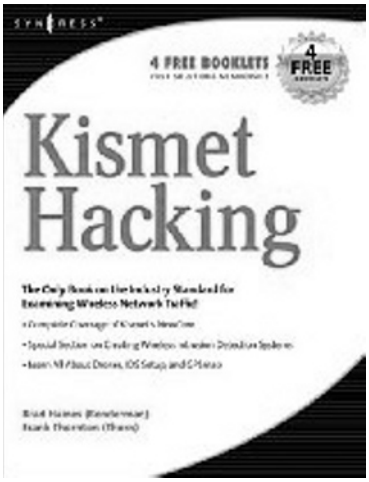
Nmap in the Enterprise: Your Guide to Network Scanning

By Angela Orebaugh and Becky Pinkard

Publisher: Syngress

ISBN-10: 1597492418

ISBN-13: 978-1597492416



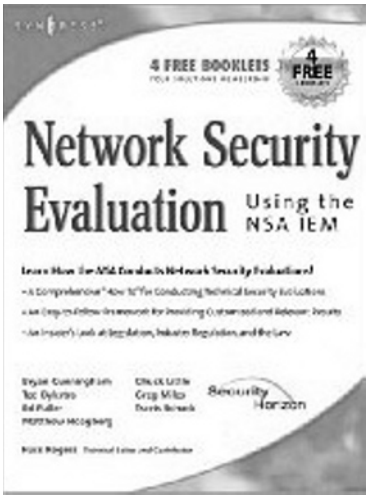
Kismet Hacking

By Brad Haines, Frank Thornton and Michael Schearer

Publisher: Syngress

ISBN-10: 1597491179

ISBN-13: 978-1597491174



Network Security Evaluation: Using the NSA IEM

By Russ Rogers, Ed Fuller, Greg Miles, Matthew Hoagberg, Travis Schack, Ted Dykstra, Bryan Cunningham, and Chuck Little

Publisher: Syngress

ISBN-10: 1597490350

ISBN-13: 978-1597490351

CHAPTER

Explore

3

Now the action has truly begun. If an attacker reaches this stage, then the defender has lost the initiative. The attacker begins to create an attack profile with the primary data collection completed in the prior steps. Exploring is the stage of refinement as initial probing turns to validation of attack vectors.

PLUG-IN

A plug-in (also known as plugin, addin, add-in, addon, add-on, snap-in or snapin, and extensions) consists of a computer program that interacts with a host application to provide a certain, usually very specific, function "on demand." A Web browser or an e-mail client would be considered as a host application. Applications support plug-ins for many reasons. Firefox plug-ins can be very powerful tools as Ravikanth's blog explains below in the "Public Record on Tap" section. Figure 3.1 shows a screen shot of a few of Firefox's add-ons.

PUBLIC RECORD ON TAP: Hacking Web 2.0 Applications with Firefox

Hacking Web 2.0 Applications with Firefox

By Shreeraj Shah

AJAX and interactive Web services form the backbone of "Web 2.0" applications. This technological transformation brings about new challenges for security professionals.

This article looks at some of the methods, tools, and tricks to dissect Web 2.0 applications (including AJAX) and discover security holes using Firefox and its plug-ins. The key learning objectives of this article are to understand the following:

1. Web 2.0 application architecture and its security concerns
2. Hacking challenges such as discovering hidden calls, crawling issues, and AJAX side logic discovery

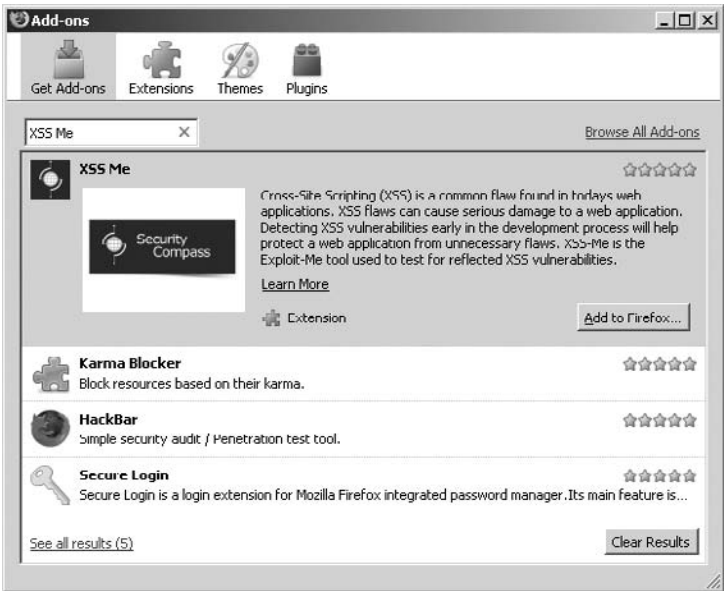


FIGURE 3.1

Firefox add-ons

3. Discovery of XHR calls with the FireBug tool
4. Simulation of browser event automation with the Chickenfoot plug-in
5. Debugging of applications from a security standpoint, using the FireBug debugger
6. Methodical approach to vulnerability detection

To read more, visit http://www.securityfocus.com/infocus/1879

PUBLIC RECORD ON TAP: Firefox Plug-ins for Security Professionals, by Chris Schmidt

Access Me

Although it doesn't find 90% of what it says it will, this plug-in can be somewhat useful for determining whether a server configuration is vulnerable to certain attacks that can be made with different request methods such as DELETE.

SQL Inject Me

I have seen this plug-in successfully detect several *easy-to-find* SQL Injection vulnerable form fields. But it doesn't really do a whole lot of checking beyond the simple obvious ones.

XSS Me
Of all of the Security Compass plug-ins, this one is by far the most useful and does most of what it says it will. However, just because the plug-in says a site is not vulnerable to XSS, it doesn't mean it truly isn't. This plugin, like SQL Inject Me, simply checks for the simplest XSS vectors.

Web Developer
Of every plug-in I use, I probably use the functionality of this one more than any other. This is an entire suite of tools aimed at assisting Web developers with things like local validation, src highlighting, form modifications, etc. That being said, the same functionality is invaluable to Web application hackers to break your forms, discover XSS vectors, and analyze your code for other problems.

FireBug
Like Web Developer, this plug-in was designed and built with the developer in mind. However, with enhanced JS debugging capabilities, and arguably the best DOM browser there is, this plug-in has single-handedly been responsible for more XSS powered CSRF exploits in my audits than every tool in my toolkit combined. This is a must-have.

Passive Recon
This is an entire suite of tools that allow you to pseudo anonymously get a pretty detailed domain recon report from a single click, or parts of that report individually. This can come in very handy when performing an audit on a site or app that you know very little about to begin with and often gives insight into the system and server architecture of the target that can prove invaluable to finding holes.

TorButton
If you haven't heard of TOR, you probably have no idea what I am talking about in most of the above plugins. While it is by no means perfect and can never replace a good proxy chain, TOR provides basic anonymization of your Internet traffic. This button allows you to switch in and out of TOR mode in Firefox with a single click.

FireCookie
FireCookie is actually an extension to the FireBug plug-in and thus requires that FireBug be running and installed. However, it provides a means to view and edit cookies in real-time.

Modify Headers
This plug-in can prove invaluable when used correctly, for everything from spoofing user-agent to spoofing client Internet Protocol (IP), this is a must-have for any hacker's toolbox.

Tamper Data
Like Modify Headers, the Tamper Data plug-in allows you to modify headers and cookies. The difference is, it does so on a per-request policy, meaning that if you are enumerating manually to isolate a bug, this plug-in will prove to be your best friend. I have broken many a Web service with this tool.

To read more, visit http://weblogs.asp.net/dvravikanth/archive/2009/04/14/firefox-plugins-for-security-professionals-by-schmidt-chris.aspx

VULNERABILITY SCANNERS

A vulnerability scanner is a computer program designed to search for and map systems for weaknesses in an application, a computer, or a network. Step 1: Typically the scanner will first look for active IP addresses, open ports, operating systems (OSs), and any applications running. Step 2: It may, at this point, create a report or move to the next step. Step 3: It will try to determine the patch level of the OS or applications. In this process, the scanner can cause an exploit of the vulnerability such as crash the OS or application. Step 4: The final phase—the scanner may attempt to exploit the vulnerability. Scanners may be either malicious or friendly. Friendly scanners usually stop at step 2 and occasionally at step 3, but never go to step 4.

INTERNET SECURITY SYSTEMS SCANNER

IBM Internet Security Systems is a security software provider, which was founded in 1994 as Internet Security Systems, and is often known simply as ISS or ISSX (after its former NASDAQ ticker symbol). Figure 3.2 shows its Web site. The company was acquired by IBM in 2006. In 1992, although attending the Georgia Institute of Technology, Christopher Klaus developed the first version of Internet Scanner. In 1994, Chris Klaus founded ISS to further develop and market Internet Scanner. Although the larger shareholder, Chris Klaus took the role of Chief Technology Officer, whereas Tom Noonan was recruited as Chief Executive Officer in 1995. In 1996, Bob Davoli from Sigma Partners leads the first round of venture capital investment in ISS. The initial public offering of the company on NASDAQ was on March 23, 1998.[1,2] Further products in security software space followed, including Network Sensor and Server Sensor which were both developed in-house. In 1998, ISS acquired the UK company March Information Systems and rebranded their Security Manager product as System Scanner. About the same time, ISS acquired the company DbSecure, founded by Eric Gonzales and Aaron C. Newman, to add a database security solution to their products. The DbSecure product was rebranded as Database Scanner. Subsequently, ISS acquired Network ICE and integrated their BlackICE technology into the ISS product range.[2]

In 2004, Chris Klaus stepped down from his role of Chief Technology Officer to pursue other interests, although he remained a significant shareholder and the company's Chief Security Advisor. His role as Chief Technology Officer was taken by Chris Rouland.[3] On August 23, 2006, IBM announced its intention to acquire ISS for $1.3 billion. On October 16, 2006, the deal was approved by ISS shareholders.[4,5]

[1]http://www.iss.net/about/index.html
[2]http://www.iss.net/about/timeline/index.html
[3]http://www.thechannelinsider.com/article2/0,1759,1609508,00.asp?kc=CZNKT03119TX1K0000596
[4]http://news.com.com/IBM+to+buy+ISS+for+1.3+billion/2100-7355_3-6108538.html
[5]http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9004169&source=rss_news50

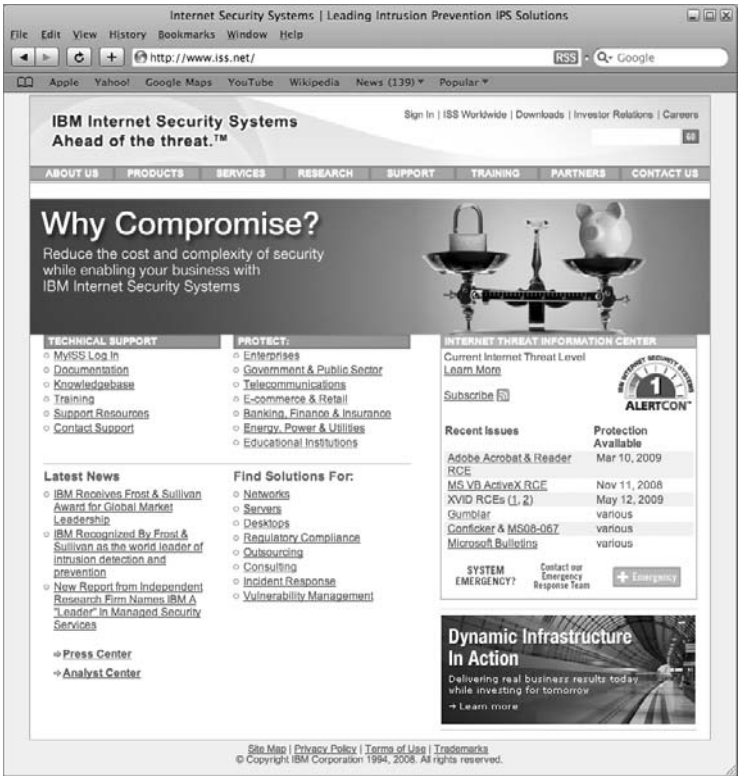


FIGURE 3.2

ISS Web site

NESSUS

In computer security, Nessus is proprietary comprehensive vulnerability scanning software. In Figure 3.3, you can check out the Nessus Web site. It is free of charge for personal use in a nonenterprise environment. Its goal is to detect potential vulnerabilities on the tested systems, for example, vulnerabilities that allow a remote cracker to control or access sensitive data on a system; misconfiguration (e.g., open mail relay, and missing patches); and default passwords, a few common passwords, and blank/absent passwords on some system accounts. Nessus can also call Hydra (an external tool) to launch a dictionary attack. Denials of service against the Transmission Control Protocol/IP stack by using mangled packets.

Unix (including Mac OS X) consists of nessusd, the Nessus daemon, which does the scanning, and Nessus, the client, which controls scans and presents the vulnerability results to the user. For Windows, Nessus 3 installs as an executable and

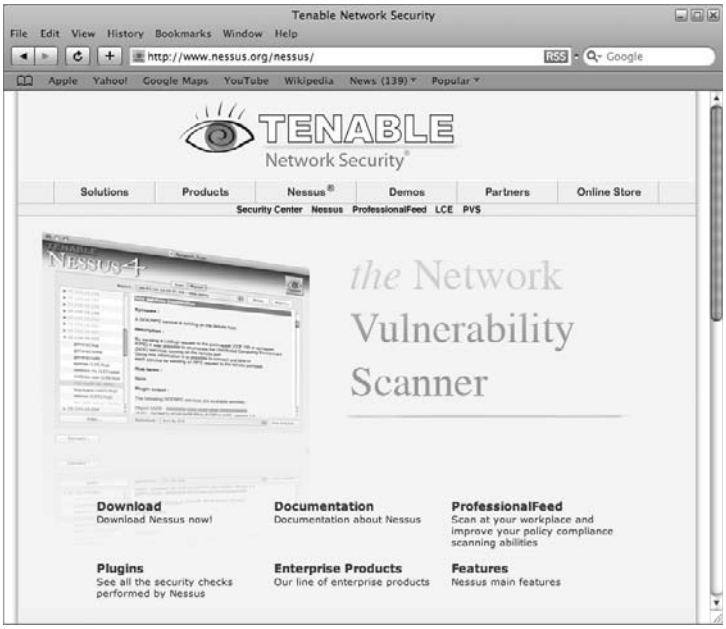


FIGURE 3.3

Nessus Web site

has a self-contained scanning, reporting, and management system.[6] Nessus is the world's most popular vulnerability scanner,[6] estimated to be used by over 75,000 organizations worldwide. It took first place in the 2000, 2003, and 2006 security tools survey from SecTools.org.

PUBLIC RECORD ON TAP: Nessus Goes Closed License

The "Nessus" Project was started by Renaud Deraison in 1998 to provide to the Internet community a free remote security scanner. Nessus is currently rated among the top products of its type throughout the security industry and is endorsed by professional information security organizations such as the SANS Institute.

On October 5, 2005, Tenable Network Security,[7] the company Renaud Deraison co-founded, changed Nessus 3 to a proprietary (closed source) license.[8] The Nessus 3 engine is still free

[6]http://blogs.iium.edu.my/jaiz/2008/09/23/10-best-hacking-and-security-software-tools-for-linux//
[7]http://www.tenablesecurity.com/
[8]http://software.newsforge.com/article.pl?sid=05/10/06/1716257&tid=132&tid=78&tid=27

of charge, though Tenable charges $100 per month per scanner for the ability to perform configuration audits for payment card industry (PCI), CIS, FDCC, and other configuration standards, technical support, SCADA vulnerability audits, the latest network checks and patch audits; the ability to audit antivirus configurations; and the ability for Nessus to perform sensitive data searches to look for credit card, social security number, and many other types of corporate data.

As of July 31, 2008, Tenable sent out a revision of the feed license, which will allow home users full access to plug-in feeds. A professional license is available for commercial use.[9]

The Nessus 2 engine and a minority of the plug-ins are still GPL. Some developers have forked independent open source projects based on Nessus. Tenable Network Security has still maintained the Nessus 2 engine and has updated it several times since the release of Nessus 3.

Nessus 3 is available for many different Unix and Windows systems, offers patch auditing of Unix and Windows hosts without the need for an agent, and is 2–5 times faster[10] than Nessus 2. There is a split-off project called OpenVAS that continues to develop a GPLed vulnerability scanner based on Nessus 2. On April 9, 2009, Tenable released Nessus 4.0.0.

TENABLE NEWT PRO 2.0

NeWT Pro 2.0 is a complete, commercially supported network vulnerability scanner from Tenable, which allows for scanning any target IP address. It includes high-speed checks for more than 2,000 of the most commonly updated vulnerabilities, a wide variety of scanning options, an easy-to-use interface, and effective reporting. NeWT 2.0 is a separate and complimentary version that only allows for scanning the local network on which it resides. Tenable NeWT and NeWT Pro 2.0 benefits include but are not limited to: effective for high-speed vulnerability audits of small, medium, and large organizations; over 2,000 quality vulnerability checks and automatic vulnerability updates; ability to write your own vulnerability checks; detailed vulnerability reports; ability to run as a Windows service; and Tenable Lightning Console compatibility.

"We are proud to mix the power of Unix-based network scanning technology with the legendary ease-of-use of Windows, to provide users with a simple, affordable and extremely robust network security scanner. With NeWT and NeWT Pro 2.0, it is now possible to determine the weaknesses of the devices on the network, ranging from routers and printers to Windows Servers, all from a simple Windows workstation,"

[9] http://www.nessus.org/news/data/nessus_feed_letter.pdf
[10] http://www.nessus.org/documentation/index.php?doc=nessus3

FIGURE 3.4

NeWT 2.0

says Renaud Deraison, Director of Research for Tenable and creator of the Nessus Vulnerability Scanner. Figure 3.4 is a screen shot of this tool.

RAPID7

Rapid7 is a software company, which provides computer vulnerability management, risk assessment, and policy compliance solutions that help organizations understand the risk of vulnerabilities in their IT environment and ensure their networks are not compromised. View Rapid7's Web site in Figure 3.5. Spun-off from a group of established software companies, Rapid7 was founded in 1999 by its current principals, who possess extensive technological expertise, sales acumen, and business operations experience. Rapid7 is privately funded and has achieved steady growth by meeting the needs of global enterprises to assess and prevent network vulnerabilities that expose the organization to data security threats and potential legal and financial liabilities.

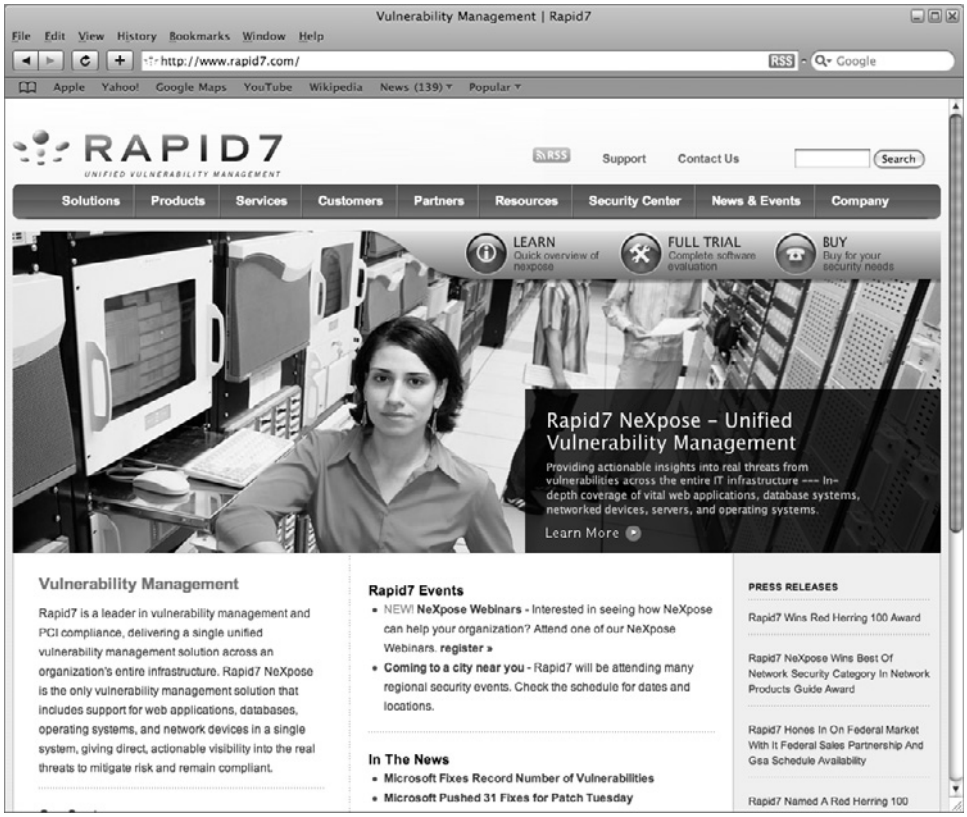


FIGURE 3.5

Rapid7 Web site

Rapid7 also has an award-winning vulnerability and risk management solution called NeXpose.

NeXpose, the company's award-winning enterprise vulnerability and risk management solution, helps IT and security professionals gain overall control of their network and protect software and applications from internal and external intruders. Figure 3.6 has a screen shot of this product. NeXpose minimizes the time spent on locating and eliminating an organization's security vulnerabilities, thereby increasing network reliability, enhancing organizational efficiencies, and improving resource management across Web applications, databases, OSs, servers, and other software applications. Rapid7 PCI Compliance Portal enables merchants, online retailers, and credit card service providers to achieve compliance with the PCI Data Security Standard via a remote, easy-to-use solution that provides the highly accurate scans required for ensuring networks are safe from hackers and protecting customers' credit card information.

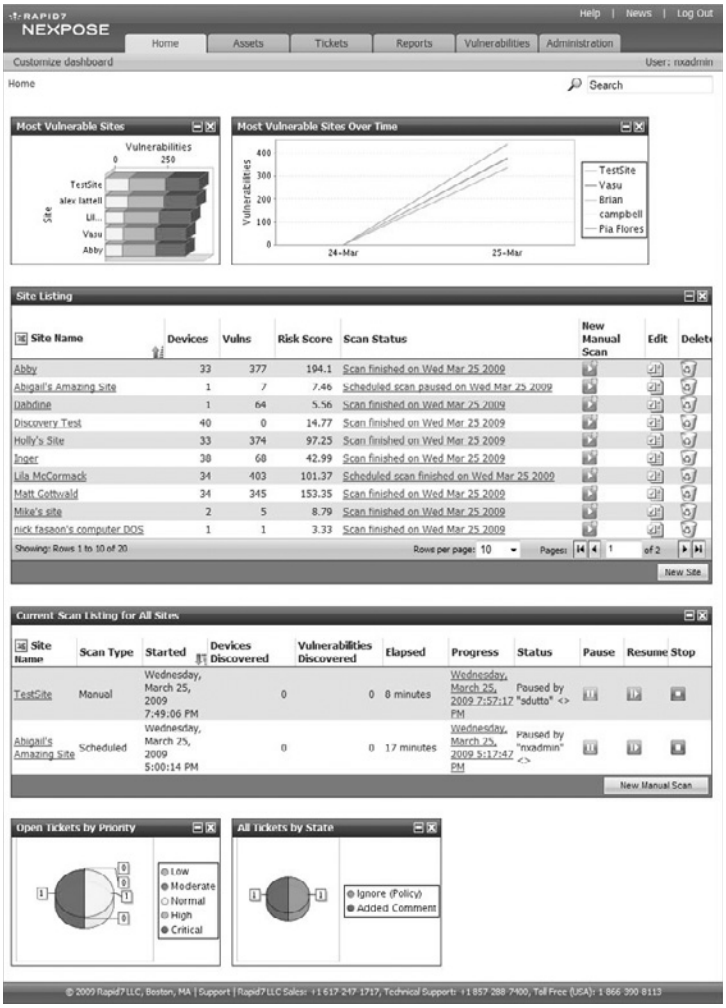


FIGURE 3.6

NeXpose

MICROSOFT BASELINE SECURITY ANALYZER

The Microsoft Baseline Security Analyzer (MBSA) is a software tool released by Microsoft to help analyze security problems in Microsoft products, namely Windows, Windows components such as the IIS Web server application, Microsoft SQL Server, and Microsoft Office. Figure 3.7 is a screen shot of this program. One example of an issue might be that permissions for one of the directories in the wwwroot folder of IIS could be set at too low a level, allowing unwanted modification of files

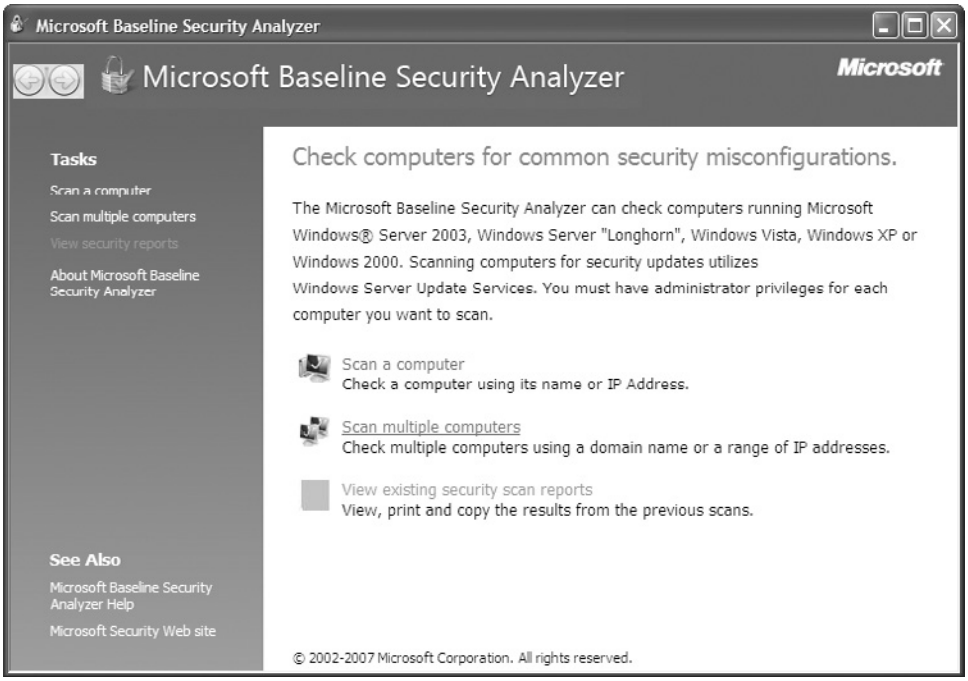


FIGURE 3.7

Microsoft Baseline Security Analyzer

from outsiders. Versions 1.2.1 and below run on Windows 2000, Windows XP, and Windows Server 2003 and provide support for IIS versions 5 through 6, SQL Server 7 and 2000, Internet Explorer 5.01 and above, and Microsoft Office 2000 through 2003. Version 2.0 adds support for Microsoft Office XP and any other software supported by Windows Update (WU). Version 2.0.1 is an update to MBSA 2.0 to enable compatibility with the new WU offline scan file. MBSA 2.1 Beta 2 maintains the current MBSA 2.0.x functionality but adds Windows Vista support.

RETINA EEYE NETWORK SECURITY SCANNER

Retina Vulnerability Assessment Scanner is a vulnerability scanner created by eEye Digital Security that remotely scans a network for security vulnerabilities and assigns a level of threat to those discovered. Figure 3.8 is eEye's Web site. It is only intended for corporate or government use. Purchase or evaluation of this product requires a corporate e-mail address and is not intended for use on home or student networks.[11]

[11]http://www.eeye.com/html/products/retina/download/index.html

FIGURE 3.8

eEye Digital Security Web site

Some issues when scanning to keep an eye out for: make sure that Retina gets good "Registry" key access. If a message stating "Registry access not granted" appears, this means that you are not getting a thorough scan; always have the machine that Retina is scanning on in the domain; use only "Domain Admin" credentials to scan for a successful scan; at least 95% of machines should be successfully scanned to get good results. Figure 3.9 shows a screen shot of this product.

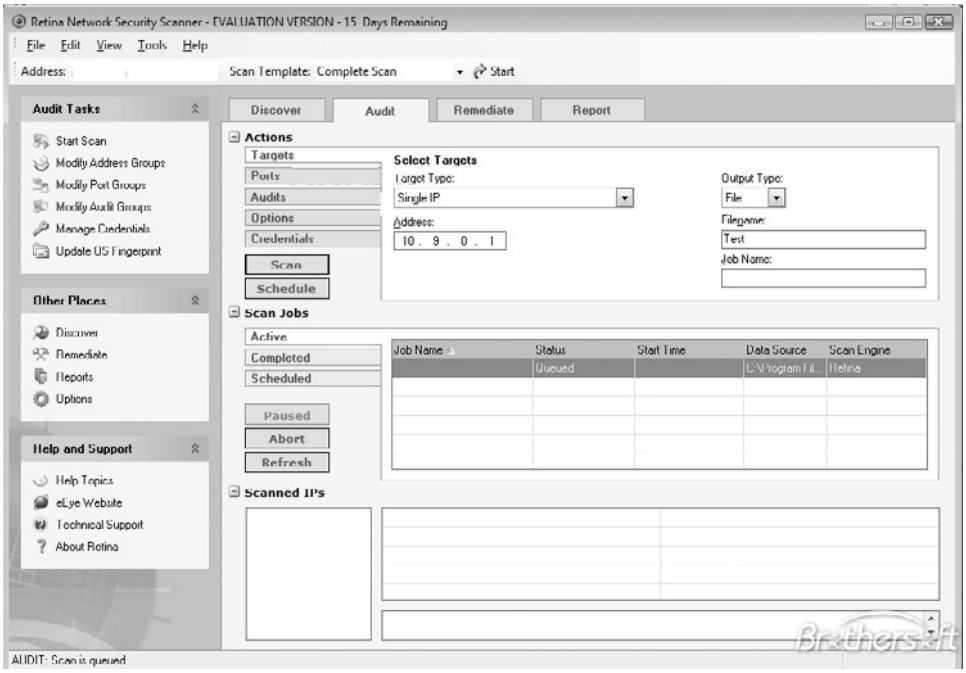


FIGURE 3.9

Retina Network Security Scanner

PUBLIC RECORD ON TAP: Open Source Vulnerability Database

Open Source Vulnerability Database (OSVDB) is an independent and open source database created by and for the community. The goal of the project is to provide accurate, detailed, current, and unbiased technical information on security vulnerabilities. The project promotes greater, open collaboration between companies and individuals, eliminates redundant works, and reduces expenses inherent with the development and maintenance of in-house vulnerability databases. The project was started in August 2002 at the Black Hat and DEFCON Conferences by several industry notables (including H.D. Moore, rain.forest.puppy, and others). Under mostly new management, the database officially launched to the public on March 31, 2004.

The Open Security Foundation (OSF) was created to ensure the project's continuing support. Brian Martin (AKA Jericho), Chris Sullo (of Nikto fame), and Jake Kouns are project leaders for the OSVDB project and currently hold leadership roles in the OSF. It is a client/server implementation that consists of a server daemon (mysqld) and many different client programs/libraries. It has a pluggable data store architecture. Figure 3.10 is a screen shot of OSVDB's Web site. To read more, visit http://osvdb.org/.

FIGURE 3.10

OSVDB Web site

BOOKS

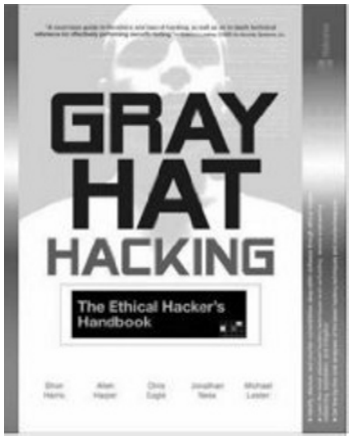
Penetration Tester's Open Source Toolkit

By Jay Beale, Roelof Temmingh, Haroon Meer, Charl van der Walt, and H.D. Moore

Publisher: Syngress

ISBN-10: 1597490210

ISBN-13: 978-1597490214



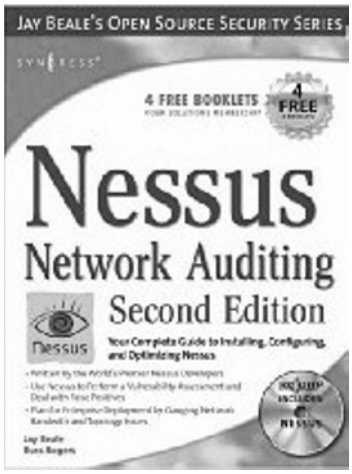
Gray Hat Hacking: The Ethical Hacker's Handbook

By Shon Harris, Allen Harper, Chris Eagle, Jonathan Ness, and Michael Lester

Publisher: McGraw-Hill Osborne Media

ISBN-10: 0072257091

ISBN-13: 978-0072257090



Nessus Network Auditing, Second Edition

By Renaud Deraison, Noam Rathaus, H.D. Moore, Raven Alder, George Theall, Andy Johnston, and Jimmy Alderson

Publisher: Syngress

ISBN-10: 1931836086

ISBN-13: 978-1931836081

This page intentionally left blank

CHAPTER

Exploit

4

After hackers conduct recon and use that information to scan and explore their targets, they will exploit the most valuable one they find. This chapter will discuss the exploits Vlad and his crew use in the fictional story.

An exploit (from the same word in the French language, meaning "achievement" or "accomplishment") is a piece of software, a chunk of data, or sequence of commands that take advantage of a bug, glitch, or vulnerability to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic (usually computerized or networked). This frequently includes such things as violently gaining control of a computer system or allowing a privilege escalation or denial of service attack.

There are several methods of classifying exploits.The most common is by how the exploit contacts the vulnerable software. A "remote exploit" works over a network and exploits the security vulnerability without any prior access to the vulnerable system. A "local exploit" requires prior access to the vulnerable system and usually increases the privileges of the person running the exploit past those granted by the system administrator. Exploits against client applications also exist, usually consisting of modified servers that send an exploit if accessed with the client application. Exploits against client applications may also require some interaction with the user and thus may be used in combination with a social engineering method. Another classification is by the action against the vulnerable system such as unauthorized data access, arbitrary code execution, and denial of service.

Many exploits are designed to provide superuser-level access to a computer system. This means that anyone who has control of the superuser account can essentially do anything they want in that computer and/or network. However, it is also possible to use several exploits, first to gain low-level access and then to escalate privileges repeatedly until one reaches root.

Normally, a single exploit can only take advantage of specific software vulnerabilities. Often, when an exploit is published, the vulnerability is fixed through a patch, and the exploit becomes obsolete for newer versions of the software. This is the reason why some black hat (malicious) hackers do not publish their exploits but keep them private to themselves or other crackers (also considered black hat hackers). Such exploits are referred to as "zero-day exploits" and to obtain access to such exploits is

the primary desire of unskilled attackers, often nicknamed "script kiddies" for their use of scripts or programs developed by others.

PUBLIC RECORD ON TAP: Exploit Used to Breach University

Report: Attackers exploit IIS hole to breach university server

By Elinor Mills from CNET News on May 20, 2009

It apparently didn't take long for hackers to try to take advantage of a zero-day hole in Microsoft Internet Information Services (IIS).

Ball State University in Muncie, Ind., told The Register that servers running the program were breached on Monday, the same day Microsoft warned the public about the vulnerability.

Students accessing their iWeb pages on Monday saw messages saying the system had been hacked, The Register reported on Wednesday. There is no evidence that data was stolen or malicious files uploaded, however, the iWeb accounts were expected to be offline until Thursday or Friday, according to Patty Lucas, a senior help desk support administrator for the university's computing services department.

Microsoft, meanwhile, said it has investigated a public report of a targeted attack on the IIS hole, but it did not specify whether it was the Ball State University breach that was looked into.

The investigation "revealed that the vulnerability was not exploited to accomplish this attack," a Microsoft spokeswoman wrote in an e-mail late on Wednesday. "Microsoft is still not aware of attacks that are trying to use this vulnerability or of customer impact at this time."

The computing services' department referred a call from CNET News on Wednesday afternoon to the communications department, which was already closed for the day.

The security vulnerability could allow an attacker to gain access to a location that typically requires authentication by using a specially crafted anonymous HTTP request, according to the Microsoft security bulletin. The problem exists in the way that the WebDAV extension for IIS handles HTTP requests.

According to a posting to the Full Disclosure security e-mail list on Friday, the IIS security vulnerability was discovered on May 12 by Nikolaos Rangos. To read more, visit http://news.cnet.com/8301-1009_3-10245815-83.html.

FICTIONAL STORY DISSECTED: Buffer Overflows

"Okay, I'm the one that showed you how to pop the sled on that buffer for the browser bug you were working on about a month ago. Since I didn't get any credit in the shout out, I know you didn't tell anyone how I helped," Max responded (p. 70).

In computer security and programming, a buffer overflow, or buffer overrun, is an anomaly where a process stores data in a buffer outside the memory the programmer set aside for it. The extra data overwrites adjacent memory, which may contain other data, including program variables and program flow control data. This may result in erratic program behavior, including memory access errors, incorrect results, program termination (a crash), or a breach of system security. Buffer overflows can be triggered by inputs that are designed to execute code or alter the way the program operates. They are, thus, the basis of many software vulnerabilities and can be maliciously exploited. Bounds checking can prevent buffer overflows. Programming languages commonly associated with buffer overflows include C and C++, which provide no built-in protection against accessing or overwriting data in any part of memory and do not automatically check that data written to an array (the built-in buffer type) is within the boundaries of that array.

FICTIONAL STORY DISSECTED: Wiping the Administrative Password

> Pavel enabled the laptop for booting from a USB device. He pulled out his keychain and plugged the tiny storage device into the port on the right of the laptop case. Instead of the normal start-up screen that Stepan saw every day, Pavel was greeted with a black screen with a few simple command options. This was a handy tool Pavel had picked up from a security Web site. It allowed him to reset any password on a Windows system as long as he could control how the system started. Pavel didn't bother giving the administrator account a new password. He set it to a blank password, disconnected his USB device, and rebooted the machine (p. 7).

All the stages of a hacker's methodology have been completed—recon, scan, and explore. Now Pavel decides to exploit Stepan's laptop to gain superuser permissions. In Windows operations systems, this is accomplished through the Administrator account that is created by default in Windows operations systems. After Pavel wiped out the Administrator password through some hacking tools (read more on his technique in Chapter 8), he decides to leave the password blank so he can reboot the computer and login to the Administrator account using no password. This is a smart move on his part because any password he assigns might link him to this activity. Leaving it blank is a common method of ensuring any investigation after the fact will reveal no possible link back to him or Vlad. Usually when people create passwords, they use common phrases they are most familiar with. For instance, many people will use a pet name, their street address, children's names, or even their birthdays to create a password. Pavel does not want to slip up now, so he decides to leave it blank.

FICTIONAL STORY DISSECTED: SubSeven

> The home computer is a Windows box and even has the SubSeven Trojan running (p. 54).

Vlad is in hot pursuit of Bob and Leon, and without any money, they cannot move quick enough to stay ahead. So they decide to hack into a house that looks like it can afford to lend a few grand and has the money lying in an account somewhere. After Leon does his initial recon, scan, and explore, he finds a Microsoft Windows machine that has a very common remote administrator tool running. This tool is called SubSeven and is a well known and popular backdoor program also known as a Trojan horse. Using this backdoor program, Leon accesses the Windows machine remotely and finds out that the user left an Internet Explorer window open with a cached Web site already loaded into the browser. This Web site would assist Leon in gaining access to the unfortunate user's online brokerage account. But first Leon needs the password to access the account. Many browsers have an option to autocomplete the field you enter text into. Each time you allow the browser to do this, it is saving the text into cache that is stored on your local computer. If someone knows where to look inside of your computer's file system, they can retrieve all your cached passwords, usernames, credit card numbers, social security numbers, and banking account numbers that you enter into the browser. Remember even though the Web site might be secured, it does not mean your cache is secure too. Figure 4.1 shows the location of the files that Leon might have used to obtain the password to the online brokerage account. Figure 4.2 shows an example of what the common fromhistory. sqlite might look like. Notice that the XML file contains usernames, IDs, e-mail addresses, and so on. This information can be very useful to a hacker. Figure 4.3 shows how some browsers cache credit cards as well. Watch out because there are Leons out there looking to take advantage of your unsecured cache!

Sub7, or SubSeven or Sub7Server, is the name of a popular backdoor program. It is mainly used for causing mischief, such as hiding the computer cursor, changing system settings, or loading up pornographic Web sites. However, it can also be used for more serious criminal applications, such as stealing passwords and credit card details. Its name was derived by spelling NetBus backwards ("suBteN") and swapping "ten" with "seven." It was originally designed by someone with the handle mobman, whose whereabouts are currently unknown. This person is suspected to be a woman from South Africa based on greetings contained in the program itself.

Among Sub7's capabilities are complete file system access and real-time keystroke logging. The latter capability makes it possible for Sub7 to be used to steal passwords and credit card information. It also installs itself into the WIN.INI file and the "run" key of the Windows Registry, in addition to adding a "runner" to the Windows Shell. Computer security expert Steve Gibson, founder of Gibson Research Corporation—most well known for its SpinRite software, once said that with these features, Sub7 allows a hacker

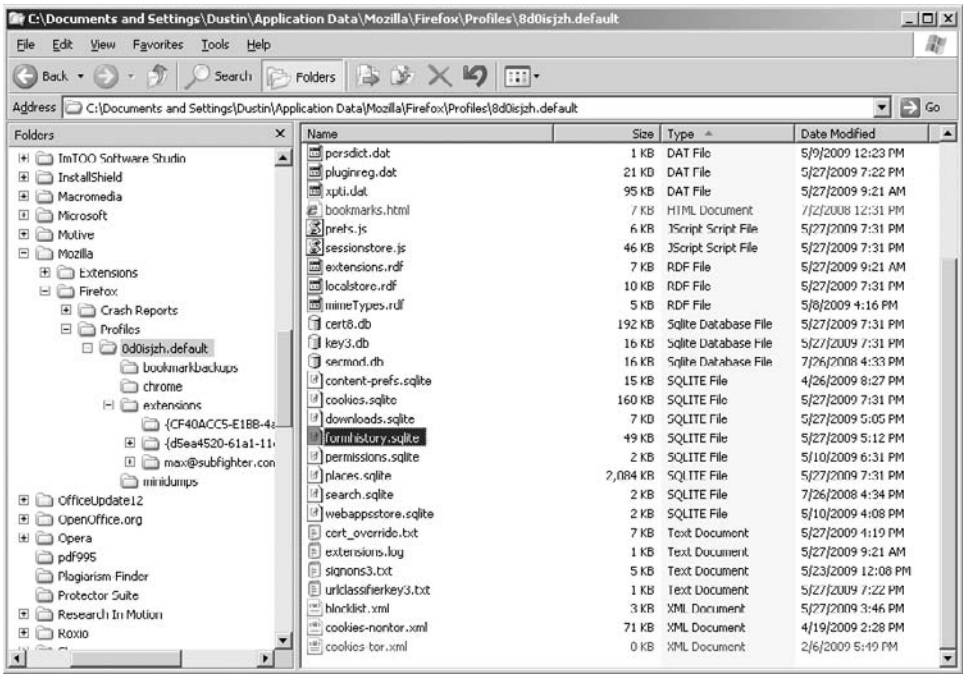


FIGURE 4.1

Firefox's autocomplete file named "fromhistory.sqlite"

to take "virtually complete control" over a computer. Sub7 is so invasive, he said, that anyone with it on their computer "might as well have the hacker standing right next to them" while using their computer.[1] Figure 4.4 shows a screen shot of SubSeven.

DON'T HACK ME PLEASE: Stopping Sub7

Sub7 is usually stopped by antivirus software and a firewall, and with popular operating systems providing these features built in, it may become less of a computer security problem. However, if the executable is compressed, like being placed inside a .zip archive, some older antivirus software may not be able to detect it. Most modern antivirus applications have support to look inside archives, so this problem is now less critical than before.

Like other backdoor programs, Sub7 is distributed with a server and a client. The server is the program that victims must be enticed to run in order to infect their machines, and the client is the program with a graphical user interface (GUI) that the user runs on their own machine to control the server. Sub7 allows crackers to set a password on the server, theoretically, so that once a machine is owned (infected), no other crackers can take control of it.

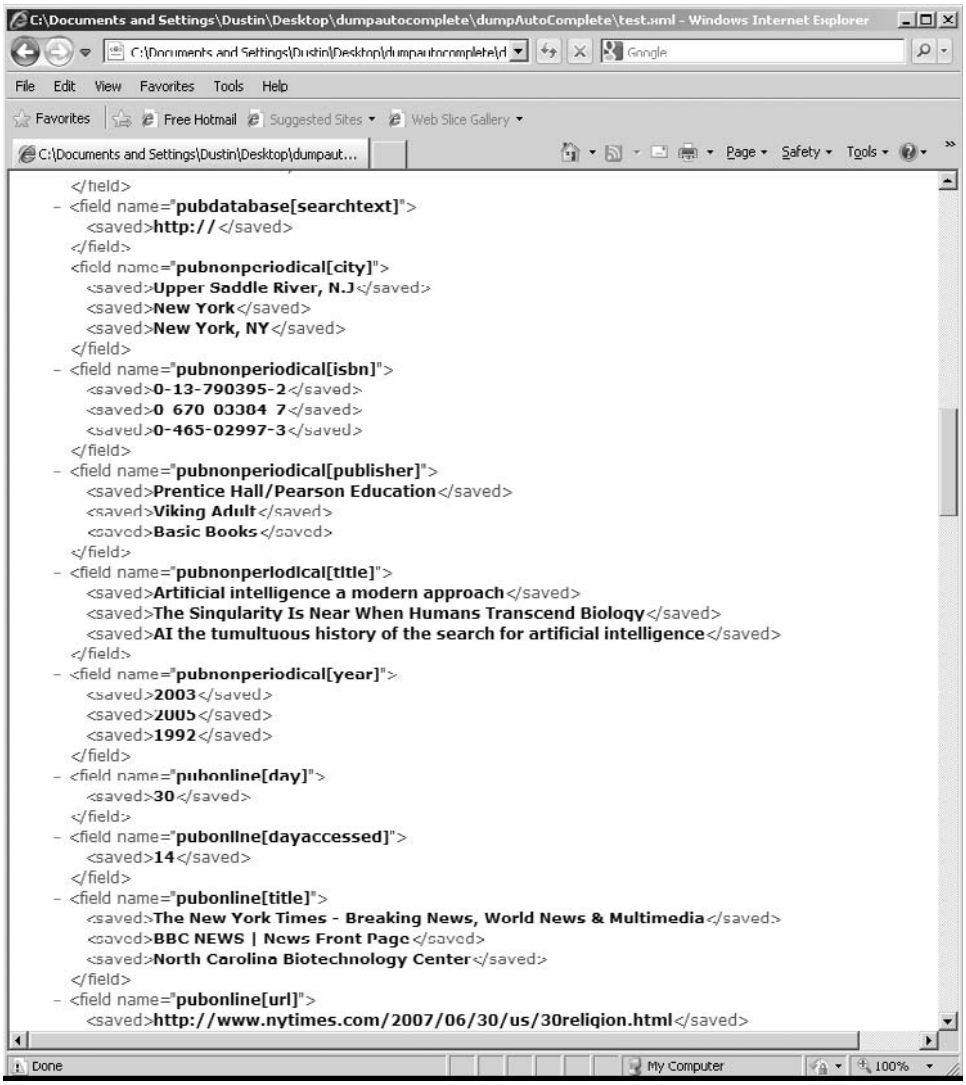


FIGURE 4.2

Contents of file name "fromhistory.sqlite"

Earlier versions, however, announced their availability by joining a secret IRC chat server where it posts all the details required for its use. They also posted the same details on a newsgroup.[1]

Sub7 has more features than Netbus (webcam capture, multiple port redirect, user-friendly registry editor, chat and more), but it always tries to install itself into Windows directory and it does not have activity logging. Sub7 is also a bit less stable than Netbus.

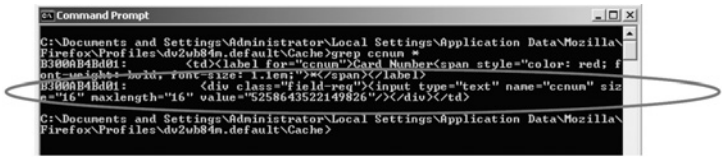


FIGURE 4.3

Firefox cached credit card number. See the credit card number "5258643522149826" in Figure 4.4.

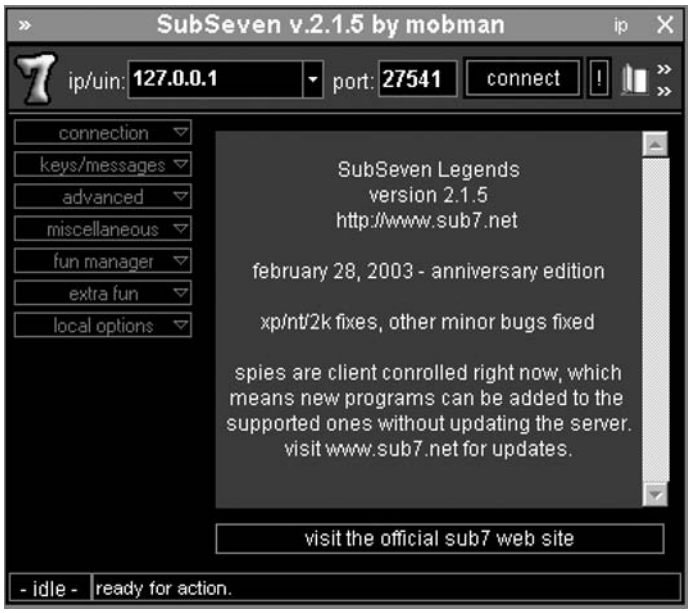


FIGURE 4.4

SubSeven tool

However, older versions of the Sub7 server also have a master password, allowing anyone who knows the master password to take over the machine. In some older versions, the master password was 14438136782715101980 but this "feature" was later scrapped.

Some versions of the client contain Hard Drive Killer Pro code, intended to destroy the hard drive of an enemy of the authors. The code checks to see if the computer has ICQ and if the user account matches a specific number (7889118, the ICQ number of Sean Hamilton, a rival trojan author), and if so, bombs the drive. It is rumored that the intended target had his drive destroyed.[1]

[1]Gibson, Steve. The strange tale of the denial of service attacks on grc.com, March 5, 2002.

FICTIONAL STORY DISSECTED: MilwOrm.com

> "I've seen some of Max—uh, her work on Milw0rm.com," R10t volunteered. If she's the same one, I can see why Bob is putting up with her—she has skills" (p. 96).

Milw0rm.com is a database of exploits categorized by type. The database makes readily available exploit codes for anyone to download for use on whatever they are trying to target. During the stages of recon, scanning, and explore, information is being gathered. This information might include search results for exploits that can be effectively used against specific applications. Milw0rm is also helpful for security professionals who can use this exploit code to defend their systems against the malicious attacker armed with the same code. Figure 4.5 is the Milw0rm Web site.

FIGURE 4.5

Milw0rm.com

FICTIONAL STORY DISSECTED: Metasploit

> Before Leon could get the mouse over to the folder to get his next tool, Bob pronounced "Use Metasploit" (p. 100).

The Metasploit Project is a computer security project, which provides information about security vulnerabilities and aids in penetration testing and IDS signature development. Most devices run Simple Network Management Protocol (SNMP) by default and using the free Metasploit tool is an easy choice because it supports SNMP hacking. The most well-known subproject is Metasploit Framework, a tool for developing and executing exploit code against a remote target machine. Figure 4.6 is a picture of what Metasploit looks like after starting the program. Other important subprojects include the Opcode Database, shellcode archive, and security research. The Metasploit Project is also wellknown for antiforensic and evasion tools, some of which are built into the Metasploit Framework. Metasploit was created in 2003 as a portable network game using the Perl scripting language. Later, the Metasploit Framework was completely

FIGURE 4.6

Metasploit

rewritten in the Ruby programming language. It is most notable for releasing some of the most technically sophisticated exploits to public security vulnerabilities. In addition, it is a powerful tool for third-party security researchers to investigate potential vulnerabilities. Like comparable commercial products such as Immunity's CANVAS or Core Security Technologies'[2] CORE IMPACT, Metasploit can be used by administrators to test the vulnerability of computer systems to protect them or by black hat hackers and script kiddies to break into remote systems. Like many information security tools, Metasploit can be used for both legitimate and unauthorized activities.

Metasploit's emerging position as the defacto vulnerability development framework has led in recent times to the release of software vulnerability advisories often accompanied by a third-party Metasploit exploit module that highlights the exploitability, risk, and remediation steps of that particular bug.[3,4] Metasploit 3.0 (Ruby language) is also beginning to include fuzzing tools, to discover software vulnerabilities in the first instance, rather than merely writing exploits for currently public bugs. Figure 4.7 shows Metasploit's Web site.

FIGURE 4.7

Metasploit's Web site

[2]http://www.coresecurity.com/

[3]http://archives.neohapsis.com/archives/vulnwatch/2005-q4/0074.html

[4]http://projects.info-pull.com/mokb/MOKB-11-11-2006.html

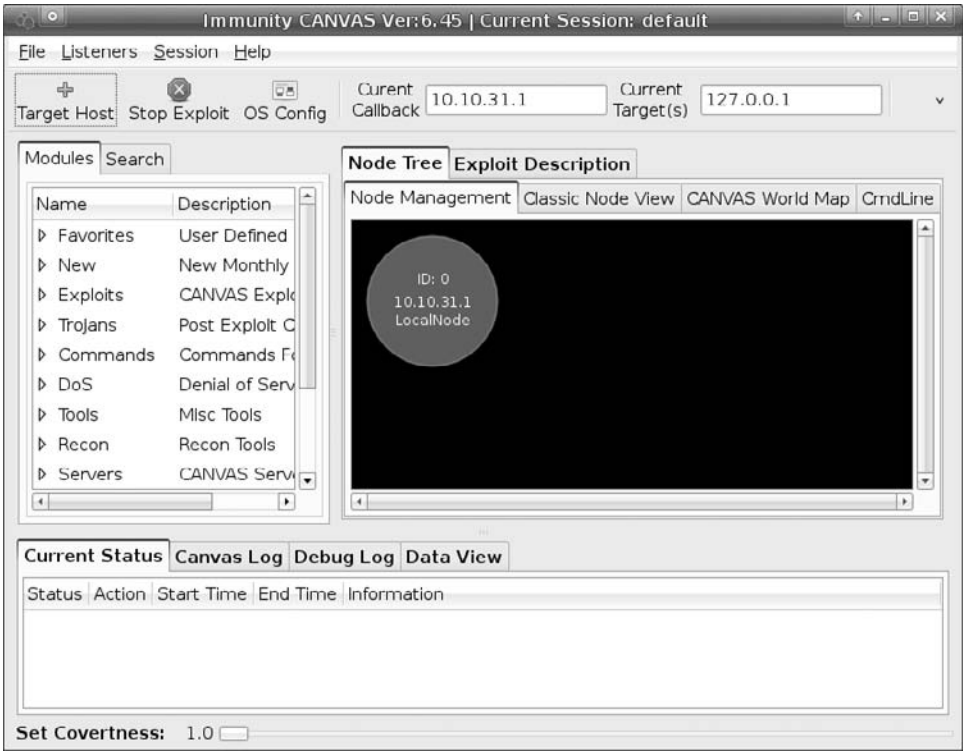


FIGURE 4.8

Immunity's Web site

CANVAS

Just as Metasploit, Immunity's CANVAS makes available hundreds of exploits, an automated exploitation system, and a comprehensive, reliable exploit development framework to penetration testers and security professionals worldwide. Figure 4.8 is Immunity's Web site. There is one difference between CANVAS and Metasploit; Metasploit is free and CANVAS is not. The supported platforms for installation include Windows, Linux, Mac OS X, and such devices as mobile phones and commercial Unixes which might only be able to run the command line version depending on a case by case basis. Figure 4.9 is a screen shot of CANVAS running in GUI mode.

CORE IMPACT

CORE IMPACT Pro is a commercial automated penetration testing software solution developed by Core Security Technologies, which allows the user to probe for and

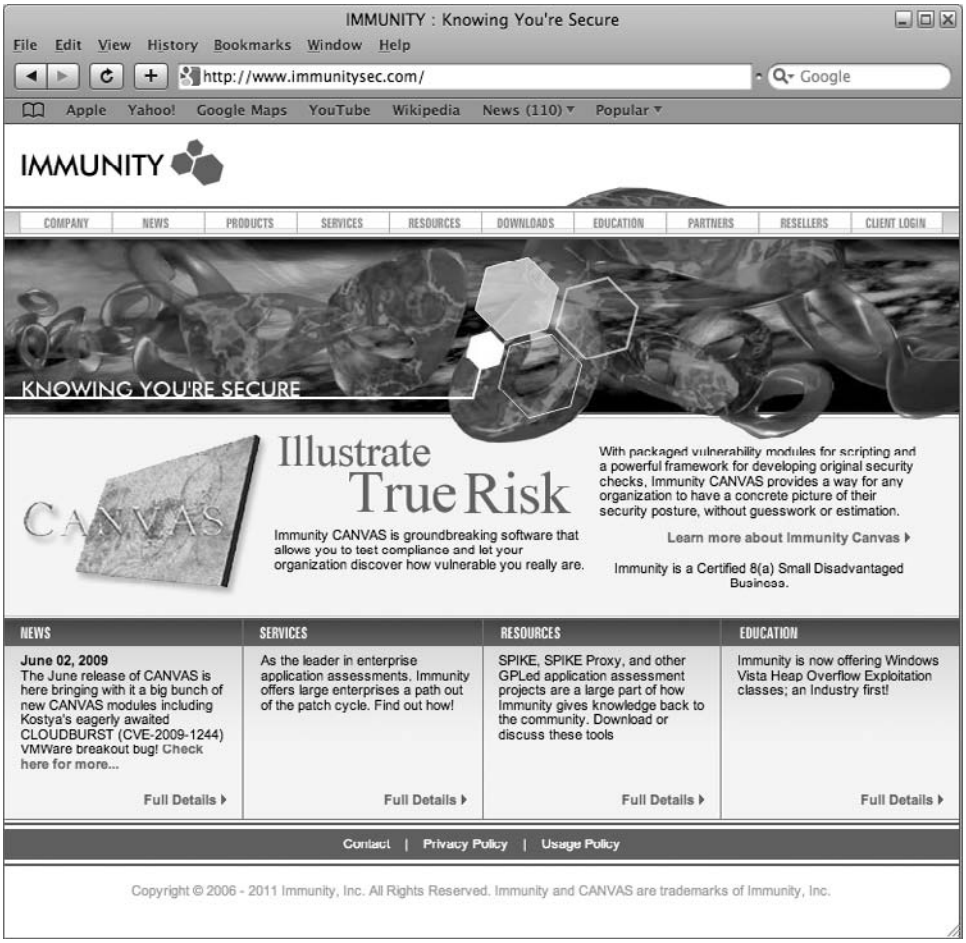


FIGURE 4.9

CANVAS

exploit security vulnerabilities in computer networks, endpoints, and web applications. Figure 4.10 is a picture of their Web site. The product's interface is designed to be usable by individuals both with and without specialized training in penetration testing and vulnerability assessment, and it includes functions for generating reports from the gathered information. Figure 4.11 is a screen shot of this tool. CORE IMPACT Pro is the only penetration testing software that allows you to see your network, endpoint, e-mail user and Web application security as an attacker would.

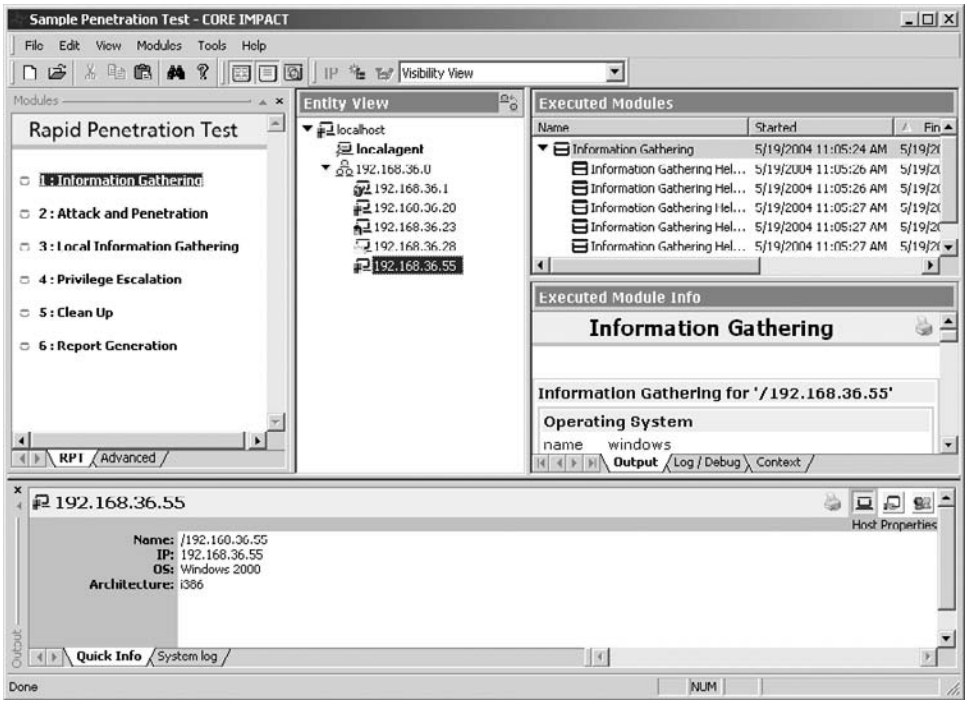


FIGURE 4.10

Core Security Technologies' Web site

FIGURE 4.11

CORE IMPACT

BOOKS

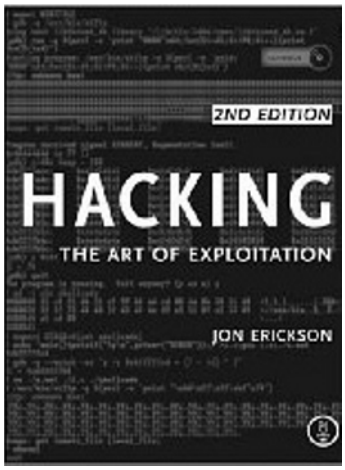
Writing Security Tools and Exploits

By James C. Foster

Publisher: Syngress

ISBN-10: 1597499978

ISBN-13: 978-1597499972



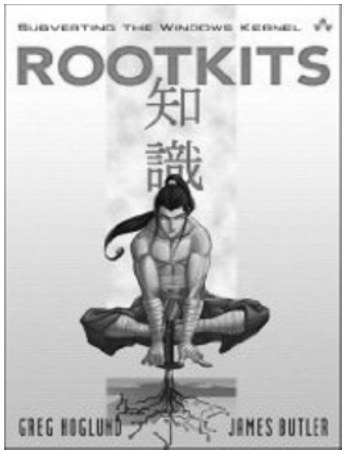
Hacking: The Art of Exploitation, 2nd Edition

By Jon Erickson

Publisher: No Starch Press

ISBN-10: 1593271441

ISBN-13: 978-1593271442



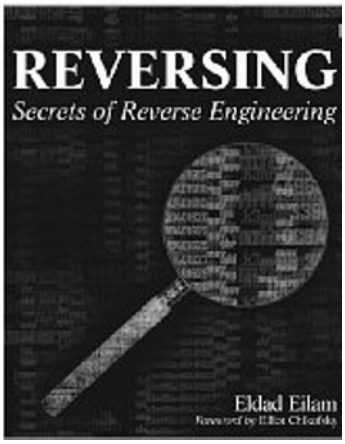
Rootkits: Subverting the Windows Kernel

By Greg Hoglund and Jamie Butler

Publisher: Addison-Wesley Professional

ISBN-10: 0321294319

ISBN-13: 978-0321294319



Reversing: Secrets of Reverse Engineering

By Eldad Eilam

Publisher: Wiley

ISBN-10: 0764574817

ISBN-13: 978-0764574818

This page intentionally left blank

CHAPTER

Expunge

5

What is expunge? Great question! In general terms, expunge is used to describe the physical action of destroying or obliterating information. In *The Dissected Hack: The F0rb1dd3n Network*, the word expunge is used to refer to the actions Pavel takes to obliterate log files and some internal system settings called registry keys from Stepan's computer. Registry keys are discussed below in the "Public Record on Tap." We will first talk about how Pavel cleared the event logs, and later we will discuss how he changed the "last logged in user" function.

PUBLIC RECORD ON TAP: Registry Keys

The Windows Registry is a database, which stores settings and options for Microsoft Windows operating systems. It contains information and settings for hardware, operating system software, most nonoperating system software, and per-user settings. The registry also provides a window into the operation of the kernel, exposing runtime information such as performance counters and currently active hardware. The registry contains two basic elements: keys and values. Registry keys are similar to folders—in addition to values; each key contains subkeys, which may contain further subkeys, and so on. Keys are referenced with syntax similar to Windows' path names, using backslashes to indicate levels of hierarchy. For example, HKEY_LOCAL_MACHINE\Software\Microsoft\Windows refers to the subkey "Windows" of the subkey "Microsoft" of the subkey "Software" of the HKEY_LOCAL_MACHINE key.

FICTIONAL STORY DISSECTED: Clear Event Logs

> Pavel took Stepan's laptop from Vlad and blanked the three Windows event log files. Next, he changed the "last logged in user" registry key so that it would appear that Stepan's account was the last one used (p. 8).

Expunging the three Windows event log files and changing the "last logged in user" is critical to covering your tracks for a hacker. Pavel is a very skilled computer hacker

and does not mind covering his tracks even though many normal computer users would not even notice things such as Windows event logs or who the last user logged in was. In fact, you have to drill down a few Windows' menus before you can bring up the Windows Event Viewer and skim over the Application, Security, and System Logs. But Pavel feels that he better be safe than sorry because hacking is easily traced if you do not cover your tracks. Little things like this need to be tightened up when malicious hackers do not want anyone to trace their activities.

So how can you prevent people like Pavel from expunging your logs? Well, in the "Don't Hack Me Please" section, we will discuss how to secure log files so that only authorized users with proper permissions can access critical log files.

DON'T HACK ME PLEASE: Securing Your Logs

Everyone wants to keep their system's logs from being tampered with, right? Windows has some powerful logging features. Unfortunately, if you're still running an older Windows system, such as a variety of Windows 2000, by default, the event logs are not protected against unauthorized access or modification. You might not realize that even though you have to view the logs through the Event Viewer, they are simply regular files just like any others. To secure them, all you need to do is locate them and apply the proper access control lists (ACLs).

Unless their locations have been changed through the Registry, you should be able to find the logs in the %SystemRoot%\system32\config directory (see Figure 5.1). The three files that

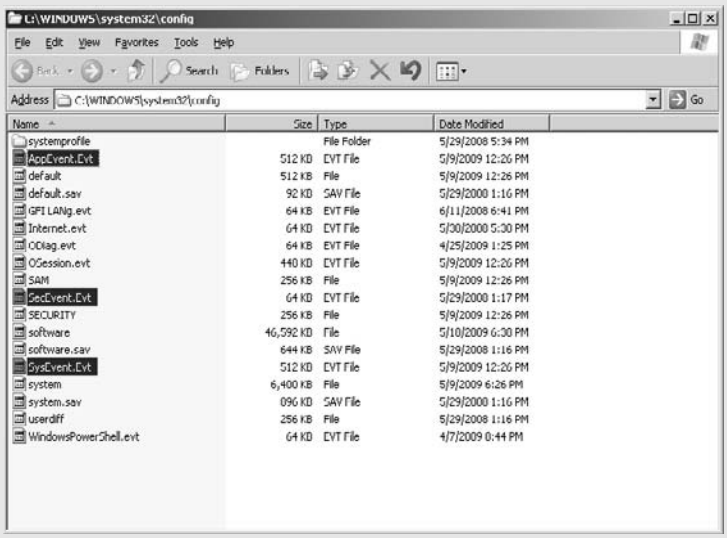


FIGURE 5.1

%SystemRoot%\system32\config directory

correspond to the Application Log, Security Log, and System Log are AppEvent.Evt, SecEvent.Evt, and SysEvent.Evt, respectively.

Now, apply ACLs to limit access to only Administrator accounts. You can do this by bringing up the Properties dialog for the files and clicking the Security tab. An example is shown in Figure 5.2 with unauthorized user permissions for the guest account. In Figure 5.3, the account for guest has been removed.

After you've done this, remove any users or groups other than Administrators and SYSTEM from the top pane.

To learn more, visit http://codeidol.com/sql/network-security-hack/Windows-Host-Security/Secure-Your-Event-Logs/.

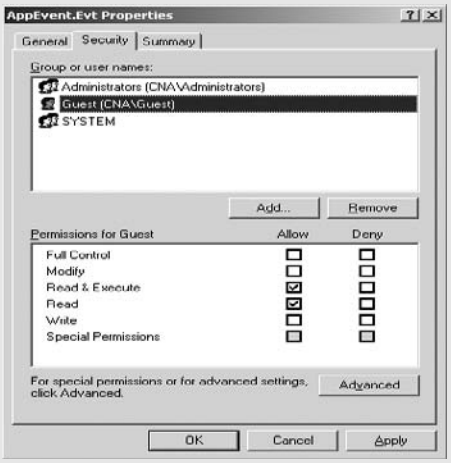


FIGURE 5.2

Application Log Properties dialog window

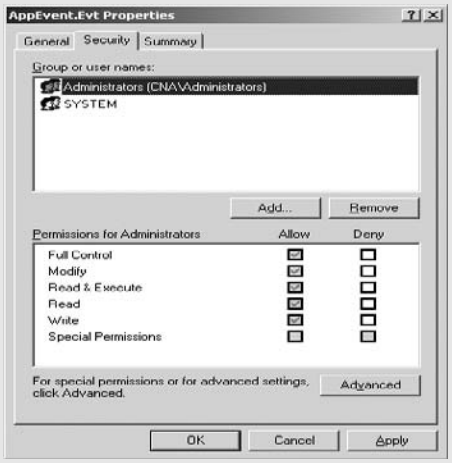


FIGURE 5.3

Application Log Properties dialog window

EVENT VIEWER

In Windows XP, an event is any significant occurrence in the system or in a program that requires users to be notified or an entry added to a log. The Event Log Service records application, security, and system events in Event Viewer. With the event logs in Event Viewer, you can obtain information about your hardware, software, system components, and monitor security events on a local or remote computer. Event logs can help you identify and diagnose the source of current system problems or help you predict potential system problems.

HOW TO: Event Log Types

A Windows XP-based computer records events in the following three logs:

Application log: The Application Log contains events logged by programs. For example, a database program may record a file error in the Application Log. Events that are written to the Application Log are determined by the developers of the software program.

Security log: The Security Log records events such as valid and invalid logon attempts, as well as events related to resource use, such as the creating, opening, or deleting of files. For example, when logon auditing is enabled, an event is recorded in the Security Log each time a user attempts to log on to the computer. You must be logged on as Administrator or as a member of the Administrator's group in order to turn on, use, and specify which events are recorded in the Security Log.

System log: The System Log contains events logged by Windows XP system components. For example, if a driver fails to load during startup, an event is recorded in the System Log. Windows XP predetermines the events that are logged by system components. To read more, visit http://support.microsoft.com/kb/308427.

To open Event Viewer, follow these steps:

1. Click **Start**, and then click **Control Panel**. Click **Performance and Maintenance**, then click **Administrative Tools**, and then double-click **Computer Management**, as seen in Figure 5.4. Or, open the MMC containing the Event Viewer snap-in.

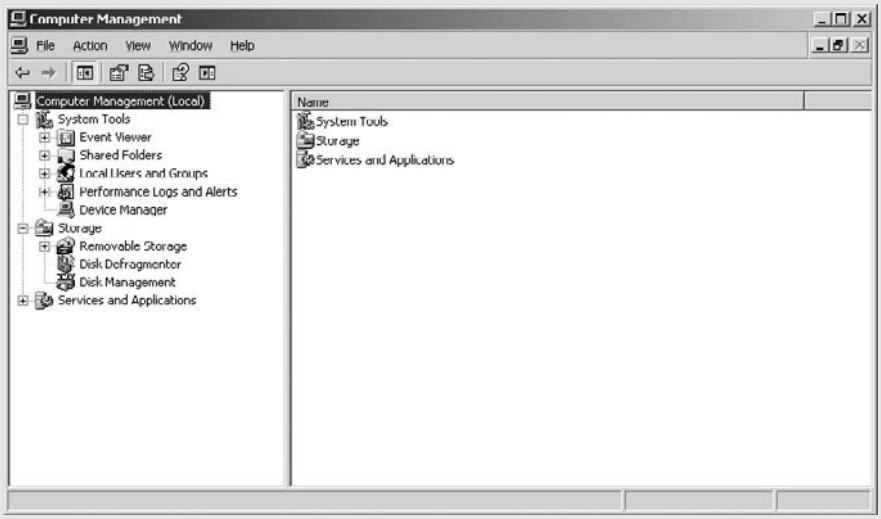


FIGURE 5.4

Computer Management

2. In the console tree, click **Event Viewer**, as seen in Figure 5.5.

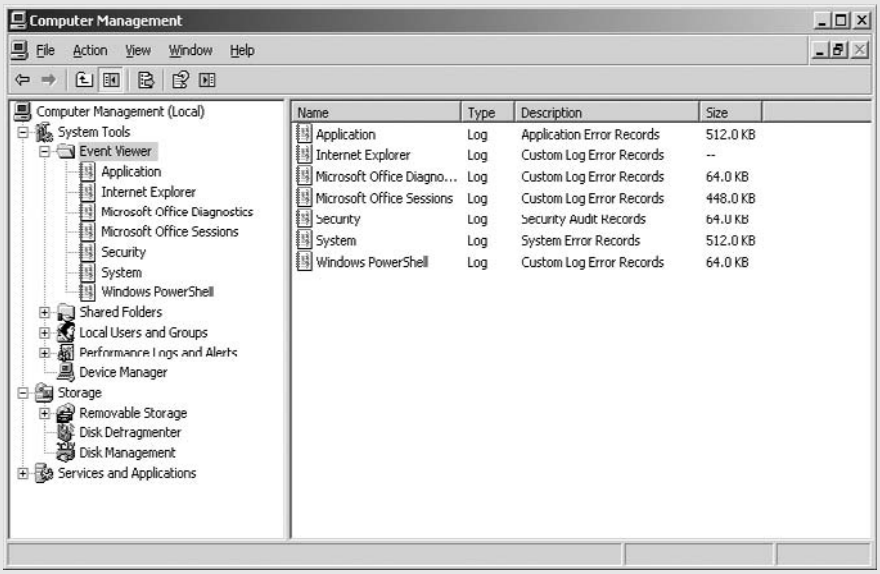


FIGURE 5.5

Event Viewer selected inside of Computer Management

The Application, Security, and System Logs are displayed in the Event Viewer window.

Pavel changes the last user logged in on Stepan's laptop, so when the computer boots up again, the dialog box does not display a username other than Stepan's username he used to log into this computer last. Pavel is smart because if he had not changed the last user logged in from appearing in the logon prompt window, Stepan would have definitely noticed it because Stepan would have to retype his username to login. In Figure 5.6, the username "Administrator" was the last user to login the computer.

FIGURE 5.6

Logon prompt

To stop Windows from showing up the username of the last user logged in successfully, you would need to apply a minor registry hack that would prevent Windows from displaying the last username logged in Windows.

HOW TO: Stop Windows From Showing the Last Username Logged in

1. Open Start menu, click Run, type "regedit," and press Enter as seen in Figure 5.7. Then Registry Editor program will appear as seen in Figure 5.8.

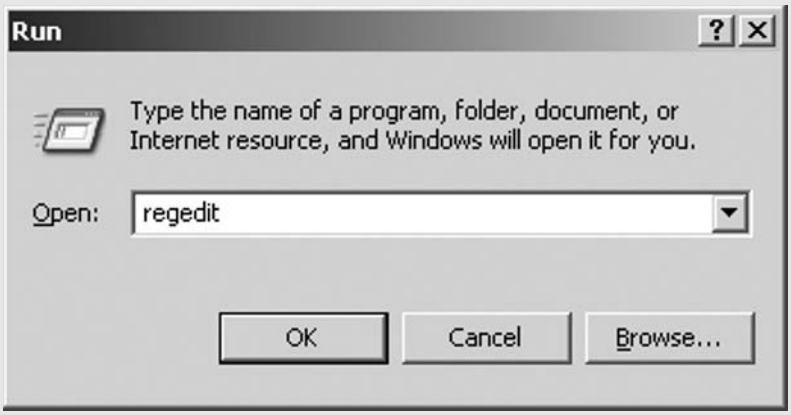


FIGURE 5.7

Run window

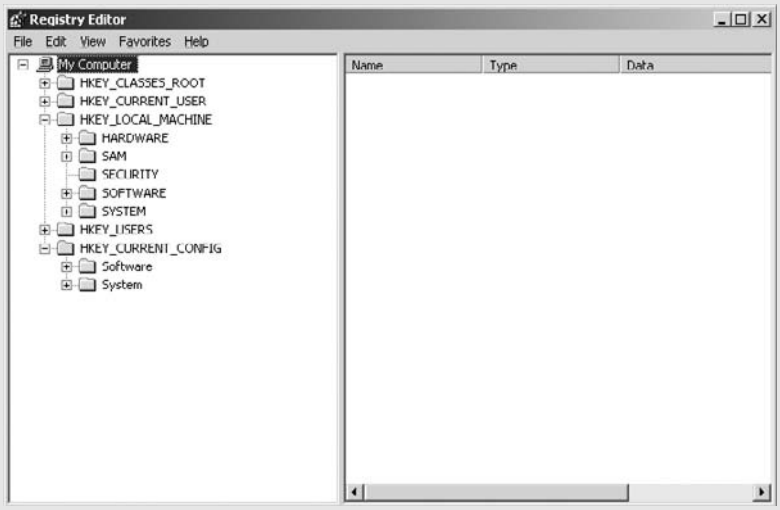


FIGURE 5.8

Registry Editor

2. Navigate to the following path as seen in Figure 5.9.

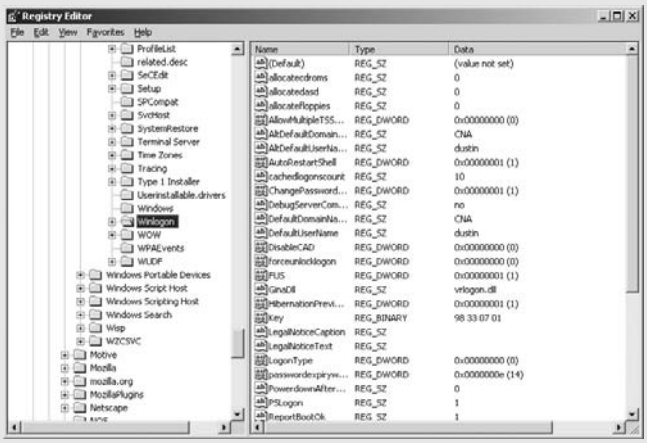


FIGURE 5.9

Registry Editor navigation

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

3. Right click in the empty area in the right pane and create a new registry key of type REG_SZ with value named DontDisplayLastUserName and set the value to 1 to enable the key as seen in Figure 5.10; on the other hand, value 0 will disable this key, and Windows will display the username of the last user logged in Windows.

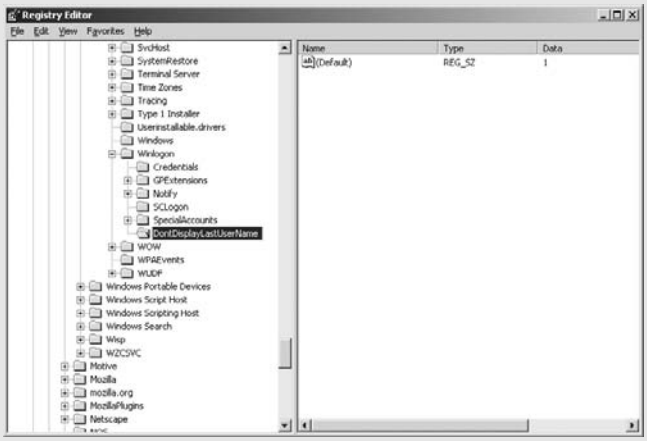


FIGURE 5.10

Registry Editor new registry key called DontDisplayLastUserName

There are a few freeware and shareware tools that can be used to change and record user logins. There is also a great tool used to expunge Internet Explorer logs. Some that we will discuss below are Lognamer, IEClean, Last True Login, lastLogoff.vbs, and Winzapper. The first two tools (Lognamer and IEClean) are used to manipulate and/or expunge the trace of malicious activity by someone who does not want to be caught missing around with a computers file system.

HOW TO: Manipulate Last User Logged on Using Lognamer Tool

Lognamer is a small tool, which lets you change the username of the last user logged in; this way you can enter any other valid username on the computer to hide your own username from appearing the login dialog box. See Figure 5.11 for a screen shot of this tool. This tool is a dialog-tool for XP and allows you to set the winlogon default usernames, so they show instead of the name you used for your current log-on. Neat if you do not want people to know who logged on the last time!

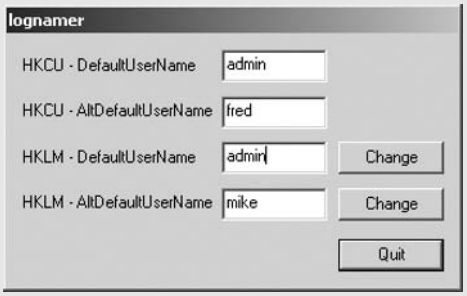


FIGURE 5.11

Lognamer tool

Download here http://www.e-sushi.net/files/lognamer.zip

HOW TO: Cleaning Out the Internet Explorer Cache, Cookies, and History Using IEClean Tool

IEClean is a simple, yet effective cleaning utility by e-sushi. Figure 5.12 shows a screen shot of this tool. It is the fastest way to clean up after yourself when you have used Internet Explorer on a computer, but do not want people to know where you surfed to. Or you can use this software to quickly reclaim some disk space. Whatever your reasons for using it may be, it cleans what it says, whipping the data found from your hard disk by overwriting the disk-sectors with 0 bytes, making undeletion near to impossible.

Download here http://www.e-sushi.net/files/ieclean.zip

FIGURE 5.12

IEClean tool

DON'T HACK ME PLEASE: Last True Login Tool

What if you could find the true last logon time for every user and computer account? That would be great! No more malicious activity will get in my way … well you can clean up your Active Directory by easily identifying unused or obsolete user and computer accounts by identifying their true last logon time and account status. The true last logon time can be a problem for system administrators as different times are stored on each domain controller. The True Last Logon tool queries all Active Directory Domain Controllers to gain the true last logon time. The easy to use interface also shows the account expiry date and time, whether or not the account is locked out and whether or not the account is currently enabled or disabled. Old or redundant accounts can be disabled or deleted from within the program, or you can choose to print or save the results to a CSV or tab delimited text file. In Figure 5.13, the option to use True Last Logon via the command line is shown. Figure 5.14 is the front end graphical user interface.

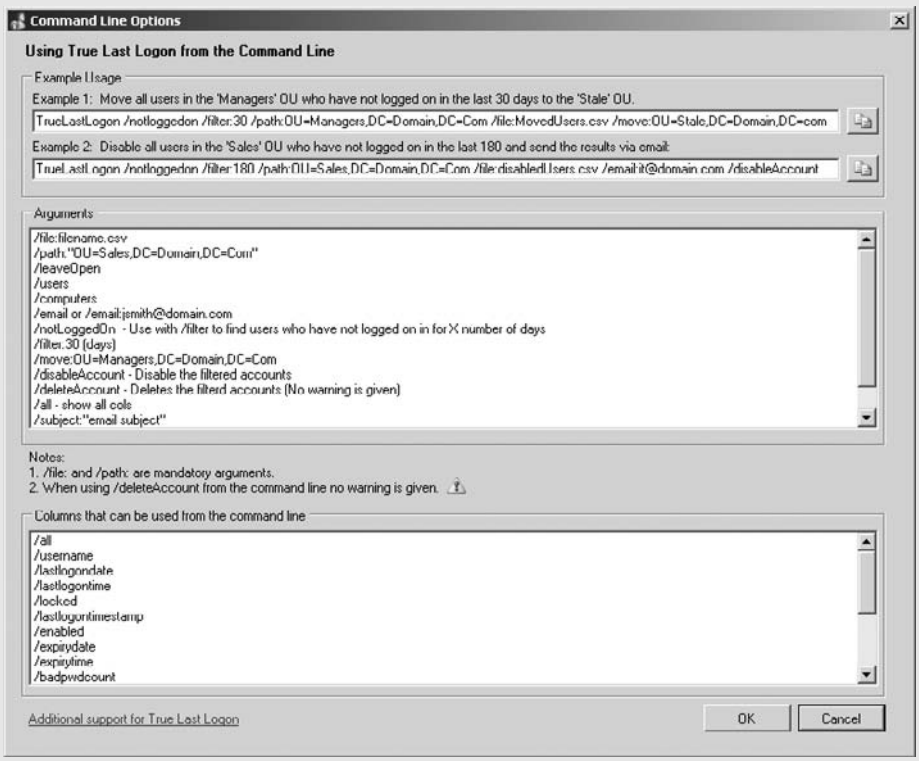


FIGURE 5.13

Last True Login Command Line Options

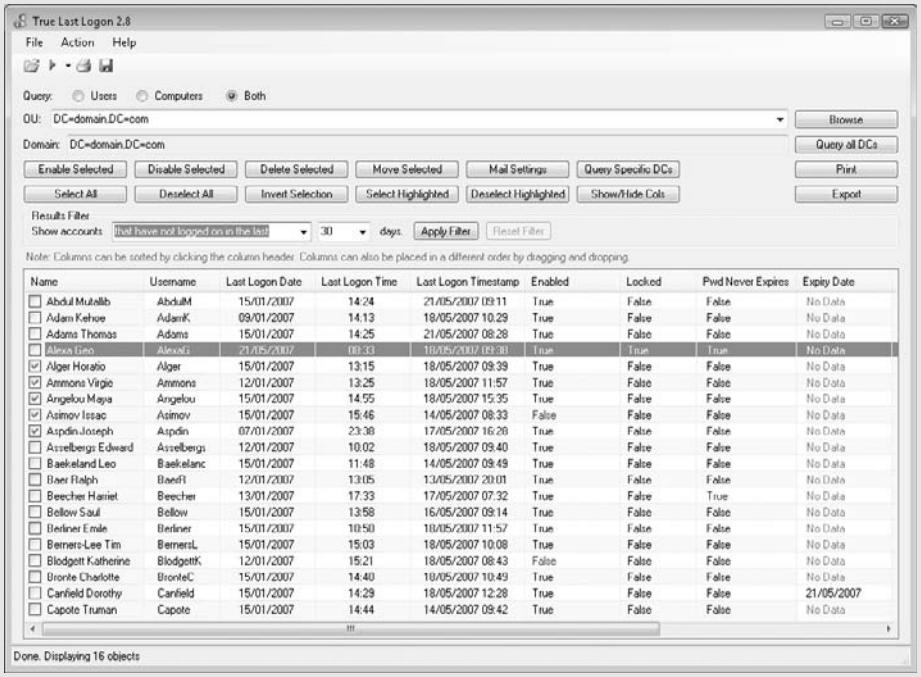


FIGURE 5.14

Last True Logon graphical user interface

Download here http://www.dovestones.com/Downloads/Demos/TrueLastLogonTrial.msi

DON'T HACK ME PLEASE: Recording Users Last Logoff Time

Active Directory contains an attribute named lastLogoff alongside the lastLogon attribute. However, unlike lastLogon, the lastLogoff attribute is not written too and doesn't appear to be used by Active Directory running on Windows 2000 or Windows Server 2003. Microsoft has plans to use this attribute in future; in the mean time, we can use the solution described below.

Recording users last logoff time

One solution is to store a user's last logoff time in another attribute, which you can easily read using Active Directory Users and Computers and True Last Logon. When a user logs off a domain-connected computer, we can store the date and time in an unused Active Directory attribute. We can do this by running a script when the user logs off. When the

script runs, it uses the credentials of the user that is logged on (well logging off); by default, a user has permission to update certain attributes within his or her Active Directory user object, some of these attributes are listed below. Active Directory does have an attribute named "lastLogoff"; unfortunately, this attribute is read-only, so we cannot use this, so we need to store the last logoff date and time in an attribute we can use.

How it works

1. Use the lastLogoff.vbs script to populate a chosen attribute with the date and time the user logged off.
2. Edit the script so that date is being stored in an attribute you aren't currently using (see list below).
3. Assign the script to run at log-off using Group Policy.
4. Add the attribute to True Last Logon by clicking on the "Add/Remove Columns" button.
5. When True Last Logon queries user accounts, the last logoff date and time will be retrieved. The last logoff date can be stored in one of the following attributes.

   General tab

   telephoneNumber

   wWWHomePage

   url

   Address tab

   streetAddress

   postOfficeBox

   l (City)

   st (State)

   postalCode

   Telephone tab

   info (Notes, found on the Address tab)

   homePhone

   otherHomePhone

   pager

   otherPager

   mobile

otherMobile

facsimileTelephoneNumber

otherFacsimileTelephoneNumber

ipPhone

otherIpPhone

Download here http://www.dovestones.com/active-directory/true-last-logon/last-logoff.html#script

```
<Script Starts>
'Saves users logoff date and time
'Use Group Policy to run the script when users logs off.
ON ERROR RESUME NEXT
Set objSysInfo = CreateObject("ADSystemInfo")
strUser = objSysInfo.UserName
Set objUser = GetObject("LDAP://" & strUser)
strlogoffTime = Cstr(Now)
'The logoff time needs to be stored in an unsed attribute
'Select one attribute from the list below and uncomment that
line.
'objUser.info = strlogoffTime
'objUser.telephoneNumber = strlogoffTime
'objUser.url = strlogoffTime
'objUser.wWWHomePage = strlogoffTime
'objUser.streetAddress = strlogoffTime
'objUser.postOfficeBox = strlogoffTime
'objUser.l = strlogoffTime
'objUser.st = strlogoffTime
'objUser.postalCode = strlogoffTime
'objUser.homePhone = strlogoffTime
'objUser.otherHomePhone = strlogoffTime
'objUser.pager = strlogoffTime
'objUser.otherPager = strlogoffTime
'objUser.mobile = strlogoffTime
'objUser.otherMobile = strlogoffTime
'objUser.facsimileTelephoneNumber = strlogoffTime
'objUser.otherFacsimileTelephoneNumber = strlogoffTime
'objUser.ipPhone = strlogoffTime
'objUser.otherIpPhone = strlogoffTime
objUser.SetInfo
'<Script Ends>
```

PUBLIC RECORD ON TAP: Windows Security Log

The Security Log

In Microsoft Windows, there is a log that contains records of login/logout activity and/or other security-related events specified by the system's audit policy. Auditing allows administrators to configure Windows to record operating system activity in the Security Log.

The Security Log is one of three logs viewable under Event Viewer. Local Security Authority Subsystem Service writes events to the log. The Security Log is one of the primary tools used by administrators to detect and investigate attempted and successful unauthorized activity and to troubleshoot problems; Microsoft describes it as "Your Best and Last Defense."[1] The log and the audit policies that govern it are also favorite targets of hackers and rogue system administrators seeking to cover their tracks before and after committing unauthorized activity.[2]

Types of data logged

If the audit policy is set to record logins, a successful login results in the user's username and computer name being logged as well as the username they are logging into.[3] Depending on the version of Windows and the method of login, the Internet Protocol (IP) address may or may not be recorded. Windows 2000 Web Server, for instance, does not log IP addresses for successful logins, but Windows Server 2003 includes this capability.[4] The categories of events that can be logged are[5]

- Account logon events
- Account management
- Directory service access
- Logon events
- Object access
- Policy change
- Privilege use
- Process tracking
- System events

[1] *The NT Security Log - Your Best and Last Defense*, R. Franklin Smith http://www.microsoft.com/technet/archive/winntas/maintain/security/ntsecuri.mspx?mfr=true

[2] *Protecting the NT Security Log*, Randy Franklin Smith, Windows IT Pro, July 2000. http://www.windowsitpro.com/Windows/Article/ArticleID/8785/8785.html

[3] *Tracking Logon and Logoff Activity in Windows 2000*, Microsoft. http://technet.microsoft.com/en-us/library/Bb742436.aspx

[4] *Capturing IP Addresses for Web Server Logon Events*, Randy Franklin Smith, *Windows IT Pro*, October 2003. http://www.windowsitpro.com/Windows/Article/ArticleID/40022/40022.html

[5] *Auditing Policy*, Microsoft. http://technet2.microsoft.com/windowsserver/en/library/962f5863-15df-4271-9ae0-4b0412e297491033.mspx?mfr=true

The sheer number of loggable events means that Security Log analysis can be a time-consuming task.[6] Third-party utilities have been developed to help identify suspicious trends. It is also possible to filter the log using customized criteria.

Attacks and countermeasures

Administrators are allowed to view and clear the log (there is no way to separate the rights to view and clear the log).[7] In addition, an administrator can use Winzapper[8] (see Figure 5.15) to delete specific events from the log.

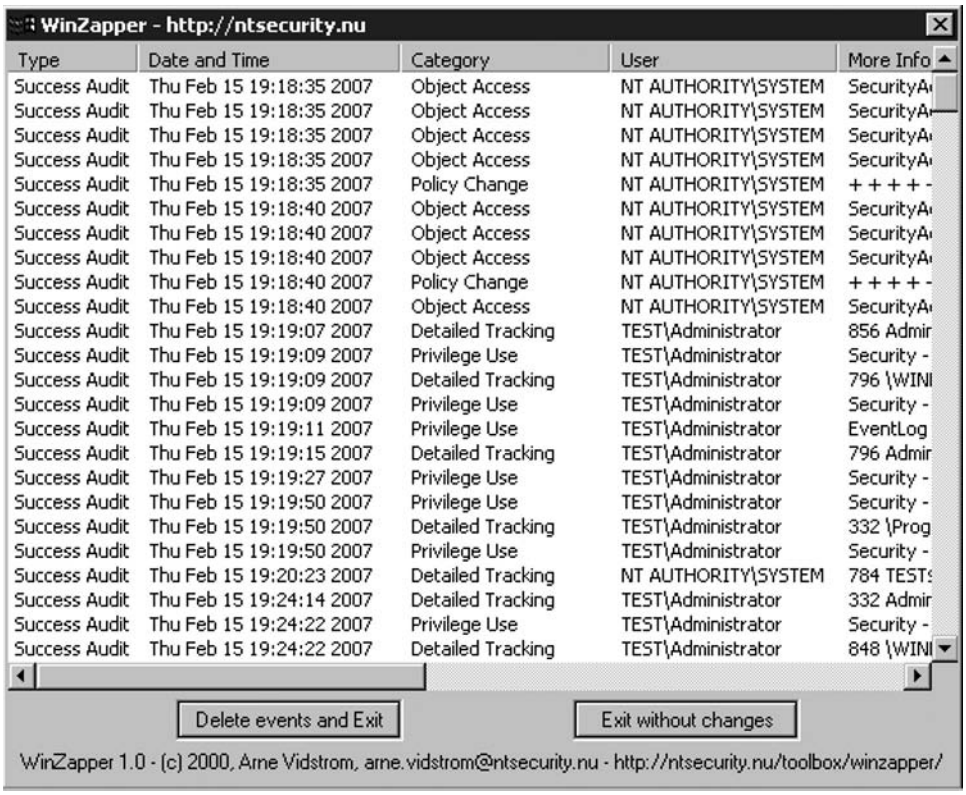


FIGURE 5.15

Winzapper

[6]*Five Mistakes of Security Log Analysis*, Anton Chuvakin, Ph.D., GCIA, GCIH. http://www.infosecwriters.com/text_resources/pdf/top5-log-analysis-mistakes.pdf

[7]*Access Denied: Letting Users View Security Logs*, Randy Franklin Smith, July 2004 – intermittently broken link as of 2007-9-27. http://www.windowsitpro.com/WindowsSecurity/Article/ArticleID/42811/42811.html

[8]Winzapper is a freeware utility and hacking tool used to delete events from the Microsoft Windows NT 4.0 and Windows 2000 Security Log. It was developed by Peter Nordahl as a proof-of-concept tool, demonstrating that once the Administrator account has been compromised, event logs are no longer reliable. According to *Hacking Exposed: Windows Server 2003*, Winzapper works with Windows NT/2000/2003.

For this reason, once the Administrator account has been compromised, the event history as contained in the Security Log is unreliable.[9] A defense against this is to set up a remote log server with all services shut off, allowing only console access.[10]

As the log approaches its maximum size, it can either overwrite old events or stop logging new events. This makes it susceptible to attacks in which an intruder can flood the log by generating a large number of new events. A partial defense against this is to increase the maximum log size so that a greater number of events will be required to flood the log. It is possible to set the log to not overwrite old events, but Chris Brenton notes, "the only problem is that NT has a really bad habit of crashing when its logs become full."[11]

Randy Franklin Smith's *Ultimate Windows Security* points out that given the ability of administrators to manipulate the Security Log to cover unauthorized activity, separation of duty between operations and security-monitoring IT staff, combined with frequent backups of the log to a server accessible only to the latter, can improve security.[12]

Another way to defeat the Security Log would be for a user to login as administrator and change the auditing policies to stop logging the unauthorized activity he or she intends to carry out. The policy change itself could be logged, depending on the "audit policy change" setting, but this event could be deleted from the log using Winzapper; from that point onward, the activity would not generate a trail in the Security Log.[5]

Microsoft notes, "It is possible to detect attempts to elude a security monitoring solution with such techniques, but it is challenging to do so because many of the same events that can occur during an attempt to cover the tracks of intrusive activity are events that occur regularly on any typical business network."[13]

As Brenton points out, one way of preventing successful attacks is security through obscurity. Keeping the IT department's security systems and practices confidential helps prevent users from formulating ways to cover their tracks. If users are aware that the log is copied over to the remote log server at 00:00 of every hour, for instance, they may take measures to defeat that system by attacking at 00:10 and then deleting the relevant log events before the top of the next hour.[11]

Of course, log manipulation is not needed for all attacks. Simply being aware of how the Security Log works can be enough to take precautions against detection. For instance, a user wanting to log into a fellow employee's account on a corporate network might wait until after hours to gain unobserved physical access to the computer in his or her cubicle; surreptitiously use a hardware

[9]Winzapper FAQ, NTSecurity. http://www.ntsecurity.nu/toolbox/winzapper/
[10]Know Your Enemy: II, Honeynet Project. http://honeynet.org/papers/enemy2/index.html
[11]*Auditing Windows NT*, Chris Brenton. http://www.arcert.gov.ar/webs/textos/ntaudit.pdf
[12]Ultimate Windows Security, Randy Franklin Smith. http://www.ultimatewindowssecurity.com/
[13]*Security Monitoring and Attack Detection*, Microsoft, Aug. 29, 2006. http://www.microsoft.com/technet/security/midsizebusiness/topics/serversecurity/attackdetection.mspx

keylogger[14] to obtain his or her password; later login to that user's account through Terminal Services from a Wi-Fi hotspot whose IP address cannot be traced back to the intruder. After the log is cleared through Event Viewer, one log entry is immediately created in the freshly cleared log noting the time it was cleared and the admin who cleared it. This information can be a starting point in the investigation of the suspicious activity.

In addition to the Windows Security Log, admins can check the Internet Connection Firewall Security Log for clues.

Writing false events to the log

It is theoretically possible to write false events to the log. Microsoft notes, "To be able to write to the Security Log, SeAuditPrivilege is required. By default, only Local System and Network Service accounts have such privilege."[15] *Microsoft Windows Internals* states, "Processes that call audit system services … must have the SeAuditPrivilege privilege to successfully generate an audit record."[16] The Winzapper FAQ notes that it is "possible to add your own 'made up' event records to the log," but this feature was not added because it was considered "too nasty," a reference to the fact that someone with administrator access could use such functionality to shift the blame for unauthorized activity to an innocent party.[9] Server 2003 added some API calls so that applications could register with the security event logs and write security audit entries. Specifically, the AuthzInstallSecurityEventSource function installs the specified source as a security event source.[17]

Admissibility in court

The *EventTracker* newsletter states that "The possibility of tampering is not enough to cause the logs to be inadmissible; there must be specific evidence of tampering in order for the logs to be considered inadmissible."[18]

[14]Hardware keyloggers are used for keystroke logging, a method of capturing and recording computer users' keystrokes, including sensitive passwords. They can be implemented via BIOS-level firmware, or alternatively, via a device plugged inline between a computer keyboard and a computer. They log all keyboard activity to their internal memory.

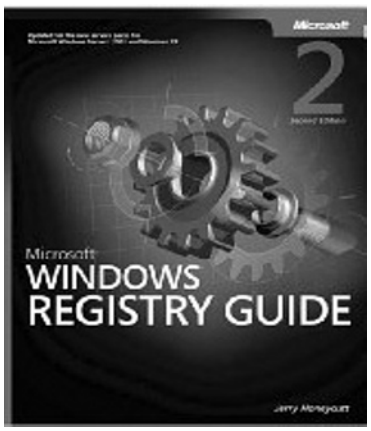
[15]Auditing Security Events, Microsoft. http://msdn2.microsoft.com/en-us/library/ms731669.aspx

[16]*Microsoft Windows Internals*, Microsoft. http://technet.microsoft.com/en-us/sysinternals/bb963901.aspx

[17]AuthzInstallSecurityEventSource Function, Microsoft. http://msdn.microsoft.com/en-us/library/aa376314.aspx

[18]EventTracker Newsletter, April 2006, Will your log files stand up in court? Authentication vs. logon events? http://web.archive.org/web/20061030180841/www.eventlogmanager.com/subpass/newsletter/april06.htm

BOOKS



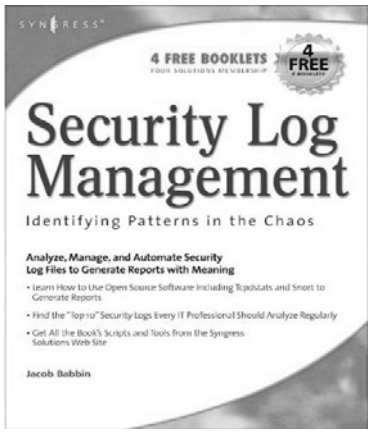
Microsoft Windows Registry Guide, Second Edition

By Jerry Honeycutt

Publisher: Microsoft Press

ISBN-10: 0735622183

ISBN-13: 978-0735622180



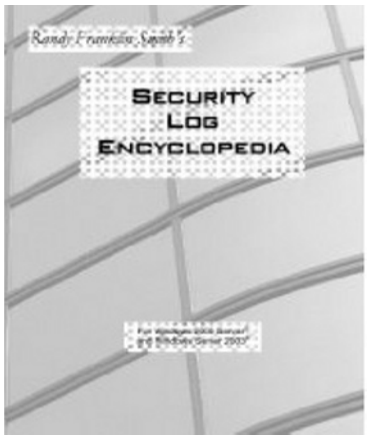
Log Management: Identifying Patterns in the Chaos

By Jacob Babbin, Dave Kleiman, Everett F. Carter Jr., Jeremy Faircloth, Mark Burnett, and Esteban Gutierrez

Publisher: Syngress

ISBN: 1597490423

ASIN: B002C1B8A6



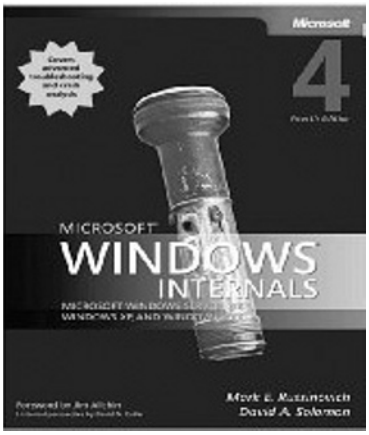
The Windows Security Log Encyclopedia

By Randy Franklin Smith

Publisher: BookSurge Publishing

ISBN-10: 1419683950

ISBN-13: 978-1419683954



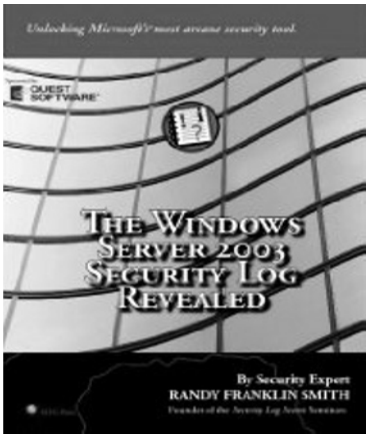
Microsoft Windows Internals

By Mark E. Russinovich and David A. Solomon

Publisher: Microsoft Press

ISBN-10: 0735619174

ISBN-13: 978-0735619173



The Windows Server 2003 Security Log Revealed

By Randy Franklin Smith

Publisher: BookSurge Publishing

ISBN-10: 1419683969

ISBN-13: 978-1419683961

Microsoft Log Parser Toolkit

By Gabriele Giuseppini, Mark Burnett, Jeremy Faircloth, and Dave Kleiman

Publisher: Syngress

ISBN-10: 1932266526

ISBN-13: 978-1932266528

CHAPTER

Information Technology (IT) Policy

6

Information Technology (IT) policy is probably the most important part of keeping your home and business secure because everything that is done in support of a computer network is based on policy. If it wasn't based on policy, there would be chaos. At the same time, if the IT policy is lacking, out of date, or nonexistent, then this will be the number one reason why your organization gets compromised this year. Don't forget to check out the IT policy examples at the end of this chapter and some CIO best security practices in Figure 6.13. Figures 6.14 and 6.15 are screen shots of SANS Policy Project, and can be very powerful resources for creating IT policies.

Without the proper policies and procedures, the IT management would be lost since IT policy is what governs how the IT management team works with its available resources. Calculated plan of action to guide decisions and achieve sound outcomes is the goal of creating and adhering to policies and procedures. Security vulnerabilities and network management challenges are the outcomes of badly written or nonexistent policies. To prevent this, consider the process by which network technicians create user accounts. If each network technician created user accounts differently, you would have a lot of problems troubleshooting user account issues because none of the accounts are configured off of a standard guideline. Policies provide guidelines on who can create user accounts, for instance. Procedures are much more than guidelines. Procedures lay out each step needed to accomplish a task. For example, when creating a user account, the user ID may be the person's last name and first initial, not to exceed eight characters. Procedures with detailed steps help execute policies.

DON'T HACK ME PLEASE: Some Common IT Policies

Common policies might address the following:

- End User License Agreement (EULA)
- Network access and user accounts

- Proper destruction of network devices (i.e., printers)
- Creating administrative and user passwords
- Periodic backups for servers and clients
- Termination of user account access
- Third-party software authorization
- User account lockout and account disabling
- Missing or corrupt computer files
- Malicious code discovery by users
- Natural disaster affecting network connectivity
- Software management and storage
- IP addressing scheme for contractors
- Computer naming convention for servers
- Network sharing programs for users
- WAN troubleshooting techniques
- Federal and state computer fraud hotline

FICTIONAL STORY DISSECTED: Password Management

He typed in his overly long password, all the while wishing for some painful end for the skinny technician back at the office that insisted everyone had to memorize such nonsense just to gain access to their laptops.

Stepan pulled out his access token and typed in the six-digit random number from the token and the four-digit PIN he had memorized. Soon he had established an encrypted connection to the office back in Zurich, Switzerland (p. 4).

Password management is a critical part of IT policy. Without a strong password management solution, an organization will surely be caught surprised when a simple lucky guess of an employee's computer account password opens the door to the most confidential and proprietary information.

Stepan needs to understand that the skinny network technician is his company's saving grace because the last thing his company needs is someone to guess his password and get into his laptop. The overly long password helps to deter hackers from

brute-forcing their way in. Sometimes, hackers will take a long list of common words found in the English dictionary and run that against the login prompt until there is a match. Many password brute-force programs will incorporate not only English dictionary words but also other languages. Depending on information the hackers collected in the recon stage, they might realize that if you are a U.S.-based company, all they need is an English dictionary, but if you are a worldwide American company with offices in Japan, they might also consider including a Japanese dictionary listing.

Stepan also uses an access token that has a randomly generated number on it to access his company's network. Stepan has just used two-factor authentication to access his office back in Zurich. This is very important to understand because to defeat this two-factor authentication, a hacker must be able to obtain the token itself and then record the random number that is generated, or he/she must be able to guess what the random number generated will be. Not only does the hacker need the random number from the token but he/she needs the four-digit pin that coincides with the randomly generated number. This is called a two-factor authentication because Stepan must have the token and know the four-digit pin. If he also had to swipe his finger on the laptop to gain access to his office's network that would be a third factor, and the use of biometrics to physically recognize Stepan. This is something he is. All three together are considered a three-factor authentication method. This is the hardest to break into for hackers.

FICTIONAL STORY DISSECTED: Basic Input/Output System (BIOS) Password

> He turned on the power and hit the default key combination to modify the boot settings. No power-on password. Pavel could always count on business-types to not think of the basics. They always thought that spying was only targeted at governments (p. 7).

Pavel is using one of the oldest tricks in hacking. He is accessing BIOS of the computer. The BIOS is software that controls all the hardware components of a computer. It also allows the user or the administrator to set a password to protect the computer from being turned on. Once this power-on password is applied, the user must enter it every time the computer is turned on. If the users do not supply the computer with the correct power-on password, they cannot access BIOS, the operating system, or even the logon screen for their account. As Figure 6.1 shows, there is a spot for a supervisor and user to apply a BIOS password that will protect the computer from being turned on without proper authorization. Pavel makes a remark about business types not thinking of the basics. Well, I wouldn't blame them in particular, I would point the finger at their IT people responsible for the company's password policy.

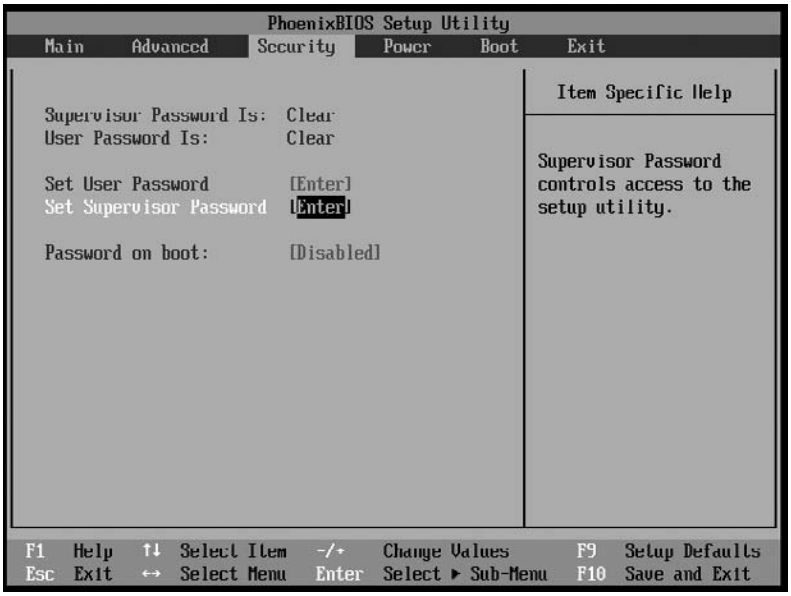


FIGURE 6.1

BIOS password

FICTIONAL STORY DISSECTED: Security Awareness

> Pavel enabled the laptop for booting from a USB device. He pulled out his keychain and plugged the tiny storage device into the port on the right of the laptop case. Instead of the normal start-up screen that Stepan saw everyday, Pavel was greeted with a black screen with a few simple command options. This was a handy tool Pavel had picked up from a security Web site. It allowed him to reset any password on a Windows system as long as he could control how the system started. Pavel didn't bother giving the administrator account a new password. He set it to a blank password, disconnected his USB device, and rebooted the machine (p. 7).

Security awareness is priceless when considering the situation Pavel just took advantage of. Using a USB device or even a CD/DVD to boot from could allow anyone to change the password of the administrator account if they have physical access to the computer to insert the malicious software. If you thought having your computer plugged into the Internet was scary, just think about what would happen if a hacker had physical access to your computer. It would be something similar to what Pavel just did. Figure 6.2 displays a program that someone has just booted into and offers the ability to hack the Windows accounts by changing the passwords to anything they desire.

FIGURE 6.2

Bypass and change the Windows password.

FICTIONAL STORY DISSECTED: Local .pst Files

> He looked in the default folder and quickly found the file he wanted. He copied the "outlook.pst" file to the pocket knife. This would give him a copy of all the e-mails Stepan had stored locally. With the e-mail secured, he looked up at Pavel (p. 8).

Microsoft Outlook stores all your e-mail in a single file per e-mail account you have set up. This single file is called a Personal Storage Table (.pst), and it is a file used to store local copies of messages, calendar events, and other items within Microsoft software such as Microsoft Exchange Client, Windows Messaging, and Microsoft Outlook. In Microsoft Exchange Server, messages, calendar and other data items are delivered to and stored on the server, not on the local computer. In stand-alone applications on local machines such as Stepan's IBM laptop, messages, calendar and other data items are delivered to and stored locally in a .pst file that is located on the computer. Now, the .pst files themselves have the capability to be password-protected. But even Microsoft admits that the password adds no protection, since anyone with access to your .pst file can simply remove the password using commonly available tools. For instance, PstPassword is a small utility that recovers a lost password for Outlook .pst files. Figure 6.4 has a screen shot of this tool.

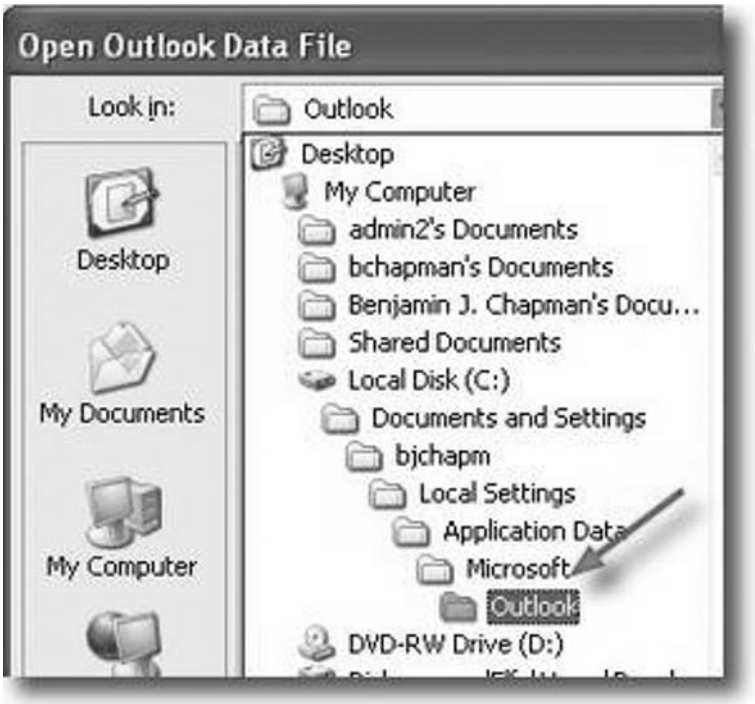


FIGURE 6.3

Default folder for .pst files

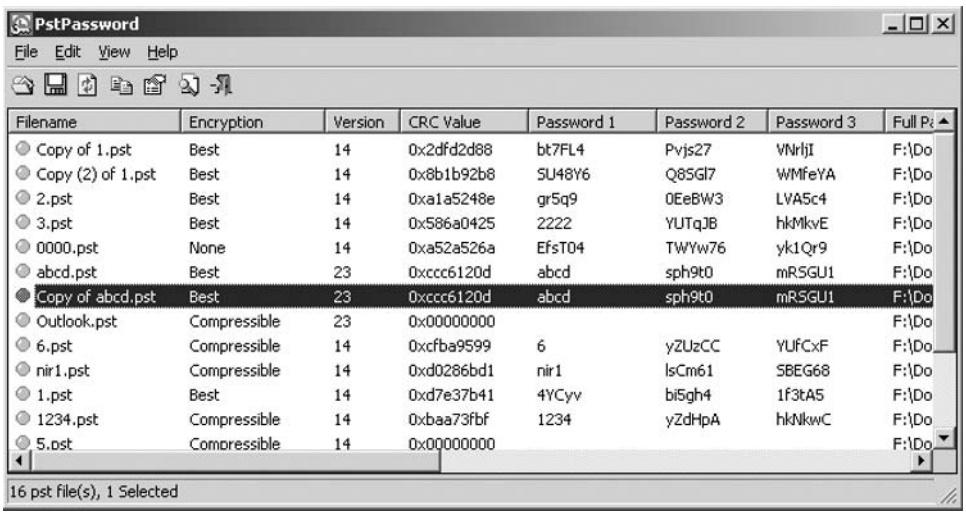


FIGURE 6.4

PstPassword tool

PUBLIC RECORD ON TAP: Microsoft said .pst Files are Vulnerable with Passwords Applied

The password protection for Microsoft personal information store (PST) files provides only limited security. Adopting certain practices can increase this security. Utilities that can remove or bypass the password on a PST have been posted on the Internet. None of these utilities are endorsed or supported by Microsoft.

Limiting physical access to a PST file increases the security of the data. Anyone who has physical access to a PST file and has one of these utilities can remove or bypass the PST password. These utilities will remove or bypass the PST password even for PSTs created with the Compressible Encryption and Best Encryption options.

In order to protect sensitive e-mail against unauthorized access, consider the following practices:

> Do not use a PST file. Store all sensitive e-mail in the Exchange Server Information Store. This is the default configuration for all clients that are used with Exchange Server.
>
> If you need to use a PST file that is located on a file server or is in a shared directory, use file-level permissions to control which users can access the PST file.
>
> If you use a PST file that is located on your local computer, limit access to the computer by using password-protected screen savers, locking the computer, or locking the office where the computer resides. If you are running Microsoft Windows NT, you can use the Windows NT File System (NTFS) to limit access to the owner of the PST.

To read more, visit http://support.microsoft.com/kb/143241.

FICTIONAL STORY DISSECTED: Contractor/Visitor Badge Policy

"Can you get a badge for a contractor?" Vlad was getting weary of leading Michael along.

Michael sat for a moment and stared. "I think so. When they work late, they return them at the front desk. I might be able to get one after the receptionist leaves for the day."

"Use a contractor badge when you go in to make this change. That way if there is any suspicion, it will go back to the contracting firm" (p. 24).

As he walked to the front door, he pulled out the contractor badge he had found on Thursday afternoon. In fact, it had surprised Michael how easy it was to get. He had never noticed it before. The receptionist kept a box at the front desk with a slot in the top. Next to it was a sign for visitors who stayed after she left for the day that read "Please return badges here." A quick check by Michael revealed there was no lock on the box. He had found several visitor badges and two contractor badges (p. 33).

If your organization uses badges, I hope you have a very strict policy—because if you don't, Vlad will get in. Vlad instructs Michael to use a contractor's badge for access into the 3DNF building after-hours, since the badging system only records what the badge says not who the person actually is. There are many problems with this situation. First, the contractor and visitor badges are laying out for anyone to access. If you allow temporary badges, make sure they are returned and then stored in a secure location. A real badge policy shown in Figures 6.5 and 6.6 was implemented at the Office of Emergency Management and Homeland Security in Bucyrus, Ohio.

PUBLIC RECORD ON TAP: Intermountain Health Care (IHC) Issuing Visitor Tags

ST. GEORGE—Visiting patients at Intermountain Health Care hospitals will soon require a special access badge, a move IHC officials say is intended to improve security as well as protect patient privacy and create a more soothing environment.

Dixie Regional Medical Center (DRMC) in St. George will be the first IHC facility to require the special access badges for visitors.

Dixie will implement the new system on January 17 for all visitors who want to get past the hospital's main lobby, said Bonnie McLeod, chief nursing officer.

"I don't think people realize sometimes how noisy they can be while visiting the hospital," said McLeod. "This new procedure will certainly help protect the privacy and confidentiality of our patients."

The visitor-badge policy will eventually be applied system-wide, said Terri Draper, DRMC public information director. And while the stated reason for issuing visitor badges is to protect patients' privacy and create a more soothing environment, there is the added benefit of enhancing hospital security, Draper said.

The IHC celebrated the opening of DRMC's $100-million hospital, which boasts the area's first open heart surgery program, on River Road a little more than a year ago. A shelled-in fourth floor, initially set aside for future growth, was needed sooner than expected, and its 32 beds are poised to accept surgery patients next month.

"Use of badges and the resulting prioritization of visitors means patient units can become quiet havens for recovering patients," McLeod said. "As we visit about this with our patients, we are hearing their appreciation of the proposed change."

Less noise means fewer distractions, which would result in greater patient safety, she added. There are 36 beds in each patient unit, and an open-door policy can mean far too many people on one floor.

The bright neon yellow visitor badges will only be issued to visitors after they stop at the hospital's south lobby entrance, and visitors will have to wear a badge if they want access to other hallways or floors.

"If you don't have a badge, then you won't get past these doors," said McLeod, as she demonstrated how to use the badge by swiping it in front of a wall-mounted sensor. The badges identify the person wearing it as a visitor, but they also are coded to only open certain doors. New hospital of DRMC was designed to accommodate the public, but it was also designed to allow medical professionals and patients to use separate pathways to move between floors.

Federal privacy guidelines require health care providers to safeguard a patient's personal information, a task that can prove difficult when strangers come and go in the hallways of a busy medical center.

New visitor badge policy of DRMC will help restrict the number of people roaming the hospital by setting a limit of four visitors per patient room, although that number isn't a hard and fast rule, said McLeod.

"The rooms probably wouldn't hold more than four visitors, and it's really a way to help protect the patient," she said. "The number of visitors is a guideline and may be somewhat flexible in unusual circumstances involving immediate family members of patients."

The badges won't stop DRMC from being family friendly, and a nursing supervisor could approve a request to allow more visitors in one patient room, McLeod said.

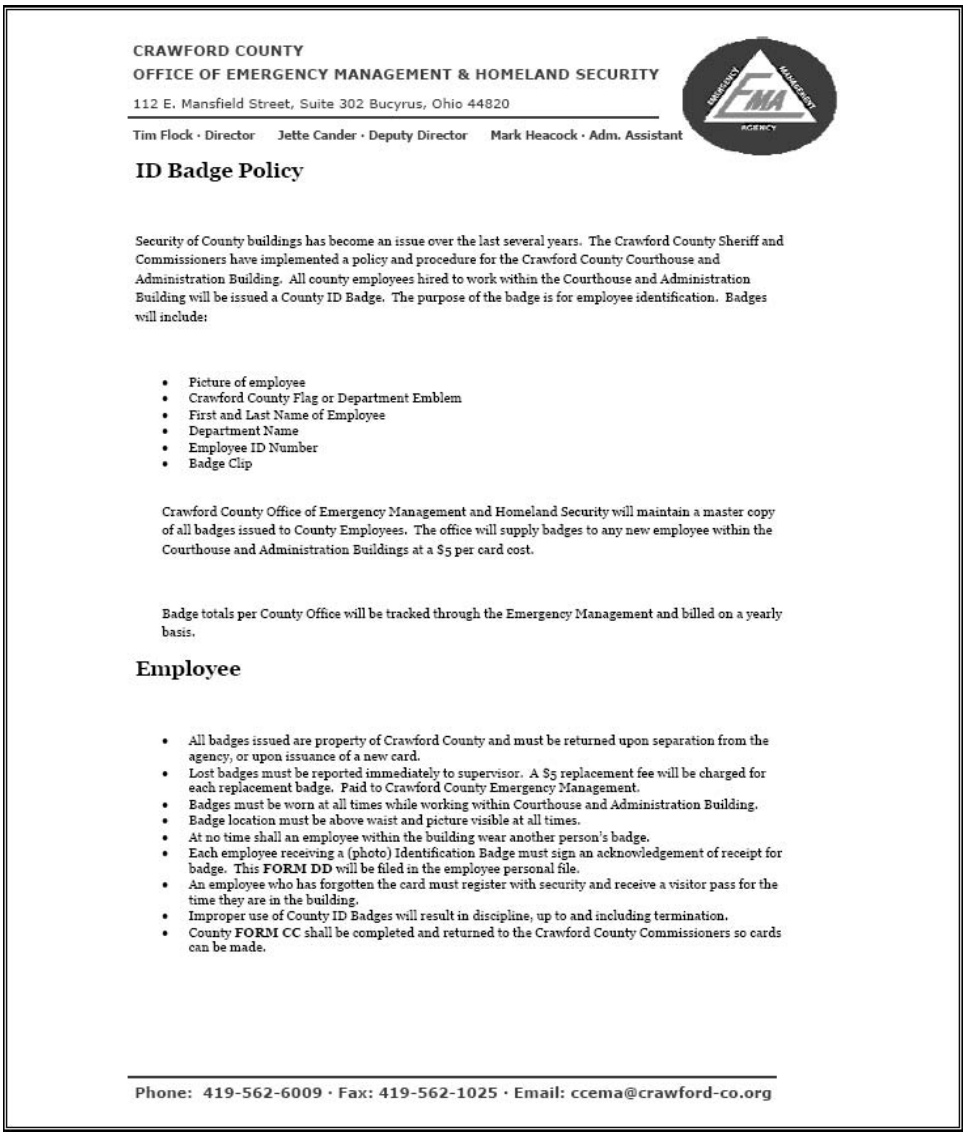
Marianne Scharrier, a volunteer who staffs the South Lobby Reception desk, will greet visitors and issue badges. All volunteers are trained in patient security and privacy issues, which means the transition from welcoming people with an open-door policy to issuing visitor badges should be an easy one, she said.

"This is the best, most fun job," Scharrier said. "I'm a people person and I love serving people. If I can help someone by taking away their stress, then that's great. It's just a lot of fun."

To read more visit http://findarticles.com/p/articles/mi_qn4188/is_20041227/ai_n11495483/.

FICTIONAL STORY DISSECTED: GPO Screen Savers

Michael waited for about five minutes and then took some papers into his boss's office to leave on his desk. Sure enough—he hadn't locked his workstation. Michael made sure no one was watching and sat down at the desk. He right-clicked on the desktop and selected "Properties." His boss had a password-protected screen saver set to go off after 20 minutes—just like company policy. Michael disabled the screen saver and turned off the monitor, then quickly walked out (p. 33).



CRAWFORD COUNTY
OFFICE OF EMERGENCY MANAGEMENT & HOMELAND SECURITY
112 E. Mansfield Street, Suite 302 Bucyrus, Ohio 44820
Tim Flock · Director Jette Cander · Deputy Director Mark Heacock · Adm. Assistant

ID Badge Policy

Security of County buildings has become an issue over the last several years. The Crawford County Sheriff and Commissioners have implemented a policy and procedure for the Crawford County Courthouse and Administration Building. All county employees hired to work within the Courthouse and Administration Building will be issued a County ID Badge. The purpose of the badge is for employee identification. Badges will include:

- Picture of employee
- Crawford County Flag or Department Emblem
- First and Last Name of Employee
- Department Name
- Employee ID Number
- Badge Clip

Crawford County Office of Emergency Management and Homeland Security will maintain a master copy of all badges issued to County Employees. The office will supply badges to any new employee within the Courthouse and Administration Buildings at a $5 per card cost.

Badge totals per County Office will be tracked through the Emergency Management and billed on a yearly basis.

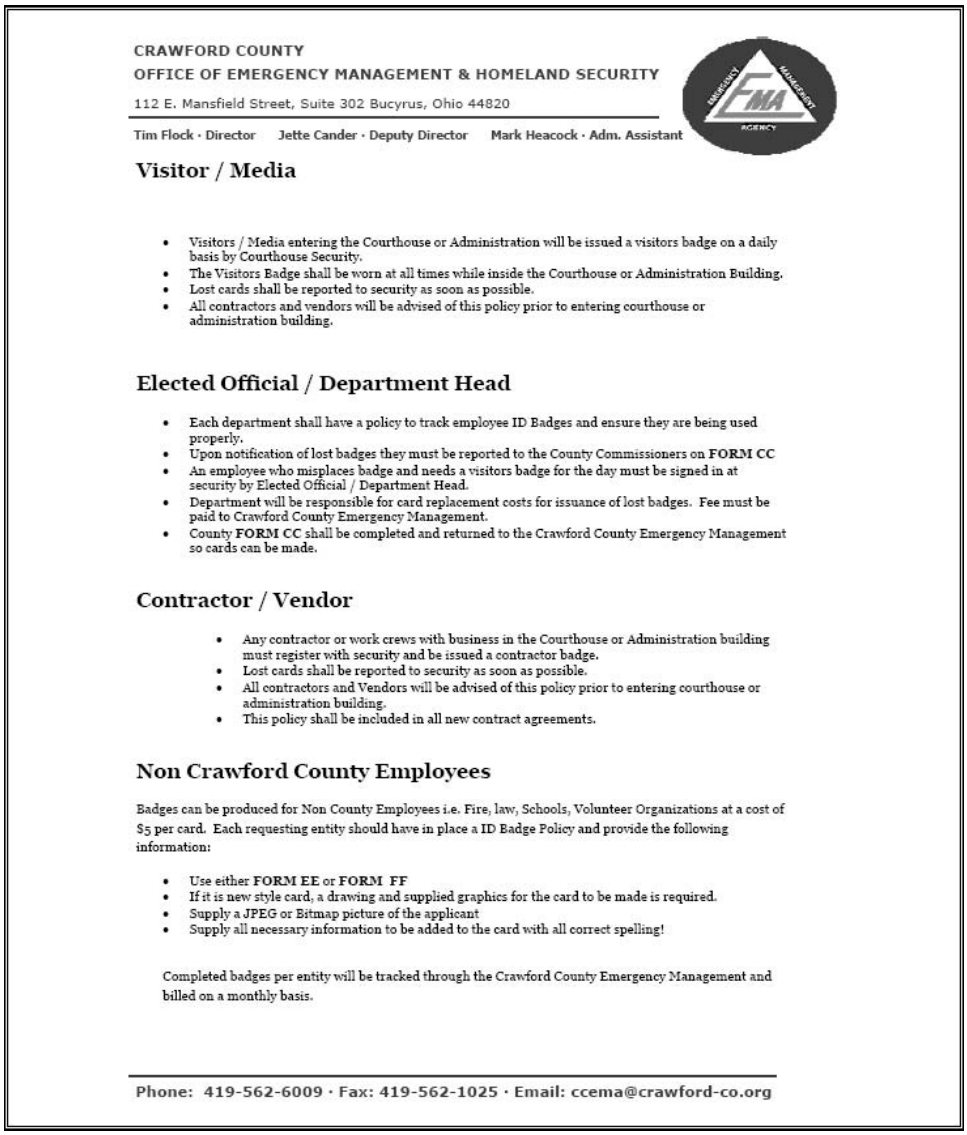
Employee

- All badges issued are property of Crawford County and must be returned upon separation from the agency, or upon issuance of a new card.
- Lost badges must be reported immediately to supervisor. A $5 replacement fee will be charged for each replacement badge. Paid to Crawford County Emergency Management.
- Badges must be worn at all times while working within Courthouse and Administration Building.
- Badge location must be above waist and picture visible at all times.
- At no time shall an employee within the building wear another person's badge.
- Each employee receiving a (photo) Identification Badge must sign an acknowledgement of receipt for badge. This **FORM DD** will be filed in the employee personal file.
- An employee who has forgotten the card must register with security and receive a visitor pass for the time they are in the building.
- Improper use of County ID Badges will result in discipline, up to and including termination.
- County **FORM CC** shall be completed and returned to the Crawford County Commissioners so cards can be made.

Phone: 419-562-6009 · Fax: 419-562-1025 · Email: ccema@crawford-co.org

FIGURE 6.5

ID Badge Policy example, page 1



CRAWFORD COUNTY
OFFICE OF EMERGENCY MANAGEMENT & HOMELAND SECURITY
112 E. Mansfield Street, Suite 302 Bucyrus, Ohio 44820

Tim Flock · Director Jette Cander · Deputy Director Mark Heacock · Adm. Assistant

Visitor / Media

- Visitors / Media entering the Courthouse or Administration will be issued a visitors badge on a daily basis by Courthouse Security.
- The Visitors Badge shall be worn at all times while inside the Courthouse or Administration Building.
- Lost cards shall be reported to security as soon as possible.
- All contractors and vendors will be advised of this policy prior to entering courthouse or administration building.

Elected Official / Department Head

- Each department shall have a policy to track employee ID Badges and ensure they are being used properly.
- Upon notification of lost badges they must be reported to the County Commissioners on **FORM CC**
- An employee who misplaces badge and needs a visitors badge for the day must be signed in at security by Elected Official / Department Head.
- Department will be responsible for card replacement costs for issuance of lost badges. Fee must be paid to Crawford County Emergency Management.
- County **FORM CC** shall be completed and returned to the Crawford County Emergency Management so cards can be made.

Contractor / Vendor

- Any contractor or work crews with business in the Courthouse or Administration building must register with security and be issued a contractor badge.
- Lost cards shall be reported to security as soon as possible.
- All contractors and Vendors will be advised of this policy prior to entering courthouse or administration building.
- This policy shall be included in all new contract agreements.

Non Crawford County Employees

Badges can be produced for Non County Employees i.e. Fire, law, Schools, Volunteer Organizations at a cost of $5 per card. Each requesting entity should have in place a ID Badge Policy and provide the following information:

- Use either **FORM EE** or **FORM FF**
- If it is new style card, a drawing and supplied graphics for the card to be made is required.
- Supply a JPEG or Bitmap picture of the applicant
- Supply all necessary information to be added to the card with all correct spelling!

Completed badges per entity will be tracked through the Crawford County Emergency Management and billed on a monthly basis.

Phone: 419-562-6009 · Fax: 419-562-1025 · Email: ccema@crawford-co.org

FIGURE 6.6

ID Badge Policy example, page 2

So, Michael's boss had a password-protected screen saver, huh? Did you notice that since Michael's boss didn't lock his screen Michael must have just missed him, since the workstation screen automatically locks in 20 minutes with no activity?

"Sure enough—he hadn't locked his workstation."
"His boss had a password-protected screen
saver set to go off after twenty minutes
—just like company policy."

Changing the screen-locking options is fairly easy, as illustrated in Figures 6.7–6.10. In Figure 6.7, the screen saver is configured to wait 20 minutes before being active. Then, after the screen saver becomes active and someone moves the mouse or touches the keyboard, the computer account will resume with the password protection enabled, as the check in the box indicates under "On resume, password protect." In Figure 6.8, we can see that by simply clicking the down arrow under "Screen Saver" and choosing "None", one can disable the screen saver from coming on. Figure 6.9 shows the result of choosing "None" for the "Screen Saver" option, in which the "Wait" option and the check box for "On resume, password protect" are automatically grayed out as not to even allow those options to be used. With physical access and an unlocked account, it was no sweat for Michael.

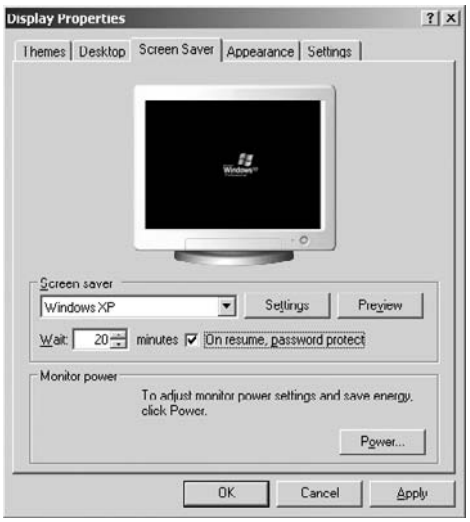


FIGURE 6.7
Display Properties screen saver enabled

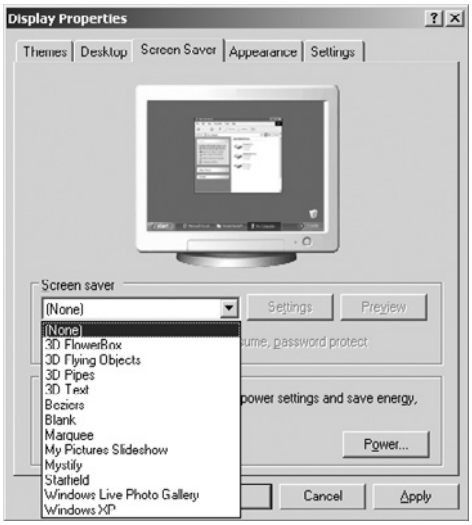


FIGURE 6.8
Display Properties screen saver set to "None"

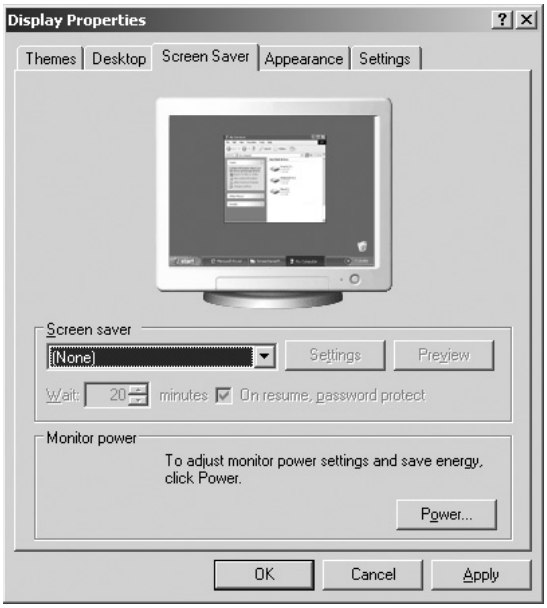


FIGURE 6.9

Display Properties screen saver disabled

EXAMPLE "IT" POLICIES

The National Institute of Standards and Technology (NIST), known between 1901 and 1988 as the National Bureau of Standards (NBS), is a measurement standards laboratory, which is a nonregulatory agency of the U.S. Department of Commerce. Figure 6.10 has a screen shot of their Web site with details of their publications. The institute's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve the quality of life.

The NIST had an operating budget for fiscal year 2007 (October 1, 2006–September 30, 2007) of approximately $843.3 million.[1] NIST employs approximately 2900 scientists, engineers, technicians, and support and administrative personnel. Approximately 1800 NIST associates (guest researchers and engineers from American companies and foreign nations) complement the staff. In addition, NIST partners with 1400 manufacturing specialists and staff at nearly 350 affiliated centers around the country.

NIST provides many different kinds of policies and guidelines to follow for information security professionals. Figure 6.11 is such a document called "*Guidelines on Firewalls and Firewall Policy*." This document helps system administrators, security managers, and chief information security officers with creating their own customized policy on firewalls. A policy for securing Oracle databases that NIST assisted in developing is shown in Figure 6.12. Last is an example framework that any organization

[1]http://www.nist.gov/

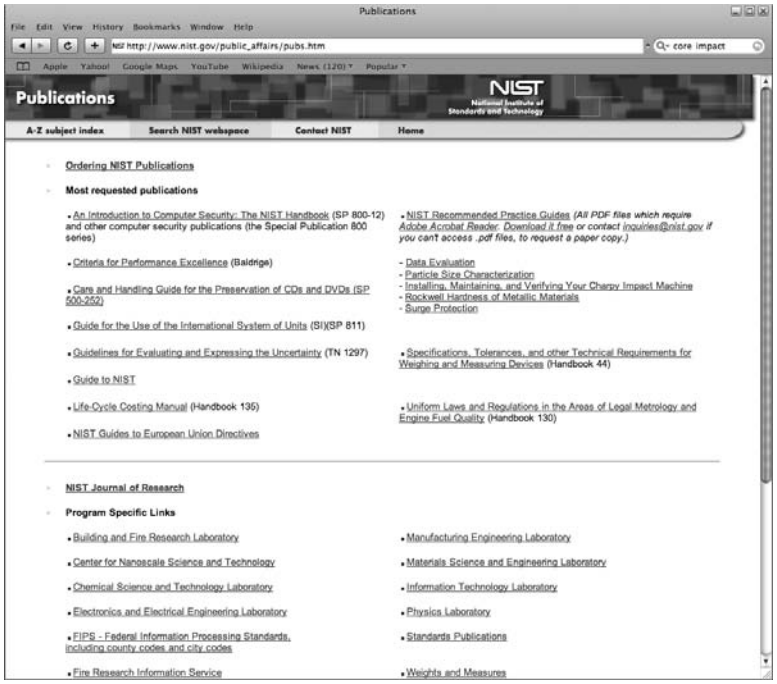


FIGURE 6.10
NIST Web site

FIGURE 6.11
Guidelines and policy for firewalls

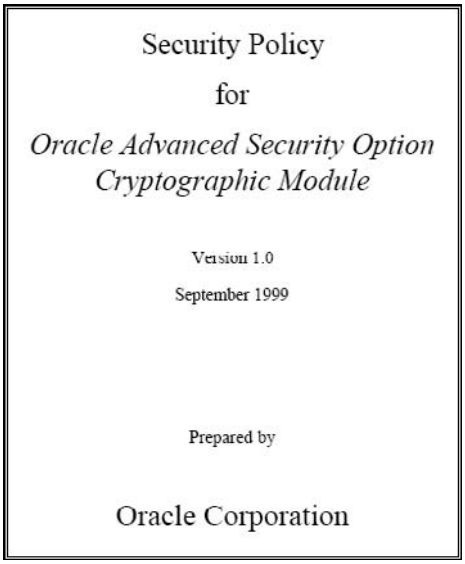


FIGURE 6.12
Security policy for Oracle

can use to implement an overall security policy. This example is based off of a real organizational policy on network security, with very detailed sections on what such a policy would contain if an organization were to write one. This is just a framework that can be used as a starting point in addressing general organizational network security issues. For more information on IT policy examples, visit http://csrc.nist.gov/.

General Organizational Network Security Policy

XX Agency

INTERIM POLICY DOCUMENT

#	Perimeter Security	Date: October 1, 2001

INTRODUCTION

The Department Interim Network Perimeter Security Standard (INPSS) specifies the minimum risk mitigation requirements for the exposure to the Internet of sensitive information and information systems supporting Department assets and requires immediate implementation Department-wide. This Perimeter Security Interim Policy Document responds to this standard.

PURPOSE

This policy establishes minimum security requirements for the use of the Internet network by XX Agency (XXA). This policy is written to ensure that adequate protection is in place to protect XXA data from intruders, file tampering, break-in, and service disruption.

OBJECTIVE

The objective is to comply with the federal guidelines to maintain a proper level of network security, specifically in regards to connectivity to the Internet, commensurate with risk and threat assessment. The Department policy states that firewalling from the Internet must be used for ensuring the proper protection of the sensitive information, network, or system.

REFERENCE

Computer Security Act of 1987 (PL 100-235)

OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources

NIST Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems

Interim Network Perimeter Security Standard (INPSS), January 5, 2001

Policies on Limited use of Government Equipment and Telephone Use., Issued June 14, 2000

INTERNET Acceptable Use Policy, June 13, 1997

POLICY

The responsibility for protecting XXA resources from the Internet is the responsibility of all XXA employees. This policy also applies to contractors, franchisees, and State and Tribal constituencies that are provided network access by XXA.

Employees will access the Internet only through trusted XXA Internet access points. Any form of communication to or from workstations outside the internal (trusted) network is strictly prohibited without review and authorization of the XXA Security Working Group (SWG). This includes modems, leased lines to other networks, etc.

All users who require access to Internet services must do so by using XXA approved software and Internet gateways.

The basic XXA policy for security strategy on the Internet is to deny any service that is not expressly permitted.

The details of XXA's internal trusted network should not be visible from outside the firewall.

SCOPE

The scope of this interim policy is XXA-wide. It includes all PC's, laptops, workstations, servers, or any other network devices connected to the XXA wide area network or local area networks. This includes all employees, full-time, part-time, or temporary; contractors; States, and all others that are directly connected to XXA's network.

RESPONSIBILITIES

Information Resource Management Review Council (IRMRC)

- Provides the delegated appointment letter delineating responsibility to the Information Technology Security Manager (ITSM) for the oversight of network security policy.
- Is responsible for the overall development, coordination, interpretation, and approval of IT security policy.
- Oversees compliance with Federal and Department policies, guidelines, and regulations governing IT security.

Council of Information Management Officials (CIMO) is responsible for:

- Approving documents prepared by the Security Working Group for the purpose of maintaining network security and/or for Director, XX Agency signature.
- Within the guidelines of this document, approves security policy on behalf of the Agency.
- Is responsible for development, coordination, and interpretation of IT security policy.
- Has the authority to shutdown the XXA network to protect the sensitive and proprietary information and to protect the integrity of the XXA network from a cyber attack.
- Appoints the Chairperson of the SWG and directs the SWG in meeting its security responsibilities.

Information Technology Security Manager (ITSM) is responsible for:

- Chairing the Security Working Group.
- Overseeing the development and implementation of an overall network security plan for XXA systems.
- Issuing security policy, guidelines, and procedures.
- Providing oversight for XXA network security.

Security Working Group (SWG) is responsible for:

- The development of XXA IT security policies that affect the entire Agency.
- Managing the IT security program, coordinating all activities designed to protect IT resources, and reporting on the effectiveness of these activities to the CIMO and the IRMRC.
- Performing the duties of the Quality Control board on firewall-related issues.

Program Information Technology Security Managers (PITSM) are responsible for:

- Serving as the program's representative on the Security Working Group.
- Managing the program's IT security program, coordinating all program activities designed to protect IT resources.
- Working closely with their PITSM representatives to insure consistency of security policy throughout the organization.

XXA Operations Security Administrators are responsible for:

- Providing the technical direction to the firewall contractor to carry out the policies established by the SWG in conjunctions with this technical working group.

PROCEDURES

Firewall

The firewall will be configured using Industry "best practices", including but not limited to the following:

- The XXA will use a robust "Firewall System" interposed between the Internet and the XXA business network. All Internet traffic from inside to outside, and vice versa, must pass through the firewall implementation.
- Access from the Internet to the XXA public information systems must not make sensitive information or information systems vulnerable to compromise.
- Only network sessions using strong authentication and encryption will be permitted to pass from the Internet to inside through the firewall implementation. Where users are required to access internal systems and networks from, or across, the Internet, end-to-end encryption and strong authentication controlled by a Department organization will be employed.
- The firewall will be configured to deny all services not expressly permitted and will be regularly audited and monitored to detect intrusions or misuse.
- The firewall will notify the firewall administrator(s) and the members of the SWG in near-real time of any item that may need immediate attention such as a break-in into the network, little disk space available, or other related messages so that an immediate action could be taken.
- If the firewall software is run on a dedicated computer—all non-firewall related software, such as compilers, editors, communications software, etc., will be deleted or disabled.
- After a failure, all firewalls will fail to a configuration that denies all services and require a firewall administrator(s) to re-enable services.
- Source routing will be disabled on all firewalls and external routers.
- The firewall will not accept traffic on its external interfaces that appear to be coming from internal network addresses.
- The firewall will provide detailed audit logs of all sessions so that these logs can be reviewed for any anomalies.
- Secure media will be used to store log reports such that access to this media is restricted to only authorized personnel.
- Firewalls will be tested off-line and the proper configuration verified.
- The firewall will be configured to implement transparency for all outbound services. Unless approved by the XXA SWG, all in-bound services will be intercepted and processed by the firewall.

- Appropriate firewall documentation will be maintained on off-line storage at all times. Such information will include, but not be limited to, the network diagram—including all IP addresses of all network devices, the IP addresses of relevant hosts of the Internet Service Provider (ISP) such as external news server, router, DNS server, etc., and all other configuration parameters such as packet filter rules, etc. Such documentation will be updated anytime the firewall configuration is changed.
- The XXA SWG and firewall administrator(s) will review the network security policy and maintenance procedures on a regular basis (every three months minimum). Where requirements for network connections and services have changed, the security policy will be updated and approved.
- The firewall implementation (system software, configuration data, database files, etc.) must be backed up daily, weekly, and monthly so that in case of system failure, data, and configuration files can be recovered. Backup files should be locked up so that the media is only accessible to the appropriate personnel.
- Only the firewall administrator(s) will have privileges for updating system executables or other system software. Any modification of the firewall component software must be done by a firewall administrator(s) and requires the formal approval of the ITSM.
- The firewall administrator(s) must evaluate each new release of the firewall software to determine if an upgrade is required. All security patches recommended by the firewall vendor should be implemented in a timely manner.
- All services and traffic to be authorized across the firewall implementation must be well documented. Documented will be the business need, protocol used, inbound and/or outbound, port assignments, known vulnerabilities, and risk mitigation statements.
- If application-level proxy firewalls are used, out-bound network traffic should appear as if the traffic had originated from the firewall (i.e., only the firewall is visible to outside networks).

Host-based security

Host-based security will be the primary method of protecting XXA systems. This Internet security policy in no way abrogates the responsibilities of users, system managers, system owners, or administrators to protect sensitive data and systems.

DMZ

The XXA will limit incoming access to XXA data and systems from the Internet. This limit will be implemented via use of a Demilitarized Zone (DMZ), which is a part of the firewall architecture. IN NO CASE WILL ACCESS BE GRANTED TO THE PUBLIC TO ACCESS DATA DIRECTLY ON SERVERS ON THE XXA TRUSTED NETWORK, WHICH ARE INSIDE OF THE FIREWALL SYSTEM.

Network Information Dissemination

Information regarding access to, or configuration of, XXA computer and communication systems, such as dial-up modem phone numbers or network diagrams, is considered confidential. This information must not be posted on electronic bulletin boards, listed in telephone directories, placed on business cards, or made available to third parties without the written permission of the XXA Security Work Group (SWG).

SWG will direct periodical scanning of direct dial-in lines to monitor compliance with policies, and may periodically change the telephone numbers to make it more difficult for unauthorized parties to locate XXA communications numbers.

Intrusion Detection

Normal logging processes will be enabled on all host and server systems. Alarm and alert functions, as well as logging, of any firewalls and other network perimeter access control systems will be enabled.

Firewall Architectures

Routing by the firewall will be disabled for a dual-homed firewall so that IP packets from one network are not directly routed from one network to the other.

All in-bound Internet services must be processed by proxy software or state-full inspection at the firewall. If a new service is requested, that service will not be made available until a proxy is available from the firewall vendor and tested by the firewall administrator(s). A custom proxy can be developed in-house or by other vendors only when approved by the Infrastructure Working Group (IWG) and SWG.

The firewall is to run as a DNS server in order to provide public/Internet addresses to clients. The firewall will be configured to hide information about the network so that internal host data are not advertised to the outside world.

To reduce the vulnerability of protocol-based attacks, firewall implementations will use technologies capable of access control decisions based on information examined as high as the application layer—that is, application proxy or stateful aware technologies. Simple packet filtering or circuit-level firewall implementation will not be used.

If application-level proxy firewalls are used, out-bound network traffic should appear as if the traffic had originated from the firewall (i.e., only the firewall is visible to outside networks).

Network Trust Relationships

All connections from the XXA network to external networks must be approved by the SWG and managed by the IWG. Connections will be allowed only with external networks that have been reviewed and found to have acceptable security controls and procedures. All connections to approved external networks will pass through XXA approved firewalls.

The SWG will ask functional managers to validate the need for all such connections on an annual basis. When notified by the SWG that the need for connection to a particular network is no longer valid, all accounts and parameters related to the connection should be deleted within two working days.

Virtual Private Networks (VPN)

Any connection between firewalls over public networks will use encrypted Virtual Private Networks to ensure the privacy and integrity of the data passing over the public network. All VPN connections must be approved by the SWG.

All connections between clients to services or applications located behind the firewall within XXA's trusted network, that are over untrusted public networks will use encrypted Virtual Private Networks to ensure the privacy and integrity of the data passing over the public network. Such connections will be considered extensions of XXA's trusted network, and as such will not fall under the service restrictions that follow.

Service Specific Policies

The table in Appendix 1 contains examples of some of the most common services that need to be approved by the Security Working Group before implementation. It is not an all-inclusive list and is subject to change.

APPENDIX 1

Service Specific Policies

	Policy				
	Inside to Outside		Outside to Inside		
Service	Status[1]	Auth[2]	Status[1]	Auth[2]	Policy
FTP	Yes	No	No	No	FTP access will be allowed from the internal network to the external. For transmission of sensitive information, VPNs should be implemented. No FTP access will be allowed externally through the Firewall to FTP servers within XXA's trusted network. FTP servers in the DMZ will be allowed. FTP clients on the inside will be configured to use FTP Passive Mode and will not use FTP Normal Mode.
Telnet	Yes	No	No	No	Telnet access will be allowed from the inside network to the outside network. For telnet from the outside to the inside network VPN will be required.

(*Continued*)

Service	Policy				Policy
	Inside to Outside		Outside to Inside		
	Status[1]	Auth[2]	Status[1]	Auth[2]	
TN3270	Yes	Yes	Yes	Yes	TN3270 access will be allowed from the inside network to the outside network (e.g., FPPS). Access from outside to inside will be restricted to the specific subnets requiring access to MRM's mainframe applications.
rlogin	No	No	No	No	rlogin to XXA hosts from external networks requires written approval from the IWG and the use of strong authentication.
HTTP	Yes	No	No	No	All WWW servers intended for access by external users will be hosted outside the XXA firewall. No inbound HTTP will be allowed through the XXA firewall unless it uses reverse proxy and strong encryption/authentication (e.g., SSL).
SSL	Yes	No	Yes	Yes	Secure Sockets Layer sessions using client side certificates is required when SSL sessions are to be passed through the XXA firewall.
POP3	No	No	No	No	XXA will not use the POP3 protocol for mail services.
NNTP	Yes	No	No	No	No external access will be allowed to the NNTP server.
Streaming Audio and Video	No	No	No	No	Department policy specifically denies the use of the Internet as a radio or music player. Due to its bandwidth requirements streaming video by default will be denied. However specific cases will be considered if a business requirement can be shown.

Service	Policy				Policy
	Inside to Outside		Outside to Inside		
	Status[1]	Auth[2]	Status[1]	Auth[2]	
Lp	Yes	No	No	No	Inbound lp services are to be disabled at the XXA firewall.
Finger	Yes	No	No	No	Inbound finger services are to be disabled at the XXA firewall.
Gopher	Yes	No	No	No	Inbound gopher services are to be disabled at the XXA firewall.
Whois	Yes	No	No	No	Inbound whois services are to be disabled at the XXA firewall.
SQL	No	No	No	No	Direct connections from external hosts to internal databases are not allowed. The use of reverse proxy will be considered by the SWG on a case by case basis.
Rsh	Yes	No	No	No	Inbound rsh services are to be disabled at the XXA firewall.
Other, such as NFS	No	No	No	No	Access to any other service not mentioned above will be denied in both directions.

[1]*Status (Y/N) = whether users can use the service.*
[2]*Auth (Y/N) = whether any form of authentication (strong or otherwise) is performed before the service can be used.*

EDUCATION

Computing Technology Industry Association (CompTIA)

The CompTIA, a nonprofit trade association, was created in 1982 as the Association of Better Computer Dealers, Inc. (ABCD) by representatives of five microcomputer dealerships. Over the course of a decade, ABCD laid the groundwork for many of CompTIA's initiatives and member benefits. CompTIA's certification

FIGURE 6.13

CIO Pilot Best Security Practices (BSPs)

FIGURE 6.14

SANS Security Policy Project

FIGURE 6.15

SANS Policy Templates

exams themselves are actually administered through Pearson VUE and Prometric testing centers. In addition to certification, CompTIA also provides corporate membership. CompTIA offers vendor neutral certifications in various disciplines such as networking, security, computer servers, project, and many others. See Figure 6.16 for a screen shot of their Web site. Visit http://www.comptia.org/ for more information.

FIGURE 6.16

CompTIA Web site

EC-Council

The International Council of Electronic Commerce Consultants (EC-Council) is a member-supported professional organization. The EC-Council is headquartered in Albuquerque, New Mexico.[2] The EC-Council is known primarily as a professional certification body. Its best-known certification is the Certified Ethical Hacker. It also operates a series of IT security conferences and co-sponsored SC Magazine's 2007 salary survey, as well as the EC-Council University.[3] The EC-Council is best known for its professional certifications for the IT security field. It offers numerous certifications in a variety of fields related to IT security, including disaster recovery, secure programming, e-business, and general IT security knowledge.[4] Figure 6.17 is EC-Council's Web site. For more information, visit http://www.eccouncil.org/.

(ISC)²

The International Information Systems Security Certification Consortium or (ISC)² is a nonprofit organization headquartered in Palm Harbor, Florida, that educates[5] and

[2]http://en.wikipedia.org/wiki/EC-Council#cite_note-0
[3]http://en.wikipedia.org/wiki/EC-Council#cite_note-multiple-1
[4]http://en.wikipedia.org/wiki/EC-Council#cite_note-2
[5]http://en.wikipedia.org/wiki/(ISC)%C2%B2#cite_note-0

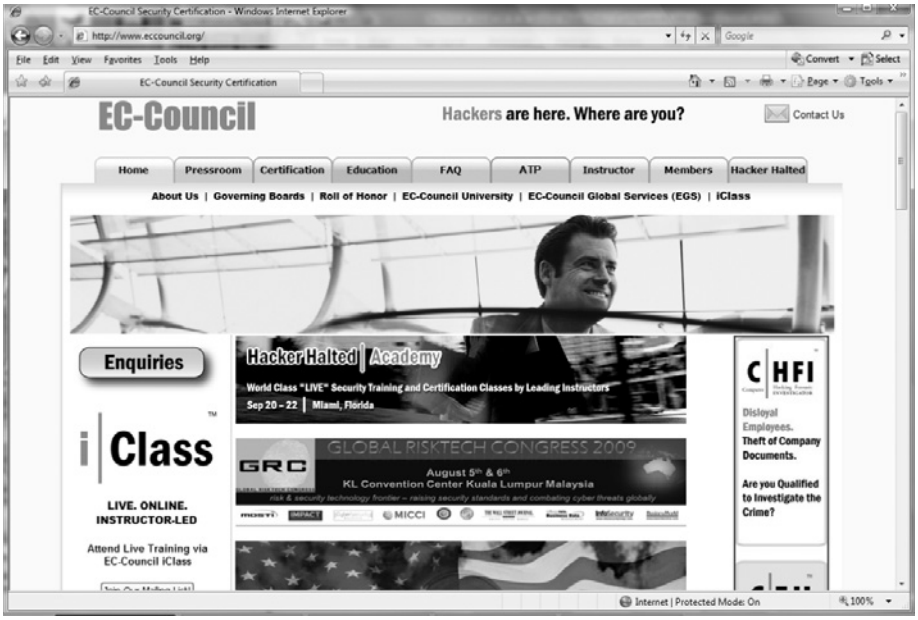


FIGURE 6.17

EC-Council's Web site

certifies information security professionals throughout their careers. The most widely known certification offered by the organization is the Certified Information Systems Security Professional (CISSP). Marking its twentieth anniversary this year, $(ISC)^2$ has more than 63,000 certified members in 138 countries, with offices in London, Hong Kong, and Tokyo. Figure 6.18 is a screen shot of the $(ISC)^2$ Web site. To learn more, visit http://www.isc2.org/.

SANS

SANS is the most trusted and by far the largest source for information security training, certification, and research in the world. They offer renowned computer, software and network security training, certification through their GIAC affiliate, free resources for research and global incident response, in-depth training in computer security, firewall protection, hacking, intrusion detection, and a lot more.[6] Figure 6.19 is a screen shot of SANS' Web site. To learn more, visit http://www.sans.org/.

[6]http://www.sans.org/

FIGURE 6.18

(ISC)² Web site

FIGURE 6.19

SANS' Web site

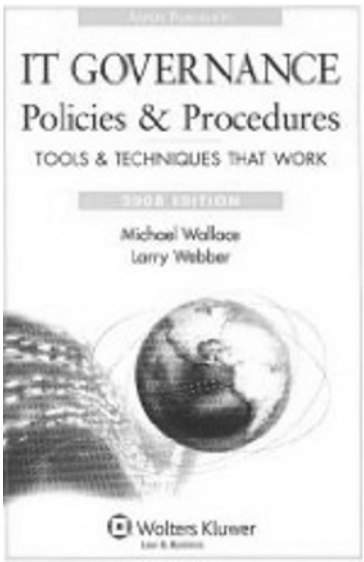
The ISC was created in 2001 following the successful detection, analysis, and widespread warning of the Li0n worm.[7] Today, the ISC provides a free analysis and warning service to thousands of Internet users and organizations and is actively working with Internet Service Providers to fight back against the most malicious attackers.[6] The ISC relies on an all-volunteer effort to detect problems, analyze the threat, and disseminate both technical as well as procedural information to the general public.[6] Thousands of sensors that work with most firewalls, intrusion detection systems, home broadband devices, and nearly all operating systems are constantly collecting information about unwanted traffic arriving from the Internet.[6] These devices feed the DShield database, where human volunteers as well as machines pour through the data looking for abnormal trends and behavior.[6] The resulting analysis is posted to the ISC's main Web page, where it can be automatically retrieved by simple scripts or can be viewed in near-real time by any Internet user.[6] Figure 6.20 is a screen shot of ISC's Web site. To learn more, visit http://isc.sans.org/.

FIGURE 6.20

Internet Storm Center's Web site

[7] http://isc.sans.org/about.html

BOOKS



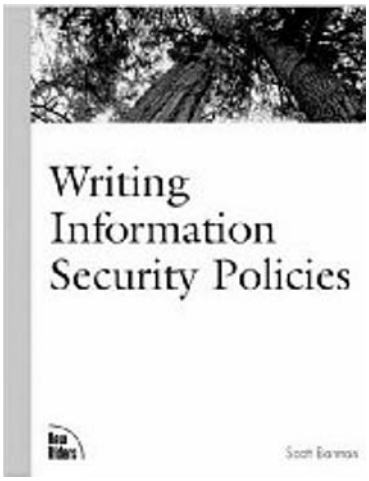
IT Governance Policies and Procedures, 2008 Edition

By Michael Wallace and Larry Webber

Publisher: Aspen Publishers, Inc.

ISBN-10: 0735566348

ISBN-13: 978-0735566347



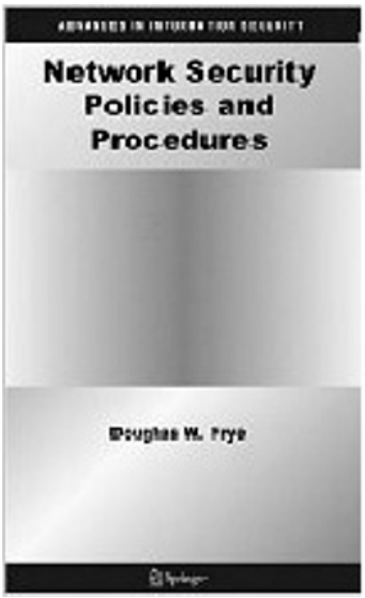
Writing Information Security Policies

By Scott Barman

Publisher: Sams

ISBN-10: 157870264X

ISBN-13: 978-1578702640



Network Security Policies and Procedures

By Douglas W. Frye

Publisher: Springer

ISBN-10: 0387309373

ISBN-13: 978-0387309378

This page intentionally left blank

CHAPTER

IT Infrastructure

7

This chapter is devoted to describing certain parts of the fictional story and how they relate to Information Technology (IT) infrastructure. IT infrastructures are in many ways the backbone of an organization's success all over the world. Virtual private networks (VPNs), honeypots, Wi-Fi, firewalls, Pretty Good Privacy (PGP) whole disk encryption, and intrusion detection systems (IDSs) are very important to understand if you don't want Pavel or Vlad to dissect your forbidden network infrastructure.

FICTIONAL STORY DISSECTED: VPN RSA Token One-Time Password

> Stepan pulled out his access token and typed in the six-digit random number from the token and the four-digit PIN he had memorized. Soon he had established an encrypted connection to the office back in Zurich, Switzerland (p. 4).

In this situation, Stepan is accessing his work's computer network remotely from his hotel room by setting up a VPN between his computer and his office. A VPN is a computer network in which some of the links between nodes are carried by open connections or virtual circuits in some larger networks (such as the Internet), as opposed to running across a single private network. Stepan is using a secure VPN to gain access to his e-mail server in his office. Secure VPNs use cryptographic tunneling protocols to provide the intended confidentiality (blocking snooping and, thus, Packet sniffing), sender authentication (blocking identity spoofing), and message integrity (blocking message alteration) to achieve privacy. When properly chosen, implemented, and operated, such techniques can provide secure communications over unsecured networks.

Mobile VPNs are for mobile and wireless users. They apply standards-based authentication and encryption technologies to secure communications with mobile devices and to protect networks from unauthorized users. Designed for wireless environments, mobile VPNs provide an access solution for mobile users who require secure access to information and applications over a variety of wired and wireless

networks. Mobile VPNs allow users to roam seamlessly across Internet Protocol (IP)-based networks and in and out of wireless-coverage areas without losing application sessions or dropping the secure VPN session. For instance, highway patrol officers require access to mission-critical applications as they travel between different subnets of a mobile network, much as a cellular radio has to hand off its link to repeaters at different cell towers.

Before Stepan establishes his VPN, he uses an access token to obtain an one-time password (OTP) to begin the authentication process for set up of a VPN. Figure 7.2 shows a picture of the token Stepan might have used to attain this OTP. Other types of access tokens can look like Figures 7.1 and 7.3. The purpose of the OTP is to make it more difficult to gain unauthorized access to restricted resources, like a computer account. Traditionally static passwords can more easily be accessed by an unauthorized intruder, given enough attempts and time. By constantly altering the password, as is done with the OTP, this risk can be greatly reduced. There are basically five types of OTPs:

1. Using a mathematical algorithm to generate a new password based on the previous password
2. Based on time-synchronization between the authentication server and the client providing the password
3. Using a mathematical algorithm, but the new password is based on a challenge (e.g., a random number chosen by the authentication server or transaction details) and a counter instead of being based on the previous password
4. Using a list of passwords printed on paper
5. Using portable electronic devices (e.g., mobile phones) as an out-of-band method for transmitting OTPs

Stepan uses the time-synchronized OTP token method. There are many different kinds of tokens; some open up doors and others are used to simply generate random numbers. For instance, Figures 7.1 and 7.2 are both tokens. But Figure 7.1 is a token

FIGURE 7.1
Access token for door

for accessing a door, and Figure 7.2 is a token used to access information from a network using the randomly generated numbers displayed in the screen. Figure 7.2 is the type of token Stepan used to access his corporate network. Inside this token is an accurate clock that has been synchronized with the clock on the authentication server. On these OTP systems, time is an important part of the password algorithm since the generation of new passwords is based on the current time rather than the previous password or a secret key. Mobile phones and personal digital assistants can also be used to generate a time-synchronized OTP. This approach could be a more cost-effective alternative because most Internet users already have mobile phones. Additionally, this approach could be more convenient because the user would not need to carry around a separate hardware token for each security domain to which he or she requires access.

FIGURE 7.2

RSA one-time password token (time-synchronized)

FIGURE 7.3

Other types of one-time password tokens (time-synchronized)

FICTIONAL STORY DISSECTED: Honey Pot

> "Why would you want to have all of the 2600 hackers pounding on your network? Are you setting up a honeypot to track someone?"
>
> "No, I need plausible deniability," Bob responded. "And don't you ever tell anyone I said that" (p. 29).

Leon asked Bob if he is setting up a honeypot because this technique is used to divert malicious hackers into a separate network from the operational or trusted network. Bob isn't interested in setting up a honeypot, but he only wants to create "plausible deniability" for when he hacks Groom Lake. If he is caught, the authorities will investigate his home and soon figure out that it was him from the evidence on his computer systems. By allowing his local 2600 chapter to hack his network trying to find the CyberBob icon, any investigations by authorities into his computers if he were to get caught hacking Groom Lake would be inadmissible in court because this network was hacked by many other people.

Making a more attractive target for hackers is the goal of a honeypot. You are trying to lure away potential intruders by allowing them to see a computer network that appears to be the operational network they are targeting. Once the malicious attackers are inside the honeypot, mechanisms are installed to observe their every move to learn their tactics and techniques and figure out who they really are and what they are after.

In computer terminology, a honeypot is a trap set to detect, deflect, or in some manner counteract attempts at unauthorized use of information systems. Generally it consists of a computer, data, or a network site that appears to be part of a network but which is actually isolated, unprotected, and monitored, and which seems to contain information or a resource that would be of value to attackers. A honeypot is valuable as a surveillance and early-warning tool. Although it is often a computer, a honeypot can take on other forms, such as files or data records, or even unused IP address space. By design, honeypots should be isolated from the main network, have no production value and hence should not see any legitimate traffic or activity. Whatever they capture can then be surmised as malicious or unauthorized. Honeypots can carry risks to a network and must be handled with care. If they are not properly walled off, an attacker can use them to break into a system. The Honeynet Project contributes to development of Honeynet tools; read more about them under "Public Record on Tap", and see Figure 7.4 for their Web site.

PUBLIC RECORD ON TAP: The Honeynet Project

The Honeynet Project: http://www.honeynet.org/about

Founded in 1999, The Honeynet Project is an international, non-profit (501c3) research organization dedicated to improving the security of the Internet at no cost to the public. With Chapters around the world, our volunteers are firmly committed to the ideals of

OpenSource. Our goal, simply put, is to make a difference. We accomplish this goal in the following three ways.

Awareness: We raise awareness of the threats and vulnerabilities that exist in the Internet today. Many individuals and organizations do not realize they are a target, nor understand who is attacking them, how, or why. We provide this information so people can better understand they are a target, and understand the basic measures they can take to mitigate these threats. This information is provided through our Know Your Enemy series of papers.

Information: For those who are already aware and concerned, we provide details to better secure and defend your resources. Historically, information about attackers has been limited to the tools they use. We provide critical additional information, such as their motives in attacking, how they communicate, when they attack systems, and their actions after compromising a system. We provide this service through our Know Your Enemy whitepapers and our Scan of the Month challenges.

Tools: For organizations interested in continuing their own research about cyber threats, we provide the tools and techniques we have developed. We provide these through our Tools Site.

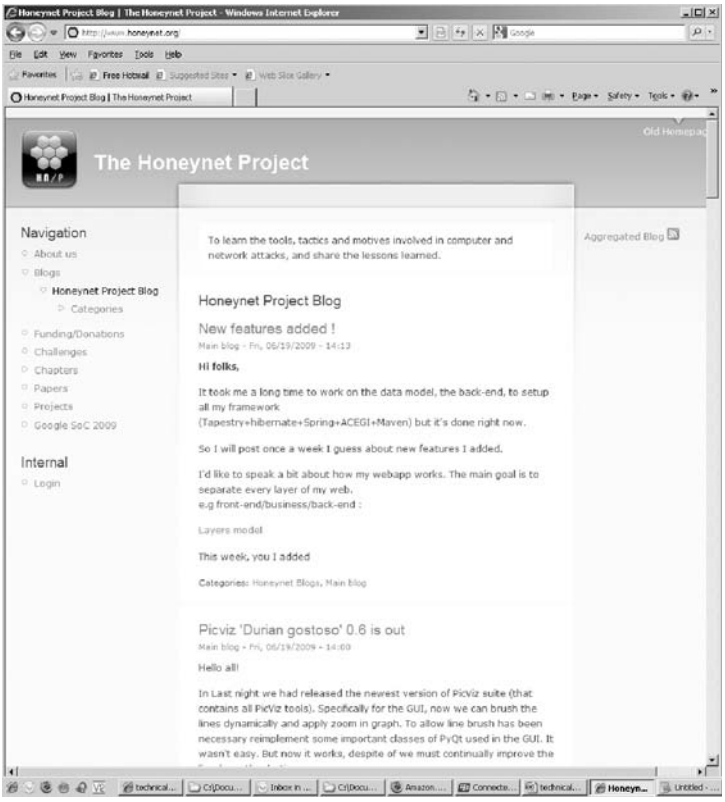


FIGURE 7.4

Honeynet Project Web site

FICTIONAL STORY DISSECTED: No Wi-Fi Should Still Check for Wi-Fi

> "How do I do this, on site?" Pavel asked.
>
> "No, you'll need your wireless gear. You brought your antenna?" Vlad's question had the sound of an order.
>
> "Always do," Pavel answered (p. 36).

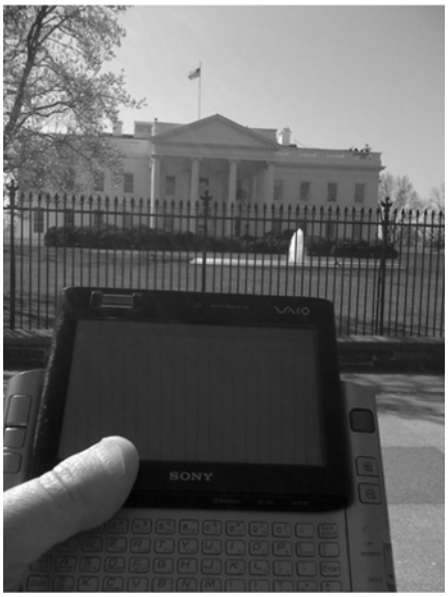


FIGURE 7.5

Wi-Fi Audit at the White House, by Jayson E. Street.

Sometimes it seems like Vlad is pushing Pavel around; but in this case, Pavel is more than ready to break into some Wi-Fi access points. Pavel is getting ready to access the wireless access point at 3DNF, so they can complete their mission. In IT infrastructures, it is imperative to assess the potential and existence of unauthorized (or rogue) wireless access points. If your organization has any policy preventing or authorizing the use of or existence of Wi-Fi, then someone in the IT staff should be auditing and scanning for unauthorized access points. Just imagine if 3DNF was doing this—they could have prevented Pavel from hacking them.

Figure 7.5 is a picture of the United States White House being audited wirelessly by Jayson E. Street, author of this book. This picture was taken in February 2009 and the audit revealed no issues. In 2007, Jayson conducted the same audit and found a few of the wireless access points leaking information. He contacted the local authorities and was able to assist them in fixing the problem. Yes, wireless audits are also for the highest offices of the land!

FICTIONAL STORY DISSECTED: Null Shares

> He left the scan to run and opened a new window from his "Run" box at the bottom of the screen. He typed the first name of a computer that looked like a server followed by the default root path
>
> \\3D-FS1\C$ (p. 41).

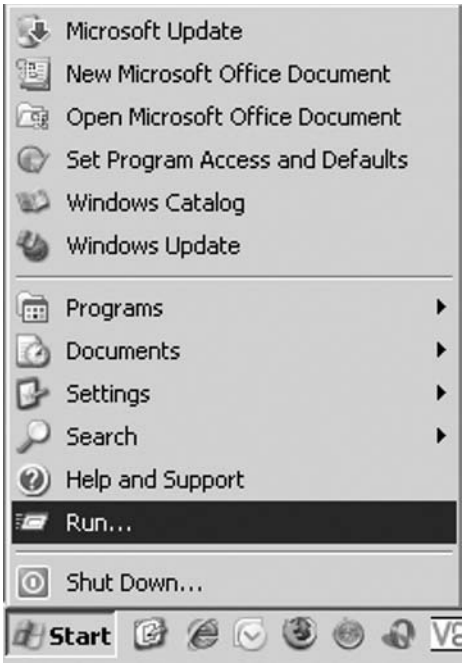


FIGURE 7.6

Start button, Run

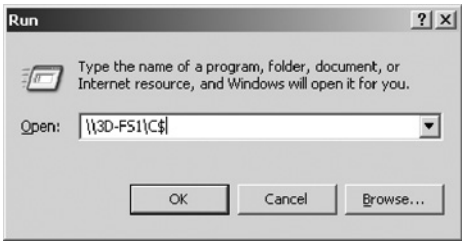


FIGURE 7.7

Run window

Bob knows the basics of networking in a Windows environment. The funny thing about this operation of accessing computers remotely by their null sessions is that it is a very common feature of Windows Microsoft, and unfortunately one which can allow an easy way in for a hacker. Figure 7.6 describes the first step in this process: Click Start, and then Run. Figure 7.7 shows how simple this was for Bob after he opened the Run window from the Start button to enter the null session command. After Bob clicked OK on the Run command, he was provided with a listing of all the files and folders for 3D-FS1 computer as seen in Figure 7.8. Figure 7.9 shows the default hidden shares that are typically created after you install a Windows operating system.

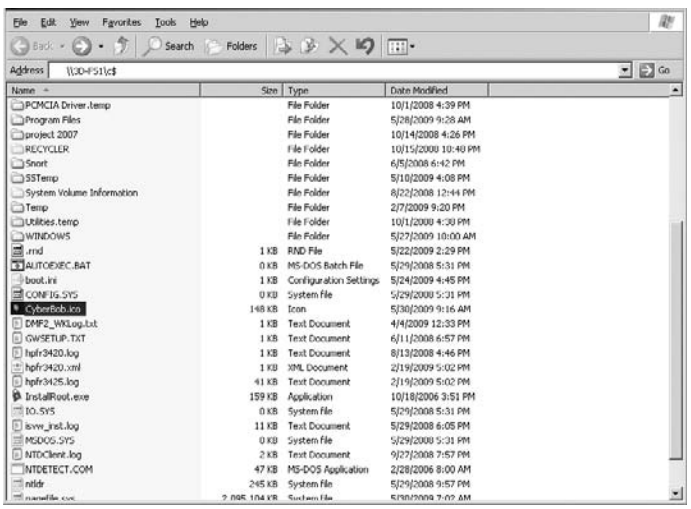


FIGURE 7.8

Results of Run command of null share

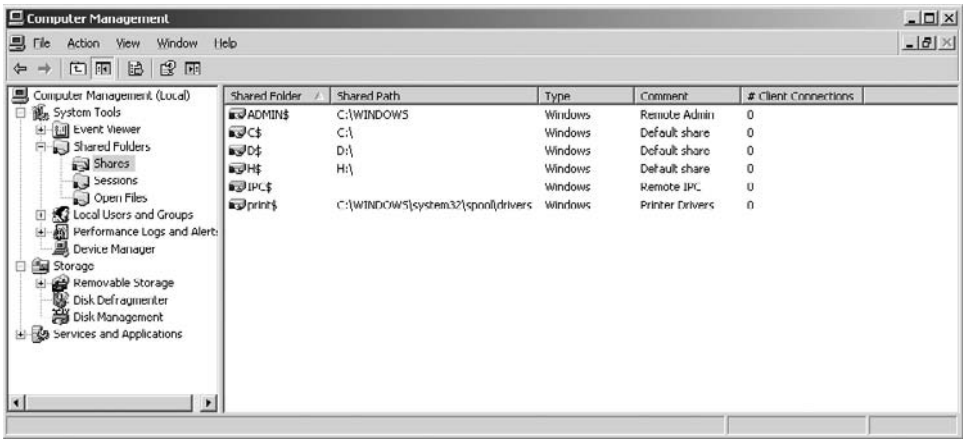


FIGURE 7.9

Computer Management

A null session is how Windows represents an anonymous user. It's a logon session that represents anonymous users, and here's how you use it. In the code that services up anonymous requests, it grabs a token to represent the anonymous logon by calling the Win32 API. This is a null session token, and it has a user SID of ANONYMOUS LOGON and a single group SID, Everyone. By granting access to Everyone, you're granting access to all users, both authenticated and anonymous. By granting access only to Authenticated Users, you're implicitly denying anonymous users. This simple model allows an administrator to use access control lists (ACLs) to control access to all users, both authenticated and anonymous. Figure 7.10 shows the Everyone user group applied to the root partition.

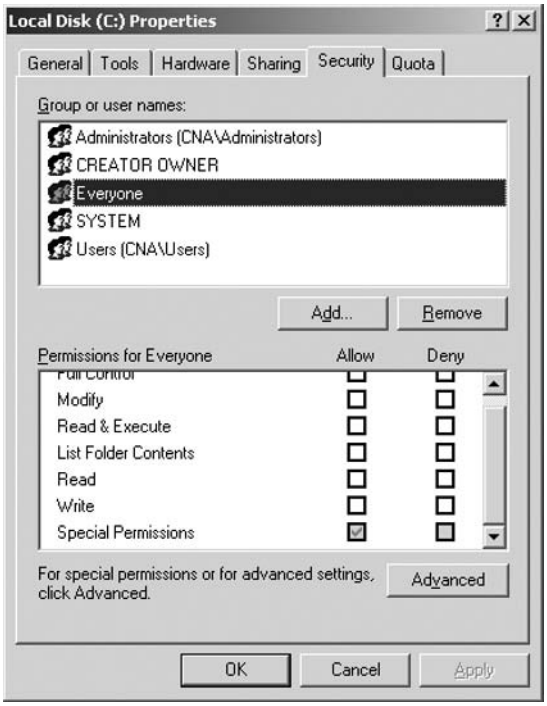


FIGURE 7.10

Local Disk (C:) Properties

PUBLIC RECORD ON TAP: Null Session Exploit

Exploiting the IPC Share

This will explain the "uses" of IPC for hackers. Inter-Process Communication is used for data sharing between applications and computers. We will be looking at Windows NT default IPC$ share use for communication between computers. This share is what we use to start to gain access to the server. What we will look at before we start is the NET commands for the console in NT. (Note I was unable to create a null connection using a 95/98 computer; I had to use an NT computer.) The net commands that we will be using are net use and net view. Now get in to the console (fake ms-dos) in windows. Pick out your target; make sure that it is an NT system, and it has port 139 open. You need port 139 open so that net-bios is on. After checking for that, you go to the console and type:

Example 1> C:\>NET USE \\TARGET\IPC$ * /USER:

Example 2> C:\>NET USE \\TARGET\IPC$ * /USER:""

Example 3> C:\>NET USE \\TARGET\IPC$ "" /USER:""

* Note: For some reason the command varies a little bit from NT to NT
* Note: TARGET is the name or IP of the computer, ex. \\211.3.4.11\ipc$ * /user:
* Note: If it works you'll get> The command completed successfully.
* Note: To check the connection type NET USE \\TARGET\IPC$

After starting a null connection you could try to access the hidden shares. The default hidden shares are C$, PRINT$, ADMIN$, IPC$. As you can probably tell, shares are hidden by putting a $ at the end of the share name. Sometime shares don't have passwords, so you can use them. When you create a null connection, you have the least possible rights. Next, you could try using net view. To do this, open the console and type:

Example:

C:\>net view \\TARGET (Shares)

Or

C:\>net view /workgroup:TARGETWG (Computers in workgroup)

Or

C:\>net view /domain:TARGETD (Computers in domain)

(Note: change TARGETWG to the name of the workgroup to see all of the computers connected)

(Note: change TARGET to the IP or name of the computer to see all none hidden shares)

(Note: change TARGETD to domain name example: /domain: Bob.com)

If you can't find an open share, you could use a program that I like a lot called winfo. Winfo will get all of the usernames from the target. Or another program is Nat (NetBIOS Auditing Tool). Nat will try names and passwords (dictionary attack) to get the right one. Another well-liked program is the set of utilities sid2user and user2sid.

Last, but not least, there are DoS attacks that could be preformed. DoS attacks become outdated quickly, but new ones are always popping up. A good DoS attack works on NT systems with printer capabilities. It kinda goes like this (null connection is needed): \\target\pipe\spoolss. Do this a lot. The next one is one that I'm not sure that works, but you fill all the connections possible on: \\target\pipe\samr; for that, I would recommend you use a program like ubend.exe. To read more, visit http://www.governmentsecurity.org/hack_exploit_ipc_share.

By Governmentsecurity.org

PUBLIC RECORD ON TAP: Null Session Vulnerability

Null Session Vulnerability

When a program or service is started by using the System user account, the service logs on with null credentials. This can be a potential security risk, because it allows for an unauthenticated logon to the system. A hacker or worm can exploit this vulnerability and potentially access sensitive data on the system.

The simplest way to reduce null session vulnerability is to disable NetBios and verify that ports 139 and 445 are closed. However, if your run-time image requires NetBIOS, you can control null session access by editing the following registry key to restrict anonymous access to sensitive data:

Key Name: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA

Value Name: RestrictAnonymous

Type: DWORD

Value: 0

The default value of this key is 0. Changing this value to 1 blocks enumeration of SAM and user accounts, and prohibits a null session from seeing user accounts and admin shares. A value of 2 disables null session access without explicit permissions. Changing this value to 2 may conflict with some applications that rely on null sessions. After you change the registry data, reboot your run-time images and test your applications to verify that they work with restricted null session access.

To read more visit http://msdn.microsoft.com/en-us/library/ms913275(WinEmbedded.5).aspx

By Microsoft Corporation on October 18, 2006

FICTIONAL STORY DISSECTED: Corporate Firewalls

> He kept this screen on and logged in all the time. It was used mostly to display logs from the firewall and the few network sensors recently deployed at 3DNF.
>
> Jonathan took a couple more swigs of his carbonated breakfast as he scanned the entries on the Snort console (p. 63).

Corporate firewalls are very important, but without proper security analyst and managers monitoring the firewalls alerts and logs, they can be useless. Below we will discuss firewalls and why they are important to be implemented in any network. Figure 7.11 is a picture of what a typical corporate firewall setup would look like.

A firewall is a part of a computer system or network that is designed to block unauthorized access while permitting authorized communications. It is a device or set of devices configured to permit, deny, encrypt, decrypt, or proxy all (in and out) computer traffic between different security domains based on a set of rules and other criteria. Firewalls can be implemented in either hardware or software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria. Figure 7.11 is a basic setup for a corporate network with a firewall in between the Internet (untrusted) and the corporate network (trusted).

There are many different kinds of firewalls that organizations can use such as Check Point (Figure 7.12), Juniper (Figure 7.13), SonicWALL (Figure 7.14), Cisco Adaptive Security Appliance (ASA) (Figure 7.15), and Microsoft Internet Security and Acceleration (ISA) (Figure 7.16).

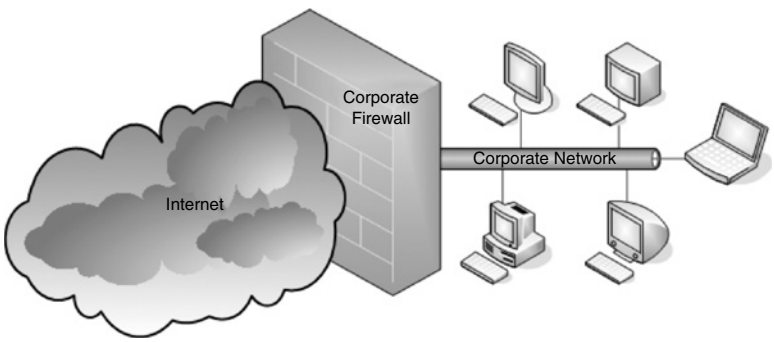


FIGURE 7.11

Corporate Firewall setup

FIGURE 7.12

Check Point firewalls

FIGURE 7.13

Juniper NetScreen-5400 firewall

FIGURE 7.14

SonicWALL firewall

FIGURE 7.15

Cisco Adaptive Security Appliance

FIGURE 7.16

Microsoft Internet Security and Acceleration Server

FICTIONAL STORY DISSECTED: PGP Whole Disk

> This is a PGP pass phrase screen—if he has anything valuable, it's going to be in this system, and we aren't going to get in (p. 51).

Something that will save the day if a mobile employee loses their laptop is full disk encryption. PGP Whole Disk Encryption is a method to encrypt the whole computer hard drive and without proper credentials, like a OTP, the data cannot be recovered. Bob is very smart to use whole disk encryption; even Pavel knows he won't be able to get in to that system.

Full disk encryption (or whole disk encryption) is a kind of disk encryption software or hardware, which encrypts every bit of data that goes on a disk or disk volume. The term "full disk encryption" is often used to signify that everything on a disk is encrypted, including the programs that can encrypt bootable operating system partitions. But they must still leave the master boot record (MBR) and thus part of the disk is unencrypted. There are, however, hardware-based full disk encryption systems that can truly encrypt the entire boot disk, including the MBR.

Full disk encryption has several benefits compared to regular file or folder encryption, or encrypted vaults. The following are some benefits of full disk encryption:

1. Nearly everything including the swap space and the temporary files is encrypted. Encrypting these files is important, as they can reveal important confidential data. With a software implementation, the bootstrapping code cannot be encrypted, however. (For example, BitLocker leaves an unencrypted volume to boot from, while the volume containing the operating system is fully encrypted.) See Figure 7.17 for BitLocker's components.
2. When using full disk encryption, the decision of which individual files to encrypt is not left up to users' discretion. This is important for situations in which users might not want or might forget to encrypt sensitive files.
3. Support for pre-boot authentication.
4. Immediate data destruction, as simply destroying the cryptography keys renders the contained data useless. However, if security toward future attacks is a concern, purging or physical destruction is advised.

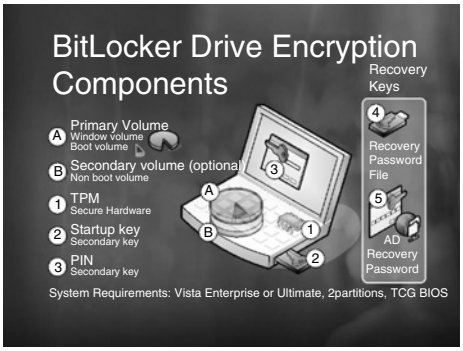


FIGURE 7.17

BitLocker components

Most full disk encryption schemes are vulnerable to a cold boot attack, whereby encryption keys can be stolen by cold-booting a machine already running an operating system, then dumping the contents of memory before the data disappears. The attack relies on the data remanence property of computer memory, whereby data bits can take up to several minutes to degrade after power has been removed.[1,2] Even a Trusted Platform Module is not effective against the attack, as the operating system needs to hold the decryption keys in memory to access the disk.[2]

PUBLIC RECORD ON TAP: PGP Whole Disk

PGP Whole Disk Encryption

Proactively secure confidential data on disks and removable media

Overview

Mobile computers are quickly emerging as the industry standard for increasing user productivity. However, the portable nature of these devices increases the possibility of loss or theft. Consequent exposure of sensitive data can result in financial loss, legal ramifications, and brand damage.

PGP® Whole Disk Encryption provides enterprises with comprehensive, nonstop disk encryption for Microsoft and Apple Mac OS X, enabling quick, cost-effective protection for data on desktops, laptops, and removable media. The encrypted data is continuously safeguarded from unauthorized access, providing strong security for intellectual property, customer and partner data, and corporate brand equity.

Easy, automatic operation–Protects data without changing the user experience.

Enforced security policies–Automatically enforce data protection with centrally managed policies.

Accelerated deployment–Achieves full disk encryption using the existing infrastructure.

Reduced operational costs–Result from centrally automating encryption policies.

As a PGP® Encryption Platform-enabled application, PGP Whole Disk Encryption can be used with PGP Universal™ Server to manage existing policies, users, keys, and configurations, expediting deployment and policy enforcement. PGP Whole Disk Encryption can also be used in combination with other PGP® encryption applications to provide multiple layers of security.

To read more visit http://www.pgp.com/products/wholediskencryption/

[1]Don't Panic—Cold Boot Reality Check. Secude. February 21, 2008. http://secude.com/htm/801/en/White_Paper%3A_Cold_Boot_Attacks.htm. Retrieved on February 22, 2008.

[2]J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W. Felten (February 21, 2008). Lest We Remember: Cold Boot Attacks on Encryption Keys. Princeton University. http://citp.princeton.edu/memory/. Retrieved on February 22, 2008.

FICTIONAL STORY DISSECTED: Snort

> Jonathan took a couple more swigs of his carbonated breakfast as he scanned the entries on the Snort console (p. 63).

Snort is a free and open-source network intrusion prevention system (NIPS) and network IDS capable of performing packet logging and real-time traffic analysis on IP networks. Snort was written by Martin Roesch and is now developed by Sourcefire, of which Roesch is the founder and CTO. Figure 7.18 is a screen shot of Sourcefire's Web site. Integrated enterprise versions with purpose-built hardware and commercial support services are sold by Sourcefire.

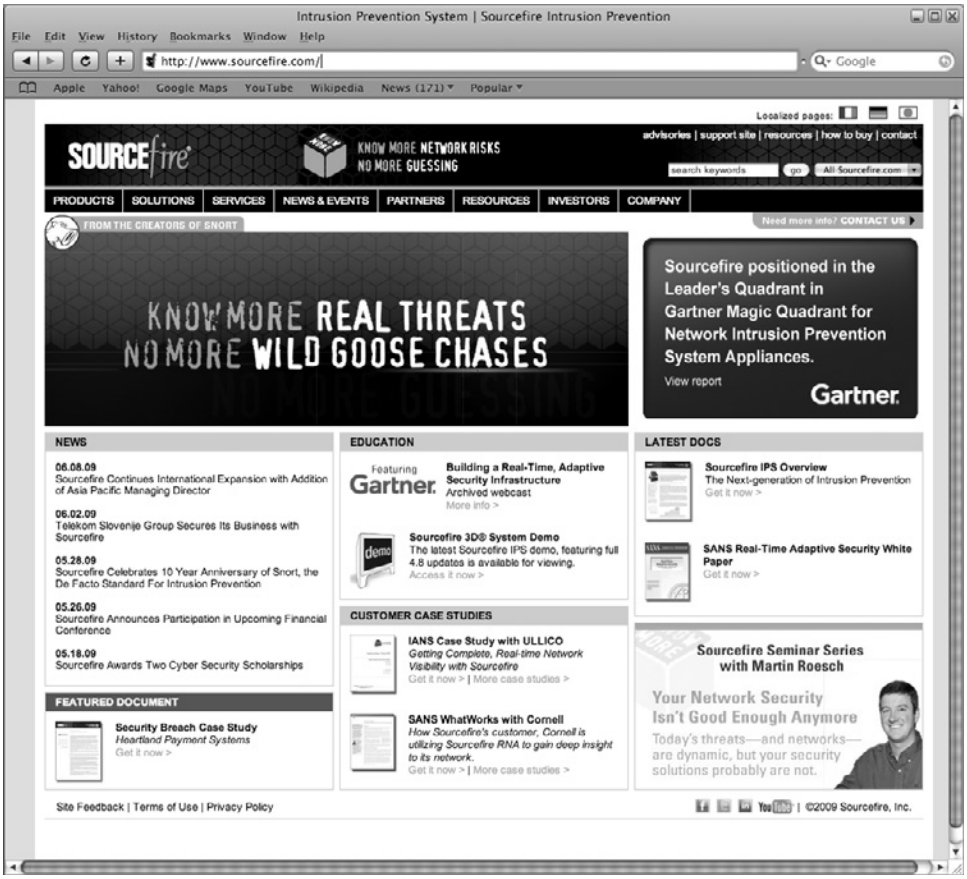


FIGURE 7.18

Sourcefire Web site

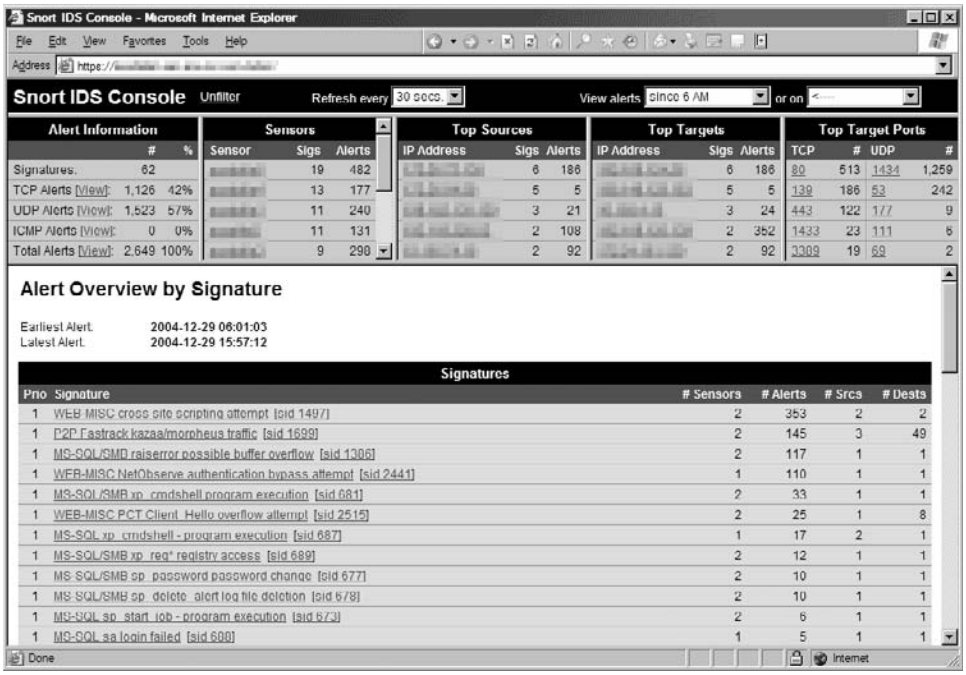


FIGURE 7.19

Snort IDS Console

Snort performs protocol analysis, content searching/matching, and is commonly used to actively block or passively detect a variety of attacks and probes, such as buffer overflows, stealth port scans, web application attacks, Server Message Block probes, and OS fingerprinting attempts, amongst other features. The software is mostly used for intrusion prevention purposes, by dropping attacks as they are taking place. Snort can be combined with other software such as SnortSnarf, sguil, OSSIM, and the Basic Analysis and Security Engine to provide a visual representation of intrusion data. With patches for the Snort source from Bleeding Edge Threats, support for packet stream antivirus scanning with ClamAV and network abnormality with SPADE in network layers 3 and 4 is possible with historical observation. Figure 7.19 is a screen shot of the Snort IDS console.

INTRUSION PREVENTION AND DETECTION

An intrusion prevention system (IPS) is a network security device that monitors network and/or system activities for malicious or unwanted behavior and can react, in real-time, to block or prevent those activities. Network-based IPS, for example, will operate inline to monitor all network traffic for malicious code or attacks. When an attack is detected, it can drop the offending packets while still allowing all other traffic

to pass. Intrusion prevention technology is considered by some to be an extension of intrusion detection (IDS) technology. The term "intrusion prevention system" was coined by Andrew Plato, who was a technical writer and consultant for NetworkICE.[3]

IPSs[4] evolved in the late 1990s to resolve ambiguities in passive network monitoring by placing detection systems inline. Early IPS included the IDS function that was able to implement prevention commands to firewalls and access control changes to routers. This technique fell short operationally, for it created a race condition between the IDS and the exploit as it passed through the control mechanism. Inline IPS can be seen as an improvement upon firewall technologies (Snort inline is integrated into one), and IPS can make access control decisions based on application content rather than IP address or ports, as traditional firewalls had done. However, to improve performance and accuracy of classification mapping, most IPSs use the destination port in their signature format. As IPS systems were originally a literal extension of IDSs, they continue to be related.

IPSs may also serve secondarily at the host level to deny potentially malicious activity. There are advantages and disadvantages to host-based IPS compared with network-based IPS. In many cases, the technologies are thought to be complementary. An IPS must also be a very good IDS to enable a low rate of false positives. Some IPS systems can also prevent yet to be discovered attacks, such as those caused by a buffer overflow. The role of an IPS in a network is often confused with access control and application-layer firewalls. There are some notable differences in these technologies. Although all share similarities, how they approach network or system security is fundamentally different.

An IPS is typically designed to operate completely invisibly on a network. IPS products do not typically claim an IP address on the protected network, but may respond directly to any traffic in a variety of ways. (Common IPS responses include dropping packets, resetting connections, generating alerts, and even quarantining intruders.) Although some IPS products have the capability to implement firewall rules, this is often a mere convenience and not a core function of the product. Moreover, IPS technology offers deeper insight into network operations providing information on overly active hosts, bad logons, inappropriate content, and many other network and application-layer functions.

Application firewalls are a very different type of technology. An application firewall uses proxies to perform firewall access control for network and application-layer traffic. Some application-layer firewalls have the capability to do some IPS-like functions, such as enforcing RFC specifications on network traffic. Also, some application-layer firewalls have also integrated IPS-style signatures into their products to provide real-time analysis and blocking of traffic. Application firewalls do have IP addresses on their ports and are directly addressable. Moreover, they use full proxy features to decode and reassemble packets. Not all IPSs perform full proxy-like processing. Also, application-layer firewalls tend to focus on firewall capabilities,

[3]http://documents.iss.net/literature/ICEcap/BlackICE_Sentry_User_Guide30.pdf

[4]http://www.google.com/url?sa=t&source=web&ct=res&cd=4&url=http%3A%2F%2Fcomputersecurity.wikia.com%2Fwiki%2FIntrusion-prevention_system&ei=65E1SunSNozYM6PiyaML&usg=AFQjCNFXmMCivjXXxyx906Gs6imR67_N6w&sig2=OJ1zTtNdAhrGUXmJQLLptg

with IPS capabilities as add-ons. Although there are numerous similarities between the two technologies, they are not identical and interchangeable. Unified Threat Management (UTM),[5] or sometimes called "Next Generation Firewalls", are also a different breed of products entirely. UTM products bring together multiple security capabilities onto a single platform. A typical UTM platform will provide firewall, VPN, anti-virus, web filtering, intrusion prevention, and anti-spam capabilities. Some UTM appliances are derived from IPS products, such as 3Com's X-series products. Others are derived from a combination with firewall products, such as Juniper's SSG (Figure 7.22) or Cisco's ASAs (Figure 7.18). And still others were derived from the ground up as a UTM appliance, such as Fortinet or Astaro. The main feature of a UTM is that it includes multiple security features on one appliance. IPS is merely one feature. IBM also has an IDS and IPS solution; see Figure 7.20 for their Web site.

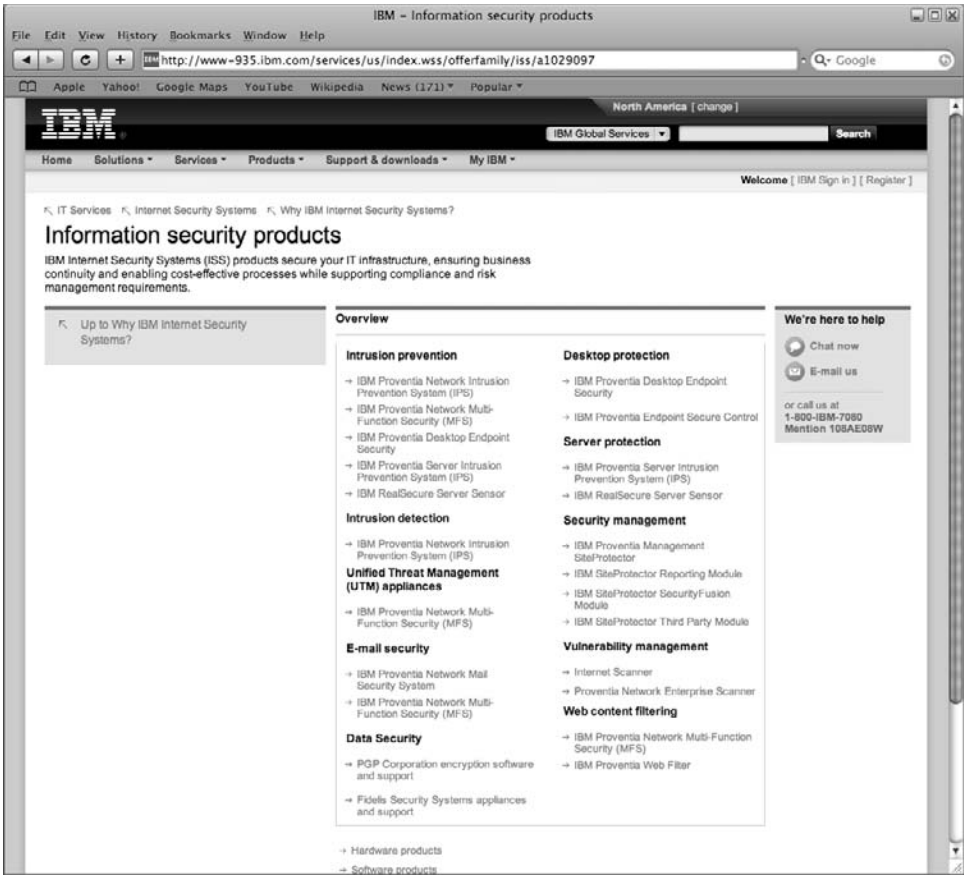


FIGURE 7.20

IBM RealSecure Web site

[5]http://www.watchguard.com/products/utm.asp

FIGURE 7.21

SonicWALL Web site

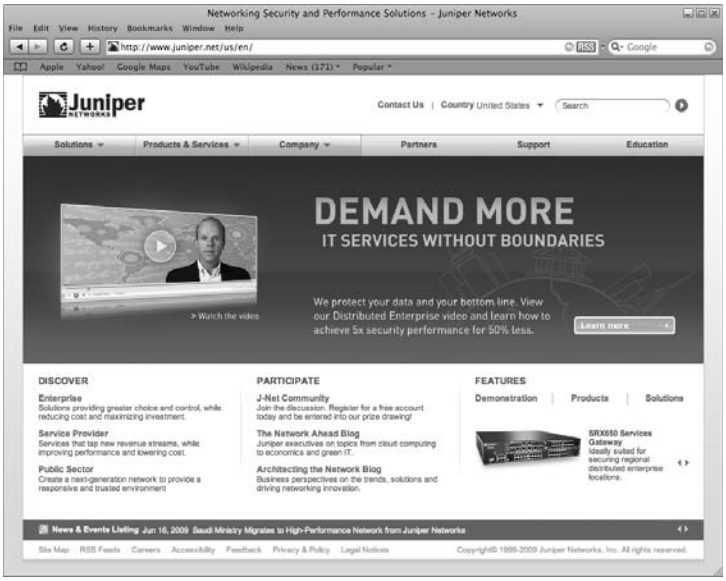


FIGURE 7.22

Juniper Networks Web site

Access control is also an entirely different security concept. Access control refers to general rules allowing hosts, users, or applications access to specific parts of a network. Typically, access control helps organizations segment networks and limit access. Although an IPS has the capability to block access to users, hosts, or applications, it does so only when malicious code has been discovered. As such, IPS does not necessarily serve as an access control device. Although it has some access control abilities, firewalls and network access control (NAC) technologies are better suited to provide these features.

IPS systems have some advantages over IDSs. One advantage is they are designed to sit inline with traffic flows and prevent attacks in real time. In addition, most IPS solutions have the capability to look at (decode) layer 7 protocols like Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), and Simple Mail Transfer Protocol, which provides greater awareness. However, when deploying network-based IPS (NIPS), consideration should be given to whether the network segment is encrypted, because not as many products are able to support inspection of such traffic.

IPS can do more than just drop packets. Because an IPS is inline, it does not have to interpret the network stack. An IPS can correct CRC, unfragment packet streams, prevent Transmission Control Protocol (TCP) sequencing issues, and clean up unwanted transport and network-layer options. IDS evasion techniques were made famous by insertion, evasion, and denial of service.

A host-based IPS (HIPS) is where the intrusion-prevention application is resident on that specific IP address, usually on a single computer. A HIP complements traditional finger-print-based and heuristic antivirus detection methods because it does not need continuous updates to stay ahead of new malware. As ill-intended code needs to modify the system or other software residing on the machine to achieve its evil aims, a truly comprehensive HIPS system will notice some of the resulting changes and prevent the action by default or notify the user for permission.

Extensive use of system resources can be a drawback of existing HIPS, which integrate firewall, system-level action control, and sandboxing into a coordinated detection net, on top of a traditional antivirus (AV) product. This extensive protection scheme may be warranted for a laptop computer frequently operating in untrusted environments (e.g., on cafe or airport Wi-Fi networks), but the heavy defenses may take their toll on battery life and noticeably impair the generic responsiveness of the computer, as the HIPS protective component and the traditional AV product check each file on a PC to see if it is malware against a huge blacklist. Alternatively, if HIPS is combined with an AV product using whitelisting technology, then there is far less use of system resources, as many applications on the PC are trusted (whitelisted). HIPS as an application then becomes a real alternative to traditional AV products.

A network-based IPS is one where the IPS application/hardware and any actions taken to prevent an intrusion on a specific network host(s) is done from a host with another IP address on the network. (This could be on a front-end firewall appliance.)

NIPSs are purpose-built hardware/software platforms that are designed to analyze, detect, and report on security-related events. NIPSs are designed to inspect traffic; and based on their configuration or security policy, they can drop malicious traffic.

A content-based IPS (CBIPS) inspects the content of network packets for unique sequences, called signatures, to detect and hopefully prevent known types of attack, such as worm infections and hacks.

A key development in IDS/IPS technologies was the use of protocol analyzers. Protocol analyzers can natively decode application-layer network protocols, like HTTP or FTP. Once the protocols are fully decoded, the IPS analysis engine can evaluate different parts of the protocol for anomalous behavior or exploits. For example, the existence of a large binary file in the User-Agent field of an HTTP request would be very unusual, and likely an intrusion. A protocol analyzer could detect this anomalous behavior and instruct the IPS engine to drop the offending packets.

Not all IPS/IDS engines are full protocol analyzers. Some products rely on simple pattern recognition techniques to look for known attack patterns. Although this can be sufficient in many cases, it creates an overall weakness in the detection capabilities. Because many vulnerabilities have dozens or even hundreds of exploit variants, pattern recognition-based IPS/IDS engines can be evaded. For example, some pattern recognition engines require hundreds of different signatures (or patterns) to protect against a single vulnerability. This is because they must have a different pattern for each exploit variant. Protocol analysis-based products can often block exploits with a single signature that monitors for the specific vulnerability in the network communications.

Rate-based IPS (RBIPS) is primarily intended to prevent denial of service and distributed denial of service attacks. They work by monitoring and learning normal network behaviors. Through real-time traffic monitoring and comparison with stored statistics, RBIPS can identify abnormal rates for certain types of traffic—for example, TCP, User Datagram Protocol or Address Resolution Protocol packets, connections per second, packets per connection, and packets to specific ports. Attacks are detected when thresholds are exceeded. The thresholds are dynamically adjusted based on time of day, day of the week, and drawing on stored traffic statistics.

Unusual but legitimate network traffic patterns may create false alarms. The system's effectiveness is related to the granularity of the RBIPS rulebase and the quality of the stored statistics. Once an attack is detected, various prevention techniques may be used, such as rate-limiting specific attack-related traffic types, source or connection tracking, and source-address, port or protocol filtering (blacklisting), or validation (whitelisting).

HIPS can handle encrypted and unencrypted traffic equally because it can analyze the data after it has been decrypted on the host. A NIP does not use processor and memory on computer hosts but uses its own CPU and memory. A NIP is a single point of failure, which is considered a disadvantage; however, this property also makes it simpler to maintain. However, this attribute applies to all network devices like routers and switches, and can be overcome by implementing the network accordingly (failover path, etc.). A Bypass Switch from a vendor like Net Optics can be deployed to alleviate the single point of failure disadvantage, though. Multi-segment Bypass Switches have recently become more popular as IPS vendors have rolled out high-density solutions. This also allows the NIPS appliance to be moved and be taken offline for maintenance when needed. NIPS can detect events scattered over the network (e.g., low-level event targeting many different hosts, like hostscan, worm) and can

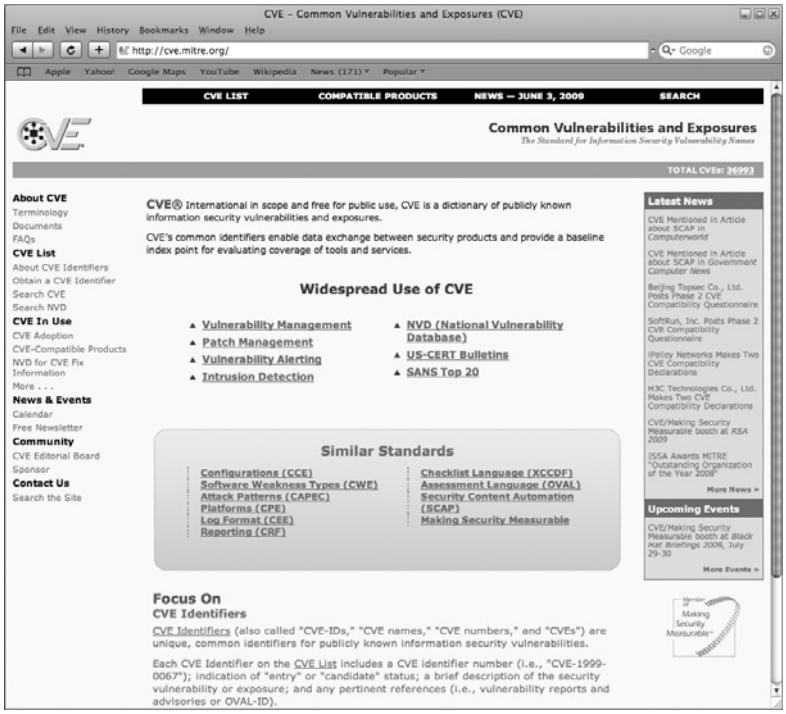


FIGURE 7.23
Common Vulnerabilities and Exposures Web site

react, whereas with a HIPS, only the hosts data itself is available to take a decision, respectively; it would take too much time to report it to a central decision-making engine and report back to block.

How IPS and IDS are updated with the latest detection and prevention code is something that being with a visit to Common Vulnerabilities and Exposures (CVE). CVE® is a dictionary of common names (i.e., CVE Identifiers) for publicly known information security vulnerabilities, whereas its Common Configuration Enumeration (CCE™) provides identifiers for security configuration issues and exposures. CVE's common identifiers make it easier to share data across separate network security databases and tools and provide a baseline for evaluating the coverage of an organization's security tools. If a report from one of your security tools incorporates CVE Identifiers, you may then quickly and accurately access fix information in one or more separate CVE-compatible databases to remediate the problem. Figure 7.23 is their Web site.

PUBLIC RECORD ON TAP: TippingPoint

TippingPoint is a leading global provider of comprehensive network security solutions that address the security and regulatory compliance needs of complex network environments. With the TippingPoint IPS-Secured Network, which includes the TippingPoint IPS and NAC

solution, network infrastructure, applications, and critical data are protected from malicious cyber attacks. TippingPoint's 360 approach to network security enables enterprises to enforce security policies across all users, devices, traffic flows, and content, while preserving existing infrastructure and ensuring business continuity to help lower total cost of ownership.

TippingPoint's security intelligence is powered by DVLabs, TippingPoint's premier team of expert internal researchers for vulnerability analysis and discovery. The team consists of industry-recognized security researchers that apply cutting-edge engineering, reverse engineering, and analysis talents in their daily operations. The by-product of these efforts fuels the creation of vulnerability filters that are automatically delivered to customers' IPSs through the Digital Vaccine® service.

DVLabs is supplemented by over 1000 external Zero Day Initiative (ZDI) researchers. Founded in 2005 by TippingPoint, ZDI rewards security researchers for responsibly disclosing vulnerabilities. ZDI strives to extend the DVLabs team by leveraging the methodologies, expertise, and time of others; encourage the reporting of zero-day vulnerabilities responsibly to the affected vendors by financially rewarding researchers; and protect TippingPoint customers through the TippingPoint IPS while the affected vendor is working on a patch. To learn more, visit http://www.tippingpoint.com/. Figure 7.24 is a screen shot of their Web site.

FIGURE 7.24

TippingPoint Web site

PUBLIC RECORD ON TAP: Web Applications Firewalls

Web App Firewalls: How to Evaluate, Buy, Implement by Mary Brandel

A Web application firewall (WAF) is designed to protect Web applications against common attacks such as cross-site scripting and SQL injection. Whereas network firewalls defend the perimeter of the network, WAFs sit between the Web client and Web server, analyzing application-layer traffic for violations in the programmed security policy, says Michael Cobb, founder of Cobweb Applications, a security consultancy.

While some traditional firewalls provide a degree of application awareness, it's not with the granularity and specificity that WAFs provide, says Diana Kelley, founder of consultancy Security Curve. For instance, the WAF can detect whether an application is not behaving the way it was designed to, and it enables you to write specific rules to prevent that kind of attack from recurring. To read more, visit http://www.cso.com.au/article/307044/web_app_firewalls_how_evaluate_buy_implement.

PUBLIC RECORD ON TAP: Enterprise Antivirus

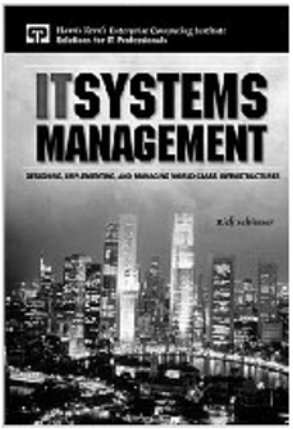
Enterprise Antivirus Software: Protect your network by WindowsITPro.com

I would venture to guess that virtually every computer network has had to deal with the downtime and expense of recovering from some type of malware infection. According to AV-Test (www.av-test.org), an independent antivirus software testing lab, 2007 saw record numbers of computer viruses, worms, and other malware, and 2008 is continuing that trend. Naturally, prevention is less costly than recovery—but how do you choose from the myriad of antivirus or anti-malware solutions on the market? Let's look at some things you should consider when choosing an enterprise antivirus product, and then you can check out the product comparison table to find the best one for your organization.

Choices, Choices: Today's antivirus market includes products that protect file servers, email gateways, Web browsers, and desktops. They may be stand-alone products, or part of an integrated security suite that might include a firewall, IDSs, IPS, NAC, and spam filtering. You can choose from desktop solutions or server-side solutions that offer centralized control for deploying, configuring, and updating the software and that eradicate malware threats before they infiltrate your network. Security appliances as well as hosted and managed security solutions that outsource the management details of your security strategy are also gaining in popularity. Because of the wide array of solution types, we've limited the scope of this Buyer's Guide to server-side enterprise antivirus products.

To read more visit http://windowsitpro.com/article/articleid/98441/enterprise-antivirus-software.html

BOOKS



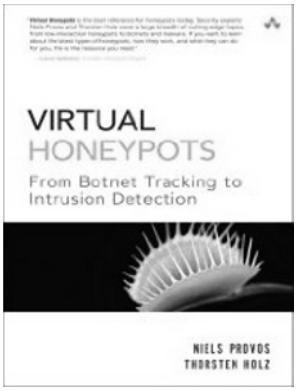
IT Systems Management: Designing, Implementing, and Managing World-Class Infrastructures

By Rich Schiesser

Publisher: Prentice Hall PTR

ISBN-10: 013087678X

ISBN-13: 978-0130876782



Virtual Honeypots: From Botnet Tracking to Intrusion Detection

By Niels Provos and Thorsten Holz

Publisher: Addison-Wesley Professional

ISBN-10: 0321336321

ISBN-13: 978-0321336323

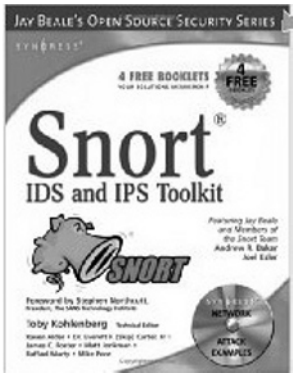
Smart Cards, Tokens, Security and Applications

By Keith Mayes and Konstantinos Markantonakis

Publisher: Springer

ISBN-10: 0387721975

ISBN-13: 978-0387721972



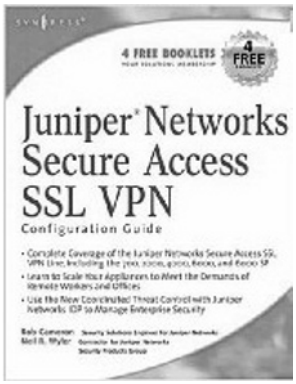
Snort IDS and IPS Toolkit

By Brian Caswell, Jay Beale, and Andrew R. Baker

Publisher: Syngress Publishing (February 1, 2007)

ISBN-10: 1597490997

ISBN-13: 978-1597490993



Juniper Networks Secure Access SSL VPN Configuration Guide

By Kevin Fletcher, Mark Lucas, Brian Burton, Trent Fausett, Patrick Foxhoven, Kevin Miller, Kevin Peterson, Brad Woodberg, and Neil Wyler

Publisher: Syngress

ISBN-10: 1597492000

ISBN-13: 978-1597492003

Firewall Policies and VPN Configurations

By Dale Liu, Stephanie Miller, Mark Lucas, Abhishek Singh, and Jennifer Davis

Publisher: Syngress

ISBN-10: 1597490881

ISBN-13: 978-1597490887

CHAPTER

Software, Hardware, and Wetware

8

This chapter focuses on what hackers and security professionals use in their pursuit to break into something or protect a computer network. Some of the topics covered include USB devices that look like something else, virtualization, on-the-fly computer forensics, plus much more. Enjoy!

FICTIONAL STORY DISSECTED: USB Knife, Swiss Army Knife with USB Storage

> He removed a Swiss Army knife from his pocket. He opened a small connector from the knife, which fit neatly into the USB port on Stepan's laptop. Soon he was copying the "My Documents" folder from Stepan's laptop to his "pocket knife" (p. 8).

Vlad has all the cool hacking hardware, including what you see in Figure 8.1. A Swiss Army knife with a USB thumb drive attached is a very convenient item to have on your person at all times for someone like Vlad. Vlad uses this device to conceal its true purpose as an external storage device. Vlad quickly snatches all Stepan's personal documents from the "My Computer" folder, the default Windows folder for a user's documents, pictures, and music.

FICTIONAL STORY DISSECTED: USB Storage Built into a Pen

> "What is the pen for?"
>
> It's a data storage device. If you pull the top off, you will see a USB connector for your computer. Inside is an encrypted file that details the instructions for your team, as well as the application we need installed on the target system (p. 11).

There are many kinds of common office supplies that are also used as a USB device for external storage. Figure 8.2 is a picture of what Stepan might have given to Vlad. Also in Figure 8.3 is another common item everybody uses: a key. This key is special because it is a USB device. It looks and smells like a key, but look closely and you will notice the rectangle-shaped body of a USB device.

FIGURE 8.1
Swiss Army knife with USB storage

FIGURE 8.2
USB pen

FIGURE 8.3
USB key

FICTIONAL STORY DISSECTED: VMware

> Vlad looked through the program list on Pavel's Linux laptop. Sure enough—VMware (p. 12).

VMware is a software suite that allows Pavel to virtually run many different computers on top of his existing operation system and also a company. VMware, Inc. is the market share leader in virtualization software.[1] The company was founded in 1998 and is based in Palo Alto, California. The company is majority-owned by EMC Corporation. The name "VMware" comes from the acronym "VM," meaning "virtual machine," combined with ware from the second part of "software." Running different virtual machines like Pavel does allows people to have a great deal of flexibility. For instance, you can suspend a virtual machine at any time and resume it. You can also take snapshots of the current state of the virtual machine. This is useful when you are configuring something; and before you make those changes, you take a snapshot. If after you apply the configuration changes the virtual machine breaks or has a lot of errors, you can revert back to the previous state when you took the snapshot. Hackers use virtual machines so that they do not infect or break their own physical machines. This capability is very powerful in testing environments; when programming, many different kinds of applications might cause the system to crash or become corrupt.

VMware's desktop software runs on Microsoft Windows, Linux, and Mac OS X. VMware's enterprise software, VMware ESX Server, runs directly on server hardware without requiring an additional underlying operating system. This is known as being platform- or hardware-agnostic. Figure 8.4 is a screen shot of VMware Infrastructure

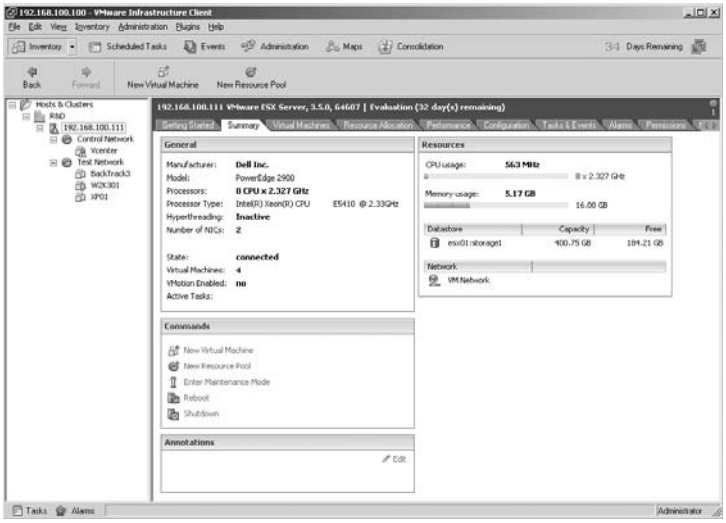


FIGURE 8.4
VMware ESX Server

[1]VMware leader in virtualization market; http://www.hostreview.com/icontent/the-blog/vmware-leader-virtualization-market

Client logged into a VMware VirtualCenter Server that hosts all the VMware ESX servers. Figure 8.5 is a screen shot of multiple virtual machines running at the same time on top of Windows XP operating system.

In the Bleeding Edge Technology section, Chapter 8, we will discuss Kostya Kortchinsky's hacking technique to defeat VMware and take over the guest operating system, called "cloudburst."[2]

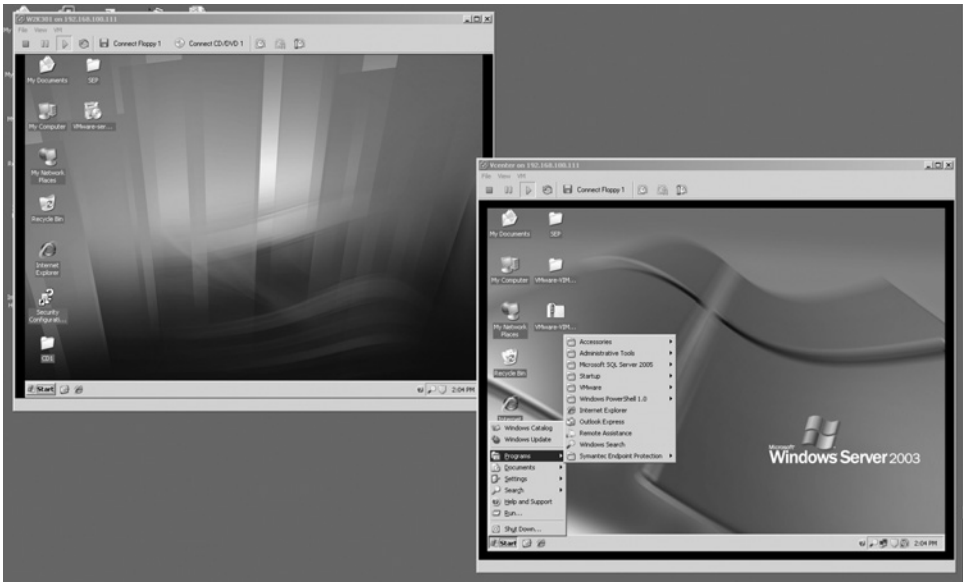


FIGURE 8.5

Multiple virtual machines running at the same time

FICTIONAL STORY ON TAP: BackTrack 4

Just the idea of digging into Vlad's plan made him nervous. Actually beginning to do it had created an involuntary response in heart rate. He pushed on and fished through his backpack for his BackTrack 4 CD (p. 21).

This time he would go through with the forensics. He was determined to see what Vlad wasn't telling him about their work.

Pavel fished through a couple of pockets in his backpack and came out with a handful of CD cases. He shuffled through pile and settled on a disk that had the words "BackTrack 4" handwritten on it (p. 90).

[2]http://www.syscan.org/Sg/program.html

PUBLIC RECORD ON TAP: BackTrack 4 Forensics Mode

New BackTrack 4 "Forensics Mode"

By CYBERSEC

For a long time now, Linux live CDs have been very useful for forensic acquisition purposes when for one reason or another you can't utilize a hardware write blocker. For a Linux Live CD to be considered for this purpose, however, it is of the utmost importance that the use of the live CD in no way alters any data in any manner.

In the past, this ruled out the use of BackTrack for forensic purposes. BackTrack would automount available drives and utilize swap. This could cause all sorts of havoc, changing last mount times, altering data on disk, and so on.

Well, no longer! The BackTrack 4 Live CD has incorporated changes to allow a boot mode which is forensically clean. This is great news, as with BackTrack being such a popular live CD, a copy can often be found close at hand. Figure 8.6 is a screen shot of BackTrack 4 boot menu for the forensics option. To read more visit http://www.cybersec.eu/?p = 128.

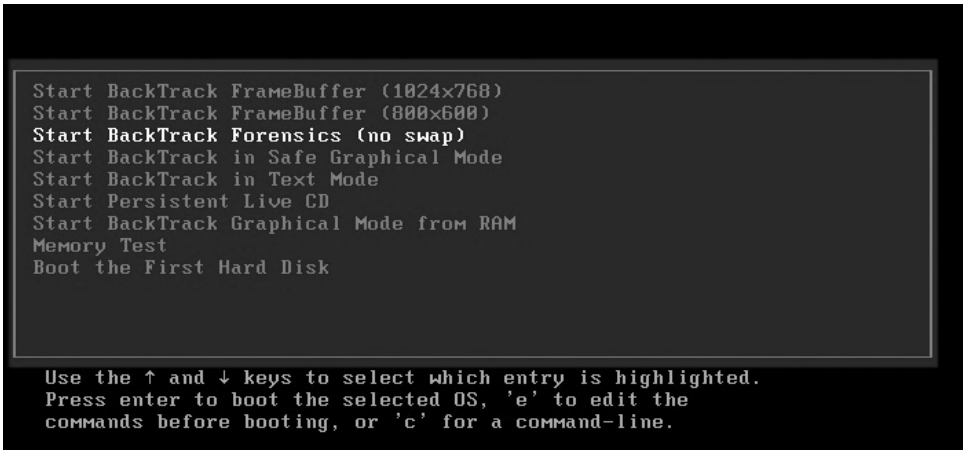


FIGURE 8.6

BackTrack 4 Forensics Boot screen

HELIX CD

There are many other alternatives to BackTrack 4 in regards to free and open source computer forensics tools and operating systems. For example, the Helix CD and Federal Computer Crime Unit (FCCU) are two other Linux boot CDs. Helix is a bootable operating system that has many different forensics tools built in to the CD.

Helix is referred to as an incident handler's choice of weapons. Computer incident handlers use Helix to investigate intrusions and malicious activity on infected machines when a compromise has been discovered. When Pavel gets Stepan's IBM notebook, he finds out that Vlad has erased and reinstalled the operating system. No matter—in computer forensics, it is still possible to pull off data from the hard drive even though it might have been erased prior. This is because all the data was technically not written over. Unless you specifically have the hard drive write over every inch of the disk with garbled data, then pulling some files that exist before might actually work. Many times organizations will have employees use the same laptop after they transfer or leave the company. Most of the time the IT department just reinstalls a fresh copy of the operating system, but many organizations must adhere to strict policy like the federal government and completely and irrecoverably wipe their hard drive before they get a fresh install. Completely eliminating any trace of computer files from previous owners is not that hard. There are many free tools that will "Department of Defense (DOD) wipe" a hard drive. DOD wipe is a common term referring to the three wipes the DOD must do to their computer hard drives. In Figures 8.7 and 8.8, there is a screen shot of what Helix looks like after you have booted it up on a computer.

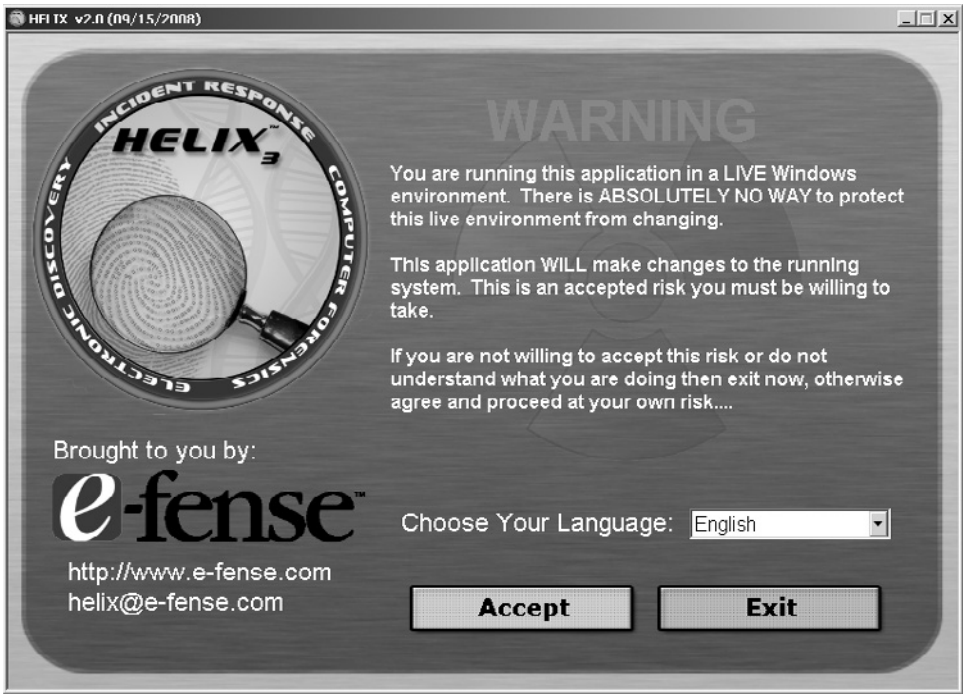


FIGURE 8.7

Helix screen shot

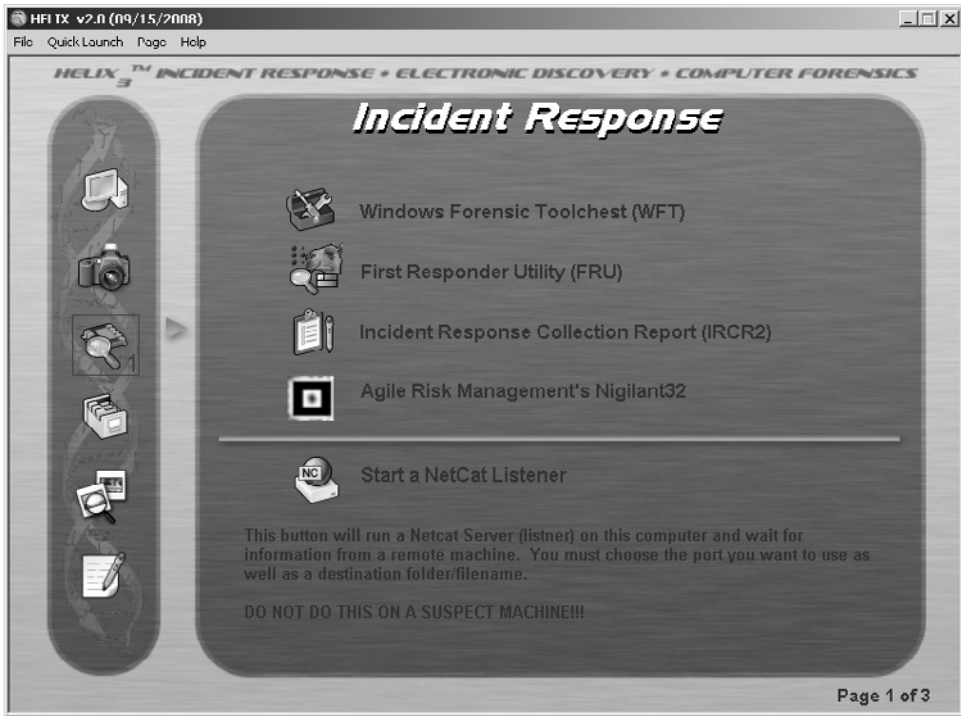


FIGURE 8.8

Helix screen shot

PUBLIC RECORD ON TAP: Helix

Helix: Computer Security Forensics

From 404 Tech Support on March 17, 2009

Computer security forensics can get pretty detailed and pretty involved. In fact, it's almost always best left to the professionals. Even your standard, run-of-the-mill IT professional can get called into court to testify regarding evidence gathered at a scene. When it comes down to justice, you might not want to be the one that gets the blame for a case being dismissed through contamination of evidence.

There are two rules to computer forensics that I've heard:

- Don't touch it.
- If you touched it, document everything (how it was before you touched it, date modified, what changes you made, when you touched it, etc. Everything!)

Helix provides a Live CD that is feature full for incident response. But just because you have a pipe wrench, it doesn't make you a plumber. Similarly, just because you have some security tools, it doesn't make you a certified computer security forensics professional. If you're going to make a case for something with the evidence available, you might want to investigate your options first. Otherwise, if you're just trying to analyze a machine for the fun of it or see what information you can gather, Helix is a great tool to play around with.

Helix comes as one CD with two different functionalities:

1. A CD chock full of Windows-friendly, freeware security utilities.
2. A Linux live CD so that the hard drive is untouched, but the system can be accessed.

When you start up Helix in a running Windows computer (or it auto-runs), you'll first be greeted by a nice big warning. Basically, it wants to tell you that the tools you are running can (and technically already has) made changes to the system. Assuming this is what you want to do, choose your language and accept.

To read more, visit http://www.404techsupport.com/2009/03/17/helix-computer-security-forensics/

BELGIAN FCCU GNU/LINUX BOOT CD

FIGURE 8.9

Belgian Federal Computer Crime Unit Gnu/Linux Forensics Boot CD screen

The FCCU GNU/Linux Forensic Boot CD is a live CD built on top of Debian. It focuses on incident response and computer forensics.[3] The authors are Christophe Monniez and Geert Van Acker.[4] This distribution's main purpose is to create images of drives and devices before the analysis process begins and it is used by the Belgian Federal Computer Crime Unit.[5] Some of the tools included in the CD include forensics acquisition, disk partition utilities, password cracker, archive tools, cryptosteganography tools, network scanner, network capture, video tools, malware collection, and undelete utilities. Figure 8.9 is a screen shot of the FCCU boot CD in its start-up mode.

[3]http://www.forensicswiki.org/wiki/FCCU_Gnu/Linux_Boot_CD
[4]http://www.lnx4n6.be/
[5]http://www.secguru.com/link/fccu_linux_forensic_bootable_cd

FICTIONAL STORY DISSECTED: Pringles can for Hacking Wireless

> I got that new directional antenna installed last night. I want to see if it works better than the Pringles can (p. 29).

Here Bob is talking about a wireless antenna capable of picking up Wi-Fi signals. These kinds of signals are also referred to as 802.11 standards. The new directional antenna he just installed looks very similar to Figure 8.10. There are many ways to create antennas for picking up a wireless signal. In Figure 8.11, you can see a Pringles can mocked up for collecting wireless signs. This is a very inexpensive and powerful way to collect wireless signs because you can focus your antenna receiver in one direction, unlike many other antennas that are omni-directional (like that shown in Figure 8.12).

FIGURE 8.10
Directional antenna

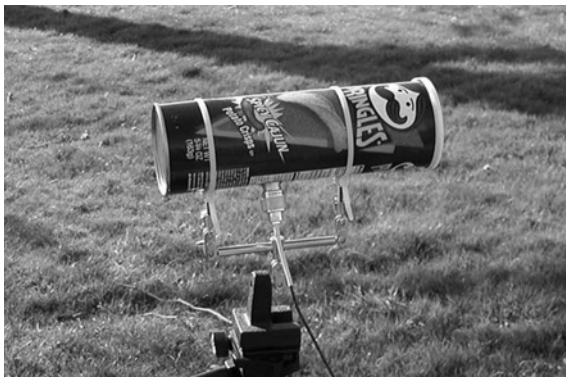


FIGURE 8.11
Pringles can as a wireless antenna

FIGURE 8.12
Omni-directional antenna

FICTIONAL STORY DISSECTED: Wireshark

> "Load Wireshark. I want to see what else is running on this network," Bob suggested as he reached in the back seat and grabbed his backpack with his main laptop inside (p. 40).

Bob and Leon use a program called Wireshark (formally known as Ethereal) to conduct packet analysis on the wireless traffic they are receiving from the 3DNF network they are accessing. Wireshark can be used on wired or wireless network to collect and see the details of data being sent across a networked connection. Wireshark is a free packet sniffer computer application. It is used for network troubleshooting, analysis, software and communications protocol development, and education. In Bob and Leon's case, they use Wireshark to find out what is going on and to collect anything that looks interesting.

Originally named Ethereal, in May 2006 the project was renamed Wireshark due to trademark issues. Wireshark is very similar to tcpdump, but it has a graphical front-end and many more information sorting and filtering options. It allows the user to see all traffic being passed over the network (usually an Ethernet network, but support is being added for others like wireless) by putting the network interface into promiscuous mode. Putting your computer's network interface care into promiscuous mode is the same thing as telling it to no longer ignore traffic that is not intended for it, but to see all the traffic on the network whether it is destined for your computer or not. Wireshark uses the cross-platform GTK+ widget toolkit, and is cross-platform, running on various computer operating systems including Linux, Mac OS X, and Microsoft Windows. Released under the terms of the GNU General Public License, Wireshark is free software. Figure 8.13 has a screen shot of what Wireshark looks like when its running. To read more, visit http://www.wireshark.org/.

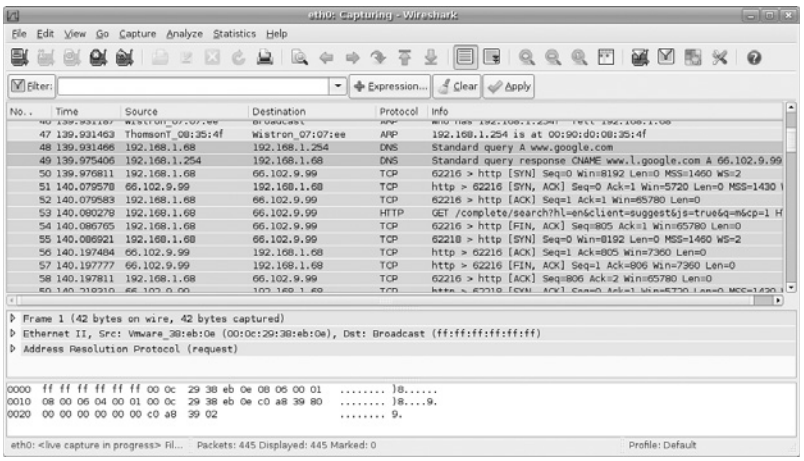


FIGURE 8.13
Wireshark

FICTIONAL STORY DISSECTED: Pretty Good Privacy Whole Disk

> This is a PGP pass phrase screen—if he has anything valuable, it's going to be in this system, and we aren't going to get in (p. 51).

As Pavel and Vlad walk into Bob's room, they start to notice that he is a computer hacker. Pavel is quick to notice things that only skilled computer hackers would have in their most personal spaces like a home office. Pavel notices that one of the computers Bob has lying around is displaying a Pretty Good Privacy (PGP) passphrase screen. This means that Bob has locked his system down with PGP, and without the proper passphrase, there will be no way Pavel or Vlad can access the data. Even if they somehow bypass having to insert a passphrase, the data is useless because PGP has encrypted it. To decrypt this information, you must have the passphrase. Bob is a smart one! Figure 8.14 is a picture of what Pavel and Vlad might be seeing on Bob's computer.

PGP is a computer program that provides cryptographic privacy and authentication. PGP is often used for signing, encrypting, and decrypting e-mails to increase the security of e-mail communications. It was originally created by Philip Zimmermann in 1991. PGP and other similar products follow the OpenPGP standard (RFC 4880) for encrypting and decrypting data.

PGP encryption uses public-key cryptography, and includes a system which binds the public keys to a username and/or an e-mail address.The first version of this system

FIGURE 8.14
PGP passphrase screen

was generally known as a web of trust to contrast with the X.509 system, which uses a hierarchical approach based on certificate authority and which was added to PGP implementations later. Current versions of PGP encryption include both options through an automated key management server. To learn more, visit http://www.pgp.com/.

FICTIONAL STORY DISSECTED: Personal Firewall

> "Look!" Bob pointed to the flashing alert on his computer. His Comodo Firewall had popped a window in front of his SuperScan (p. 42).

Pavel is scanning the 3DNF network while Bob's computer is wirelessly connected. Because Bob is on the same network, Pavel's scan touches Bob's computer. Bob's computer has a personal software firewall installed, and this is what alerts him to Pavel's scan. Figure 8.15 is a picture of the firewall Bob is using, and in Figure 8.16, you will see a popup window similar to the one Bob received.

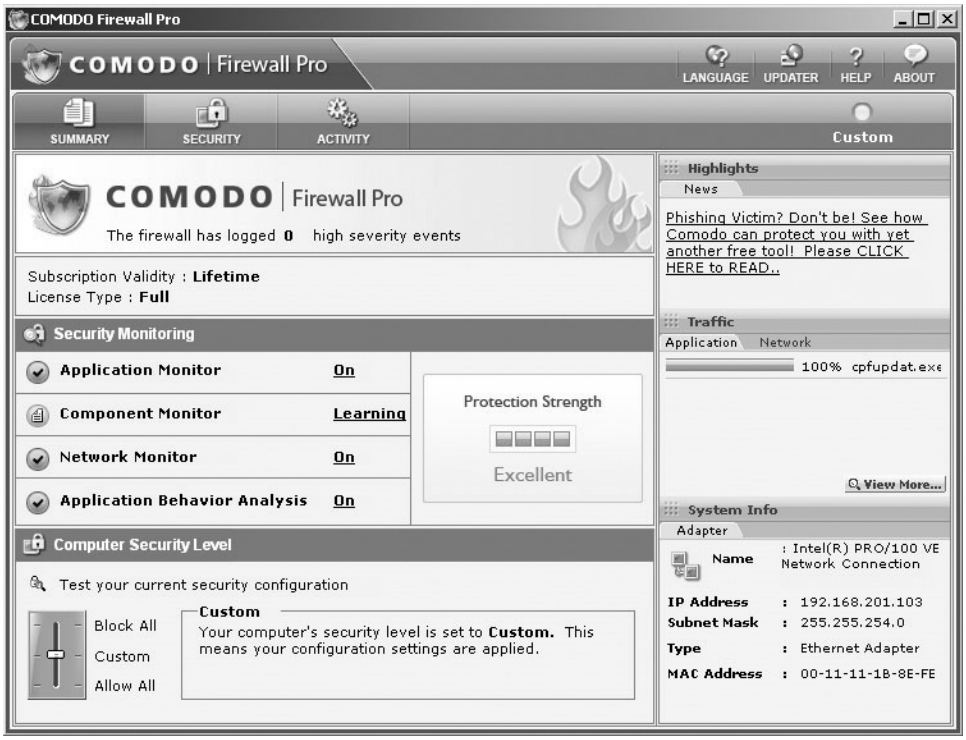


FIGURE 8.15

Comodo Firewall

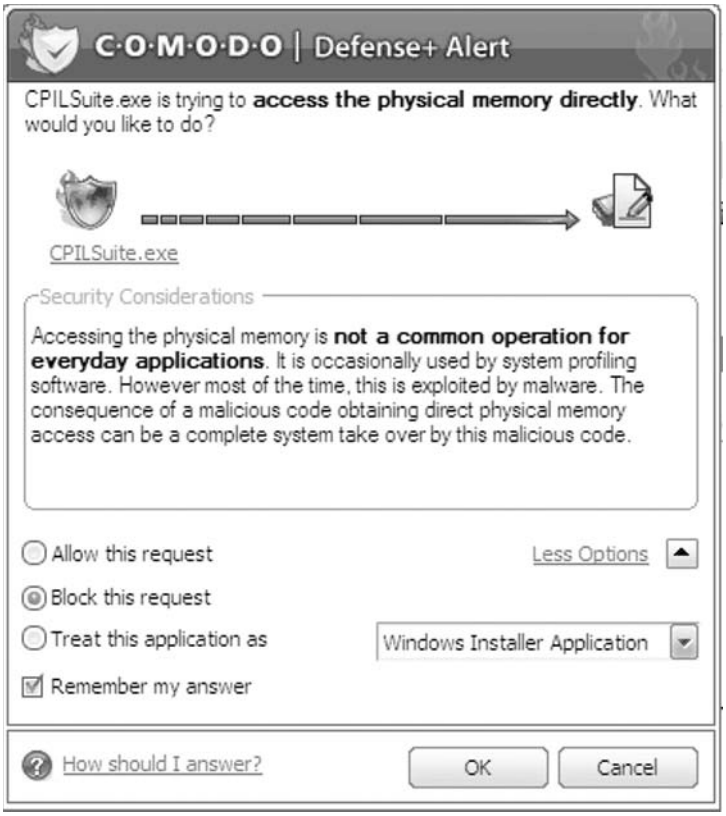


FIGURE 8.16

Comodo Firewall alert

A personal firewall is an application that controls network traffic to and from a computer, permitting or denying communications based on a security policy. A personal firewall differs from a conventional firewall in terms of scale. Personal firewalls are typically designed for use by end-users. As a result, a personal firewall will usually protect only the computer on which it is installed. Many personal firewalls are able to control network traffic by prompting the user each time a connection is attempted and adapting security policy accordingly, just as Bob's Comodo Personal Firewall prompted him. Personal firewalls may also provide some level of intrusion detection, allowing the software to terminate or block connectivity where it suspects an intrusion is being attempted. Some common personal firewalls include ZoneAlarm Pro (Figure 8.17), Outpost Firewall Pro (Figure 8.18), Norman Personal Firewall (Figure 8.19), eConceal Pro (Figure 8.20), Webroot Desktop Firewall (Figure 8.21), and InJoy Firewall (Figure 8.22).

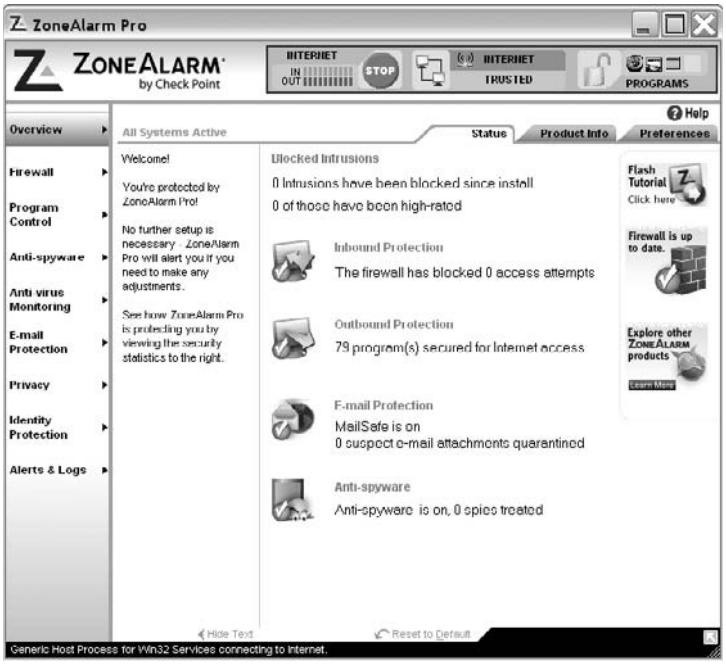


FIGURE 8.17

ZoneAlarm Pro

FIGURE 8.18

Outpost Firewall Pro

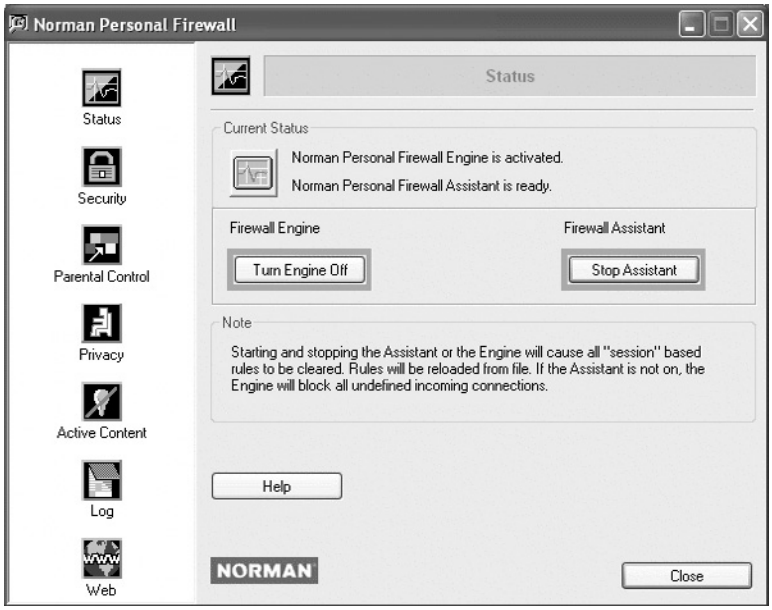


FIGURE 8.19

Norman Personal Firewall

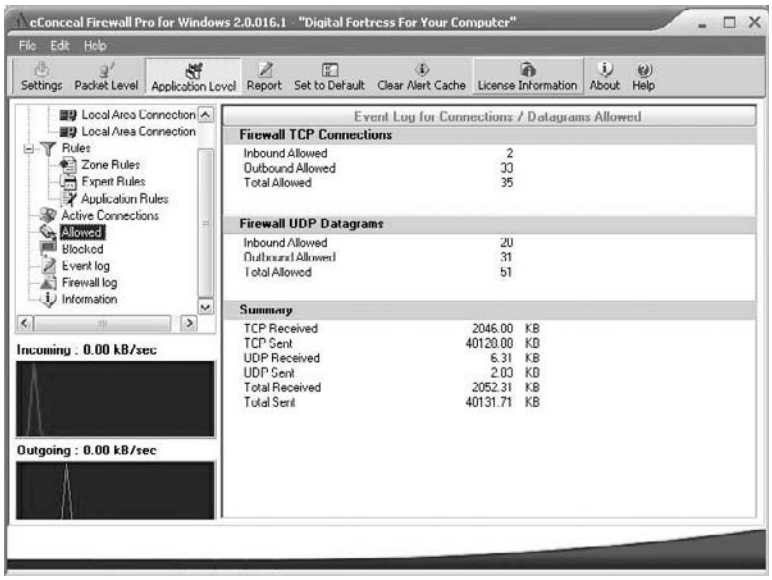


FIGURE 8.20

eConceal Firewall Pro

FIGURE 8.21

Webroot Desktop Firewall

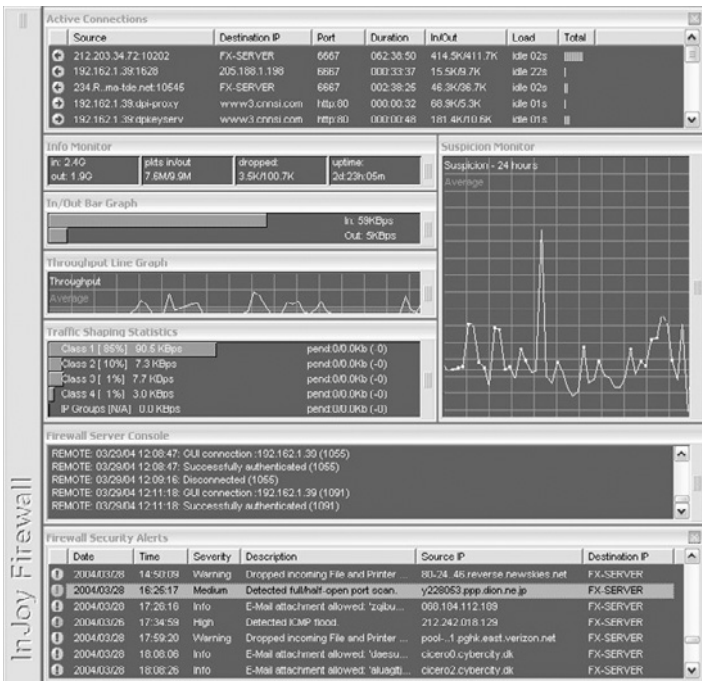


FIGURE 8.22

InJoy Firewall

FICTIONAL STORY DISSECTED: Perl Script

> "Dobbs is one of the smartest ones at the 2600 meetings. I swear if you put a keyboard on a '57 Chevy he could write a Perl script to improve the gas mileage."
>
> "What's a pearl script?" Chris asked (pp. 78–79).

Mark is referring to a type of programming language that is common knowledge of most security professionals and hackers. Perl is a high-level, general-purpose, interpreted, dynamic programming language. Perl was originally developed by Larry Wall, a linguist working as a systems administrator for NASA in 1987, as a general purpose Unix scripting language to make report processing easier.[6,7] Since then, it has undergone many changes and revisions and become widely popular among programmers. Larry Wall continues to oversee development of the core language and its upcoming version, Perl 6. Perl borrows features from other programming languages including C, shell scripting (sh), AWK, and sed.[8] This language provides powerful text processing facilities without the arbitrary data length limits of many contemporary Unix tools,[9] facilitating easy manipulation of text files. It is also used for graphics programming, system administration, network programming, and applications that require database access and CGI programming on the Web. Perl is nicknamed "the Swiss Army chainsaw of programming languages" due to its flexibility and adaptability.

PUBLIC RECORD ON TAP: Writing a Perl Script by Doug Sheppard

Beginner's Introduction to Perl (part 1)

By Doug Sheppard on October 16, 2000

First, a Little Sales Pitch

Welcome to Perl.

Perl is the Swiss Army chainsaw of scripting languages: powerful and adaptable. It was first developed by Larry Wall, a linguist working as a systems administrator for NASA in the late 1980s, as a way to make report processing easier. Since then, it has moved into a large number

[6]What is Perl; http://perl.about.com/od/gettingstartedwithperl/p/whatisperl.html

[7]Sheppard, Doug, Beginner's Introduction to Perl; http://www.perl.com/pub/a/2000/10/begperl1.html

[8]Ashton, Elaine (1999). *The Timeline of Perl and its Culture (v3.0_0505)*; http://history.perl.org/PerlTimeline.html

[9]Wall, Larry, Tom Christiansen, and Jon Orwant; *Programming Perl, Third Edition*. O'Reilly. ISBN 0-596-00027-8. July 2000.

of roles: automating system administration, acting as glue between different computer systems, and, of course, being one of the most popular languages for CGI programming on the web.

Why did Perl become so popular when the web came along? Two reasons: first, most of what is being done on the web happens with text and is best done with a language that is designed for text processing. More importantly, Perl was appreciably better than the alternatives at the time when people needed something to use. C is complex and can produce security problems (especially with untrusted data); Tcl can be awkward, and Python didn't really have a foothold.

It also didn't hurt that Perl is a friendly language. It plays well with your personal programming style. The Perl slogan is "There's more than one way to do it" and that lends itself well to large and small problems alike.

In this first part of our series, you'll learn a few basics about Perl and see a small sample program.

A Word about Operating Systems

In this series, I'm going to assume that you're using a Unix system and that your Perl interpreter is located at `/usr/local/bin/perl`. It's OK if you're running Windows; most Perl codes are platform independent.

Your First Perl Program

Take the following text and put it into a file called `first.pl`:

```
#!/usr/local/bin/perl

print "Hi there!\n";
```

(Traditionally, first programs are supposed to say `Hello world!`, but I'm an iconoclast.)

Now, run it with your Perl interpreter. From a command line, go to the directory with this file and type `perl first.pl`. You should see

```
Hi there!
```

The `\n` indicates the "newline" character; without it, Perl doesn't skip to a new line of text on its own.

Functions and Statements

Perl has a rich library of *functions*. They're the verbs of Perl, the commands that the interpreter runs. You can see a list of all the built-in functions on the perlfunc main page. Almost all functions can be given a list of *parameters*, which are separated by commas.

The `print` function is one of the most frequently used parts of Perl. You use it to display things on the screen or to send information to a file (which we'll discuss in the next article). It takes a list of things to output as its parameters.

```
print "This is a single statement.";

print "Look, ", "a", "list!";
```

A Perl program consists of *statements*, each of which ends with a semicolon. Statements don't need to be on separate lines; there may be multiple statements on one line, or a single statement can be split across multiple lines.

```
print "This is"; print "two statements.\n"; print "But this",
"is only one statement.\n";
```

To read more about Perl visit Doug's site at http://www.perl.com/pub/a/2000/10/begperl1.html.

FICTIONAL STORY DISSECTED: Twitter

> "I told you they were Feds!" Bob tried again.
>
> "We don't know that," Leon responded. "That's just what Dobbs said in his Twitter" (p. 81).
>
> "I'm going to check a few things, and then I'm going to send some DMs on Twitter. I don't want to do a tweet in case the Feds—or whoever is chasing us—is listening" (p. 92).

Many people are using mobile social media to network and communicate (more so in the subculture), called micro-blogging.[10] Micro-blogging is a term used to define very small messages that can be sent from a single device; while the recipients receive the message, it is also being populated all over the Internet. Here, Leon describes how he received a message (via the application called Twitter) that Dobbs sent warning them that some FBI agents are on their way to meet them. DM in Twitter means "direct message". This is a feature that allows one person to send a message to another without having to share the messages contents with everybody else. Twitter is a free social networking and micro-blogging service that enables its users to send and read other users' updates, known as tweets. Tweets are text-based posts of up to 140 characters in length, which are displayed on the user's profile page and delivered to other users who have subscribed to them (known as followers).[11] Senders can restrict delivery to those in their circle of friends or, by default, allow anybody to access them. Users can send and receive tweets via the Twitter Web site, Short Message Service (SMS), or external applications. The service is free to use over the Internet, but using SMS may incur phone service provider fees. Since its creation in 2006 by Jack Dorsey, Twitter has gained extensive notability and popularity worldwide. It is sometimes described as the "SMS of the Internet,"[12] in that the site provides the functionality—via its application programming interface (API)—for other desktop and web-based applications to send and receive short text messages, often obscuring the Twitter service itself. In Figure 8.23, you can see a common interface for Twitter. For more information, visit http://www.twitter.com/.

[10]http://microblogging.com/

[11]http://twitter.com/

[12]D'Monte, Leslie; "Swine flu's tweet tweet causes online flutter." Business Standard. http://www.business-standard.com/india/news/swine-flu%5Cs-tweet-tweet-causes-online-flutter/356604/; May 2009.

FIGURE 8.23
Twitter.com

PUBLIC RECORD ON TAP: Twitter and the Swine Flu

Swine flu's tweet tweet causes online flutter

By Leslie D'Monte from the Business Standard on April 29, 2009

The swine flu outbreak has not only reached beyond Mexican borders and into the US but also invaded cyberspace. General web sites including wikipedia, social networking sites and blogs have put up useful data on the risks, symptoms, and other updates.

In some cases, though, misinformation is said to have caused online panic too. A simple real-time search on Swine Flu or #swineflu on twitter.com will reveal results such as "time for people to stop eating pigs!" and "this pigflu thing seems quite bad, you might even call it a hamdemic."

Unofficial swine flu information on Twitter may lead people to unwise decisions, opines Evgeny Morozov, a fellow at the Open Society Institute and a blogger on ForeignPolicy.com.

Mahesh Murthy, founder of Pinstorm, a digital advertising firm, and an avid user of Twitter himself (he has over 1000 followers), counters that the problem on Twitter arose from a single site @breakingnews "which kept sending a tweet every 10 minutes on swine flu. I got around 100 updates—many of them clearly based on rumours. The problem is that @breakingnews is

an automated site. I personally had to 'unfollow' the site and instead go to @CNN for authentic information."

He explains that Twitter is just like SMS, which can also spread rumours. However, unlike an SMS (where you do not know the other recipients), you can alert other twitters on twitter.com and dispel such rumours, says Murthy.

Kiruba Shankar, CEO, Business Blogging—an active Twitter himself—concurs: "Twitter is a powerful tool and even corporates are getting aware of its power to inform. Such incidents do not take away from the power of Twitter."

The increased conversations around swine flu on Twitter, where swine flu found its way into nearly 2 per cent of all tweets, are indicative of the spike in conversations around the web, states Nielsen Online. Even the Centre for Disease Control (CDC) has its presence on twitter .com/cdcemergency.

Also known as the "SMS of the internet," Twitter is a free social networking and micro-blogging service which enables users to send and read other users' updates (known as tweets) which are text-based posts of up to 140 characters. The tweets are displayed on the user's profile page and delivered to other users (via mobiles too) who have subscribed to them (known as followers).

Since its creation in 2006 by Jack Dorsey, Twitter has gained extensive popularity. It has an estimated 500,000 users in India and around 20 million worldwide. Veteran (in internet time) sites like Facebook and Orkut have 6.7 million users in India and 14.5 million users in India, respectively. To read more, visit http://www.business-standard.com/india/news/swine-flu%5Cs-tweet-tweet-causes-online-flutter/356604/.

PUBLIC RECORD ON TAP: Twitter and Iran?

Iran Elections: A Twitter Revolution?

By Evgeny Morozov from the Washington Post June 17, 2009

Evgeny Morozov, blogger for *Foreign Policy* magazine and a fellow with Open Society Institute, was online Wednesday, June 17, at 3 p.m. ET to discuss the role of Twitter and other social-networking services and Web sites in coverage of the Iranian elections.

The State Department asked social-networking site Twitter to delay scheduled maintenance earlier this week to avoid disrupting communications among tech-savvy Iranian citizens as they took to the streets to protest Friday's reelection of President Mahmoud Ahmadinejad.

The move illustrates the growing influence of online social-networking services as a communications medium. Foreign news coverage of the unfolding drama, meanwhile, was limited by Iranian government restrictions barring journalists from "unauthorized" demonstrations.

In an e-mail interview with washingtonpost.com Morozov said, "it has been of great help in terms of getting information out of the country. Whether it has helped to organize protests—something that most of the media are claiming at the moment—is not at all certain, for, as a

public platform, Twitter is not particularly helpful for planning a revolution (authorities could be reading those messages as well!). However, in terms of involving the huge Iranian diaspora and everyone else with a grudge against Ahmadinejad, it has been very successful. Inevitably, there have been negative effects as well—for example, several campaigns to organize cyber-attacks on pro-government Web sites have been publicized via Twitter, which I think shows that there is also a very dark side to new media that is yet to be explored." To read more, visit http://www.washingtonpost.com/wp-dyn/content/discussion/2009/06/17/DI2009061702232.html.

PUBLIC RECORD ON TAP: Privacy and Security Issues in Social Networking

Privacy and Security Issues in Social Networking

By Brendan Collins from Fast Company

Given the rising popularity of social networks, it's little surprise that there have been several high-profile breaches of security on sites as huge as MySpace and Facebook. With over 350 million members combined, all it takes is one single person to cause a major damage. Learn how the networks are dealing with the breaches—and how to protect yourself.

When it comes to privacy and security issues on social networks, "the sites most likely to suffer from issues are the most popular ones," Graham Cluley, Chief Technology Officer at UK tech security firm Sophos says. But security issues and privacy issues are entirely two different beasts. A security issue occurs when a hacker gains unauthorized access to a site's protected coding or written language. Privacy issues, those involving the unwarranted access of private information, don't necessarily have to involve security breaches. Someone can gain access to confidential information by simply watching you type your password. But both types of breaches are often intertwined on social networks, especially since anyone who breaches a site's security network opens the door to easy access to private information belonging to any user. But the potential harm to an individual user really boils down to how much a user engages in a social networking site, as well as the amount of information they're willing to share. In other words, the Facebook user with 900 friends and 60 group memberships is a lot more likely to be harmed by a breach than someone who barely uses the site.

Security lapses on social networks don't necessarily involve the exploitation of a user's private information. Take, for example, the infamous "Samy" MySpace XSS worm that effectively shut the site down for a few days in October 2005. The "Samy" virus (named after the virus' creator) was fairly harmless, and the malware snarkily added the words "Samy Is My Hero" to the top of every affected user's MySpace profile page. A colossal inconvenience, naturally, but nobody's identity was stolen and no private information was leaked. In the end, the problem galvanized the MySpace team to roll up their sleeves and seriously tighten the site's security. Result: no major break-ins since. Unfortunately, these kinds of breaches, purely for sport in "Samy's" case, are rare.

The reason social network security and privacy lapses exist results simply from the astronomical amounts of information the sites process each and every day that end up making it that much easier to exploit a single flaw in the system. Features that invite user participation—messages, invitations, photos, open platform applications, etc.—are often the avenues used to gain access to private information, especially in the case of Facebook. Adrienne Felt, a Ph.D. candidate at Berkeley, made small headlines last year when she exposed a potentially devastating hole in the framework of Facebook's third-party API which allows for easy theft of private information. Felt and her co-researchers found that third-party platform applications for Facebook gave developers access to far more information (addresses, pictures, interests, etc.) than needed to run the app.

This potential privacy breach is actually built into the systematic framework of Facebook, and unfortunately the flaw renders the system almost indefensible. "The question for social networks is resolving the difference between mistakes in implementation and what the design of the application platform is intended to allow," David Evans, Assistant Professor of Computer Science at the University of Virginia, says. There's also the question of whom we should hold responsible for the oversharing of user data. That resolution isn't likely to come anytime soon, says Evans, because a new, more regulated API would require Facebook "to break a lot of applications, and a lot of companies are trying to make money off applications now." Felt agrees, noting that now "there are marketing businesses built on top of the idea that third parties can get access to data on Facebook."

The problems plaguing social network security and privacy issues, for now, can only be resolved if users take a more careful approach to what they share and how much. With the growth of social networks, it's becoming harder to effectively monitor and protect site users and their activity because the tasks of security programmers become increasingly spread out. Imagine if a prison whose inmate count jumped from a few dozen to 250 million in less than five years only employed 300 guards (in the case of MySpace). In response to the potential threats that users are exposed to, most of the major networks now enable users to set privacy controls for who has the ability to view their information. But, considering the application loophole in Facebook, increased privacy settings don't always guarantee privacy. But even when the flawed API was publicly exposed, "Facebook changed the wording of the user agreement a little bit, but nothing technically to solve the problem," says Evans. That means if a nefarious application developer wanted to sell the personal info of people who used his app to advertising companies, he or she could. To read more visit http://www.fastcompany.com/articles/2008/10/social-networking-security.html.

PUBLIC RECORD ON TAP: Online Social Networking

Online Social Networking Dangers and Benefits

By University of the Pacific

One of the most popular social networking sites is Facebook. While Facebook restricts members to those who use an ".edu" email address, this may give you a false sense of security. There are hundreds of thousands of active ".edu" email addresses of current students and alumni

in just the United States and many of them can gain access to your site. Some colleges and universities will grant free email addresses to alumni; however, they do not always follow-up to check whether the individual is an actual alumnus—therefore making it relatively easy to create false ".edu" accounts on Facebook and gain access to the site. Other social networking sites such as Myspace, Friendster, and Xanga offer even less security and protection because they are open to anyone.

Because students often post detailed and specific information on Facebook (including phone numbers, addresses, class schedules, social plans, etc.) you can be more easily stalked by strangers (or even acquaintances). To read move visit http://web.pacific.edu/x4989.xml.

FICTIONAL STORY DISSECTED: Bluesnarf

> "With this and the Bluesnarf software we configured, you can use this either to detect a Bluetooth device in the area or to even jack in on some of the older models" (p. 95).

Bob and R10t are using a technique called Bluesnarf to detect Bluetooth-enabled devices and possibly pair with those devices and extract things like contacts, tasks, e-mails, SMS messages, and incoming and outgoing calling history.

Bluesnarfing is the unauthorized access of information from a wireless device through a Bluetooth connection, often between phones, desktops, laptops, and PDAs. This allows access to a calendar, contact list, e-mails, and text messages; and on some phones, users can copy pictures and private videos. Currently available programs must allow connection and to be "paired" to another phone to copy content. There may be other programs that can break into the phones without any control; but if they exist, they are not made publicly available by the developer. One instance of Bluesnarfing software that was demonstrated (but never made available for download) used weaknesses in the Bluetooth connection of some phones. This weakness has since been patched by the Bluetooth standard. There seem to be no available reports of phones being Bluesnarfed without pairing, since the patching of the Bluetooth standard.

Bluesnarfing is much more serious than Bluejacking, but both exploit others' Bluetooth connections without their knowledge. Any device with its Bluetooth connection turned on and set to "discoverable" (able to be found by other Bluetooth devices in range) may be susceptible to Bluejacking, and possibly to Bluesnarfing when and if Bluesnarfing of the current Bluetooth security becomes possible. By turning off this feature, the potential victim can be safer from the possibility of being Bluesnarfed, although a device that is set to "hidden" may be Bluesnarfable by guessing the device's MAC address via brute force. However, this is difficult because Bluetooth uses a 48-bit unique MAC address, so there are over 280 trillion possible addresses to guess (although the first 24 bits are common to a

manufacturer,[13] only 24 bits need be guessed). Because Bluesnarfing is an invasion of privacy, it is illegal in many countries.

It is important not to confuse Bluesnarfing with Bluejacking. Although Bluejacking is essentially harmless and does not result in the exposure of any data in the victim's handset, Bluesnarfing is the copying of information from the victim's Bluetooth device. See Figure 8.24 for a Web site full of Bluejacking tools; in fact, they claim to have the biggest collection of Bluetooth tools on the Internet.

In Figure 8.25, the tool BTCrawler is being used to look for Bluetooth-enabled devices. Figure 8.26 shows BTCrawler scanning and discovering devices. Finally in Figure 8.27, BTCrawler has paired with victim device 0060 and is downloading their phonebook.

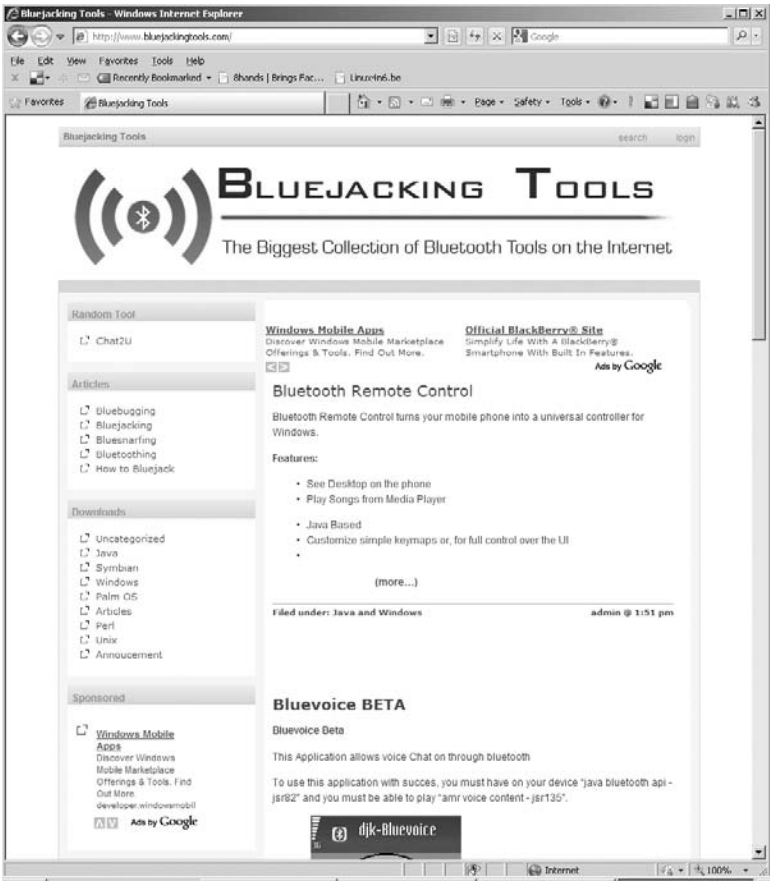


FIGURE 8.24
Bluejacking Tools Web site

[13]SecurityFocus; Bluetooth Security Review, Part 1; http://www.securityfocus.com/infocus/1830

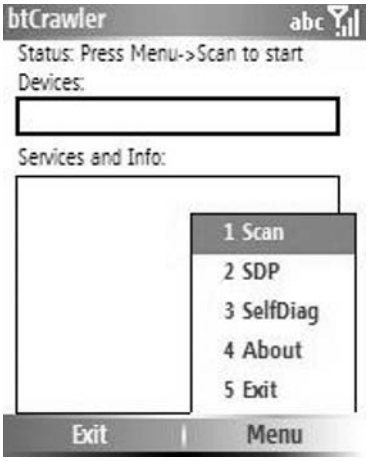


FIGURE 8.25

BTCrawler scanning for Bluetooth-enabled devices

FIGURE 8.26

BTCrawler results

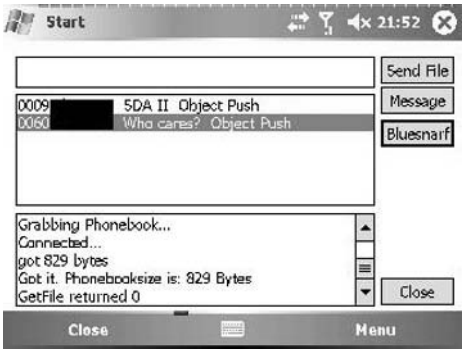


FIGURE 8.27

BTCrawler grabbing phone book of Bluetooth device 0060

PUBLIC RECORD ON TAP: The Role of Bluesnarfing

The Role of Bluesnarfing

By a Bluesnarfer's view from bluesnarf.blogspot.com

There are people who have predicted the doom of bluetooth tooth attacks like bluesnarfing. Their reasoning is that Wi-Fi will eventually replace the need for bluetooth devices and without bluetooth, it make sense there will be no bluetooth attacks.

While convincing and logical, bluetooth has yet to be phased out long after WiFi is in use. In fact, there are more and more devices using bluetooth technology. The main reason: It's free. Unlike wifi which is a overall network and you are just a "user" in the network, you "own the network." You can switch in on and off anytime you like, and you don't have to pay a cent. There is no logic for example to use wifi for connecting with your headset, but bluetooth fits that function perfectly.

In fact, this neglect on the importance of bluetooth has led to an added advantage to bluesnarfers. Because every is concern about their wifi security, they neglect the fact that their short ranged network which is their bluetooth can easier be hacked into for someone who is nearby or even far away but with the right equipment. The reason why there is little news about bluesnarfing is that there is no good solution to the problem at the moment, save for switching off your bluetooth device. So my advice is, be careful if you keep confidential information on your bluetooth devices. To read more visit http://bluesnarf.blogspot.com/.

PUBLIC RECORD ON TAP: Bluetooth Hacking Tools

Bluetooth Hacking Tools Part 1

By Rashmi Jadhav on March 24, 2009

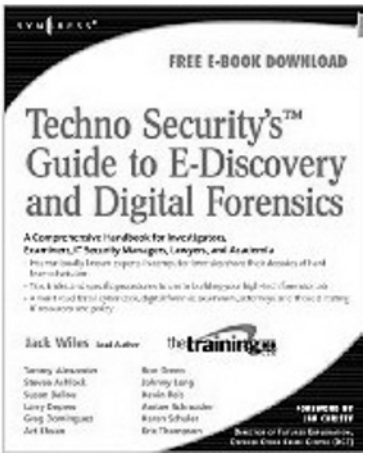
There are some tools essential for bluetooth hacking purposes:

1. BlueScanner: In this the tool hacker searches for bluetooth enable device. After that it will try to extract as much information as possible for each newly discovered device.
2. BlueSniff: Blue Sniff is a GUI-based utility for finding discoverable and hidden Bluetooth-enabled devices.
3. BlueBugger: The buggers exploit the vulnerability of the device. The bluebugger is set for the bluetooth security holes found in some bluetooth-enabled device. They can access the images, phone-book, messages, and other personal information.
4. Bluesnarfer: Bluesnarfing is a serious problem which is discovered in several Bluetooth-enabled mobile phones. If a Bluetooth of an device is switch on, then it is possible to connect to the phone without alerting the owner, and gain to access to restricted portions of the stored data.
5. BlueDiving: Bluediving is a Bluetooth penetration testing. It implements attacks like Bluebug, BlueSnarf, BlueSnarf++, and BlueSmack. While also has features such as Bluetooth address spoofing, an AT and a RFCOMM socket shell and implements tools like carwhisperer, L2CAP, packet generator, L2CAP connection resetter, RFCOMM scanner and greenplaque scanning mode.
6. Transient Bluetooth Environment Auditor: T-BEAR is a security-auditing platform for the Bluetooth-enabled devices. The platform consists of Bluetooth discovery tools, sniffing

tools and also various cracking tools. There are also some more hacking tools such as the BTBrowser, BTCrawler. Can I hack With Bluetooth (CIHWB), BTcrack, BlueTest, and BTAudit.

To read more, visit http://www.hackersenigma.com/.

BOOKS



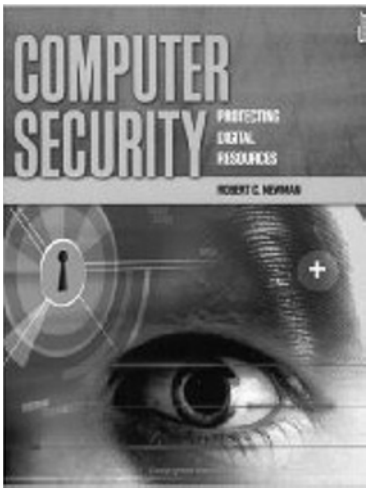
Techno Security's Guide to E-Discovery and Digital Forensics:"A Comprehensive Handbook for Investigators, Examiners, IT Security Managers, Lawyers, and Academia"

By Jack Wiles

Publisher: Syngress

ISBN-10: 159749223X

ISBN-13: 978-1597492232



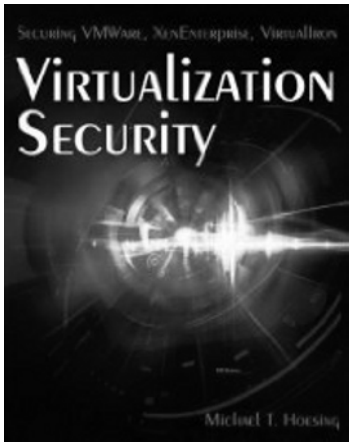
Computer Security: Protecting Digital Resources

By Robert Newman

Publisher: Jones & Bartlett Publishers

ISBN-10: 0763759945

ISBN-13: 978-0763759940



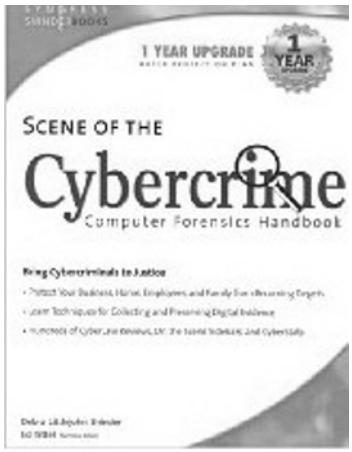
Virtualization Security: Securing VMware, XenEnterprise, VirtualIron

By Michael T. Hoesing

Publisher: Wiley

ISBN-10: 0470177063

ISBN-13: 978-0470177068



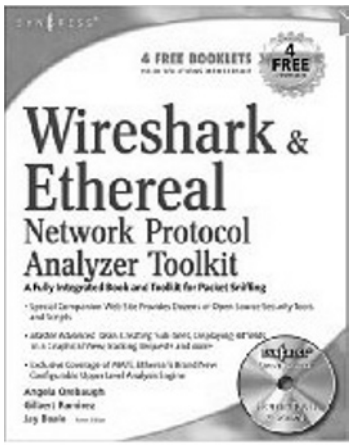
Scene of the Cybercrime: Computer Forensics Handbook

By Syngress

Publisher: Syngress

ISBN-10: 1931836655

ISBN-13: 978-1931836654



Wireshark & Ethereal Network Protocol Analyzer Toolkit

By Angela Orebaugh, Gilbert Ramirez, and Jay Beale

Publisher: Syngress

ISBN-10: 1597490733

ISBN-13: 978-1597490733

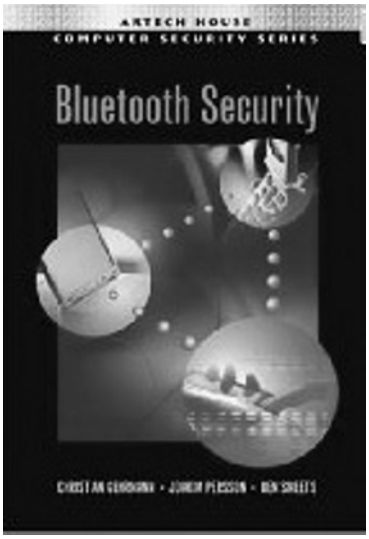
Twitter Tips, Tricks, and Tweets

By Paul McFedries and Pete Cashmore

Publisher: Wiley

ISBN-10: 0470529695

ISBN-13: 978-0470529690



Bluetooth Security (Artech House Computer Security Series)

By Christian Gehrmann, Joakim Persson, and Ben Smeets

Publisher: Artech House Publishers

ISBN-10: 1580535046

ISBN-13: 978-1580535045

CHAPTER

Bleeding Edge Technology

9

Bleeding edge technology is sometimes kept a secret in large organizations working on the next-generation solution for their customers. But in a hacker's mind, bleeding edge technology must be released to the public. Many times this is done through conferences held around the world for security professionals and well-known hackers. Bleeding edge is a term that refers to technology that is so new that the user is required to risk reductions in stability and productivity to use it. It also refers to the tendency of the latest technology to be extremely expensive. This is a corporate definition of bleeding edge—as for the rest of the security community, bleeding edge is anything that has a higher degree of risk compared with the known methods in the industry. The term is formed as an allusion to "leading edge" and its synonym cutting edge, but implying a greater degree of risk: the "bleeding edge" is in front of the "cutting edge." A technology may be considered bleeding edge under the following conditions:

1. Lack of consensus: Competing ways of doing some new thing exist, and no one really knows for certain which way the market is going to go.
2. Lack of knowledge: Organizations are trying to implement a new technology or product that the trade journals have not even started talking about yet, either for or against.
3. Industry resistance to change: Trade journals and industry leaders have spoken against a new technology or product, but some organizations are trying to implement it anyway because they are convinced it is technically superior.

FICTIONAL STORY DISSECTED: Infrared Hotel Attack

> "At DEFCON, Major Malfunction presented a hack using a Linux box to break into hotel information systems through the TV set in a room. You can grab reservation information, TV movies they've watched, and sometimes even credit card information or read their e-mails" (p. 8).

Adam Laurie, technical director of The Bunker, a managed network data services firm, is known as Major Malfunction in the hacker community. In 2005 at the Riviera Hotel & Casino in Las Vegas, Nevada, Major Malfunction stood up and walked to the podium at a well-known conference called DEFCON. He was about to give a presentation describing how he was able to view hotel guests information using the in-room TV. Using a laptop, an infrared transmitter, and a USB TV tuner, Major Malfunction was able to pick up information through the hotel TV from the backend databases. These backend databases contained such things as billing for the minibar, remote-minibar locking system, room-cleaning status, and billing systems used to check account balances.[1] This bleeding edge technique allowed him to view the channels he wanted without the hotel knowing anything. It also gave him the ability to view other hotel guest's private channels where they would normally check their hotel bill from the TV. The whole thing started when he was bored in his Miami hotel one day and decided to see if he could watch some adult movies for free. To read more about Major Malfunction, visit http://www.defcon.org/html/defcon-13/dc13-speakers.html#major.

FICTIONAL STORY DISSECTED: MD5 Hash

> "And no hacking the judge's PC for the MD5 hash files, or trying to work out a collision on your PS3," Bob added (p. 32).

Bob and Leon are setting up the rules for the game "Capture the Flag." Leon knows that anyone could copy a CyberBob icon and pass it off as if they had found it in a nearby neighborhood. To prevent people from cheating, Leon and Bob decide to hash the CyberBob icon files. Hashing is the process of a mathematical function to convert large amounts of data into a small datum. This datum is always a unique string of numbers and letters identifying the original file to be one of a kind when compared to this hash. In cryptography, MD5 (Message-Digest algorithm 5) is a widely used cryptographic hash function with a 128-bit hash value. As an Internet standard (RFC 1321), MD5 has been used in a wide variety of security applications and is also commonly used to check the integrity of files.

Hashing a file is very easy. For instance, in Figure 9.1, the tool WinM5D is used to open a file named test_01.txt and test_02.txt to compare their hashes. The file names are different but their hashes are the same. This is because the contents of each file are identical; they are both blank text files. Now in Figure 9.2, I have inserted a line of text into the file named test_01.txt. As Figure 9.3 shows, the file named test_01.txt now has a completely different hash value, since it has content inside of the file that is different from the content inside the file named test_02.txt. For more information on this MD5 tool, visit http://www.blisstonia.com/software/WinMD5/.

[1] "A Hacker Games the Hotel," by Kim Zetter, Wired.com, http://www.wired.com/politics/security/news/2005/07/68370.

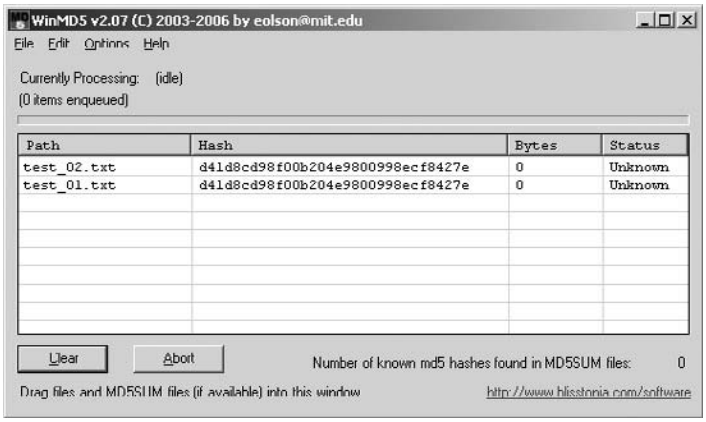


FIGURE 9.1

WinMD5 tool

FIGURE 9.2

Text file test_01.txt

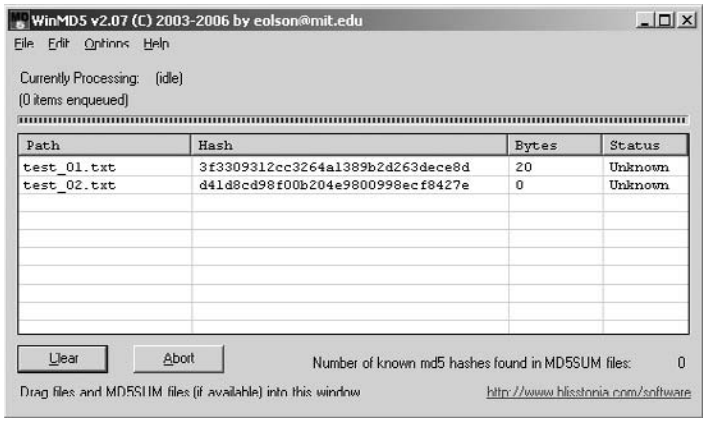


FIGURE 9.3

WinMD5 tool with new content in file test_01.txt

DON'T HACK ME PLEASE: Breaking SSL Using 200 PS3s[2]

25c3: Hackers Completely Break SSL Using 200 PS3s

By Eliot Phillips from Hack A Day, December 30, 2008

FIGURE 9.4

A team of security researchers and academics has broken a core piece of Internet technology. They made their work public at the 25th Chaos Communication Congress in Berlin today (See Hacking Culture, chapter 10, for more information on the Chaos Communication Congress). The team was able to create a rogue certificate authority and use it to issue valid SSL certificates for any site they want. The user would have no indication that their HTTPS connection was being monitored/modified.

This attack is possible because of a flaw in MD5. MD5 is a hashing algorithm; each unique file has a unique hash. In 2004, a team of Chinese researchers showed creating two different files that had the same MD5 hash. In 2007, another team showed theoretical attacks that took advantage of these collisions. The team focused on SSL certificates signed with MD5 for their exploit.

The first step was doing some broad scans to see what certificate authorities (CA) were issuing MD5 signed certs. They collected 30K certs from Firefox trusted CAs. 9K of them were MD5 signed. 97% of those came from RapidSSL.

Having selected their target, the team needed to generate their rogue certificate to transfer the signature to. They used the processing power of 200 Playstation 3s to get the job done. For this task, it's the equivalent of 8000 standard CPU cores or $20K of Amazon EC2 time. The task takes ~1–2 days to calculate. The tricky part was knowing the content of the certificate that would be issued by RapidSSL. They needed to predict two variables: the serial number and the time stamp. RapidSSL's serial numbers were all sequential. From testing, they knew that RapidSSL would always sign 6 s after the order was acknowledged. Knowing these two facts, they were able to generate a certificate in advance, and then

[2]http://hackaday.com/2008/12/30/25c3-hackers-completely-break-ssl-using-200-ps3s/.

purchase the exact certificate they wanted. They'd purchase certificates to advance the serial number and then buy on the exact time they calculated. The cert was issued to their particular domain; but since they controlled the content, they changed the flags to make themselves an intermediate certificate authority. That gave them authority to issue any certificate they wanted. All these "valid" certs were signed using SHA-1. If you set your clock back to before August 2004, you can try out their live demo site. This time is just a security measure for the example and this would work identically with a certificate that hasn't expired. There's a project site and a much more detailed write-up than this.

To fix this vulnerability, all CAs are now using SHA-1 for signing, and Microsoft and Firefox will be blacklisting the team's rogue CA in their browser products. To read more, visit http://hackaday.com/2008/12/30/25c3-hackers-completely-break-ssl-using-200-ps3s/.

FICTIONAL STORY DISSECTED: Echelon

"I knew it!" Dobbs exclaimed. "You guys and your Patriot Act are watching all of us!"

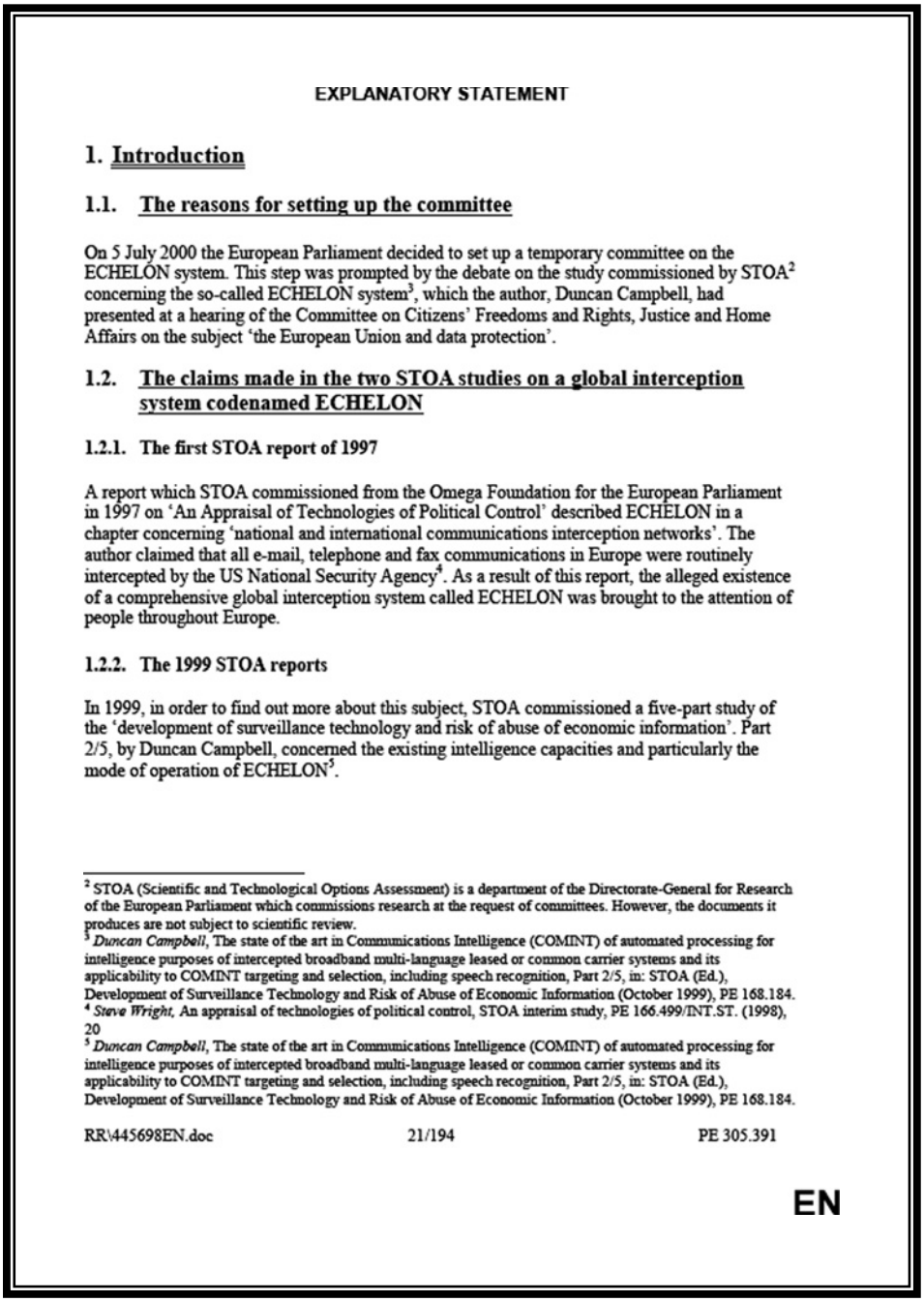
Mark revealed a look of exasperation and annoyance as he raised both his hands slightly towards Dobbs. "I'm just a tech who has learned it's best not to tell everyone where I work."

"That's crap! I bet you are part of a whole program made just to watch people like us. You just need to put some faces with all the data you've been scraping with Echelon!" (pp. 9, 77–78).

Dobbs demonstrates some intuition here, and reveals his paranoia over the use of the Patriot Act and the eavesdropping system commonly referred to as Echelon. This is bleeding edge technology since it is not public knowledge that these systems exist or how they work.

ECHELON is a name used in global media and in popular culture to describe a signals intelligence (SIGINT) collection and analysis network operated on behalf of the five signatory states to the UK–U.S. Security Agreement. They include countries such as Australia, Canada, New Zealand, the United Kingdom, and the United States, also known as AUSCANZUKUS.[3] It has also been described only as the software system that controls the download and dissemination of the intercept of commercial satellite trunk communications.[4] The system has been reported in a number of public sources.[5] Its capabilities and political implications were investigated by a committee of the European Parliament during 2000 to 2001 with a report published in 2001,[6] and by author James Bamford in his books on the National Security Agency of the United States.[2]

[3]AUSCANNZUKUS Information Portal, http://auscannzukus.net/.
[4]Bamford, James; *Body of Secrets*, Anchor, ISBN 0-385-49908-6; 2002.
[5]New Statesman news article entitled *Someone's Listening* in 1988; http://www.newstatesman.com/
[6]Schmid, Gerhard; *European Parliament: Temporary Committee on the ECHELON Interception System*; http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//EN&language=EN.



EXPLANATORY STATEMENT

1. Introduction

1.1. The reasons for setting up the committee

On 5 July 2000 the European Parliament decided to set up a temporary committee on the ECHELON system. This step was prompted by the debate on the study commissioned by STOA[2] concerning the so-called ECHELON system[3], which the author, Duncan Campbell, had presented at a hearing of the Committee on Citizens' Freedoms and Rights, Justice and Home Affairs on the subject 'the European Union and data protection'.

1.2. The claims made in the two STOA studies on a global interception system codenamed ECHELON

1.2.1. The first STOA report of 1997

A report which STOA commissioned from the Omega Foundation for the European Parliament in 1997 on 'An Appraisal of Technologies of Political Control' described ECHELON in a chapter concerning 'national and international communications interception networks'. The author claimed that all e-mail, telephone and fax communications in Europe were routinely intercepted by the US National Security Agency[4]. As a result of this report, the alleged existence of a comprehensive global interception system called ECHELON was brought to the attention of people throughout Europe.

1.2.2. The 1999 STOA reports

In 1999, in order to find out more about this subject, STOA commissioned a five-part study of the 'development of surveillance technology and risk of abuse of economic information'. Part 2/5, by Duncan Campbell, concerned the existing intelligence capacities and particularly the mode of operation of ECHELON[5].

[2] STOA (Scientific and Technological Options Assessment) is a department of the Directorate-General for Research of the European Parliament which commissions research at the request of committees. However, the documents it produces are not subject to scientific review.
[3] *Duncan Campbell*, The state of the art in Communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems and its applicability to COMINT targeting and selection, including speech recognition, Part 2/5, in: STOA (Ed.), Development of Surveillance Technology and Risk of Abuse of Economic Information (October 1999), PE 168.184.
[4] *Steve Wright*, An appraisal of technologies of political control, STOA interim study, PE 166.499/INT.ST. (1998), 20
[5] *Duncan Campbell*, The state of the art in Communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems and its applicability to COMINT targeting and selection, including speech recognition, Part 2/5, in: STOA (Ed.), Development of Surveillance Technology and Risk of Abuse of Economic Information (October 1999), PE 168.184.

RR\445698EN.doc 21/194 PE 305.391

EN

FIGURE 9.5

Temporary Committee on the ECHELON Interception System Report page

In its report, the European Parliament states that the term *ECHELON* is used in a number of contexts, but that the evidence presented indicates that it was the name for a SIGNIT collection system. The report concludes that, on the basis of information presented, ECHELON was capable of interception and content inspection of telephone calls, fax, e-mail, and other data traffic globally through the interception of communication bearers including satellite transmission, public-switched telephone networks (which carries most Internet traffic), and microwave links.[4] Bamford describes the system as the software controlling the collection and distribution of civilian telecommunications traffic conveyed using communication satellites, with the collection being undertaken by groundstations located in the footprint of the downlink leg.[4]

FIGURE 9.6

A radome at RAF Menwith Hill

In Figure 9.5, you can see p. 304 of the report describing the reasons why the European Parliament decided to conduct an investigation. Figure 9.6 is a picture of radar/dome known as a radome. This particular one is located at RAF Menwith Hill, a site with satellite downlink capabilities believed to be used by ECHELON system.

FICTIONAL STORY DISSECTED: TOR Network

> I'll use a VMware browser appliance through TOR to a Web site that sends texts" (p. 83).

We should have already guessed that Bob has some plan to get in touch with Jeb without leaving a trace. Bob decides to use TOR, also known as The Onion Router (Tor). The Tor is a free software implementation of second-generation onion routing—a system that claims to enable its users to communicate anonymously on the Internet. Roger Dingledine, Nick Mathewson, and Paul Syverson presented "Tor: The Second-Generation Onion Router" at the 13th USENIX Security Symposium.[7] Tor cannot and does not try to protect against monitoring of traffic at the edge of the Tor network, i.e., the traffic entering and exiting the network.

[7]Dingledine, Roger; Mathewson, Nick; Syverson, Paul; "Tor: The Second-Generation Onion Router;" Proc. 13th USENIX Security Symposium; http://www.usenix.org/events/sec04/tech/dingledine.html.

The U.S. government,[8] for example, has the capability to monitor any broadband Internet traffic using devices mandated by the Communications Assistance For Law Enforcement Act (CALEA) and can therefore monitor both ends of a U.S.-based Tor connection. Tor tries to protect against traffic analysis, but Tor does not have the ability to prevent traffic confirmation (also called end-to-end correlation). Originally sponsored by the U.S. Naval Research Laboratory, Tor became an Electronic Frontier Foundation (EFF) project in late 2004, and the EFF supported Tor financially until November 2005.[9] Tor software is now developed by the Tor Project, which since December 2006 is a 501(c)(3) research/education nonprofit organization based in the United States of America that receives a diverse base of financial support.[7]

FICTIONAL STORY DISSECTED: Yagi Rifle

> "I thought I'd start with 0hm and M00d1mus. They've been working on a Yagi rifle that we can use for a distant wireless hookup" (p. 92).

This is really bleeding edge technology—who do you know walks around with a makeshift antenna mounted on a rifle's chassis? Bob probably heard about Yagi rifles at DEFCON, as the "Public Record on Tap" explains where and when this technology was first released. Wi-Fi is not the only technology that is being exploited from Yagi rifles: Bluetooth is as well. (See "Public Record on Tap: Bluetooth Yagi Rifle.") Figure 9.7 is a picture of what is known as a "Sniper Yagi," powerful enough to connect to WLANs over 9 miles away.[10,11] A Yagi-Uda Antenna, commonly known simply as a Yagi antenna or Yagi, is a directional antenna system[12] consisting of an array of a dipole and additional closely coupled parasitic elements (usually a reflector and one or more directors), as seen in Figure 9.7. The dipole in the array is driven; and another element, 10% longer, operates as a reflector. Other shorter parasitic elements are typically added in front of the dipole as directors. This arrangement gives the antenna directionality that a single dipole

FIGURE 9.7

Yagi Antenna

[8]Tor website. February 18th, 2009. http://blog.torproject.org/blog/one-cell-enough.

[9]Tor sponsors; https://www.torproject.org/sponsors.

[10]http://www.theregister.co.uk/2004/08/03/wi-fi_aerial_gun/.

[11]http://www.engadget.com/2004/08/01/live-from-defcon-the-sniper-yagi/.

[12]"What is a Yagi-Uda antenna?" http://what-is-what.com/what_is/Yagi_Uda_antenna.html.

lacks. Yagis are directional along the axis perpendicular to the dipole in the plane of the elements, from the reflector through the driven element and out via the director(s). If one holds out one's arms to form a dipole and has the reflector behind oneself, one would receive signals with maximum gain from in front of oneself.

PUBLIC RECORD ON TAP: Sniper Yagi Rifle

Wi-Fi "sniper rifle" debuts at DEFCON

By John Leyden, August 3, 2004

FIGURE 9.8

Conventional Wi-Fi aerials are all well and good, but they don't really cut it if you want to impress fellow hackers and scare the general populace. Forget a modified Pringles can—what you really need at somewhere like last weekend's DEFCON shindig is something that looks like an M-16 but with its firing mechanism replaced by a 14.6 dBi Yagi antenna that can get you online at up to 10 miles (16.1 km). Yes indeed. Adapt this so that it fits into a briefcase and what you have is Day of the Jackal-style foldaway technology plus access to remote, insecure Wi-Fi networks. A must for every would-be Jason Bourne. Perfectly pitched towards the geekier members of the Michigan Militia, we doubt the US Secret Service would be as enthusiastic though—especially if they're on presidential protection duties at the time. To read more, visit http://www.theregister.co.uk/2004/08/03/wi-fi_aerial_gun/.

PUBLIC RECORD ON TAP: Bluetooth Yagi Rifle

Security Cavities Ail Bluetooth

By Kim Zetter August 6, 2004

Serious flaws discovered in Bluetooth technology used in mobile phones can let an attacker remotely download contact information from victims' address books, read their calendar appointments, or peruse text messages on their phones to conduct corporate espionage.

An attacker could even plant phony text messages in a phone's memory, or turn the phone sitting in a victim's pocket or on a restaurant table top into a listening device to pick up private conversations in the phone's vicinity. Most types of attacks could be conducted without leaving a trace.

Security professionals Adam Laurie and Martin Herfurt demonstrated the attacks last week at the Black Hat and DefCon security and hacker conferences in Las Vegas. Phone companies say the risk of this kind of attack is small, since the amount of time a victim would be vulnerable is minimal, and the attacker would have to be in proximity to the victim. But experiments, one using a common laptop and another using a prototype Bluetooth "rifle" that captured data from a mobile phone a mile away, have demonstrated that such attacks aren't so far-fetched.

FIGURE 9.9

The BlueSniper rifle for capturing data from Bluetooth-enabled phones is constructed from a Choate Ruger Mini-14 Stock, 14dBi semi-directional Yagi antenna, standard rifle scope, electrical tape, zip ties, and cardboard.

Laurie, chief security officer of London-based security and networking firm ALD, discovered the vulnerability last November. Using a program called Bluesnarf that he designed but hasn't released, Laurie modified the Bluetooth settings on a standard Bluetooth-enabled laptop to conduct the data-collection attacks.

Then, German researcher Herfurt developed a program called Bluebug that could turn certain mobile phones into a bug to transmit conversations in the vicinity of the device to an attacker's phone.

Using Bluebug from a laptop, an attacker could instruct a target phone to call his phone. The phone would make the call silently and, once connected, open a channel for the attacker to listen to conversations near the targeted phone. The attacker's phone number would appear on the victim's phone bill, but if the attacker used a throwaway phone, the number would be out of service.

"(A victim) will know that his phone made a call that it shouldn't have made, but he won't necessarily come to the right conclusion that someone listened in on the conversation that he was having at that particular time," Laurie said. "He may think he accidentally pressed buttons to make the call while the phone was in his back pocket."

An attacker could also install a gateway on the victim's phone to reroute phone calls through his own phone so that he could hear and record conversations between parties without their knowledge. And he could send text messages from his computer through a victim's phone to another phone so the receiver would think the message originated from the victim. There would be no record of the sent message on the victim's phone unless the attacker planted it there.

"I can plant the message on the phone and make it look like he sent a message that he never sent. So when the FBI grabs the phone (for evidence), the message will be in the first guy's outbox," Laurie said. "It has really serious consequences."

The use of Bluetooth, a wireless technology that lets two devices exchange information over a short distance, is growing rapidly in Europe and the United States. About 13 percent of mobile phones shipped in the United States this year have Bluetooth, according to IDC research. The number will grow to about 53 percent globally and 65 percent in the United States by 2008.

These are just the phones. According to IMS Research, 2 million Bluetooth-enabled devices—phones, laptops and PDAs—are shipped weekly in the world. Laurie and Herfurt have only tested phones for vulnerabilities so far.

"They're talking about putting Bluetooth in everything: home security, medical devices," Laurie said. "If they don't do something about security, there is some really serious stuff ahead of us."

The attacks, dubbed "Bluesnarfing" and "Bluebugging," work on several models of the most popular brands of mobile phones: Ericsson, Sony Ericsson, and Nokia (Laurie provides a chart of affected phones on his website). In each case, the researchers needed access to the target phone for only a few seconds to conduct attacks.

To read more, visit http://www.wired.com/

FIGURE 9.10

Sniper Yagi

FICTIONAL STORY DISSECTED: gh0stRAT

"Good, that will be what you target as soon as we arrive. Next, we need a more standard malware that we can drop on a couple of systems inside 3DNF."

"Won't this just set off alarms?" Pavel protested.

"I just want a couple, and they will be enough to make it look like they were sloppy with their surfing habits—which I'm sure they are. That way they won't be looking for external activity."

"All right. I've got a copy of the gh0stRAT," Pavel offered.

"Good—everyone loves to blame the Chinese. The Americans will spend their time looking in the wrong place," Vlad agreed (p. 93).

More bleeding edge than anything else we have discussed would be government-sponsored malicious tools and techniques used to hack into other governments' computer networks. Here Vlad is very smart because he is using a known Chinese hacking technique to exploit 3DNF's network. If ever the time comes and the malicious code is discovered by authorities, Vlad and his criminal buddies won't be implicated because it will all point to the Chinese hackers.

Ghost Rat (or Gh0st RAT) is a Trojan horse that Chinese operatives of GhostNet used to hack into some of the most sensitive computer networks on Earth.[13] It is a cyber spying computer program. The "Rat" part of the name refers to the software's ability to operate as a "Remote Access Tool."

The GhostNet system disseminates malware to selected recipients via computer code attached to stolen emails and addresses, thereby expanding the network by allowing more computers to be infected.[14] According to the Infowar Monitor (IWM), "GhostNet" infection causes computers to download a Trojan known as "Ghost Rat" that allows attackers to gain complete, real-time control.[15] Such a computer can be controlled or inspected by its hackers, and even has the ability to turn on the camera and audio-recording functions of an infected computer that has such capabilities, enabling monitors to see and hear what goes on in a room.

PUBLIC RECORD ON TAP: GhostNet

Chinese hackers 'using ghost network to control embassy computers'

By Mike Harvey, March 30, 2009

A spy network believed to have been controlled from China has hacked into classified documents on government and private computers in 103 countries, according to internet researchers. The spy system, dubbed GhostNet, is alleged to have compromised 1295 machines at Nato and foreign ministries, embassies, banks, and news organizations across the world, as well as computers used by the Dalai Lama and Tibetan exiles.

The work of Information Warfare Monitor (IWM) investigators focused initially on allegations of Chinese cyber-espionage against the Tibetan exile community, but led to a much wider network of compromised machines. The IWM said that while China appeared to be the main source of the network, it had not been able conclusively to identify the hackers. The IWM is composed of researchers from an Ottawa-based think tank, SecDev Group, and the Munk Centre for International Studies at the University of Toronto.

[13]Toronto Star, "Cyberspies' code a click away." Mar 31, 2009; http://www.thestar.com/News/World/Article/610860.

[14]New York Times, "Vast Spy System Loots Computers in 103 Countries." March 28, 2009; http://www.nytimes.com/2009/03/29/technology/29spy.html.

[15]The Times, "Chinese hackers 'using ghost network to control embassy computers.'" March 29, 2009; http://www.timesonline.co.uk/tol/news/uk/crime/article5996253.ece.

They found that the foreign ministries of Iran, Bangladesh, Latvia, Indonesia, the Philippines, Brunei, Barbados, and Bhutan had been spied on remotely; and the embassies of India, South Korea, Indonesia, Romania, Cyprus, Malta, Thailand, Taiwan, Portugal, Germany, and Pakistan hacked.

The operation is thought to be the most extensive yet uncovered in the political world, and is estimated to be invading more than a dozen new computers a week. Other infected computers were found at the accountancy firm Deloitte & Touche in New York.

The IWM report said "GhostNet represents a network of compromised computers in high-value political, economic, and media locations in numerous countries worldwide. These organizations are almost certainly oblivious to the compromised situation in which they find themselves. The computers of diplomats, military attachés, private assistants, secretaries to prime ministers, journalists, and others are under the concealed control of unknown assailant(s)."

"In Dharamsala (the headquarters of the Tibetan government in exile) and elsewhere, we have witnessed machines being profiled and sensitive documents being removed. Almost certainly, documents are being removed without the targets' knowledge, keystrokes are logged, web cameras are being silently triggered, and audio inputs are surreptitiously activated."

Chinese hackers are thought to have targeted Western networks repeatedly. Computers at the Foreign and Commonwealth Office and other Whitehall departments were attacked from China in 2007. In the same year, Jonathan Evans, the MI5 Director General, alerted 300 British businesses that they were under Chinese cyber attack.

British intelligence chiefs have warned recently that China may have gained the capability effectively to shutdown Britain by crippling its telecoms and utilities. Equipment installed by Huawei, the Chinese telecoms giant, in BT's new communications network could be used to halt critical services such as power, food, and water supplies, they said.

The Chinese Embassy in London said that there was no evidence to back up the claim that the Chinese Government was behind GhostNet and alleged that the report had been "commissioned by the Tibetan government in exile."

Liu Weimin, a spokesman, said "I will not be surprised if this report is just another case of their recent media and propaganda campaign. In China, it is against the law to hack into the computers of others, and we are victims of such cyber attack. It is a global challenge that requires global cooperation. China is an active participant in such cooperation in the world."

Once the hackers had infiltrated the systems, they gained control using malware—software installed on the compromised computers—and sent and received data from them, the researchers said. "The GhostNet system directs infected computers to download a Trojan known as Ghost Rat that allows attackers to gain complete, real-time control," IWM said. "These instances of Ghost Rat are consistently controlled from commercial Internet access accounts located on the island of Hainan, in the People's Republic of China."

Hainan is home to the Lingshui SIGINT facility and the Third Technical Department of the People's Liberation Army, IWM said.

Greg Walton, editor of IWM, said "Regardless of who or what is ultimately in control of GhostNet, it is the capabilities of exploitation, and the strategic intelligence that can be harvested from it, which matters most. Indeed, although the Achilles' heel of the GhostNet system allowed us to monitor and document its far-reaching network of infiltration, we can safely hypothesize that it is neither the first nor the only one of its kind."

BREAKING DISK ENCRYPTION

Defeating disk encryption is a lot easier than many security professionals tend to think. A great example of how easy it is to break disk encryption is demonstrated by students from Princeton University and the "Don't Hack Me Please" section below. Cold boot attack is the name of the method used by people who want to get the encryption keys to your computer so they can unlock your encrypted hard drive. Visit http://citp.princeton.edu/memory/ for the video by Princeton University describing and demonstrating how easy it is to bypass disk encryption.

DON'T HACK ME PLEASE: Cold Boot Attack

In cryptography, a cold-boot attack, platform-reset attack, cold-ghosting attack, or ice-man attack is a type of side-channel attack in which an attacker with physical access to a computer is able to retrieve encryption keys from a running operating system after using a cold reboot to restart the machine from a completely "off" state.[16,17] The attack relies on the data remanence property of DRAM and SRAM to retrieve memory contents which remain readable in the seconds to minutes after power has been removed.

To execute the attack, the machine is cold-booted (power is cycled "off" then "on" without letting the computer shut down cleanly); a light weight operating system is then immediately booted (e.g., from a USB flash drive), and the contents of pre-boot memory dumped to a file. Alternatively, the memory modules are removed from the original system and quickly placed in another machine under the attacker's control, which is then booted to access the memory. Further analysis can then be performed against the information that was retrieved from memory to find the sensitive keys contained in it.

The attack has been demonstrated to be effective against full disk encryption schemes of various vendors and operating systems, even where a Trusted Platform Module (TPM)

[16]http://www.secguru.com/files/hitbsecconf2006kl/DAY%202%20-%20Douglas%20MacIver%20-%20Pentesting%20BitLocker.pdf.
[17]http://citp.princeton.edu/memory/.

secure cryptoprocessor is used.[16] This is because the problem is fundamentally a hardware (insecure memory) issue, and not a software issue. While the focus of current research is on disk encryption, any sensitive data held in memory are vulnerable to the attack.[16]

The time window for an attack can be extended to hours by cooling the memory modules. Furthermore, as the bits disappear in memory over time, they can be reconstructed, as they fade away in a predictable manner.[16] In the case of disk encryption applications that can be configured to allow the operating system to boot without a pre-boot PIN being entered or a hardware key being present (e.g., Bitlocker in a simple configuration that uses a TPM without a two-factor authentication PIN or USB key), the time frame for the attack is not limited at all[16]:

"Notably, using BitLocker with a Trusted Platform Module (TPM) sometimes makes it less secure, allowing an attacker to gain access to the data even if the machine is stolen while it is completely powered off…"

PUBLIC RECORD ON TAP: Cold-Boot Attack

Cold-Boot Encryption Attack—code release

By Xeni Jardin, July 19, 2008

Jacob Appelbaum, one of the security researchers who worked on the paper cold-boot attack on encryption keys, tells Boing Boing the code has just been released today at the [last] HOPE hacker con in NYC. It's up, it's signed, and here it is. Memory Research Project Source Code can be found at http://www.citp.princeton.edu/memory/code/. To watch the video, visit http://www.boingboing.net/2008/07/19/cold-boot-encryption.html.

FIGURE 9.11

Cold-boot encryption attack video

VIRTUALIZATION EXPLOITS

As discussed in Chapter 8 (Software, Hardware, and Wetware), here we will talk about exploiting VMware, also known as Cloudburst. Recently Immunity researcher Kostya Kortchinsky has exploited a serious vulnerability in VMware's hypervisor that allows Guest to Host escaping. Kostya explained the vulnerability primitives, how to combine these primitives into a reliable exploit that bypasses EP/ASLR, how to make that exploit reliable across Linux, Windows XP, and Windows Vista, and how to obtain post-exploitation control of the host without any network access.[18] See Figures 9.12–9.16 for a screen shot of the exploit being demonstrated by Kostya Kortchinsky.

PUBLIC RECORD ON TAP: Virtual Machine Exploit

Virtual-machine exploit lets attackers take over host

By Matthew Broersma, June 10, 2009 from ZDNet UK

Penetration-testing company Immunity has exploited a flaw in VMware software that allows malicious code running in a virtual machine to take over the host operating system. Immunity included the attack code in an update to its commercial penetration-testing tool, Canvas 6.47, released last week. The attack code is in a module of the tool called Cloudburst.

Cloudburst uses a vulnerability in the virtual-machine display functions of VMware Workstation that can be exploited by a specially crafted video file. The malicious file, when executed within a virtual machine, could allow an intruder to take over the host operating system, according to security researchers.

The bug itself affects VMware Workstation 6.5.1 and earlier, or the associated Player versions. The software can be running on any host system, including Linux, according to VMware. However, the Cloudburst exploit currently has certain limitations: it will only succeed on Workstation 6.5.0 or 6.5.1 or the associated Player versions. In addition, the guest and host must be Windows-based, among other requirements, Immunity said in its release notes.

The bug, which has been assigned the Common Vulnerabilities and Exploits (CVE) reference CVE-2009-1244, was disclosed in January, and VMware issued a patch in April. However, system administrators do not always keep their systems up to date with patches, Immunity said.

The bug is dangerous partly because it works with default VMware settings, according to security researchers. Secunia, a third-party security firm, gave the flaw a "highly critical" rating. The flaw was discovered by Immunity researcher Kostya Kortchinsky, and Immunity published a video demonstrating its attack in April. "The exploit is amazing," Immunity chief executive Dave Aitel said in a newslist post announcing the exploit video. To read more and view the video, visit http://www.zdnetasia.com/news/security/0,39044215,62054876,00.htm.

[18] http://www.syscan.org/Sg/program.html.

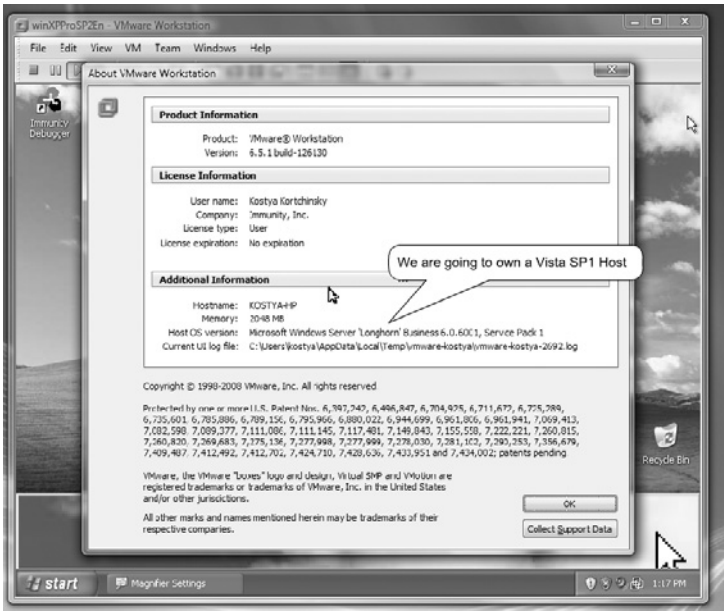


FIGURE 9.12

We are going to own a Vista SP1 host.

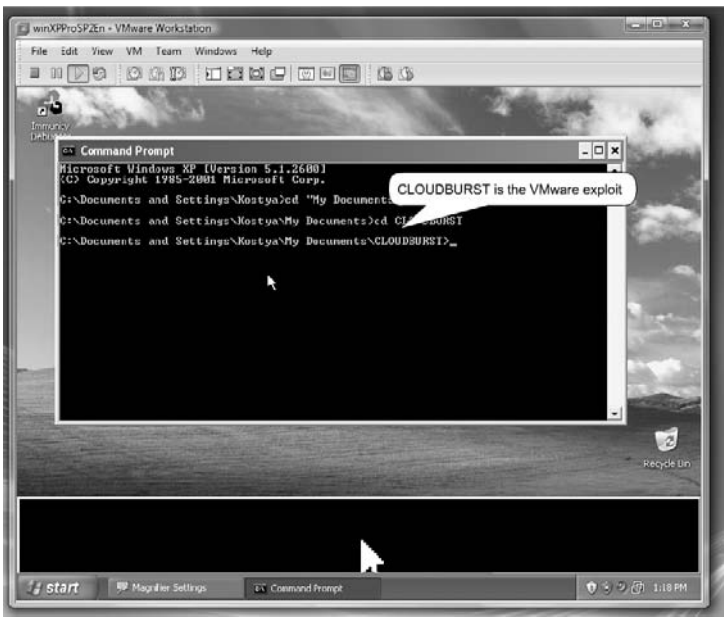


FIGURE 9.13

Cloudburst is the VMware exploit

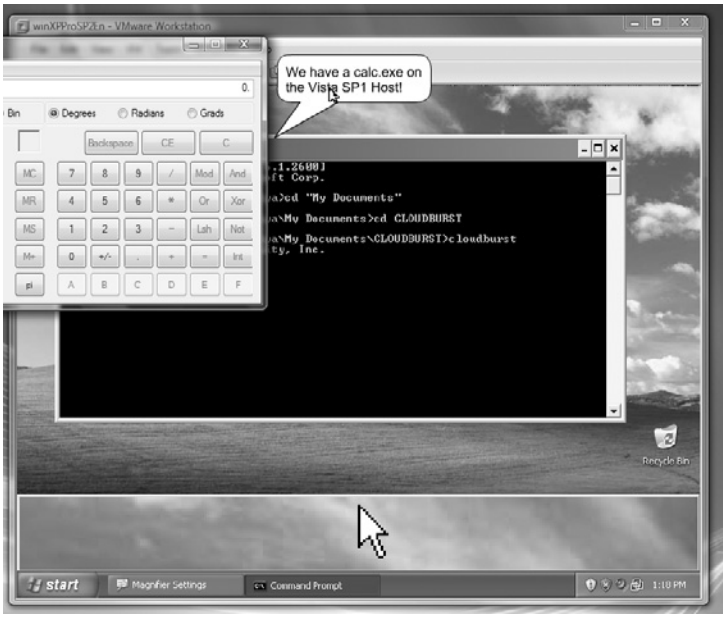


FIGURE 9.14

We have a calc.exe on the Vista SP1 host.

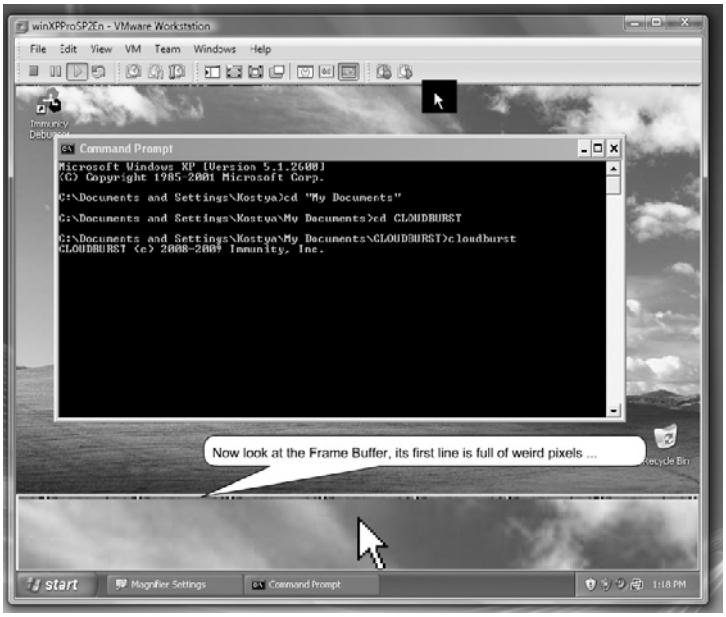


FIGURE 9.15

Frame buffer full of weird pixels (data leakage).

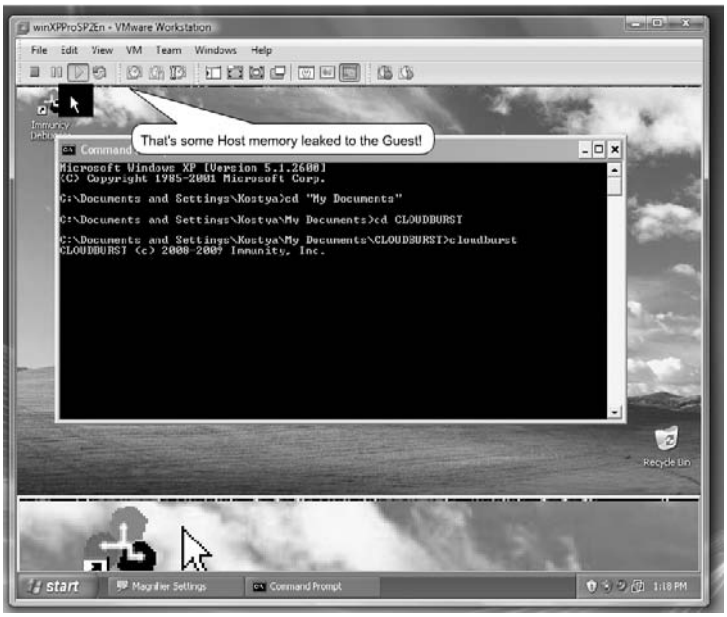


FIGURE 9.16

Host memory leaked to the Guest virtual machine.

PUBLIC RECORD ON TAP: Cloudburst

Cloudburst: A Weaponised Attack on the Cloud

By Ben Chai, June 5, 2009 from SecurityVibes.com

Back in April, Security Vibes published a members' report on the potential risks to the security of the cloud from the virtualised machines that make up the cloud. One risk mentioned was Virtual Machine Escape, where a guest virtual machine (VM) could infiltrate and hack its host system.

Now a commercial tool has been released by the Miami-based penetration testing company Immunity, who specialise in products that include exploitation development tools, vulnerability assessment tools, and remote control technologies.

The tool called Cloudburst is from Immunity's CANVAS penetration testing framework and exploits a vulnerability within VMWare which enables infiltration of the host operating system. A description from their Web site states,

"For those of you who are unaware, CLOUDBURST exploits a vulnerability in VMware Display functions in order to execute code from within a Guest VM into the controlling Host. Once exploited, the exploit tunnels a MOSDEF connection over the Frame Buffer of the Guest to communicate with the Host."

VMWare version 6.5.0 and 6.5.1 are affected, as well as all host operating systems, including Linux. The good news is that there is a patch whose problem description begins.

Host code execution vulnerability from a guest operating system

A critical vulnerability in the virtual machine display function might allow a guest operating system to run code on the host.

The risk here is that in a Cloud environment, a virtual machine can run a program that escapes into the Host O/S and be used on other virtual machines belonging to other companies. These compromisation attacks could be identity or intellectual property theft, confidentiality, or simply hide a Trojan for delayed attack on other systems.

If you have applications currently within the Cloud, hopefully your Cloud vendor has remembered to patch their system before cybercrime either purchases Cloudburst or figures out how to do something similar! To read more, visit http://www.securityvibes.com/cloudburst-a-weaponsied-attack-on-the-cloud-benchai7-news-3003225.html.

DON'T HACK ME PLEASE: Weaponizing the Web at DEFCON 17

Weaponizing the Web: New Attacks on User-generated Content

By Shawn Moyer and Nathan Hamiel

Ultimately, basing the value proposition of your site on user-generated and external content is a kind of variant on Russian Roulette, where in every turn the gun is pointed at your head, regardless of the number of players. You may win most of the time, but eventually a bullet is going to find its way into the chamber with your name on it.

We spent some time last year looking at this problem as it related specifically to Social Networks, but that left a lot of the territory unexplored. This time around we'll be talking about a previously unnoticed attack vector for lots and lots of web applications with user-generated content, and releasing a handy tool to exploit it. Bundled in are some thoughts on Web 2.0 attack surface, a few new exploitation techniques, and as in last year, a hefty helping of lulz, ridicule, and demos-of-shame at the expense of a few of your and (our) favorite sites.

Dr. Shawn Moyer's best work remains, by definition, undocumented. Some claim he is one of the unseen architects of both Iraq Wars, while others pay no credence to this rumor, based on reports that he has been heading a covert Psychological Warfare operation in Cyprus at the behest of the Greek government for much of the past 15 years.

His involvement in the poisoning of Victor Yushenko is largely conjecture, but records do show that he was at the same restaurant on the night in question and sent his Borscht

back, untouched. He unquestionably is the owner of a Spetznaz-issue Vostok watch, and a handlebar mustache that fits several witness descriptions.

Still, the larger questions remain... Why did Dr. Moyer abruptly change his travel plans for Flight 93? Why was he spotted near the Book Depository, carrying what appeared to be a box of 6.5-mm shells? Why is his testimony conspicuously absent from all records of the Warren Commission? And most of all, why is he currently listed as a Principal Security Consultant with FishNet Security's Assessment Practice?

"Nathan Hamiel" (not his real name) dropped out of high school to work as a deckhand on an oil tanker in the Sargasso Sea. On its maiden voyage, the tanker "The Lady Nikita" was caught in a freak So'Wester that swamped its engines and damaged the electrical systems. Hopelessly lost and without radio or navigation, the crew ran aground somewhere near the coast of French Guyana.

Relying on natural language and negotiation skills, "Nathan" bartered several of his crew members into white slavery for safe passage overland to Caracas. Once there, he found work as a night janitor in the Miraflores palace during the Perez regime. When the junta came, he was forced to flee by night as a suspected American spy.

From there, "Nathan" fled overland through Panama, where he secured passage to Florida on a forged diplomatic passport. He still resides there today, posing as a Senior Consultant of impeccable credentials with Idea Information Security. To read more visit http://www.defcon.org/html/defcon-17/dc-17-speakers.html#Moyer.

DON'T HACK ME PLEASE: Taking Over Voice Over IP (VOIP) Conversations at DEFCON 17

The Middler 2.0: It's Not Just for Web Apps Anymore

By Jay Beale Co-Founder, InGuardians, Inc.; and Justin Searle, Sr. Security Analyst, InGuardians

The Middler is a next-generation man-in-the-middle tool that takes the focus beyond the raw mechanics of the protocol on to the application itself. New for DEFCON, it now can man-in-the-middle Voice over IP (VoIP), producing the opportunity to interactively redirect calls, join them, or take them over. All of these effects join The Middler's goal of putting the victim into a kind of matrix by implementing man-in-the-middle attacks specific to each Web application. We've also added a graphical interface, allowing for interactive target selection based on information that The Middler gathers about potential victims. We've added more applications and enhanced the set of nonapplication-specific capabilities, including easy session cloning, IFRAME injection, and a Java script exploit library that can

force the user into the Browser Exploitation Framework (BeEF) or a Metasploit exploit. This demo-filled talk will enhance your man-in-the-middle powers just in time for one of the most hostile networks ever seen.

Jay Beale has created a number of security tools, including Bastille Unix and the CIS Unix Scoring Tool, both of which are widely used throughout industry and government. He has served as an invited speaker at many industry and government conferences, a columnist for Information Security Magazine, Security Portal and SecurityFocus, and a contributor to nine books, including those in his Open Source Security Series and the "Stealing the Network" series. Jay works as a security analyst at InGuardians. Justin Searle Bio to come. To read more, visit http://www.defcon.org/html/defcon-17/dc-17-speakers.html#Beale.

DON'T HACK ME PLEASE: The Blue Pill

Vista hacked at Black Hat

By Joris Evers from CNET News, August 4, 2006

Joanna Rutkowska, a Polish researcher at Singapore-based Coseinc, showed that it is possible to bypass security measures in Vista that should prevent unsigned code from running.

And in a second part of her talk, Rutkowska explained how it is possible to use virtualization technology to make malicious code undetectable, in the same way a rootkit does. She code-named this malicious software Blue Pill.

"Microsoft is investigating solutions for the final release of Windows Vista to help protect against the attacks demonstrated," a representative for the software maker said. "In addition, we are working with our hardware partners to investigate ways to help prevent the virtualization attack used by the Blue Pill."

At Black Hat, Microsoft gave out copies of an early Vista release for attendees to test. The software maker is still soliciting feedback on the successor to Windows XP, which is slated to be broadly available in January.

Rutkowska's presentation filled a large ballroom at Caesars Palace to capacity, even though it was during the last time slot on the final day of the annual Black Hat security confab here. She used an early test version of Vista for her research work.

As one of the security measures in Vista, Microsoft is adding a mechanism to block unsigned driver software to run on the 64-bit version of the operating system. However, Rutkowska found a way to bypass the shield and get her code to run. Malicious drivers could pose a serious threat because they run at a low level in the operating system, security experts have said.

"The fact that this mechanism was bypassed does not mean that Vista is completely insecure. It's just not as secure as advertised," Rutkowska said. "It's very difficult to implement a 100 percent efficient kernel protection."

To stage the attack, however, Vista needs to be running in administrator mode, Rutkowska acknowledged. That means her attack would be foiled by Microsoft's User Account Control, a Vista feature that runs a PC with fewer user privileges. UAC is a key Microsoft effort to prevent malicious code from being able to do as much damage as on a PC running in administrator mode, a typical setting on Windows XP.

"I just hit accept," Rutkowska replied to a question from the audience about how she bypassed UAC. Because of the many security pop-ups in Windows, many users will do the same without realizing what they are allowing, she said.

Microsoft has touted Vista as its most secure version of Windows yet. It is the first operating system client to go through the company's Security Development Lifecycle, a process to vet code and stamp out flaws before a product ships.

"Windows Vista has many layers of defense, including the firewall, running as a standard user, Internet Explorer Protected Mode, /NX support, and ASLR, which help prevent arbitrary code from running with administrative privileges," the Microsoft representative noted.

After the presentation on bypassing the driver shield, Rutkowska presented a way to create the stealthy malicious software she code-named Blue Pill. The technique uses Pacifica, a Secure Virtual Machine, from chipmaker Advanced Micro Devices, to go undetected.

Blue Pill could serve as a backdoor for attackers, Rutkowska said. While it was developed on Vista and AMD's technology, it should also work on other operating systems and hardware platforms. "Some people suggested that my work is sponsored by Intel, as I focused on AMD virtualization technology only," she said, adding that is untrue. To read more, visit http://news.cnet.com/2100-7349_3-6102458.html.

DON'T HACK ME PLEASE: Ph-neutral Talks

Voice security and privacy: confidentiality protection, today solutions, and upcoming technologies and standards

By Naif

The changes of telecommunication markets, from telco monopolist of the 80's to multiple operators working across different countries, along with the diffusion of new technologies like VoIP, completely changed the rules and the needs of law enforcement that are required to intercept communications, and of private citizens that want to protect their privacy. An overview analysis of voice protection and voice interception technologies available now

and in the near future, used and usable by private and by governments will be shown. Technical, political, and jurisdictional issues about interception and protection systems will be presented. Zphone, VPN, voice security standards, passive interception technologies, tactical interception technologies, satellite-related issue, ETSI lawful interception rules, national European and North American laws, the Chinese threat are part of the information that will be presented. A new "open standard" secure telephony protocol, based on ZRTP and developed jointly with Philip Zimmermann, will be introduced and presented compared to other available technologies. To read more, visit http://ph-neutral.darklab.org/talks.html.

Sniff Keystrokes With Lasers/Voltmeters—Side Channel Attacks Using Optical Sampling Of Mechanical Energy And Power Line Leakage

By Andrea Barisani and Daniele Bianco

TEMPEST attacks, exploiting Electro Magnetic emissions in order to gather data, are often mentioned by the security community, movies, and wanna-be spies (or NSA employees we guess...). While some expensive attacks, especially the ones against CRT/LCD monitors, have been fully researched and described, some others remain relatively unknown and haven't been fully (publicly) researched. Following the overwhelming success of the SatNav Traffic Channel hijacking talk, we continue with the tradition of presenting cool and cheap hardware hacking projects. We will explore two unconventional approaches for remotely sniffing keystrokes on laptops and desktop computers using mechanical energy emissions and power line leakage. The only thing you need for successful attacks are either the electrical grid or a distant line of sight; no expensive piece of equipment is required. We will show in detail the two attacks and all the necessary instructions for setting up the equipment. As usual, cool gear and videos are going to be featured in order to maximize the presentation. To read more, visit http://ph-neutral.darklab.org/talks/andrea.html.

SyferLock's bleeding edge technology has changed how people use and will eventually exploit traditional passwords. To view their Web site, see Figure 9.17. No longer is a simple password going to be easily brute-forced or guessed; in fact, no longer will a hidden keylogger program on a corporate laptop put your organization at risk. Figure 9.18 is a picture of what a basic username and password look like today. Using SyferLock's patented enhanced authentication technology this password, Grid1 is no longer unsecure by being input and transmitted as a static password because by choosing a corner (or position), as depicted in Figure 9.19, your password is now mapped to a possibility of four (or eight or more) other numbers per character. At login, a user simply refers to the security grid user interface, as seen in Figure 9.20. Looking at the keys or characters corresponding to their password *and* the selected target corner, the user will enter the number of the target corner or position as their GridCode, which is displayed in Figure 9.20. Upon every refresh and/or new login, the

corner numbers randomly change, creating a new one-time password. SyferLock's methodology and/or the use of additional security functions (DecoyDigits™, Add-on Security Modifier, etc.) make it nearly impossible for a malicious attacker to easily capture their password and reuse it. To learn more, visit http://www.syferlock.com/.

FIGURE 9.17

SyferLock's Web site

FIGURE 9.18

Basic [always constant] username and password

FIGURE 9.19

Choosing a corner to substitute log-in

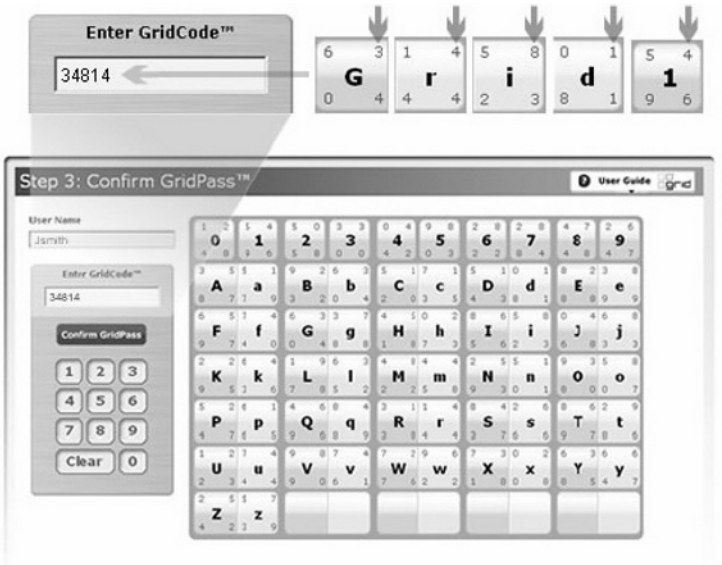


FIGURE 9.20

Grid1 becomes a one-time password.

PUBLIC RECORD ON TAP: Changing How Humans Use Passwords

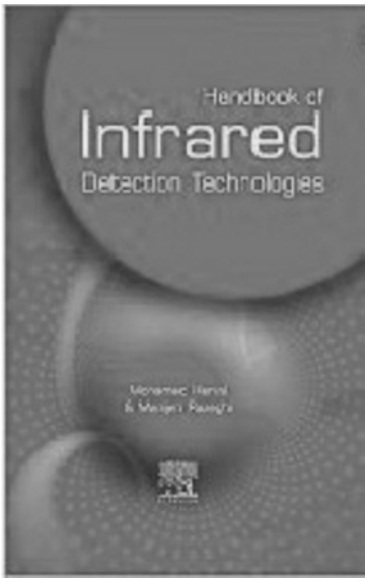
SyferLock Almost Solves the Password Security Problem

By Krishnan Subramanian, June 3, 2009 from CloudAve

Few months back, I was worrying about the readiness of SaaS [Software as a Service] vendors to protect users from password related attacks, either through phishing or key logging or any of the many different ways in which users' passwords can be snatched. When thinking about how we use SaaS, I am worried about the risks associated with the password reuse by most of the users. This is a major concern as we move into a SaaS based world. Sooner than later, we are going to see multiple schemes to grab the passwords of SaaS applications causing havoc on a scale that we haven't yet seen in this web era. With more and more adoption of SaaS in the SME [Small and Medium Enterprises] sector and, even, bigger enterprise players, the attempts to snatch the passwords are only going to increase big time. In my previous avatar as a System Admin, I have seen how users greatly help the attackers by keeping a very simple, easy-to-guess passwords and, also, how they keep the same password on all the services starting from email to even bank accounts. In my earlier post mentioned above, I was talking about a security vendor who might have a right solution for such problems. The only way to completely solve the password security problem is by not allowing system access to anyone, including the admin. However, such a system is completely meaningless and, as an alternative, we can only try to minimize the impact of

such attacks on the users' passwords. SyferLock is one such vendor using an innovative way to reduce the impact of attacks on passwords drastically. To read more, visit http://www.cloudave.com/link/syferlock-almost-solves-the-password-security-problem.

BOOKS



Handbook of Infrared Technologies

By M. Henini and M. Razeghi

Publisher: Elsevier Science

ISBN-10: 1856173887

ISBN-13: 978-1856173889

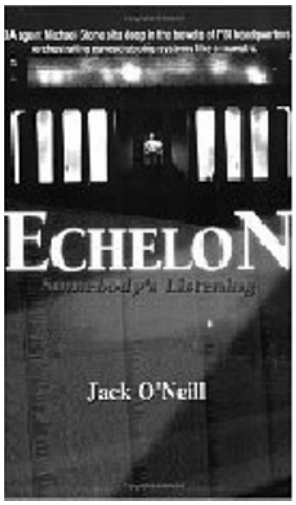
Advances in Cryptology

By Moni Naor

Publisher: Springer

ISBN-10: 3540725393

ISBN-13: 978-3540725398



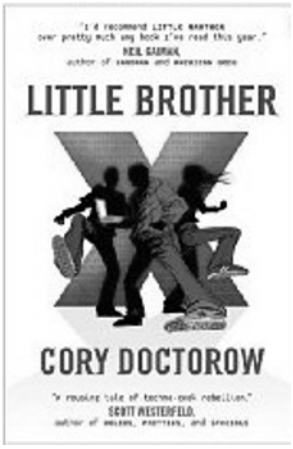
ECHELON: Somebody's Listening

By Jack O'Neill

Publisher: Word Association

ISBN-10: 159571071X

ISBN-13: 978-1595710710



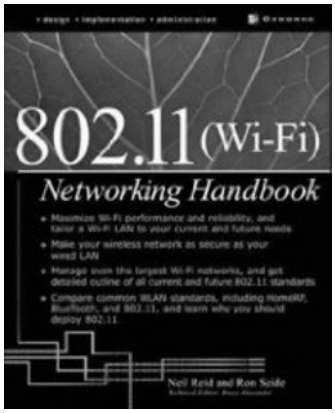
Little Brother

By Cory Doctorow

Publisher: Tor Teen

ISBN-10: 0765319853

ISBN-13: 978-0765319852



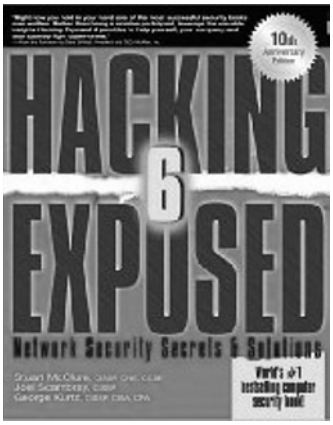
(802.11) Wi-Fi Network Handbook

By Neil P. Reid and Ron Seide

Publisher: McGraw-Hill Osborne Media

ISBN-10: 0072226234

ISBN-13: 978-0072226232



Hacking Exposed 6: Network Security Secrets and Solutions, Sixth Edition (Paperback)

By Stuart McClure, Joel Scambray, and George Kurtz

Publisher: McGraw-Hill Osborne Media

ISBN-10: 0071613749

ISBN-13: 978-0071613743

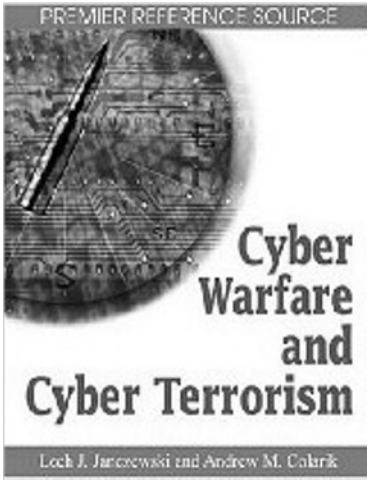
Technological Empowerment: The Internet, State, and Society in China (Hardcover)

By Yongnian Zheng

Publisher: Stanford University Press (November 8, 2007)

ISBN-10: 0804757372

ISBN-13: 978-0804757379



Cyber Warfare and Cyber Terrorism

By Lech J. Janczewski and Andrew M. Colarik

Publisher: IGI Global

ISBN-10: 1591409918

ISBN-13: 978-1591409915

This page intentionally left blank

CHAPTER

Hacker Culture 10

The hacker culture is a very dynamic and fast-paced environment. At any given moment, there are people around the world attending security conferences, discussing the latest vulnerabilities in operating systems, and even going to meetups like the Linux Users Groups that have been created in most cities in America. In this chapter, we focus on the hacker culture by describing some of the fictional stories, hacker culture references, common meeting places, conferences, blogs, and books that hackers are actively involved in or have contributed to. In each section, we discuss why it is important to stay connected with the hacker culture through conference attendance, subscribing to blogs, and reading the latest hacker books.

So what is a hacker? To answer this, we will turn to Steven Levy, an American journalist who has published several articles and books for leading media outlets like *The New York Times Magazine* and *Rolling Stone*, to name a few. Levy is known for a lot of his works, but first and foremost his publication in 1984 that changed the way people thought about the hackers and the hacker culture. *Hackers: Heroes of the Computer Revolution* was the first of its kind. In that work Levy describes hackers as, "adventurers, visionaries, risk-takers, [and] artists." Levy also included the hacker ethic what became very popular with the American readers in 1984. Levy's hacker ethic dictates:

FOR PUBLIC RELEASE: Levy's Hackers' Ethic

1. Access to computers—and anything which might teach you something about the way the world works—should be unlimited and total. Always yield to the Hands-on Imperative!
2. All information should be free.
3. Mistrust authority—promote decentralization.
4. Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position.
5. You can create art and beauty on a computer.
6. Computers can change your life for the better.

The code, as Levy refers to the hacker ethic, is "a philosophy, an ethic, and a dream," which was declared by the six basic ideas stated above. True hackers (nonmalicious) are performing a service for the common good of humanity, almost like Robin Hood did for the overtaxed township of Nottingham. These ideas still exist today and were founded in the 1940s. The hacking culture has evolved since the 1940s, when the United States broke the German Enigma code in secret with some of the most talented hackers working in secret labs across America. As the U.S. military secretly funds and develops what is now known as the Internet (ARPAnet), hackers were also working in secret labs designing secure systems to ensure America was safe during a nuclear attack.

As the old-school hackers of the 1940 and 1950 worked in secret, a new era of hackers was emerging, as the 1960s is kicked started with the beginning of the Vietnam War. During this time, there were many research universities that contributed to major technological advances funded by and in support of government projects, with a focus on military application. Soon all the old-school hackers moved to California to begin what is now known as Silicon Valley, the big corporations that now drive more of today's technological advances.

In the 1970s, the PC became a reality through Steve Jobs and Steven Wozniak. During this time, the first of its kind appeared on the national scene: the phone phreakers. John Draper, a.k.a Captain Crunch, used a plastic whistle that came from a 1970s, still popular, Captain Crunch cereal box. When blown, the whistle made a perfect 2600-Hz tone which allowed him to make free long-distance phone calls on the public-switched telephone network. Soon after Draper's discovery, a new device was created called a "blue box" that worked to emit the 2600-Hz tone. Draper, Jobs, and Wozniak built their own blue boxes and sold them to students at Berkeley. This was a new era for the hacking culture. Remember hacker ethic number 2? All information should be free. Well, soon this would no longer be true, as Bill Gates and Paul Allen wrote the first computer language for a computer mainframe based on public source code from the Dartmouth researchers Thomas Kurtz and John Kemeny. Soon after, many hackers would begin the long journey into corporate America and create many organizations we now know as Microsoft Corporate and Apple Incorporated.

FICTIONAL STORY DISSECTED: Spot the Fed

> "It looks like word got out since our last meeting. I don't recognize quite a few faces. If anyone here spots a Fed in the group, speak up" (p. 31).

"Spot the Fed" is a contest that is played at DEFCON, a cyber security conference. Here is a snapshot of how it works. "Like a paranoid version of "pin the tail on the donkey", the favorite sport at this gathering of computer hackers and phone

phreaks seems to be hunting down real and imagined telephone security and federal and local law enforcement authorities who, the attendees are certain, are tracking their every move... Of course, they may be right," said John Markoff from the New York Times.[1] From DEFCON 13—"Basically, the contest goes like this: If you see some shady MIB (Men in Black) earphone-, penny loafer, sunglass-wearing Clint Eastwood, to live and die in LA, type lurking about, point him out. Just get my attention and claim out loud you think you have spotted a Fed. The people around at the time will then (I bet) start to discuss the possibility of whether or not a real Fed has been spotted. Once enough people have decided that a Fed has been spotted, and the Identified Fed (I.F.) has had a say, and informal vote takes place; and if enough people think it's a true Fed, or Fed wanna-be, or other nefarious-style character, you win a "I spotted the Fed!" shirt, and the I.F. gets an "I am the Fed!" shirt."

For more information, visit https://forum.defcon.org/forumdisplay.php?f=439

FICTIONAL STORY DISSECTED: London NASA Hacker

> "I want to try a hack on Groom Lake. Remember when Gary McKinnon was busted for breaking into U.S. government computers from London?" (p. 29).

A Briton accused of hacking into NASA and U.S. military computer networks. See Chapter 11, "Easter Eggs," for more information on Gary McKinnon.

FICTIONAL STORY DISSECTED: 2600

> Soon they were inside and making their way down to the food court. As they approached Ninfa Express, they could see that the usual crowd was supplemented with extra people this time. This was the monthly 2600 Club meeting. Leon and Bob were regular attendees. Today they were leading the prep for the first Capture the Flag war drive put on by the Houston chapter (p. 30).

Beginning in late 1980s, 2600 has been publishing periodicals focusing on the hacker ethic of "information wants to be free." Some call the information they publish forbidden knowledge because it describes how things work and function, that you would normally not find in a local bookstore. Emmanuel Goldstein is the editor of 2600 and has been an activist for hackers around the world.

[1]DEFCON 13, http://www.defcon.org/html/defcon-13/dc13-spotthefed.html

The magazine's name comes from the phreaker discovery in the 1960s that the transmission of a 2600-hertz tone (which could be produced perfectly with a plastic toy whistle given away free with Cap'n Crunch cereal—discovered by friends of John Draper) over a long-distance trunk connection gained access to "operator mode" and allowed the user to explore aspects of the telephone system that were not otherwise accessible. Mr Corley chose the name because he considered it a "mystical thing," commemorating something that he evidently admired.

2600: The Hacker Quarterly is a quarterly American publication that specializes in publishing technical information on a variety of subjects—including telephone switching systems, Internet protocols and services, as well as general news concerning the computer "underground" and left wing, and sometimes (but not recently), anarchist issues. 2600 has established the Hackers On Planet Earth (HOPE) conferences as well as monthly meetings in Argentina, Australia, Austria, Brazil, Canada, Denmark, England, Finland, France, Greece, Ireland, Italy, Japan, Mexico, New Zealand, Norway, Poland, Puerto Rico, Russia, Scotland, South Africa, Sweden, Switzerland, and the United States. The meetings generally take place on the first Friday of the month at 5:00 P.M. local time, with various exceptions. 2600 meetings provide a forum to teach, learn, and discuss events in technology land. Meetings are open to anyone, regardless of age or level of expertise. For more information, visit http://www.2600.com/ and http://2600.wrepp.com/index.php for the complete archive of past 2600 articles.

FICTIONAL STORY DISSECTED: Capture the Flag

> "Hey everybody! Looks like we've got a pretty good crew. Today we're going to set the rules for Capture the Flag," Bob started. Slowly the talking stopped and everyone looked up from many different sticker-covered laptops to watch Bob (p. 31).

Here, Bob and Leon are setting up a game commonly referred to as "Capture the Flag (CTF)," using a small icon file, which is simply a very small picture. CTF is a traditional outdoor sport often played by children or sometimes adults, where two teams each have a flag (or other marker); and the objective is to capture the other team's flag, located at the team's "base," and bring it safely back to their own base. Enemy players can be "tagged" by players in their home territory; these players are then, depending on the agreed rules, out of the game, members of the opposite team, or "in jail." (One variation of the game includes a "jail" area in addition to the flag on each team's territory.)

FICTIONAL STORY DISSECTED: Gary McKinnon

> "I want to try a hack on Groom Lake. Remember when Gary McKinnon was busted for breaking into U.S. government computers from London?" (p. 29).

Gary McKinnon (Figure 10.1), also known as SOLO (born February 10, 1966), is a Scottish hacker facing extradition to the United States to face charges of perpetrating what has been described by one prosecutor as the "biggest military computer hack of all time."[2] Following legal hearings in the United Kingdom, it was decided in July 2006 that he should be extradited to the United States. In February 2007, his lawyers argued against the ruling in an appeal to the High Court in London,[3] which was turned down on April 3.[4]

FIGURE 10.1
Gary McKinnon

On July 30, 2007, the House of Lords agreed to hear the appeal;[5] and on June 17, 2008, the Law Lords began hearing the case.[6] This judgment was delivered on July 30, 2008, with the Law Lords judging that Gary McKinnon could be extradited to the United States.[7] He was given 2 weeks to appeal to the European Court of Human Rights before extradition, but the Court halted the extradition for an additional 2 weeks to allow time to hear his appeal on August 28, which was subsequently rejected.[7] His legal team subsequently decided to lodge another appeal, which was granted, based on the fact that McKinnon has recently been diagnosed with Asperger

[2]Boyd, Clark (July 30, 2008). "Profile: Gary McKinnon." BBC News. http://news.bbc.co.uk/2/hi/technology/4715612.stm. Retrieved on November 15, 2008.

[3]"British hacker fights extradition." BBC News. February 14, 2007. http://news.bbc.co.uk/1/hi/scotland/glasgow_and_west/6360917.stm. Retrieved on November 15, 2008.

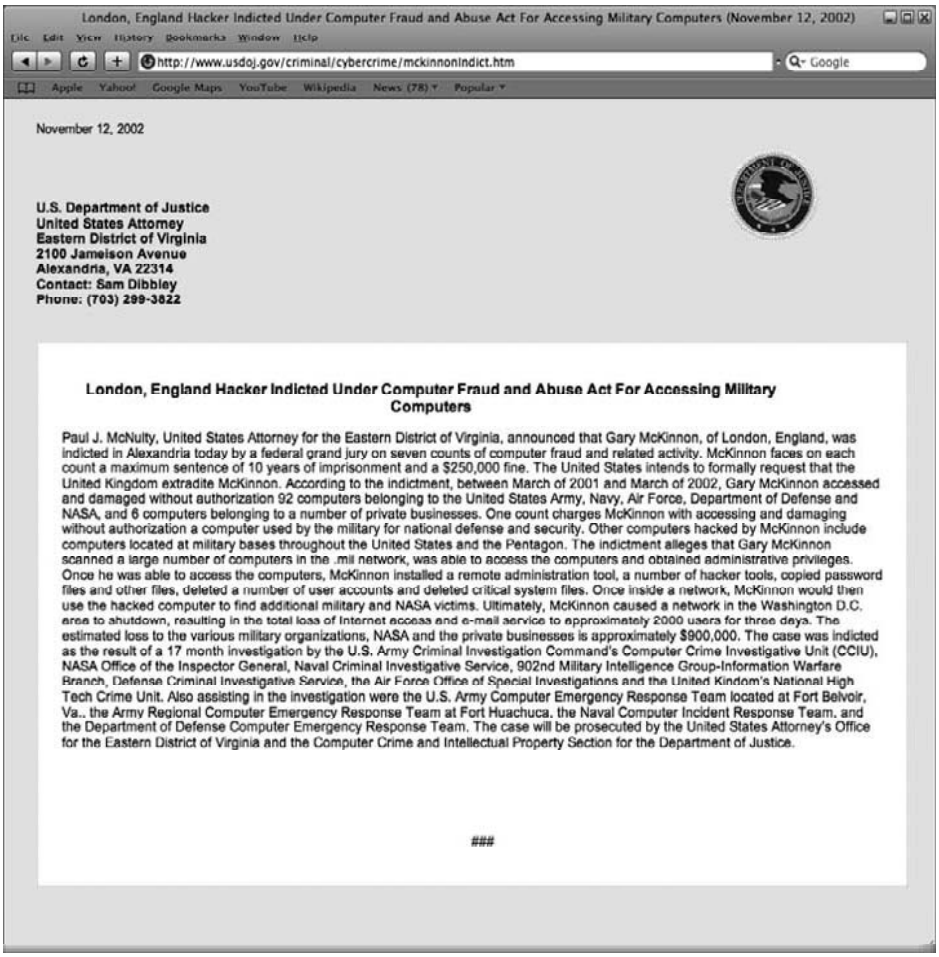
[4]"UK hacker loses extradition fight." BBC News. April 3, 2007. http://news.bbc.co.uk/1/hi/uk/6521255.stm. Retrieved on November 15, 2008.

[5]Campbell, Duncan (July 31, 2007). "Lords to hear 'hacker' appeal." The Guardian. http://www.guardian.co.uk/uk_news/story/0,,2138351,00.html. Retrieved on November 15, 2008.

[6]"Law Lords consider UK hacker case." BBC News. June 17, 2008. http://news.bbc.co.uk/1/hi/uk/7456216.stm. Retrieved on November 15, 2008. "Hacker Indicted Under Computer Fraud and Abuse Act For Accessing Military Computers." U.S. Department of Justice. November 12, 2002. http://www.usdoj.gov/criminal/cybercrime/mckinnonIndict.htm. Retrieved on November 15, 2008.

[7]"European Court of Human Rights refuses request for interim measures by Gary McKinnon." European Court of Human Rights. August 28, 2008. http://cmiskp.echr.coe.int/tkp197/view.asp?action=html&documentId=839381&portal=hbkm&source=externalbydocnumber&table=F69A27FD8FB86142BF01C1166DEA398649. Retrieved on September 1, 2008. "Hacker loses extradition appeal." BBC News. August 28, 2008. http://news.bbc.co.uk/1/hi/uk/7585861.stm. Retrieved on November 15, 2008.

syndrome.[8] His diagnosis was made in August 2008 by the eminent psychologist Prof. Simon Baron-Cohen,[9] and has attracted criticism.[10] Figure 10.2 is a U.S. Department of Justice report on Gary McKinnon.


London, England Hacker Indicted Under Computer Fraud and Abuse Act For Accessing Military Computers (November 12, 2002)

File Edit View History Bookmarks Window Help

http://www.usdoj.gov/criminal/cybercrime/mckinnonIndict.htm

Apple Yahoo! Google Maps YouTube Wikipedia News (78) Popular

November 12, 2002

U.S. Department of Justice
United States Attorney
Eastern District of Virginia
2100 Jamieson Avenue
Alexandria, VA 22314
Contact: Sam Dibbley
Phone: (703) 299-3822

London, England Hacker Indicted Under Computer Fraud and Abuse Act For Accessing Military Computers

Paul J. McNulty, United States Attorney for the Eastern District of Virginia, announced that Gary McKinnon, of London, England, was indicted in Alexandria today by a federal grand jury on seven counts of computer fraud and related activity. McKinnon faces on each count a maximum sentence of 10 years of imprisonment and a $250,000 fine. The United States intends to formally request that the United Kingdom extradite McKinnon. According to the indictment, between March of 2001 and March of 2002, Gary McKinnon accessed and damaged without authorization 92 computers belonging to the United States Army, Navy, Air Force, Department of Defense and NASA, and 6 computers belonging to a number of private businesses. One count charges McKinnon with accessing and damaging without authorization a computer used by the military for national defense and security. Other computers hacked by McKinnon include computers located at military bases throughout the United States and the Pentagon. The indictment alleges that Gary McKinnon scanned a large number of computers in the .mil network, was able to access the computers and obtained administrative privileges. Once he was able to access the computers, McKinnon installed a remote administration tool, a number of hacker tools, copied password files and other files, deleted a number of user accounts and deleted critical system files. Once inside a network, McKinnon would then use the hacked computer to find additional military and NASA victims. Ultimately, McKinnon caused a network in the Washington D.C. area to shutdown, resulting in the total loss of Internet access and e-mail service to approximately 2000 users for three days. The estimated loss to the various military organizations, NASA and the private businesses is approximately $900,000. The case was indicted as the result of a 17 month investigation by the U.S. Army Criminal Investigation Command's Computer Crime Investigative Unit (CCIU), NASA Office of the Inspector General, Naval Criminal Investigative Service, 902nd Military Intelligence Group-Information Warfare Branch, Defense Criminal Investigative Service, the Air Force Office of Special Investigations and the United Kingdom's National High Tech Crime Unit. Also assisting in the investigation were the U.S. Army Computer Emergency Response Team located at Fort Belvoir, Va., the Army Regional Computer Emergency Response Team at Fort Huachuca, the Naval Computer Incident Response Team, and the Department of Defense Computer Emergency Response Team. The case will be prosecuted by the United States Attorney's Office for the Eastern District of Virginia and the Computer Crime and Intellectual Property Section for the Department of Justice.

###

FIGURE 10.2

U.S. Department of Justice Report

[8]Campbell, Duncan (August 29, 2008). "British computer hacker faces extradition to US after court appeal fails." The Guardian. http://www.guardian.co.uk/technology/2008/aug/29/hacking.law. "Hacker appeals to home secretary." BBC News. September 1, 2008. http://news.bbc.co.uk/1/hi/uk/7592884.stm. Retrieved on November 15, 2008.

[9]Hacker wins court review decision." BBC News. January 23, 2009. http://news.bbc.co.uk/1/hi/uk/7846442.stm. Retrieved on January 23, 2009.

[10]Crawford, Ted. "McKinnon to use Asperger's defense? Critics polarized over diagnosis." Daily Mail. September 3, 2008.

PUBLIC RECORD ON TAP: Gary McKinnon

In March 2002, Gary McKinnon was arrested for accessing U.S. military networks simply by using a Perl script that searched for blank passwords; in other words, his report suggests that there were computers on these networks with the default passwords active. McKinnon's initial interest in searching through networks for blank passwords was to find information on UFOs. Donna Hare was a researcher for NASA that McKinnon was interested in because she testified that she had seen photos of UFOs. For more information on Gary McKinnon, check out the URLs below:

Protests chant outside Britain's Home Office in support of Gary McKinnon. (Credit: Tom Espiner/ZDNet UK).

http://freegary.org.uk/
http://www.londontv.net/latestnews.htm
http://news.bbc.co.uk/1/hi/technology/4715612.stm
http://www.politics.co.uk/news/legal-and-constitutional/british-hacker-loses-extradition-appeal-$1238262.htm
http://www.guardian.co.uk/world/2008/jul/27/internationalcrime.hacking
http://www.hackervoice.co.uk/show/archive/2007/hackervoiceradio19mar2007.MP3

PUBLIC RECORD ON TAP: *The Hacker's Handbook*

Gary McKinnon was inspired by *The Hacker's Handbook*, by Hugo Cornwall. *The Hacker's Handbook* is a legendary nonfiction book from the 1980s, effectively explaining how computer systems of the period were hacked. It contains candid and personal comments from the British author of the book, Hugo Cornwall (a pseudonym of Peter Sommer), who is now a research fellow in Information Systems Security at the London School of Economics and frequently appears in the United Kingdom courts as an expert on digital evidence and computer forensics, as well as media pundit and author on information security topics. One popular aspect of the book is the salacious printouts of actual hacking attempts (although confidential details, such as passwords, are blocked out). The first edition, which is the version most easily available for download, was published in 1985, and the last of four editions (edited by Steve Gold) appeared in 1989. In 1990, the UK Parliament passed the Computer Misuse Act—publication of additional editions would likely have been considered an incitement to commit an offence under that Act. The full text can be found here:

http://www.textfiles.com/etext/MODERN/hhbk

PUBLIC RECORD ON TAP: Donna Hare

Donna Hare had a secret clearance while working for NASA contractor, Philco Ford. She testifies that she was shown a photo of a picture with a distinct UFO. Her colleague explained that it was his job to airbrush such evidence of UFOs out of photographs before they were released to the public. She also heard information from other Johnson Space Center employees that some astronauts had seen extraterrestrial craft, and that when some of them wanted to speak out about this they were threatened." To learn more, visit:

http://www.examiner.com/x-2024-Denver-UFO-Examiner~y2009m1d15-Whistleblowers-evidence-of-NASA-UFO-fraud-might-kill-UK-hacker-case

Donna Hare

FICTIONAL STORY DISSECTED: PSP Hack

"Hey—how's it goin'?" Leon said as he slid over in the booth to make room for Rudy.

"Same old. I was at home working on a new boot screen for my PSP. Sousanator released a new prx you can use to make a custom startup."

"Cool—bring it to the next 2600. I'd like to see how you do that," Leon replied (p. 48).

Prx is a data file used for updating the firmware of the PlayStation Portable (PSP); and with the right modifications it can also upgrade custom firmware that may be included with firmware dumps, and is often used to add extra features such as enabling screen captures and adding Flash support to the Web browser. Figure 10.3 is a screen shot of PSP-HACKS.com, where this hack can be found with many others for the PSP.

Below is a simple prx for Custom Firmware to load up on boot up. When you start up, it will display a custom message (of your choice), then go to your regular Xross-MediaBar (XMB). Currently, it says Hello in ASCII text, but you can set it to anything else (including ASCII graphics). Add to the config.txt

```
# Extra PRX's to load on boot.
loadmodule0 = "ms0:/psp/system/Hello.prx"
or loadmodule1 = "ms0:/psp/system/Hello.prx"
or loadmodule2 = "ms0:/psp/system/Hello.prx"
```

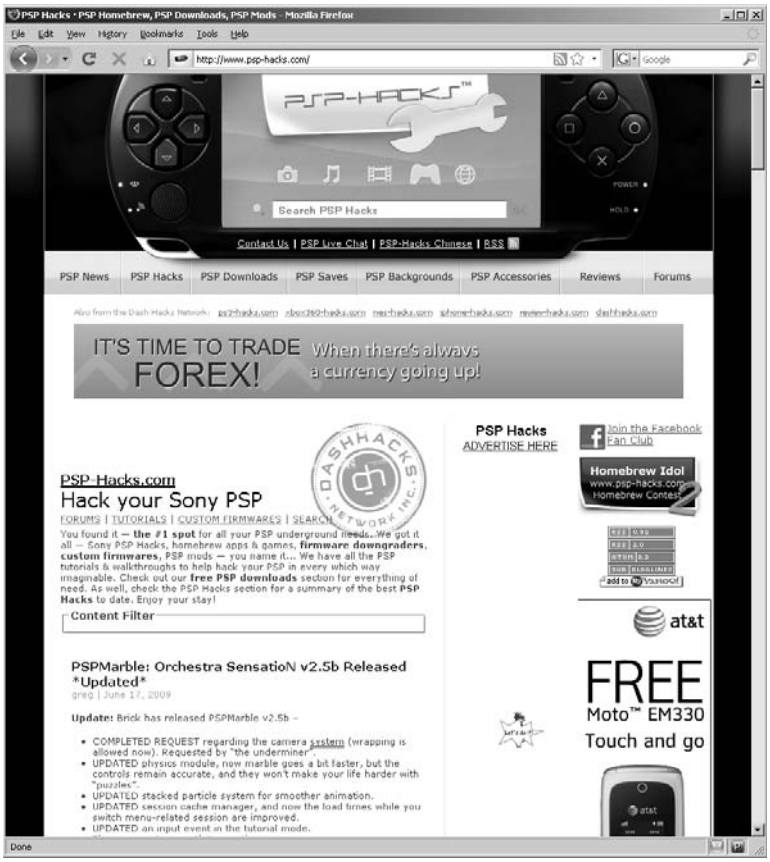


FIGURE 10.3

PSP-HACKS.com

FICTIONAL STORY DISSECTED: iDefense and ZDI

> "I sell vulnerabilities I find to iDefense."
>
> "You do? I've been selling to TippingPoint's ZDI!" (p. 53).

"The iDefense Vulnerability Contributor Program (VCP) began in 2002. The founders created the program when they realized that there exists an abundance of technical security knowledge concerning undisclosed vulnerabilities. This knowledge base is constantly being expanded by individuals and security groups. Some of this information may see the light of day on security mailing lists, or eventually be disclosed

as the result of a post-mortem analysis for a compromised computer system. iDefense created the VCP to compensate individuals who provide iDefense with advance notification of unpublished vulnerabilities and/or exploit code."[11]

"The iDefense VCP consists of two interrelated programs, the main program and an annual challenge. The main program focuses on actionable research submissions, presented to iDefense by the general public, defining new vulnerabilities, and/or exploits uncovered in prominent enterprise-level software and infrastructure components. iDefense defines actionable as anything representing a significant threat of damage or compromise to its customers and/or the general public, thus requiring protective action. iDefense defines prominent software and components as anything known by iDefense to be in general use by its customers and/or known to be in widespread public use. iDefense will offer as much as $15,000 (US), depending on the nature of the vulnerability, for acceptable well-documented research with reliable proof-of-concept exploit code."[3] View their homepage in Figure 10.4.

FIGURE 10.4

Labs.idefense.com

[11]http://labs.idefense.com/vcp/

Today, there still remains a perception by some in the information security industry that vulnerability researchers are malicious hackers looking to do harm. While there clearly are skilled malicious hackers out there, this remains a very small minority of the total number of people who actually discover new software flaws. In reality, the number of benevolent researchers with the expertise required to discover a software vulnerability is a sizeable and fast-growing group. The dissemination of publicly available vulnerability analysis and discovery tools has helped foster this group of security enthusiasts. Also, it is not uncommon for "white hat" security professionals to stumble onto a new flaw while doing their day-to-day security work.

TippingPoint has its own security research organizations via DVLabs. It made perfect sense, however, to augment DVLabs with the additional zero-day research of this growing network of "extended researchers." Our approach was the formation of the Zero Day Initiative (ZDI), launched on August 15, 2005. (You can read some more retrospective on the initial beginnings of the ZDI in this blog posting.) The main goals of the ZDI are to:

- Extend our DVLabs research team by leveraging the methodologies, expertise, and time of others
- Encourage the reporting of zero-day vulnerabilities responsibly to the affected vendors by financially rewarding researchers
- Protect our customers through the TippingPoint Intrusion Prevention Systems (IPS) while the affected vendor is working on a patch

We do not resell or redistribute the vulnerabilities that are acquired through the ZDI. http://www.zerodayinitiative.com/

TARGET ACQUIRED… An INFOSEC/Hacking Pioneer: Adam Laurie (a.k.a. Major Malfunction)

Adam Laurie is chief security officer and a director of The Bunker Secure Hosting Ltd. He started in the computer industry in the late 1970s, working as a computer programmer on PDP-8 and other minicomputers, and then on various Unix, Dos, and CP/M-based microcomputers as they emerged in the 1980s. He quickly became interested in the underlying network and data protocols and moved his attention to those areas and away from programming, starting a data conversion company, which rapidly grew to become Europe's largest specialist in that field (A.L. downloading Services).

TARGET ACQUIRED… An INFOSEC/Hacking Pioneer: Dan Kaminsky

Dan Kaminsky is a security researcher and Director of Penetration Testing for IOActive. He formerly worked for Cisco and Avaya.[12,13] He is known among computer security experts for his work on DNS cache poisoning, including showing that the Sony Rootkit had infected at least 568,200 computers,[14] and for his talks at the Black Hat Briefings.[9]

TARGET ACQUIRED… An INFOSEC/Hacking Pioneer: Felix "FX" Lindner

FX is the technical and research lead of Recurity Labs with 18 years computer technology experience, and over 10 years experience in the computer industry (almost all of them in consulting for large enterprise and telecommunication customers). FX is well-known in the computer security community, and has presented Phenoelit's security research and his research on Black Hat Briefings, CanSecWest, PacSec, DEFCON, Chaos Communication Congress, MEITSEC, and numerous other events.

TARGET ACQUIRED… An INFOSEC/Hacking Pioneer: Goodwell and China Eagle

The Green Army was founded by a Shanghai hacker going by the online name of Goodwell; it was reported to have had a membership of around 3000 people from Shanghai, Beijing, and Shijiazhuang. The other four key members of the group went by the pseudonyms Rocky, Dspman (HeHe), Solo, and LittleFish.[15] It also attracted others, considered to be part of China's first generation hackers: the likes of Xie Zhaoxia, Brother Peng, PP (Peng Quan), Tian Xing (Cheng Weishan), IceWater (Huang Lei), and Little Rong. The group disbanded in 2000, and its rise and fall was described as "confusing" by insiders who

[12]http://blog.wired.com/27bstroke6/2008/04/isps-error-page.html
[13]http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1313632,00.html
[14]http://www.wired.com/politics/security/news/2005/11/69573
[15]http://www.squidoo.com/thedarkvisitor

consider it one of the enduring symbols of the Chinese hacker movement. The Green Army is said to have hacked "uncountable foreign web sites." Indeed, many of China's top hackers were past members of this group. A year ago, almost 1000 websites in the US were defaced and two US government websites were under a denial-of-service attack, among other cyber attacks. The leader of the China Eagle Union hacker group admits to coordinating the 120-plus hackers in their siege from April 28 to May 8. After several months of research, iDEFENSE Intelligence Operations offers this profile of the China Eagle Union with details on its leader, its members, and a possible connection to a senior Chinese government official.[16] To read more, visit https://www.hackinthebox.org/modules.php?op=modload&name=News&file=article&sid=6164&mode=thread&order=0&thold=0.

TARGET ACQUIRED… An INFOSEC/Hacking Pioneer: HD Moore

HD Moore (born 1981) is a security researcher who has been active on internet mailing lists since 1998[17]. HD Moore works as the Director of Security Research for BreakingPoint Systems, where he focuses on the security testing features of the BreakingPoint product line. Prior to joining BreakingPoint, HD co-founded Digital Defense, a managed security services firm, where he developed the vulnerability assessment platform and led the security research team[18]. Moore helped create the concept of the Open Source Vulnerability Database (OSVDB) and participated in the original design of OSVDB. He continues to provide a consulting role, as well as being an advocate for the success of OSVDB.[19]

TARGET ACQUIRED… An INFOSEC/Hacking Pioneer: Jake Kouns

Jake Kouns is the cofounder and President of the Open Security Foundation, which oversees the operations of the OSVDB. Kouns' primary focus is to provide management oversight and define the strategic direction of the project. Kouns is currently the Director of Security and Network Services for a specialty insurance company. Prior to his current role, he was Senior Network Security Manager for Capital One.

[16]https://www.hackinthebox.org/modules.php?op=modload&name=News&file=article&sid=6164&mode=thread&order=0&thold=0
[17]http://marc.info/?l=bugtraq&m=91454756930070&w=2
[18]http://www.fosdem.org/2007/schedule/speakers/h+d+moore
[19]http://osvdb.org/contributors

TARGET ACQUIRED... An INFOSEC/Hacking Pioneer: Jeff Moss

Jeff Moss, also known as Dark Tangent, is the founder of the Black Hat and DEFCON computer hacker conferences.[20] Moss graduated from Gonzaga University with a BA in Criminal Justice. He worked for Ernst & Young, LLP in their Information System Security division and was a director at Secure Computing Corporation, where he helped establish the Professional Services Department in the United States, Asia, and Australia[21]. Moss is currently based in Seattle, where he works as a security consultant for a company that is hired to test the company's computer systems.[22] He's been interviewed on issues including the internet situation between the United States and China,[23] spoofing and other e-mail threats[16] and the employment of hackers in a professional capacity,[24] including in law enforcement[25]. He is also a member of the Homeland Security Advisory Council.[26]

TARGET ACQUIRED... An INFOSEC/Hacking Pioneer: Joanna Rutkowska

Joanna Rutkowska is a Polish security specialist, primarily known for her research on stealth malware and contributions to Windows Vista backdoor installation and hiding techniques. In August 2006 at the Black Hat Briefings conference in Las Vegas, Rutkowska presented system compromise techniques that could be used on Windows Vista systems, and subsequently has been named one of five hackers who put a mark on 2006 by *eWeek Magazine* for her research on the topic[27]. In the first part of the presentation, Rutkowska discussed how to bypass Vista kernel protection, demonstrating how to load unsigned code into the Vista kernel. The second part of the presentation introduced a technique dubbed Blue Pill. It could be described as a rootkit technology, allowing potentially malicious code to covertly take control over the system through the use of

[20]http://pcworld.about.com/news/Apr032001id43842.htm
[21]http://www.blackhat.com/html/bh-about/about.html
[22]http://www.cnn.com/TECH/computing/9808/13/hacker.idg/index.html
[23]http://archives.cnn.com/2001/WORLD/asiapcf/east/04/27/china.hackers/index.html
[24]http://www.forbes.com/1999/02/08/feat.html
[25]http://www.forbes.com/2000/08/02/mu5.html
[26]http://news.cnet.com/8301-1009_3-10258634-83.html
[27]http://www.eweek.com/article2/0,1895,2078362,00.asp

CPU virtualization. This method, although presented and implemented on Vista system, is OS-independent and does not exploit any weakness in the Vista system itself. The effectiveness of the latter approach, dubbed Blue Pill, is a subject of a debate among some researchers. Visit her blog at http://theinvisiblethings.blogspot.com/.

TARGET ACQUIRED… An INFOSEC/Hacking Pioneer: Johnny Long

Johnny Long, otherwise known as "j0hnny" or "j0hnnyhax," is a renowned computer security expert, author, and public speaker in the United States. Long is well-known for his background in Google hacking, a process by which vulnerable servers on the Internet can be identified through specially constructed Google searches. He has gained fame as a prolific author and editor of numerous computer security books. He also founded a nonprofit organization called Hackers For Charity.

TARGET ACQUIRED… An INFOSEC/Hacking Pioneer: Kevin Mitnick

With more than 15 years of experience in exploring computer security, Kevin Mitnick is a largely self-taught expert in exposing the vulnerabilities of complex operating systems and telecommunications devices. His hobby as an adolescent consisted of studying methods, tactics, and strategies used to circumvent computer security and to learn more about how computer systems and telecommunication systems work.

TARGET ACQUIRED… An INFOSEC/Hacking Pioneer: Stephan Northcutt

Stephen Northcutt founded the Global Information Assurance Certification (GIAC) and currently serves as president of the SANS Technology Institute, a postgraduate level IT security college (http://www.sans.edu). Stephen is author/coauthor of *Incident Handling Step-by-Step*, *Intrusion Signatures and Analysis, Inside Network Perimeter Security* second edition, *IT Ethics Handbook*, *SANS Security Essentials, SANS Security Leadership Essentials, and Network Intrusion Detection* third edition. He was the original author of the

Shadow Intrusion Detection system before accepting the position of chief for information warfare at the Ballistic Missile Defense Organization.

TARGET ACQUIRED… An INFOSEC/Hacking Pioneer: Tony Watson

Paul Watson is currently employed as a network security engineer with Google. Watson has over 15 years of experience in the information technology area, including 13 years focused on information security. During his career, he had presided over three start-ups, as well as having been employed by fine organizations such as the U.S. Air Force, Iridium LLC, CapitalOne Financial, VeriSign, Rockwell Automation, and Google. Oh, by the way, he saved the Internet. Visit to read more at http://www.themanwhosavedtheinternet.com/ and http://www.paw.org/about.html.

FICTIONAL STORY DISSECTED: Kaminsky and Watson

Bob turned to Leon. A smile spread across his face as the enormity of the story he had just told sunk in. "Dude, do you know what we just did? We just saved the United States! That's bigger than saving the Internet! That means we're bigger than Dan Kaminsky! Or Tony Watson!"

Leon looked exasperated. "Bob, we aren't even up there with GOBBLES. Or n3td3v for that matter."

Bob's shoulders dropped a little and he asked almost plaintively, "Well, then won't we at least get an interview with Stephen Colbert?"

"Sorry, Dude, I wouldn't be expecting a call even from Letterman," Leon responded with a satisfied smile as things got back to normal (p. 125).

PUBLIC RECORD ON TAP: Wikiality

On July 31, and again on August 2, Wikipedia was featured on the news satire *The Colbert Report*. The show's host, Stephen Colbert, poked fun at Wikipedia's nature and encouraged viewers to insert falsehoods into existing articles. As a result, a number of articles were protected from editing, and some still remain semiprotected as of press time.

The Colbert Report has a regular feature known as "The WØRD", where a word or phrase, sometimes a portmanteau, is featured (in the show's debut episode, "truthiness" was coined).

Last Monday's episode of *The Colbert Report* featured the word "Wikiality", a portmanteau of wiki and reality. Colbert said that "any website that has a longer entry on truthiness than Lutheranism has got its priorities straight." After "confusion" over his favorite pejorative term for Oregon, Colbert showed a screen shot of *The Colbert Report* noting that he referred to the state as both "the Canada of California" and "Washington's Mexico" (a fact actually found in a separate article). Colbert decided instead that Oregon was "Idaho's Portugal," and purportedly edited the article to say so. He commented on the process, saying "Any user can change any entry, and if enough other users agree with them, it becomes true." Colbert also stated that "George Washington never owned slaves", and "Africa has more elephants today than it did 10 years ago."

Near the end of the segment, Colbert says "Find the page on Elephants on Wikipedia, and create an entry that says the number of elephants has tripled in the last six months … Together, we can create a reality that we can all agree on—the reality that we just agreed on." See Figure 10.5. After the segment's airing, elephant was immediately semiprotected by MarkSweep, then fully protected 1 min later by Fire Star. However, clever viewers made similar edits to pages on numerous species of elephants (and other, unrelated articles such as Elefant [band]), prompting the semiprotection of most articles relating to elephants. Other articles mentioned in the segment such as Oregon, Portugal, and Colbert-related articles were subject to similar elephant-related additions.

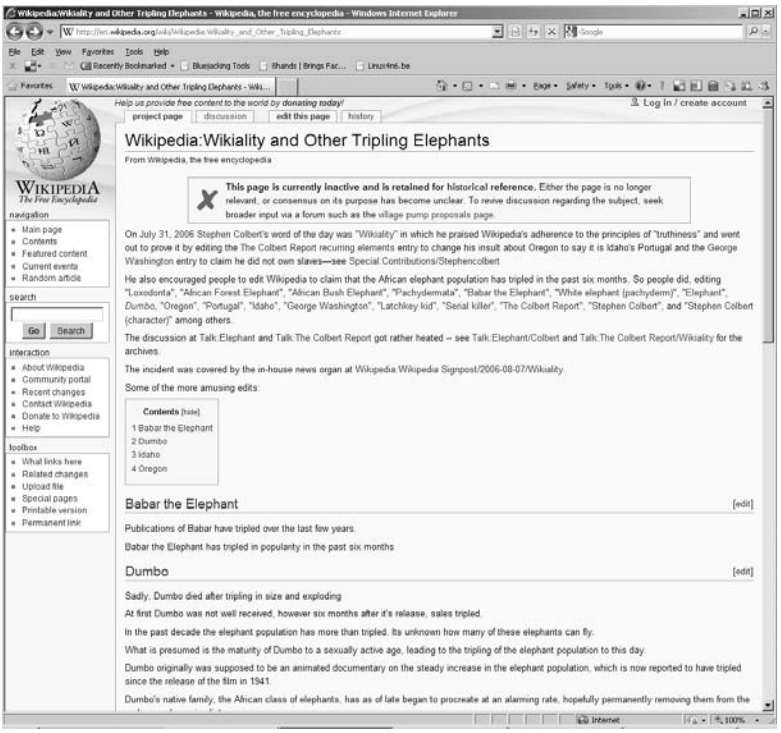


FIGURE 10.5
Elephants triple in 6 months

Before the segment aired, the username Stephencolbert was registered, and two edits were made: first stating that Oregon was Idaho's Portugal,[28] and second saying "In conclusion, George Washington did not own slaves.[29] Though the edits were made around the time that *The Colbert Report* is taped, some question was raised over whether the edits were actually made by Colbert; while he pretended to edit Wikipedia on the show, it's possible that audience members could have edited via mobile phone. As such, the account was blocked indefinitely, under the username policy. Blocking administrator Tawker attempted to contact Comedy Central to confirm the account's identity, but no response has yet been received.

To view the video visit: http://www.colbertnation.com/the-colbert-report-videos/72347/july-31-2006/the-word---wikiality?videoId=72347 or http://tinyurl.com/pklx6g

PUBLIC RECORD ON TAP: Megyeri Bridge Naming Poll

The Megyeri Bridge, previously known as the Northern M0 Danube bridge, is a cable-stayed bridge that spans the River Danube between Buda and Pest, respectively, the west and the east sides of Budapest, the capital of Hungary. It is a very important section of the M0 (motorway) ring road around Budapest.

The bridge costs 63 billion forints (approximately US$300M).[30] It was officially opened on September 30, 2008[6]; however, the National Transport Authority of Hungary has only issued a temporary permission because of the disagreement of the suburban cities surrounding the bridge. It has received much media attention due to the naming poll started to name the bridge.

The Ministry of Economic Affairs and Transport of Hungary organized a public vote online to solicit possible names for the new bridge. The three names with the most votes, as well as suggestions from local governments, cartographers, linguists, and other experts, were to be reviewed by a government committee before a final name for the bridge was chosen. New nominations were accepted until August 21, 2006; and the voting ended on September 8, 2006, with Stephen Colbert winning with 93,163 votes, and Jon Stewart and Zrínyi close behind with 85,171 and 83,966 votes, respectively.

[28]http://en.wikipedia.org/w/index.php?title=The_Colbert_Report_recurring_elements&diff=prev&old id=66945346
[29]http://en.wikipedia.org/w/index.php?title=George_Washington&diff=prev&oldid=66945427
[30]http://index.hu/gazdasag/magyar/megya080930/

Reuters reported that the top candidate according to the online poll was the "Chuck Norris híd," named for American action star Chuck Norris.[31] On August 11, 2006, American satirist Stephen Colbert discussed the story on his comedy program *The Colbert Report*, instructing his viewers to visit the polling Web site and vote for him instead of Norris. The next day the number of votes for him had grown 230 times, and he now asked his viewers to follow a link from his own "Colbert Nation" Web site to avoid "all that illegible Hungarian." On August 15, 2006, he repeated his call to be voted top of the Hungarian poll; and by August 22, 2006, the "Stephen Colbert híd" was in first with 17 million votes, about 14 million votes ahead of the second-placed Zrínyi híd, named after the Hungarian national hero, Miklós Zrínyi, and about 7 million more than the entire population of Hungary. The same day, the site announced a new round of voting, which would require registration to participate, and Colbert asked his viewers to "call off the dogs," requesting on his Web site that fans stop using scripts to vote. Despite this, the "Stephen Colbert híd" remained in the top position on the Web site in the second round.

On September 14, 2006, András Simonyi, the ambassador of Hungary to the United States, announced on *The Colbert Report* that Stephen Colbert had won the vote. Unfortunately for Colbert, Ambassador Simonyi declared that under Hungarian law, Colbert would have to be fluent in Hungarian and would have to be deceased to have the bridge named for him. However, after saying the rules could most likely be bent, he invited Colbert to visit Hungary and view the construction in person and gave him a Hungarian passport and a 10,000 HUF Bill, with an approximate value of, as the ambassador put it, "fifty dollars, fifty good US dollars." Colbert promptly tried to bribe him with said money.

PUBLIC RECORD ON TAP: NASA and Colbert

NASA names treadmill after Colbert

By Jake Coyle from AP Entertainment on April 14, 2009

One small step for NASA, one giant running leap for Stephen Colbert. NASA announced Tuesday that it won't name a room in the international space station after the comedian. Instead, it has named a treadmill after him. NASA earlier held an online contest to name a room (or "node") at the international space station. With write-in votes, the name "Colbert" beat out NASA's four suggested options: Serenity, Legacy, Earthrise, and Venture.

On Tuesday's "The Colbert Report" on Comedy Central, astronaut Sunita Williams announced that NASA—which always maintained it had the right to choose an appropriate name—would not name the node after Colbert. Instead, Node 3 will henceforth be called Tranquility, the eighth most popular response submitted by respondents in the poll. The node's name alludes to where Apollo 11 landed on the moon—the Sea of Tranquility.

[31] http://today.reuters.co.uk/news/newsArticle.aspx?type=oddlyEnoughNews&storyID=2006-08-01T094605Z_01_L01355692_RTRIDST_0_OUKOE-UK-HUNGARY-BRIDGE.xml

NASA and Colbert compromised by naming a treadmill used for exercising in space after Colbert. NASA, itself an acronym (National Aeronautics and Space Administration), often names things so they spell out something fun. And that's what they did with the Combined Operational Load Bearing External Resistance Treadmill (COLBERT).

Sophisticated treadmills are crucial for living in space for long periods of time, as astronauts do on the space station; they help keep astronauts fit and their bones from losing strength. Williams ran a marathon on one while living at the space station in 2007, jogging in place to coincide with the Boston Marathon.

The COLBERT treadmill is a new version that will be operational in August, NASA spokesman Mike Curie said. "We don't typically name U.S. space station hardware after living people, and this is no exception," Bill Gerstenmaier, NASA's associate administrator for space operations, said, adding: "We have invited Stephen to Florida for the launch of COLBERT, and to Houston to try out a version of the treadmill that astronauts train on." To read more visit http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2009/04/14/entertainment/e171111D36.DTL&type=health.

PUBLIC RECORD ON TAP: Gobbles

GOBBLES is the greatest group of trolls that have ever existed. Their drama-generating techniques used were truly of far greater magnitude than anything that has been seen since. The skill and grace with which they whipped the entire whitehat security industry into a frothing, hateful rage make even hardened masters of trollery like the GNAA look retarded and inefficient. GOBBLES was such a master of trollery that songs will be sung of their feats for many generations of trolls to come. To read more visit http://encyclopediadramatica.com/GOBBLES.

PUBLIC RECORD ON TAP: n3td3v

Researcher attempts to shed light on security troll

By Robert Lemos on October 20, 2006 from SecurityFocus

The troll—as such taunting posters are dubbed—would frequently ignite massive angry e-mail responses, or flame wars, at times limiting the usefulness of the Full Disclosure list. Over time, n3td3v took on multiple online personalities, or gained members of the n3td3v group, and attempted to create an online security hub. The group's favorite targets included Yahoo!, Google, and other researchers and security news reporters, including this one.

Even after n3td3v gave up the virtual ghost in September 2006, no one knew the name of the person who infuriated, and amused, so many researchers. Now, an independent security

consultant believes that linguistic forensics—a branch of science that attempts to identify authors by the content and style of their writings—has linked n3td3v with a previous security-list troll and hacking group known as Gobbles.

In a 19-page report published on Friday, consultant Neal Krawetz argues that statistical analysis of mailing-list messages posted by n3td3v and advisories written by Gobbles indicates that each group appears to be three, or possibly four, people, and the writing styles of the people making up the two groups appear to match. The report uses five different metrics of writing style to determine whether the authors are American or non-American, male or female, and their degree of education. While the five indicators have large margins of error, using the methods together minimizes the error, Krawetz claimed.

"Because these methods are not perfect, I definitely could be wrong—I just don't think I am," Krawetz said in an interview with SecurityFocus. The conclusion is not new: Several security researchers that subscribe to the Full-Disclosure mailing list have also noted that n3td3v's tactics seemed similar to Gobbles. However, this is the first time that science seemingly backs up the conclusion.

Krawetz argued that the link could mean that n3td3v's claims of having zero-day vulnerabilities in Microsoft, Yahoo! and Google software could have some basis in reality. In 2001, Gobbles taunted the community, was written off as a troll, but then surprised many researchers by releasing a number of respectable vulnerabilities in late 2001 and 2002.

"Assuming that they are the same group and they are following the same pattern, then (n3td3v) are probably sitting on a lot of zero-day exploits and, probably, for Windows Vista," Krawetz said, stressing that the hypothesis was only conjecture. Yet, others believe that any link between the two groups is purely circumstantial. "Gobbles showed some real techniques; n3td3v is nothing but a troll," said Brian Martin, a network security consultant, who asked that his company name not be mentioned. "If you sit down and really think about trolls, Gobbles is going to come to mind. But for no other reason than he's a notable troll."

Martin has met the primary researcher—who used the pseudonym "Gobbles"—in the past and characterized the person, who he refused to name, as "polite and soft-spoken." He doubted that the person who primarily used the Gobbles nom de plume would devolve into more prolific troll.

"Several years later, I don't see him turning into n3td3v at all," Martin said. "Sure he was a troll, but several years later, I don't see him getting worse." To read more, visit http://www.securityfocus.com/news/11419

CONFERENCES

If you attend any of the conferences below, you might sense a feeling of pride and maybe a pinch of rebellious energy toward authority figures because true hackers want to share information on how insecure our infrastructure really is. Whether or not the

media stereotypes of hackers is right in dictating a negative perception of hackers, our infrastructure demands that hackers continue this honorable battle of finding the insecure technologies and fixing it.

ARES: The International Dependability Conference (The International Conference on Availability, Reliability and Security)

The annual ARES Conference brings together researchers and practitioners in the area of dependability.ARES aims at a full and detailed discussion of the research issues of dependability as an integrative concept that covers (amongst others) availability, safety, confidentiality, integrity, maintainability, and security in the different fields of applications. ARES will emphasize the interplay between foundations and practical issues of dependability in emerging areas such as e-government, m-government, location-based applications, ubiquitous computing, autonomous computing, chances of grid computing, and so forth.ARES is devoted to the critical examination and research challenges of the various aspects of Dependable Computing and the definition of a future road map.
Location: worldwide
http://www.ares-conference.eu/conf/

Best of Open Source Security (BOSS) Conference

The BOSS Conference has been driven to meet the needs of customers, partners, and staunch advocates of the open-source security community.The inaugural two-day event is slated for 2009.
Location: United States
http://www.bossconference.com/

Black Hat

The Black Hat Briefings and Training have become the biggest and the most important security conference series in the world by sticking to our core value: serving the information security community by delivering timely, actionable security information in a friendly, vendor-neutral environment.
Locations: worldwide
http://www.blackhat.com/

BlueHat

BlueHat is a by-invitation-only Microsoft security conference aimed at bringing Microsoft security professionals and external security researchers together in a relaxed environment to promote the sharing of ideas and social networking. BlueHat is a cutting-edge conference aimed at improving the security of Microsoft products.

BlueHat continuously seeks out new and innovative material, highlighting important emergent technologies, techniques, and industry best practices.
Location: Microsoft Headquarters, Redmond, Washington, United States
http://technet.microsoft.com/en-us/security/cc261637.aspx

BruCON

BruCON is an annual two-day conference by and for the security and hacker community. The conference offers lectures and workshops on a multitude of topics like computer security, privacy, and information technology and its implications on society.
Location: Brussels, Belgium
http://www.brucon.org/index.php/Main_Page

New Camelot Council

This conference is a balanced-mix convention where technical and nontechnical people can meet and freely share all kinds of information. It supports a focus on continuous improvement and developing greater efficiencies effort to global cyber coherence. This conference will look at what we have learned and how we can better apply ourselves and resources to help and avoid IT conflicts in time. Through our conference, we will look for opportunities to build a joint coordination team by discussing what we can do today with leading-edge technologies, networks, and infrastructures, which result in commercial and social mitigation of hacking environments. We seek to increase our partnerships across the Government official and with industry. The conference is 3 days of active discussions, presentations, workshops, and games for sharing experience around new attacks, defensive techniques, and information security (including funky experiments).
Location: Shanghai, China
http://www.newcamelotcouncil.com/indexEN.html

CanSecWest

CanSecWest, the world's most advanced conference focusing on applied digital security, is about bringing the industry luminaries together in a relaxed environment which promotes collaboration and social networking. The annual conference lasts for 3 days and features a single track of thought-provoking presentations, each prepared by an experienced professional and talented educator who is at the cutting edge of his or her field. We give preference to new and innovative material, highlighting important, emergent technologies, techniques, or best industry practices. CanSecWest: Security Masters Dojo addresses the need for intermediate and advanced educational requirements that go beyond the introductory materials typically found in most currently existing training (which are often geared towards the novice level). For professionals who already have significant work experience, and

want to further improve their skills, we have assembled a curriculum of hands-on, one day, training programs—delivered by industry-renowned experts who are pre-eminent in their fields.
Location: Vancouver, Canada
http://cansecwest.com/index.html
http://cansecwest.com/dojo.html

Chaos Communication Congress (CCC)

CCC is an annual four-day conference organized by the Chaos Computer Club (CCC) in Berlin, Germany. First held in 1984, it since has established itself as "The European Hacker Conference", attracting a diverse audience of thousands of hackers, scientists, artists, and utopists from all around the world. Join and be a part of this unique event, which serves as a public platform for cross-culture inspiration and borderless networking. 26C3 (the 26th annual Chaos Communication Congress) will be held in 2009.
Location: Berlin, Germany
http://events.ccc.de/congress/2009/

Computer and Communications Security (CCS)

The annual ACM Computer and Communications Security Conference is a leading international forum for information security researchers, practitioners, developers, and users to explore cutting-edge ideas and results, and to exchange techniques, tools, and experiences. We invite submissions from academia, government, and industry presenting novel research on all theoretical and practical aspects of computer security, as well as case studies and implementation experiences.
Location: United States
http://www.sigsac.org/ccs/CCS2009/

Computer and Enterprise Investigations Conference (CEIC)

An annual conference offering world-class training and education with a focus on best practice methods and new techniques in computer forensics and cybercrime, electronic discovery (eDiscovery), records retention, data auditing and policy compliance, internal investigations, information assurance, and computer incident response.
Location: United States
http://www.ceicconference.com/

Computer Forensics Show

For some companies, it is not a question if one of their computers will be used as evidence in a legal matter, it is a question of when. Like it or not, every computer is a potential crime scene and must be treated with care. When companies need to

conduct internal investigations—especially those involving litigation—discovering and maintaining evidence becomes paramount. This Computer Forensics Show is the "Don't Miss" event of the year for all litigation, accounting, and IT professionals.
Location: United States
http://www.computerforensicshow.com/

Computer Security Institute Annual Conference (CSI)

The industry's premier and longest-running security conference, CSI will keep you updated, connected and innovative—everything you need to maintain your competitive advantage, keep costs down, and protect your organization. The security landscape is rapidly changing, along with the world; but the need for proactive, effective, and comprehensive security strategies is still paramount. Lectures, case studies, keynotes, discussions, workshops, vendors and networking—you'll find it all at the annual CSI conference.
Location: United States
http://www.gocsi.com/

Computer Security Institute Security Exchange (CSI-SX)

The CSI-SX conference is a unique opportunity for security professionals to discuss and learn security solutions in a smaller, more intimate environment, with a select group of peers and experts. CSI-SX attendees are security professionals of all levels, from companies large and small, across all industries. Attendees are CIOs/CSOs/CISOs, information security managers and directors, security senior staff and specialists, network and communication security managers and directors, network engineers, IT audit managers. Experience level ranges from individuals new to security to professionals with decades of experience.
Location: United States
http://www.csisx.com/

CONFidence

CONFidence is an annual IT security conference held in Krakow, Poland. The best speakers, latest issues, laid-back atmosphere, and Krakow crazy night life—that is why CONFidence has become a meeting point of hackers' community in Europe.
Location: Krakow, Poland
http://2009.confidence.org.pl/

DeepSec In-Depth Security Conference

This conference brings together the world's most renowned security professionals from academics, government, industry, and the underground hacking community.

The DeepSec IDSC is an annual European two-day in-depth conference on computer, network, and application security. DeepSec IDSC aims to bring together the leading security experts from all over the world. DeepSec IDSC is a nonproduct, nonvendor-biased conference event. Our aim is to present the best research and experience from the fields' leading experts. Intended target audience: security officers, security professionals and product vendors, IT decision makers, policy makers, security, network, and firewall admins, hackers, and software developers.
Location: Europe
https://deepsec.net/

DEFCON

DEFCON is one of the oldest continuous running hacker conventions around, and also one of the largest. DEFCON is generally in the last week of July or first week of August in Las Vegas, Nevada, USA.
Location: United States
http://www.defcon.org/

DojoSec Monthly Briefings

The mission of DojoSec is to provide an environment for people to master the art of information security. DojoSec Monthly Briefings are an example of the commitment that we are making to accomplish this goal. Audience of DojoSec Monthly Briefings have seen talks by Johnny Long, Ron Gula, Joseph McCray, Marcus J. Ranum, and Bruce Potter—to name a few speakers. Attendees enjoy technical demonstrations, industry expert speakers, and a meal. It's like a dinner theater for security geeks! The events take place on the first Thursday of every month.
Location: United States
http://www.dojosec.com/

Ekoparty Security Conference

Ekoparty is a one-of-a-kind event in South America; an annual security conference held in Buenos Aires where security specialists from all over Latin America (and beyond) have the chance to get involved with state-of-art techniques, vulnerabilities, and tools in a relaxed environment, which has not been seen before.
Location: Buenos Aires, Argentina
http://www.ekoparty.com.ar/

EUsecWest London

This conference is where the world's security professionals converge to discuss new technology and share best practices. The most significant new discoveries, technologies, and products will be presented at the annual EUSecWest conference, brought to

you by the organizers of PacSec and CanSecWest. The latest in cutting-edge information security threats, defenses, applications, and theory will be showcased in a series of one-hour presentations by the brightest minds in the security field from all nations.
Location: London, United Kingdom
http://eusecwest.com/index.html

FRHACK International IT Security Conference

France's own International IT Security Conference by hackers, for hackers. FRHACK is an annual conference offering technical trainings and workshops with talented and highly skilled trainers.
Location: France
http://www.frhack.org/

Hack.in

Hack.in aims to bring together researchers, practitioners, programmers, administrators, professionals, and others interested in the security of computer systems and networks. Hack.in is primarily a systems security workshop and will focus on the design and implementations of security systems, including protocols and case studies. This annual workshop in Kanpur, India consists of contributed papers, invited talks, workshops, and panel discussions.
Location: Kanpur, India
http://www.security.iitk.ac.in/hack.in/2009/

Hack in the box—HITBSecConf

The premier network security event takes place in Asia and the Middle East. The main aim of our conference is to enable the dissemination, discussion, and sharing of deep knowledge network security information. Since 2003, HITBSecConf has routinely brought some of the most respected members of the mainstream network security arena, as well as the underground or black hat community, to Asia. Our events have always highlighted new and ground-breaking attack and defense methods that have not been seen or discussed in public before.
Locations: Asia and the Middle East
https://conference.hackinthebox.org/

Hacker Halted

Hacker Halted USA is a complete and comprehensive information security conference, with information security experts from all around the world presenting intriguing topics and discussing global security threats, as well as world-class trainers leading top-notch security training classes at H@cker|Halted Academy. The objective

of Hacker Halted is to raise international awareness toward increased education and ethics in information security.

The global series of Hacker Halted is owned by EC-Council, a leading information security certification body, and the creators of the world-renowned Certified Ethical Hacker program, as well as other certification programs.
Location: United States
http://www.hackerhalted.com/

IPTComm: Principles, Systems and Applications of IP Telecommunications

The aim of the IPTComm conference is to serve as a platform for researchers from academia and research labs, industry, and government to share their ideas, views, results, and experiences in the field of IP-based telecommunication. IPTComm will include presentations of theoretical and experimental achievements, innovative security systems, prototyping efforts, case studies, and advancements in technology directly affecting IP-based telecommunication in general and VoIP and IMS services in particular.
Location: United States
http://iptcomm.org/

Infosecurity Europe

Infosecurity Europe is Europe's most comprehensive gathering of information security professionals. It showcases the most diverse range of new and innovative products and services, and addresses today's strategic and technical issues in an unrivaled free-to-attend education program.
Location: United Kingdom
http://www.infosec.co.uk/

International Conference on Security and Cryptography (SECRYPT)

The purpose of SECRYPT, the International Conference on Security and Cryptography, is to bring together researchers, engineers, and practitioners interested on information systems and applications in the context of wireless networks and mobile technologies. Information systems and information technology are pervasive in the whole communications field, which is quite vast, encompassing a large number of research topics and applications: from practical issues to the more abstract theoretical aspects of communication; from low-level protocols to high-level networking and applications; from wireless networking technologies to mobile information systems. Many other topics are included in the scope of SECRYPT.
Location: Europe
http://www.secrypt.org/

International Workshop on Fast Software Encryption (FSE)

The workshop concentrates on fast and secure primitives for symmetric cryptography, including the design and analysis of block ciphers, stream ciphers, encryption schemes, analysis and evaluation tools, hash functions, and message authentication codes (MACs). FSE is organized by the COSIC research group of the Katholieke Universiteit Leuven and sponsored by the International Association for Cryptologic earch.
Location: Worldwide
https://www.cosic.esat.kuleuven.be/fse2009/

Internet Security Operations and Intelligence (ISOI)

Location: United States
http://www.isotf.org/isoi6.html

Kiwicon

Kiwicon is primarily geared toward pretty technical computer security topics. Computer nerds, geeks, and people who think lego is awesome will be in the majority for once. However, computer security affects a wide range of people in modern society, and so many of the topics discussed will be of interest to the layperson, even if some of the nitty-gritty detail is opaque. Children are welcome to attend Kiwicon; however, we'd request that children below the age of 14 are accompanied by a parent or guardian. Many of the techniques discussed at Kiwicon can be used to break the law, so strong moral guidance is recommended for those of all ages.
Location: New Zealand
http://www.kiwicon.org/

LayerOne

LayerOne is a computer security conference located in Anaheim, California. We feature speakers from all across the globe, and on topics ranging from lockpicking and MPLS security to covert data gathering and HIPPA compliance. Our speakers come from a diverse background, and include a focus not just on the nuts and bolts of technology but the social impact as well. Our event is located at the Anaheim Marriott and is just a few minutes' walk from many venues, eateries, and attractions.
Location: United States
http://layerone.info/

PacSec

To address the increasing importance of information security in Japan, the best known figures in the international security industry will get together with leading

Japanese researchers to share best practices and technology.The most significant new discoveries about computer network hack attacks are those presented for discussion at the annual PacSec conference.The PacSec meeting provides an opportunity for foreign specialists to be exposed to Japanese innovation and markets and collaborate on practical solutions to computer security issues. In a relaxed setting with a mixture of material bilingually translated in both English and Japanese, the eminent technologists can socialize and attend training sessions.
Location: Japan
http://pacsec.jp/

RSA

RSA Conference is the unbiased resource which thousands of information security professionals around the world have come to rely upon for unparalleled networking and knowledge sharing opportunities. We explore every leading topic in the field from cryptography to legislation, to government and policy mandates. Customize your agenda from the 220+ available sessions. Attend keynotes, breakout sessions or tutorials—across 17 different class tracks. The sessions and tutorials cover all facets of information security, IT management, programming, development, and executive management.
Locations: USA, Japan, and Europe.
https://365.rsaconference.com/index.jspa

Rocky Mountain Information Security Conference (RMISC)

The Annual Rocky Mountain Information Security Conference (RMISC) is the region's only opportunity to learn about trends, receive relevant education, and experience hands-on mock situations for executives, engineers, and anyone involved in information security across all industries. Topics range from identity theft and e-discovery of files to application security and surviving security audits, offering something for anyone involved in information security. The conference is hosted by the Denver chapter of the Information Systems Security Association (ISSA), the world's premier association for information security professionals.
Location: United States
http://www.issa-denver.org/RMISC.htm

SEaCURE.IT

SEaCURE.IT is the first international technical conference ever held in Italy on security-related topics, aimed at bringing together the leading experts from all over the world, to create a unique setting for networking and discussion among the speakers and the attendees.The first SEaCURE.IT Conference will be held in Sardinia in May 2010.
Location: Sardinia, Italy
http://www.seacure.it/

SecTor: Security Education Conference Toronto

This conference illuminates the Black Art of Security. SecTor brings the world's brightest (and darkest) minds together to identify, discuss, dissect, and debate the latest digital threats facing corporations today. Unique to central Canada, SecTor provides an unmatched opportunity for IT professionals to collaborate with their peers and learn from their mentors. Held at the Metro Toronto Convention Centre in downtown Toronto, the SecTor conference runs two full days. The event features keynotes from North America's most respected and trusted experts. Speakers are true security professionals with depth of understanding on topics that matter. SecTor is a must-attend event for every IT Professional.
Location: Toronto, Canada
http://www.sector.ca/

SecureWorld Expo

SecureWorld Expo brings together the security leaders, experts, senior executives, and policy makers who are shaping the very face of security. SecureWorld is at the intersection of Information Security, Physical Security, Compliance, IT Audit, Computer Forensics, Enterprise Risk Management, Business Continuity, and Security Management.
Location: United States
http://www.secureworldexpo.com/

Shakacon

One of the most beautiful places on Earth serves as the backdrop for a unique conference experience. Secure DNA's Shakacon Conference features seminars, lectures, and interactive demonstrations presented by speakers from all over the world.
Location: Hawaii, United States
http://www.shakacon.org/

ShmooCon

ShmooCon is an annual East coast hacker convention hell-bent on offering three days of an interesting atmosphere for demonstrating technology exploitation, inventive software & hardware solutions, and open discussions of critical information security issues. The first day is a single track of speed talks, One Track Mind. The next two days, there are three tracks: Break It!, Build It!, and Bring It On!
Location: Washington DC, United States
http://www.shmoocon.org/

SOURCE Conference

Speakers and topics for SOURCE are hand-picked by leading security minds in the industry. The SOURCE advisors are renowned security experts, and select talks

based on strict technical criteria. SOURCE is unique; combining top technological minds in the security industry with business professionals, executives, senior management, and industry experts providing insight into successful business practices for the security community. In addition to our advanced technical talks, SOURCE offers workshops on entrepreneurship, management strategies, job interviewing, presentation skills, and proficiencies and strategies designed for the security industry.
Locations: Boston, MA, United States; and Barcelona, Spain
http://www.sourceconference.com/

SyScan

The Symposium on Security for Asia Network aims to be a very different security conference from the rest of the security conferences that the information security community in Asia has come to be so familiar and frustrated with. SyScan is a nonproduct, nonvendor-biased security conference. It is the aspiration of SyScan to congregate in Asia the best security experts in their various fields to share their research, discovery, and experience with all security enthusiasts in Asia.
Locations: Singapore, Taipei, Shanghai, and Hong Kong.
http://www.syscan.org/

Techno Forensics Conference

The Techno Forensics & Digital Investigations Conference is founded on the principles of standardization in the field of digital evidence investigation. The conference covers many of the general disciplines in the areas of digital evidence investigation to include some of the latest information on software and hardware solutions.
Location: Gaithersburg, Maryland, United States
http://www.thetrainingco.com/html/TechnoForensics2009.html

Techno Security Conference

The annual international Techno Security Conference is held in sunny Myrtle Beach each year, and promises to be the international meeting place for IT Security professionals from around the world. The conference features some of the top speakers in the industry, and raises international awareness toward increased education and ethics in IT security. Techno has become known as a world-class training and networking event, now having had attendees register from 42 different countries. Our conference has also been on the GSA schedule for several years now. Our conferences are well-known for the excellent networking that takes place between attending members of law enforcement and industry.
Location: Myrtle Beach, South Carolina, United States
http://www.thetrainingco.com/html/Techno2009.html

ToorCamp

ToorCamp is the United State's first ever full-scale hacker camp. Modeled after the camps in Holland and Germany, ToorCamp will focus on all of the technology topics that ToorCon has become famous for, but will expand out into other areas of society. ToorCamp will offer 2 days of talks on many different topics—Security, Internet, Emerging Technologies, Hardware Hacking, and Privacy are just some of the areas we will be covering. ToorCamp will also feature 2 days of hands-on workshops on a multitude of different skills that you may have never found yourself interested in learning about before. Blacksmithing, Lock Picking, Orienteering, Logic Design, Archery—these are just a few of the topics you can expect.
Location: Moses Lake, Washington, United States
http://www.toorcamp.org/

ToorCon

ToorCon is San Diego's hacker conference bringing together the top security experts to present their new tricks of the trade and to have fun in the sunny and beautiful city of San Diego.
Location: San Diego, California, United States
http://www.toorcon.org/

uCon

uCon is a vendor-neutral and single track conference on hacking, technology and information, and telecommunication security; and aims to bring together academics, hackers and information security enthusiasts from all over the country to share cutting-edge ideas and thoughts about their latest developments and techniques in the field. Attendees will have the opportunity to network with like-minded people during social events, such as lunch break and after-conference party and during the Capture-the-Flag competition. This event is part of a larger effort at CIn-UFPE to create a "Permanent Forum on Cybersecurity and The Public Domain", the aim of which is to discuss contemporary themes related to Internet security, privacy, and intellectual property in the digital age, and cyber law. The Forum will be run by the Cybersecurity Laboratory at CIn-UFPE and will include participants from academia, industry, government, and privacy rights organizations.
Location: Brazil
http://ucon-conference.org/

USENIX Security Symposium

Join researchers, practitioners, system administrators, and system programmers for the latest advances in the security of computer systems and networks.
Location: United States and Canada
http://www.usenix.org/

Workshop on Collaboration and Security (COLSEC)

This Workshop on Security and Collaboration focuses on security issues related to collaborative systems with emphasis on distributed environments, smartcards, grid, clusters, and multiagent systems (mobile and wireless cooperation). The aim is to have a dedicated workshop that fosters closer interactions among researchers and user communities, providing an excellent opportunity for them to meet and discuss their ideas. It addresses specifically relationships between collaborative systems and security. It intends to present new challenges and solutions related to latest security requirements, specific methods of access control enabling large-scale cooperation, usage of mobile technologies and smartcards, new security infrastructures supporting better prevention, detection, recovery, and healing in the context of cooperative systems.
Location: United States
http://www.univ-orleans.fr/lifo/Manifestations/COLSEC/

BLOGS

Adrian Lamo—http://pax.vox.com/

Benny Ketelslegers—http://blog.security4all.be/

Chris Gates—http://carnal0wnage.blogspot.com/

Christophe Veltsos—http://blog.drinfosec.com/

Dan Kaminsky—http://www.doxpara.com/

Dustin L. Fritz—http://blog.dustinlfritz.com/

Felix 'FX' Lindner—http://www.phenoelit.net/lablog/

HD Moore—http://blog.metasploit.com/

Jayson E. Street—http://jayson-street.tumblr.com/

Joanna Rutkowska—http://theinvisiblethings.blogspot.com/

Joe Grand—http://en.wordpress.com/tag/joe-grand/

Joe McCray—http://www.learnsecurityonline.com/

Johnny Long—http://www.hackersforcharity.org/

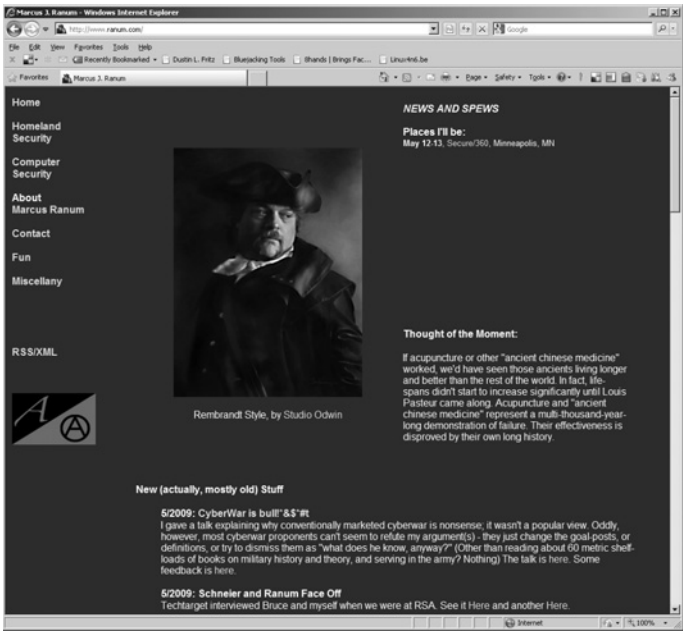
Kevin Mitnick—http://www.kevinmitnick.com/

Kevin Poulsen—http://www.wired.com/

Linus Torvalds—http://torvalds-family.blogspot.com/

Marcus J. Carey—http://blog.marcusjcarey.com/

Marcus J. Ranum—http://www.ranum.com/



Richard Bejtlich—http://taosecurity.blogspot.com/

Richard Stallman—http://www.fsf.org/blogs/rms

Rob Fuller—http://www.room362.com/

Robert Tappan Morris—http://pdos.csail.mit.edu/~rtm/

Ron Gula—http://blog.tenablesecurity.com/

Stephen Wozniak—http://www.woz.org/

Tim Berners-Lee—http://dig.csail.mit.edu/breadcrumbs/blog/4

PODCASTS

PaulDotCom—http://pauldotcom.com/

Securabit—http://securabit.com/

Security Justice—http://securityjustice.com/

BOOKS

For the latest and greatest books on hacking visit http://www.amazon.com/s/ref=nb_ss?url=search-alias%3Dstripbooks&field-keywords=hacking, as seen in Figure 10.6.

FIGURE 10.6

Amazon Web site with keyword "hacking"

CHAPTER

Easter Eggs

11

This is where s0me of the h1dden treasures of the story can be found—for those who don't want to take the t1me t0 figure it 0ut on the1r 0wn! Do you remember when you were a k1d and y0ur parents went 1n the back yard on Easter and h1d s0me c0lorful eggs, some hard bo1led and some that hot p1nk plast1cs c0lor? After they spent a few m1nutes h1ding th0se eggs behind s0me trees and bushes, they told you to go search for them, r1ght? Well, 1n that same sp1r1t, this chapter is very similar. The authors have hidden some Easter eggs within the text for each chapter. Each Easter egg has a very unique back story. Oh, by the way, did you catch the Easter egg in the text above?

FICTIONAL STORY DISSECTED: 3DNF

> He had some information about a small firm in Houston, Texas called 3DNF, Inc. that had been acquired by Data Mining within the last six months (p. 9).

So the company 3DNF was derived from the database normalization technique called third normal form (3NF). 3NF is a normal form used in database normalization. It was originally defined by E.F. Codd in 1971.[1] Codd's definition states that a table is in 3NF if and only if both of the following conditions hold:

1. The relation R (table) is in second normal form (2NF).
2. Every nonprime attribute of R is nontransitively dependent (i.e., directly dependent) on every key of R.

In the field of relational database design, normalization is a systematic way of ensuring that a database structure is suitable for general-purpose querying and free of certain undesirable characteristics—insertion, update, and deletion anomalies—that could lead

[1]Codd, E.F. Further Normalization of the Data Base Relational Model. (Presented at Courant Computer Science Symposia Series 6, "Data Base Systems," New York City, May 24th–25th, 1971.) IBM Research Report RJ909 (August 31st, 1971). Republished in Randall J. Rustin (ed.), Data Base Systems: Courant Computer Science Symposia Series 6. Prentice-Hall, 1972.

to a loss of data integrity.[2] E.F. Codd, the inventor of the relational model, introduced the concept of normalization and what we now know as the first normal form in 1970.

FICTIONAL STORY DISSECTED: The Account Number

> Vlad took a pen and small piece of paper from his coat pocket and wrote "Volksbank, 111-8-18-1-13-15-27-1" from memory (p. 11).

Vlad's Volksbank account number is a derivative of the number used in the Bourne Identity. "A wounded man is found by a village doctor on beach in France. Taking care of the found, the doctor finds a microfilm under the man's skin. Under the microscope, the microfilm shows a Swiss bank account number. Because the man has lost all memory of his life and identity, he decides to go to Switzerland and find out what he can about himself from the account number. We later learn that this man is an American spy called Jason Bourne."[3]

FICTIONAL STORY DISSECTED: Odysseus

> Vlad took Pavel's laptop and looked over the list of files they had just acquired from Stepan's laptop. He didn't have much time, so he sorted the files by "Last Modified Date" and scanned the list. One file caught his eye immediately. It was called "Odysseus.doc" and was last updated just one day before (p. 9).

Odysseus is associated with the Greek story of the Trojan horse. In Greek mythology, the Trojan War was waged against the city of Troy by the Achaeans after Paris of Troy stole Helen from her husband Menelaus, the king of Sparta. The war is among the most important events in Greek mythology and was narrated in many works of Greek literature, including the Iliad and the Odyssey by Homer. The Iliad relates a part of the last year of the siege of Troy, whereas the Odyssey describes the journey home of Odysseus, one of the Achaean leaders. Other parts of the war were told in a cycle of epic poems, which has only survived in fragments. Episodes from the war provided material for Greek tragedy and other works of Greek literature, and for Roman poets like Virgil and Ovid.[4]

[2]Codd, E.F. The Relational Model for Database Management: Version 2. Addison-Wesley (1990), p. 271.
[3]http://swiss-bank-accounts.com/e/fiction/bourne-identity-1988/index.html
[4]Rutter, Jeremy B. "Troy VII and the Historicity of the Trojan War." http://projectsx.dartmouth.edu/classics/history/bronze_age/lessons/les/27.html. Retrieved on July 23, 2007.

FICTIONAL STORY DISSECTED: Thompson

> Thompson had a reputation in the Bureau for bringing together a strong team of more traditional FBI agents and technical talent he had personally recruited from the Air Force (p. 16).

Thompson is the name of Sober K Worm, which was the virus sending out the e-mail with the subject "You visit illegal Web sites. Dear Sir or Madam, we have logged your IP-address on more than 40 illegal Web sites." It was signed "Yours faithfully, Fredrick Thompson." See Figure 11.1 for the actual e-mail with the infected worm attached.

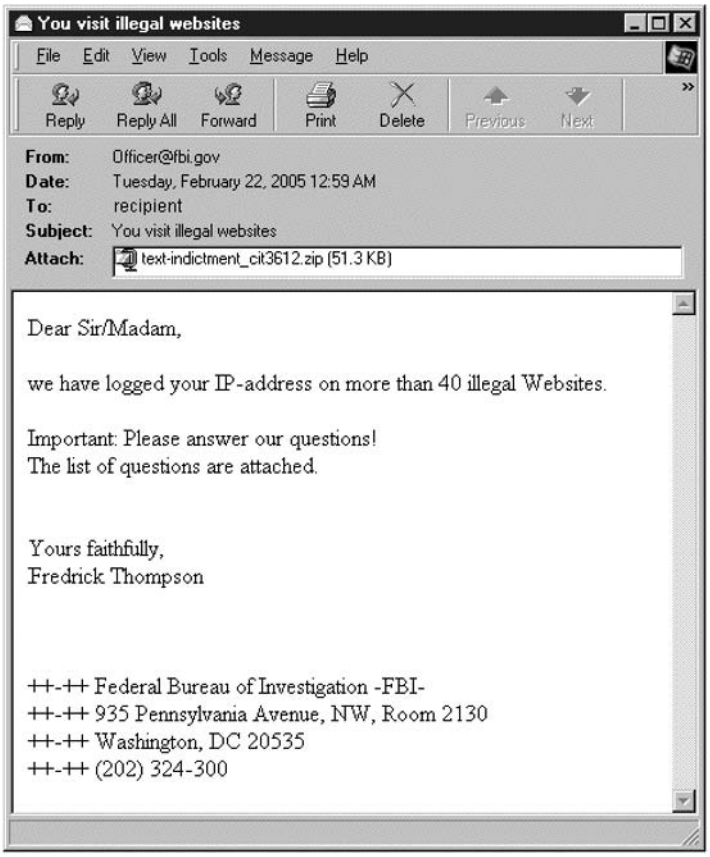


FIGURE 11.1

Sober K Worm e-mail

FICTIONAL STORY DISSECTED: Resol

> Michael Resol is the best target. He is a network admin who has worked at 3DNF for five years (p. 10).

Semordnilap is a name coined for a word or phrase that spells a different word or phrase backwards. In the case of this book, change the spelling of the last name and he calls himself what he is, a "loser."

Another Easter egg is the name Leon. Leon is name derived from the Christmas term NOEL. Spell noel backwards and you get LEON.

A palindrome is a word, phrase, number, or other sequence of units that can be read the same way in either direction (the adjustment of punctuation and spaces between words is generally permitted). Composing literature in palindromes is an example of constrained writing. The characters Hannah and Bob are palindromes because you can read their name backwards and still have the original name hannaH and boB.

FICTIONAL STORY DISSECTED: Falken

> For the uninitiated, Bob Falken's bedroom looked like part-NASA control room and part high-tech junkyard. To Bob, it was both lab and sanctuary—the one place where he was in control of his world (p. 27).

Falken is the name of the artificial intelligence researcher in the movie *WarGames* who created a back door into the War Operation Plan Response (WOPR).

PUBLIC RECORD ON TAP: What is *WarGames?*

During a secret simulation of a nuclear attack, one of two U.S. Air Force officers is unwilling to turn a required key to launch a missile strike. The officer's refusal to perform his duty convinces systems engineers at NORAD that command of missile silos must be maintained through automation, without human intervention. Control is given to a NORAD supercomputer, WOPR, which is programmed to predict possible outcomes of nuclear war.

David Lightman (Matthew Broderick) is a bright but unmotivated Seattle high school student and computer hacker. After receiving a failing grade in school, he uses his IMSAI microcomputer and modem to hack into the district's computer system using an unsecured password. He then changes his grade and does the same for his friend and classmate Jennifer Mack (Ally Sheedy).

After seeing an advertisement for a set of forthcoming computer games, Lightman has his computer dial every number in Sunnyvale, California, in an attempt to find its system. When later

reviewing the results, he finds one of the systems has a very "basic" interface, which he finds intriguing. After trying a few commands, he succeeds in finding a list of games, starting with simple games but then progressing to titles like Theaterwide Biotoxic and Chemical Warfare and Global Thermonuclear War. More intrigued than ever, Lightman continues to try to hack into the system without success.

Lightman enlists the aid of an older hacker, who explains the concept of a backdoor password and suggests tracking down the "Falken" referenced in Falken's Maze, the first game listed. Following this lead, Lightman discovers that Stephen Falken was an early artificial intelligence researcher, and from there tracks down every lead he can find on the man's life. He discovers that Falken had a son, Joshua, and finds that this name can be used to gain access to the unidentified system.

Response at NORAD to Soviet missile launches Unknown to Lightman; the Sunnyvale phone number was cross-connected and is actually connecting him to WOPR in the Cheyenne Mountain military complex. WOPR was originally programmed, in part by Falken, to run simulations on various warfighting scenarios and attempt to find winning strategies. The list of "games" Lightman found was the various scenarios. Lightman glibly starts a game of Global Thermonuclear War, playing as the Soviet Union, selecting Las Vegas and his home town of Seattle as first-strike targets. WOPR starts running a simulation of a missile attack on the NORAD displays, leading the human military attendants to believe that actual Soviet nuclear missiles are inbound.

When they investigate, they determine that WOPR is running a simulation and defuse the situation. The phone line and backdoor password are removed to ensure the event does not reoccur. However, unknown to NORAD, WOPR continues to run the simulation in an attempt to trigger the scenario and win the game. WOPR continuously feeds false data such as Soviet bomber incursions and submarines deployments to the humans at NORAD, goading them into raising the DEFCON level and pushing them toward a retaliation that will start World War III. News of the events leaks out to television, and Lightman learns the true nature of his actions when a news broadcast makes light of the situation later that day. He is soon tracked down and arrested by the FBI and taken to NORAD.

http://en.wikipedia.org/wiki/WarGames

FICTIONAL STORY DISSECTED: Groom Lake

> "I want to try a hack on Groom Lake. Remember when Gary McKinnon was busted for breaking into U.S. government computers from London?" (p. 29).

The location of the famous "Area 51" that the U.S. military used for secret weapons development including the famous F-111 Stealth Fighter and the U-2 might just be the same location where the "Aurora" project is being tested and developed.

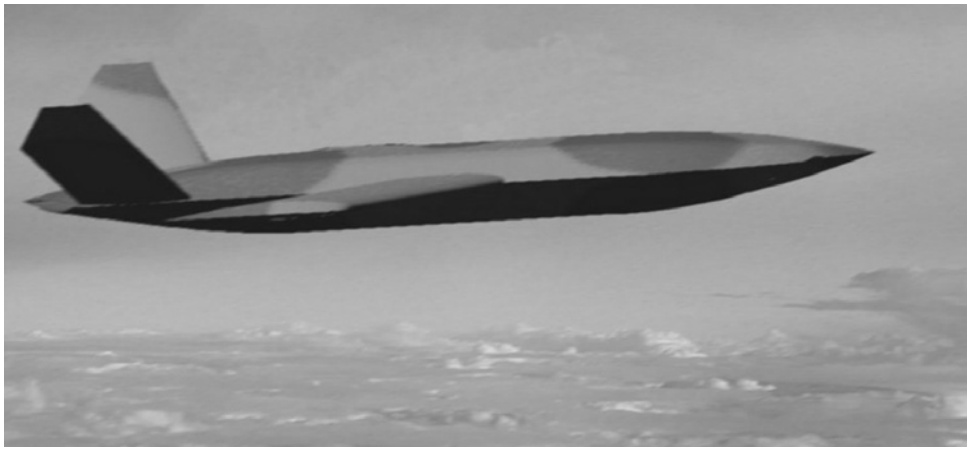


FIGURE 11.2

Aurora

PUBLIC RECORD ON TAP: What is Aurora?

Beginning in the mid-1980s, the Air Force and NASA have supported a number of studies of aircraft that are consistent with accounts of the Aurora project. Although these studies have not been linked to actual development efforts, they provide some insight into the potential configuration and capabilities of Aurora.

In 1985, McDonnell Douglas conducted studies of a Mach 5, 12,000-km range and 305-passenger hypersonic commercial transport (HSCT) powered by regenerative air turboramjet engines. Initial research led to claims that this type of aircraft was not only feasible but remarkably efficient. According to these studies, a ramjet was the best option at Mach 5, and that methane was the preferred fuel. Hydrogen was also considered, but it takes up to five times as much space. If the large HSCT was scaled down to the dimensions of an SR-71, the aircraft could have a range of approximately 10,000 miles with a crew of two and a 1-ton sensor suite.

Lockheed's renowned Skunk Works has been the incubator of several programs that could evolve or could already have evolved, into an SR-71 replacement. Presently, Lockheed engineers are reportedly studying the development of a liquid methane-fueled aircraft that could penetrate enemy airspace to perform reconnaissance missions.

"The sleek aircraft would cruise at Mach 5 (3,350 mph) speed at a maximum altitude of about 100,000 feet. The aircraft would be made primarily of titanium with its outer edges constructed of Inconel, a heat-resistant stainless steel. At Mach 5 speed, the leading edges of the air-frame would glow red above "1000º Fahrenheit." Power for this futuristic airplane would come from four turbo-ramjets. The engines would operate as turbojets at low speeds, but at higher speeds, the compressor and turbine would be overridden, so the engines would operate as ramjets."

Other aircraft designs that would fly between Mach 4 and Mach 8, fueled by hydrocarbon or liquid hydrogen, are also being considered. And in the mid-1980s, Lockheed proposed a Mach 7–8 "transatmospheric vehicle" or TAV as an SR-71 replacement. Intriguingly enough, the name "Aurora" was also used in conjunction with this proposal.

To learn more, visit http://www.fas.org/irp/mystery/aurora.htm and http://accelerationresearch.tripod.com/.

FICTIONAL STORY DISSECTED: CyberBob

"Like anyone would want to watch a couple of unemployed nerds drop CyberBob icons," Leon mumbled as he turned back to his monitor…"Of course." Bob went back to his "T00Lz" folder and clicked on the SuperScan icon. If someone was transferring a file to the .200 box, then there must be other interesting things in that network. This would be a good bonus site for the CyberBob icon. Once the program loaded, Bob started the scan to explore the 10.24.53.x network and see what he could find (p. 40).

He was quickly rewarded with a listing of files and folders. He wasted no time in dragging a copy of the CyberBob icon from his desktop to this new window (p. 41).

"Bob, we weren't there. We got a call that that they found a CyberBob icon file on one of their servers. That sounds like you were planting stuff for the Capture the Flag" (p. 85).

Hannah complied and turned right off of the access road just before the small shop where Bob and Leon had sat just a couple of days before dropping a CyberBob icon for a game. She drove down the street and pulled to the front of an empty three-story office building. It was dark outside, so once she turned off the headlights, they were well obscured by shadows (p. 96).

CyberBob is from the movie *The Net* with Sandra Bullock.

FICTIONAL STORY DISSECTED: Sydney Bristow

"Where is Sydney Bristow when you need her?" (p. 33).

Jennifer Anne Garner Affleck[5] (born April 17, 1972), best known as Jennifer Garner, is an American actress. She is best known for her role as CIA agent Sydney Bristow on the TV show *Alias*, as well as for her roles in the films *Juno; Pearl Harbor; Dude; Where's My Car?, 13 Going on 30, Catch Me if You Can, Daredevil, Elektra, Catch and Release*, and *The Kingdom*.

[5]Garner Changes Her Name to Affleck at Hollywood.com: http://www.hollywood.com/news/Garner_Changes_Her_Name_to_Affleck/3473623

Later in 2001, J. J. Abrams (who produced *Felicity*) approached Garner about starring in a new show he was working on for ABC. Garner auditioned for and was cast in the role of Sydney Bristow in the spy drama *Alias*. The series became a success, and Garner won the award for "Best Actress in a Television Series—Drama" at the January 2002 Golden Globes. *Alias* had just begun a few months beforehand, and Garner won the award with only half the season's episodes aired. The series was successful, concluding in May 2006 after a fifth, abbreviated season (due to Garner's pregnancy, a development that was written into the storyline of the fifth season). Garner's salary for the show began at $45,000 an episode, rising to $150,000 per episode by the series' end. During the show's run, Garner received four consecutive Golden Globe nominations for her lead performance. She also received four consecutive Emmy nominations for "Outstanding Lead Actress in a Drama Series." Garner won the "Actor Award" from the Screen Actors Guild in 2005. In March 2005, Garner directed the fourth-season *Alias* episode, "In Dreams," which aired in May. Garner received producer credit during the series' final season.

http://www.rottentomatoes.com/celebrity/jennifer_garner/biography.php

FICTIONAL STORY DISSECTED: Kimeron

> "They were just bought by Kimeron, a large U.S. defense contractor" (p. 37).

Kimeron was taken from the film *Mission: Impossible II* (M:i-2), where a Russian scientist is forced to create a deadly bioweapon called "Chimera."

PUBLIC RECORD ON TAP: Chimera Film and Mythology

Inside M:i-2

Although working at Biocyte, an Australian company, Nekhorvich, a Russian scientist, is forced to develop a deadly bioweapon named "Chimera" that lies dormant in its host for 20 h after infection, but then it rapidly causes the body's red blood cells to disintegrate and cause hemorrhaging and death while becoming highly infectious. At the same time, Nekhorvich has developed a potent counteragent "Bellerophon" to stop the effects of Chimera while in incubation. Nekhorvich realizes he must expose Biocyte's research and contacts his old friend Ethan Hunt, whom he refers to as "Dmitri," to help assist him to reach the U.S. Government; in order to transfer Chimera, Nekhorvich uses his own body as a petri dish and makes sure he can reach the United States within 20 h of departure to ensure he's in time to administer Bellerophon. However, as he and Hunt cross the Rocky Mountains on a passenger plane, the captain—Hugh Stamp—claims that there is a drop in cabin pressure and releases the oxygen masks, and the rest of the crew and passengers are anesthetized due to an NO_2 tank being supplemented to the oxygen mask air supply, and "Hun" reveals himself to be Sean Ambrose, another IMF agent, who then breaks Nekhorvichs' neck and takes the briefcase containing his

research. Ambrose and the rest of his team jump from the plane before it crashes, killing all those aboard.

freeonlinehindimovie.blogspot.com/.../mission-impossible-2m-i-2-hollywood.html

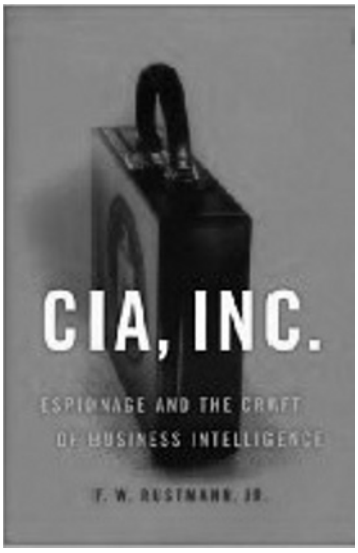
FIGURE 11.3

"Chimera of Arezzo," an Etruscan bronze piece—period 400 B.C., found in Arezzo, an ancient Etruscan and Roman city in Tuscany.

Mythology of Chimera

In Greek mythology, the Chimera (Greek Χίμαιρα (Chímaira); Latin Chimaera) was a monstrous fire-breathing creature of Lycia in Asia Minor, composed of the parts of multiple animals: upon the body of a lioness with a tail that terminated in a snake's head and the head of a goat arose on her back at the center of her spine. The Chimera was one of the offspring of Typhon and Echidna and a sibling of such monsters as Cerberus and the Lernaean Hydra. The term Chimera has also come to mean, more generally, an impossible or foolish fantasy. Figure 11.3 is a statue of Chimera from 400 B.C.

BOOKS



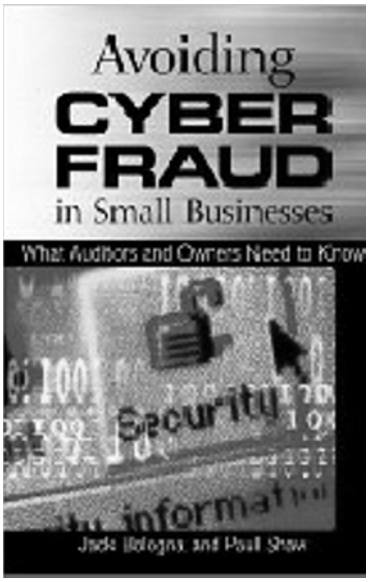
CIA, Inc: Espionage and the Craft of Business Intelligence

By F.W. Rustmann

Publisher: Brassey's Inc.

ISBN-10: 1574883887

ISBN-13: 978-1574883886



Avoiding Cyber Fraud in Small Businesses: What Auditors and Owners Need to Know

By Jack Bologna and Paul Shaw

Publisher: Wiley

ISBN-10: 0471372978

ISBN-13: 978-0471372974

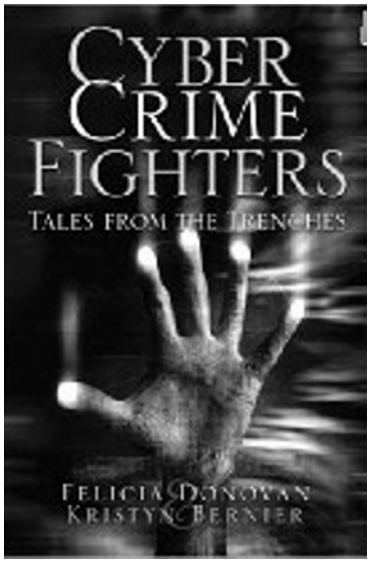
Phishing Exposed

By Lance James

Publisher: Syngress; 1st edition (January 20, 2006)

ISBN-10: 159749030X

ISBN-13: 978-1597490306



Cyber Crime Fighters: Tales from the Trenches
By Felicia Donovan and Kristyn Bernier
Publisher: Que
ISBN-10: 0789739224
ISBN-13: 978-0789739223

EASTER EGG NOT FOUND

Oh yeah, if you are still looking for the Easter egg on p. 42 it doesn't exist.

This page intentionally left blank

CHAPTER

Miscellaneous 12

In this chapter, we will discuss some of the miscellaneous technical topics and situations from the fictional story such as Perverted Justice, malicious credit card hackers, virtual worlds communication, InfraGard, vehicles and Wi-Fi, and bumping locks.

FICTIONAL STORY DISSECTED: Perverted Justice

> We got a tip from Perverted Justice. They're today's online version of the Guardian Angels from the 1970s. They got into a discussion with this pervert in a chat room. He claimed he had some "content" that he had personally created, and they talked him into giving a sample. When they got that, they called us. Jamison had given Perverted Justice a Yahoo! e-mail account (p. 18).

Mark and Chris are talking about how they used a nonprofit foundation called Perverted Justice to catch cyber criminals. Figure 12.1 has a screen shot of their Web site. Perverted Justice Foundation, Inc.,[1,2] more commonly known as Perverted-Justice (also known as PeeJ), is a California-based nonprofit organization that investigates, identifies, and publicizes adults who solicit online sexual conversations with adults posing as children. Perverted-Justice's methods are controversial, and a number of critics have labeled these actions harassment.[3] Perverted-Justice consists of volunteers who carry out sting operations by posing as 10- to 15-year-old minors on chat sites and waiting for adults to approach them. After obtaining identifying

[1]http://kepler.sos.ca.gov/corpdata/ShowAllList?QueryCorpNumber=C2928198

[2]http://www.pjfi.org/

[3]http://www.dallasnews.com/sharedcontent/dws/news/city/collin/stories/091006dnmetpervertedjustice.347ae52.html; http://www.yaledailynews.com/articles/view/20326; http://abcnews.go.com/US/story?id=260587&page=2; http://www.rickross.com/reference/perverted_justice/perverted_justice13.html; http://www.ethicsscoreboard.com/list/dateline.html;http://www.rollingstone.com/news/story/15723886/to_catch_a_predator_is_nbcs_primetime_dragnet_the_new_american_witch_hunt/3

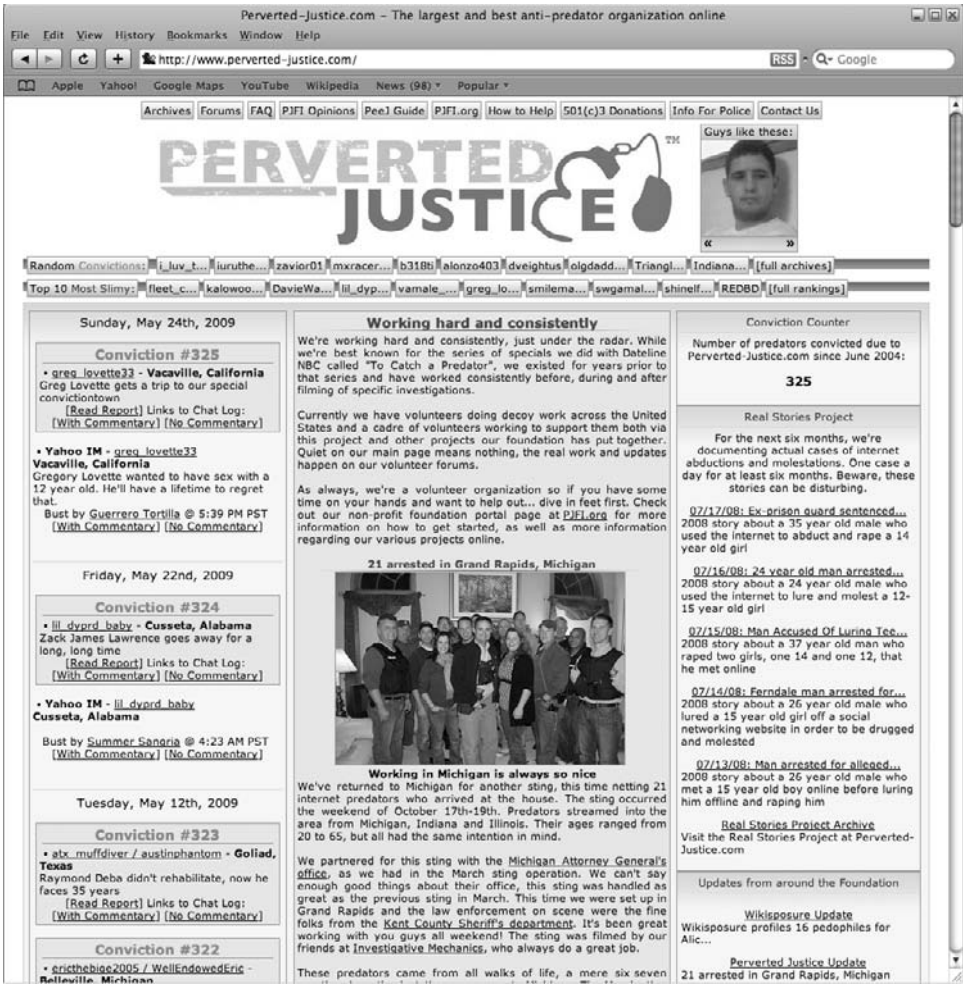


FIGURE 12.1

Perverted Justice Web site

information from these men, who may offer their telephone numbers and other details so that meetings can be arranged, the organization passes the information on to law-enforcement.[4] Perverted-Justice has attracted media attention, both laudatory and critical, as a result of their collaboration with Dateline NBC on a series of televised sting operations called "To Catch a Predator."

[4]http://www.perverted-justice.com/

Perverted-Justice also operates a site that targets groups and individuals it identifies as being involved in the pedophile activist community,[5] a site that provides information to abuse victims on their legal recourse,[6] a site that gives advice to children and teenagers on dealing with grooming on the Internet,[7] and a site that targets organizations that Perverted-Justice believes allow pedophile activists to use their services.[8] The foundation also offers free online training to law enforcement officers[9] and has an intern program for college students.[10]

FICTIONAL STORY DISSECTED: Plausible Deniability (Legal Defense)

> "Why would you want to have all of the 2600 hackers pounding on your network? Are you setting up a honeypot to track someone?"
>
> "No. I need plausible deniability," Bob responded. "And don't you ever tell anyone I said that."
>
> "You need plausible deniability for what?"
>
> "I want to try a hack on Groom Lake. Remember when Gary McKinnon was busted for breaking into U.S. government computers from London? (p. 29)

Bob is really interested in hacking into Groom Lake, also known as Area 51. Area 51 is a nickname for a military base that is located in the southern portion of Nevada in the western United States (83 miles north-northwest of downtown Las Vegas). Situated at its center, on the southern shore of Groom Lake is a large secretive military airfield. The base's primary purpose is to support development and testing of experimental aircraft and weapons systems.[11] Turn to Chapter 11 to read more about Groom Lake.

Bob wants to have plausible deniability when he hacks into Groom Lake; if authorities somehow catch him and they investigate his home computers and networks, they will discover that other hackers gained access and thereby nullify any creditable evidence they might have found—they cannot attribute it to Bob because other hackers were in his home computers and network.

[5]http://www.wikisposure.com/Main_Page
[6]http://www.resourceforarecourse.com/
[7]http://www.howtodealwithcreepypeople.com/
[8]http://www.corporatesexoffenders.com/
[9]http://www.pjfi.org/?pg=academy
[10]http://www.pjfi.org/?pg=internship
[11]Peter W. Merlin; DREAMLAND: Fifty Years of Secret Flight Testing in Nevada; http://www.dreamlandresort.com/area51/dreamland_50years.html

FICTIONAL STORY DISSECTED: IRC Carders

> Leon quickly had a window open on Bob's computer that displayed the desktop of the computer in the target house. He browsed through several different directories and soon had a cached copy of the password used for an online brokerage account. A quick browser session confirmed that the password worked, and there was enough money in the account for their needs.
>
> Next Leon opened an IRC session and was quickly logged into a carder site.
>
> `I need a quick cash out. $10K guaranteed 30/70 split. No rippers. No Nigerians` (p. 54).

Carder is a term to identify people who illegally obtain credit card numbers and other private and personal information. Many "carders" use instant messaging software like the Internet Chat Relay (IRC) program to meet other "carders" to resell and exchange credit card numbers for cash or goods. Figure 12.2 has a screen shot of such activity.

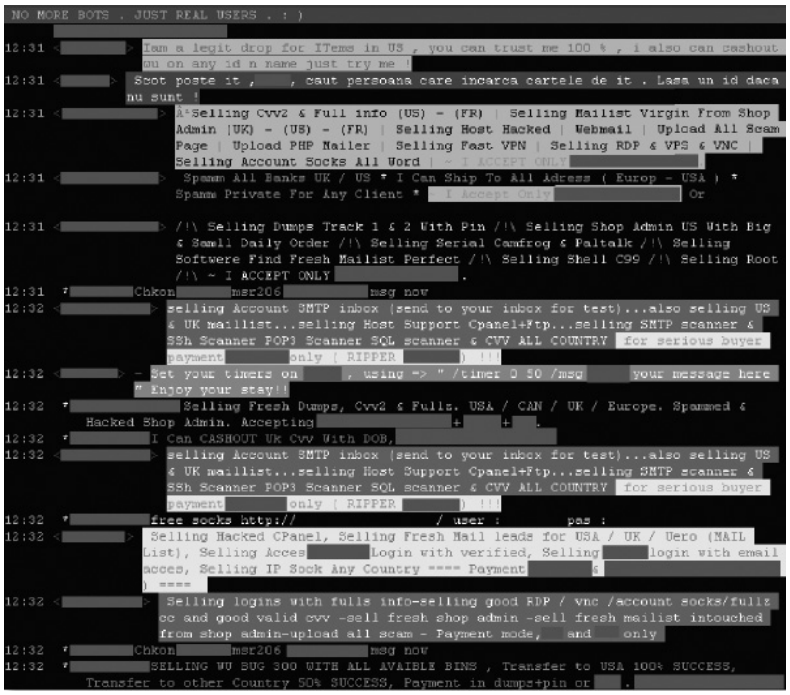


FIGURE 12.2

Screen shot of IRC discussion between people buying and selling tools for cybercrime. Credit: Symantec.

Bob watches Leon as he posts a message to those in the chat channel asking for some help getting money using someone else's credit card information. The two "Public Record on Tap" sections describe the real world threat.

PUBLIC RECORD ON TAP: Credit Card Scam

Arrests Made in Credit Card Scam

From The Garden City News on May 29, 2009

The Garden City Police report the arrest of four Queens residents for a credit card scam involving the encoding of credit cards. On Monday May 18, Garden City detectives were contacted by Sears Loss prevention of a possible credit fraud. Sears investigators stated that two subjects entered the Garden City Sears and purchased several thousands of dollars of electronics equipment paying for them with a credit card. However, the account number on the card did not match the account number on the receipt.

Further investigation by GCPD Detectives revealed that several other purchases were made in the past using encoded cards. Also, the subjects had purchased a large flat screen TV but had not picked it up yet. Two subjects were identified and the vehicle they were using was located. A surveillance of the location was initiated. The merchandise pickup account for the TV was also monitored.

On Thursday, May 21, four subjects were observed arriving at the Sears merchandise pick up area requesting the large screen TV. After a brief investigation at the scene they were placed under arrest. The subjects were found in possession of nine fraudulently encoded cards. Also an encoding machine was recovered from one subject's home.

The investigation revealed that one subject had purchased a credit card encoder from the Internet. This is a machine that adds account information to the magnetic stripe on the rear of a credit card. He then purchased account information which is referred to as "dumps." These dumps are a 37-digit number, which contain account information of unsuspecting victims. They are illegally obtained and sold on the Internet.

Using a computer and special program, the subject would then take a credit card which was issued in his own name and change the magnetic stripe to a "dump." When the subject made a purchase and was asked for identification from the cashier, the information on the face of the credit card would match the information on the corresponding ID. However, when swiped the magnetic stripe would contain the information of an identity theft victim who would then be charged for the merchandise.

The subjects were charged with 18 counts of Grand Larceny, Criminal Possession of Forged Instruments, and Identity Theft. At this time, the total loss is valued in excess of $17,000. They were processed and held pending arraignment in First District Court. The investigation is continuing.

To read more, visit: http://www.gcnews.com/news/2009/0529/Front_page/004.html

PUBLIC RECORD ON TAP: Carders

Carders Using Secure IM to Thwart Law Enforcement

Article from WyldRyde on April 1, 2007

Carders are finally moving away from using Internet Relay Chat. Carders illegally obtain credit card numbers and other private and personal information and have used IRC to meet and resell the data they obtained in exchange for cash or goods.

Now, they've created their own encrypted IM program called, CarderIM. This program reportedly prevents law enforcement from monitoring the carder's unsecured IRC channels. WyldRyde has never permitted carder channels and reports all illegal activities such as this to authorities.

FICTIONAL STORY DISSECTED: MPORPG for Communications Channel

He looked over his shoulder and watched as Bob loaded World of Warcraft. Soon his character was running down a stone road in the middle of a dark forest. There was no one around, but occasionally there was movement off to either side. Bob ignored the motion and kept running like he was on a mission.

"I thought we came here so you could get some help from Max," Leon asked as he pulled a chair up next to Bob.

"We did, and that's exactly what I'm about to do."

"It looks to me like you're playing a game when you ought to be making a phone call."

Bob didn't take his eyes off the laptop. "There's no way I'd call him. This has to be done out of band" (p. 61).

Here Bob uses a game called World of Warcraft (WoW) to talk with Max in secret. This is one method of obscuring or hiding communications that you do not want anyone else to capture. Figure 12.3 shows Bob's WoW character running down stairs and going through a spinning blue light. Figure 12.4 shows Bob after he passed through the spinning blue light and entered the instance. Figure 12.5 is a screen shot of another gaming platform similar to the virtual reality world of WoW where you can create a character and talk to other characters in the game using the keyboard as if you were sending an instant message. In There.com, just as WoW, you can go off into far places where no other characters are at and talk privately. The only way someone can see your speech in these types of games is if they are nearby. Bob knows this and this is one reason why he took his WoW character far into the depths of the cathedral

FIGURE 12.3

Bob entering Instance Server

FIGURE 12.4

Bob's character after entering Instance Server

FIGURE 12.5

Virtual World program called There.com

catacombs to talk with Max's character. This is why he took his WoW character into the instance to talk with Max's WoW character.

World of Warcraft, often referred to as WoW, is a massively multiplayer online role-playing game (MMORPG) by Blizzard Entertainment. As with other MMORPGs, players control a character avatar within a game world in third person view (with the option of playing in first person), exploring the landscape, fighting various monsters, completing quests, and interacting with NPCs or other players. In common with many other MMORPGs, WoW requires the player to pay for a subscription, either by buying game cards for a preselected amount of playing time, or using a credit or debit card to pay on a regular basis.[12] To enter the game, the player must select a realm (or server). Each realm acts as an individual copy of the game world, and falls into one of four rule-set categories. Realms are either player versus player (PvP), where open combat among players is more common, or player versus environment (PvE), where the focus is more focused on defeating monsters and completing quests; roleplay (RP) variants of both realm types are also available. On a PvP or RP-PvP server, a player may create characters belonging to either the Horde or the Alliance factions, but not both. Realms are also categorized by language, with in-game support in the

[12]http://www.gamespot.com/pc/rpg/worldofwarcraft/review.html

FIGURE 12.6

Second Life virtual worlds

language available.[13] Players can move established characters between realms for a fee.[14] Then, the player may either select one of their previously made characters or create a new one.

Another similar program to There.com and WoW is Second Life (SL). Figure 12.6 is a screen shot of President Obama's campaign headquarters in SL. SL is a virtual world developed by Linden Lab that launched on June 23, 2003 and is accessible via the Internet. A free client program called the Second Life Viewer enables its users, called Residents, to interact with each other through avatars. Residents can explore, meet other residents, socialize, participate in individual and group activities, and create and trade virtual property and services with one another, or travel throughout the world, which residents refer to as the grid. SL caters to users aged 18 and over, while its sister site, Teen Second Life, is for younger users.

Built into the software is a three-dimensional modeling tool based around simple geometric shapes that allows a resident to build virtual objects. This can be used in combination with the Linden Scripting Language that can be used to add functionality to objects. More complex three-dimensional sculpted prims (colloquially known as sculpties), textures for clothing or other objects, and animations and gestures can be created using external software. The Second Life Terms of Service ensure that users retain copyright for any content they create, and the server and client provide simple digital rights management functions.

[13]http://www.worldofwarcraft.com/info/basics/realmtypes.html
[14]http://www.gamespot.com/pc/rpg/worldofwarcraft/news.html?sid=6153338&mode=news

PUBLIC RECORD ON TAP: WoW has Terrorists!

Government to Seek Terrorists in World of Warcraft: The Full Proposal

By Ryan Singel on April 10, 2008 from Wired.com

Loyal readers might remember that the government's spooks are working on software that can spot terrorists lurking in massive, multiplayer games, something it dubs the Reynard Project. THREAT LEVEL just got a copy of the November 2007 proposal for the cutting edge project from the Intelligence Advanced Research Projects Activity (IARPA). In it, Dr. Rita Bush and Kenneth Kisiel from IARPA's Disruptive Technology Office cite the current advantages of terrorism in the online world—anonymity, covert communication channels, and the ease of information warfare as reason to start studying multiplayer games and virtual worlds like Second Life and World of Warcraft.

FIGURE 12.7

The proposal opens with a scenario of what would happen if the nation's intelligence community failed to get a head start: I had been following the recruiter through this virtual world for several weeks now and was finally able to catch him in the act of soliciting a new recruit. It took some quick thinking and shape shifting but I was able to follow the new recruit to a primitive training island and watched while he was given some rudimentary instructions. In the meantime, I relayed this new information back to the Intelligence Analysis Center and requested background information on the new recruit.

As I watched the team approach the gate, the requested information appeared in floating billboards (that only I could see) next to each soldier. The information was not good. I have once again been investigating kids who have been trying unsuccessfully for many months to get into this base when I should have been looking for actual terrorists. There has to be a better way of telling them apart. The rest of the proposal describes the history of online gaming and virtual worlds, describes cyber terrorism as the imminent apocalypse and then speculates on how terrorists will soon be using virtual worlds to train for terrorism in the real world.

That's why Reynard Project is necessary: The virtual world is rapidly evolving into a close representation of the real world with all the opportunities and consequences of the real world. However, there may be many things possible in the virtual world that can't be done in the real world. Our challenge is to figure out what these actions are before our adversaries. To do this, we need to be able to recognize the behavior of a real threat and exploit the information that is available to us in the virtual world. As our adversaries continue to expand their presence and use of virtual environments, we need to keep pace and possibly leapfrog their abilities; else, we will miss the indicators for the next attack. To read more, visit http://www.wired.com/threatlevel/2008/04/government-to-s/.

FICTIONAL STORY DISSECTED: InfraGard

> "Hey, uh hello. This is Jonathan Tao at 3DNF. We met at the InfraGard meeting a couple of weeks ago" (p. 65).

InfraGard is a United States Federal Bureau of Investigation (FBI) public–private partnership that began in the Cleveland, Ohio, Field Office in 1996. It was a local effort to gain support from the information technology industry and academia for the FBI's investigative efforts in the cyber arena. The program expanded to other FBI Field Offices, and in 1998 the FBI assigned national program responsibility for InfraGard to the former National Infrastructure Protection Center (NIPC) directed by RADM James B. Plehal USNR and to the FBI's Cyber Division in 2003.

Since 2003, InfraGard Alliances and the FBI said that they have developed a TRUST-based public–private sector partnership to ensure reliability and integrity of information exchanged about various terrorism, intelligence, criminal, and security matters. It supports FBI priorities in the areas of counterterrorism, foreign

FIGURE 12.8

InfraGard's Web site

counterintelligence, and cybercrime. Figure 12.8 shows InfraGard's Web site. Just as InfraGard, the Information Systems Security Association is a great place to network with the security community. Figure 12.9 shows a screen shot of their Web site.

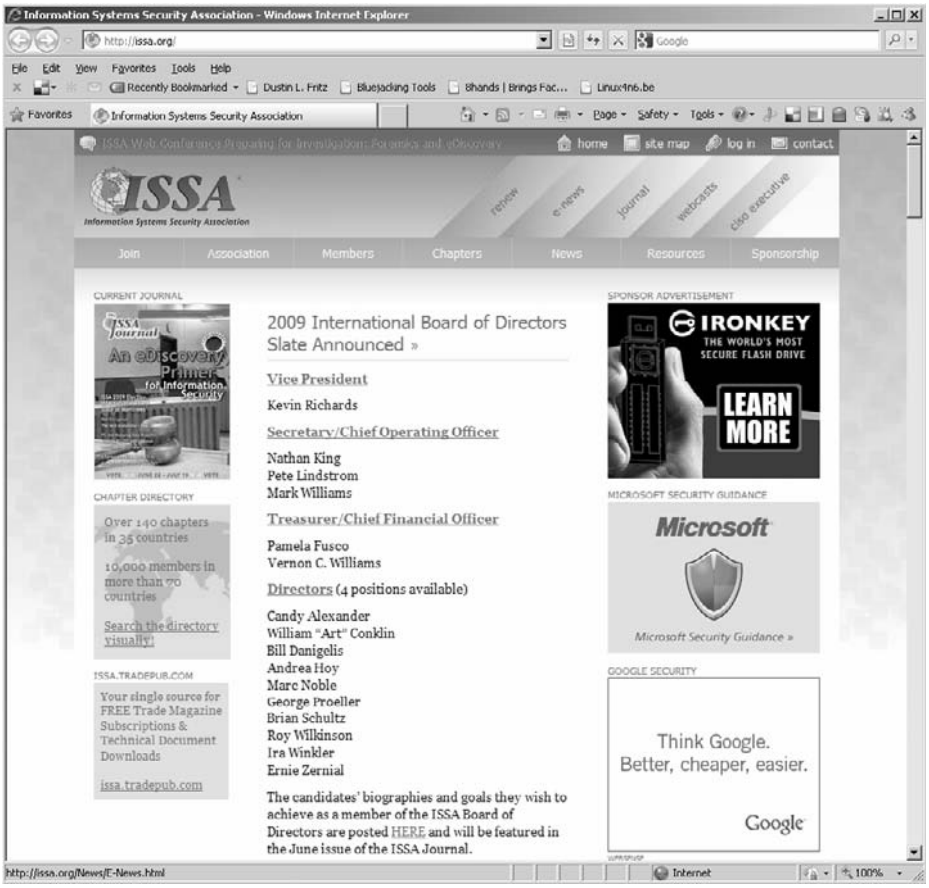


FIGURE 12.9

Information System Security Association (ISSA) Web site

FICTIONAL STORY DISSECTED: Police Car APs

Bob had his iPaq running WiFiFoFum. The software gave him a radar-like display of wireless access points in the area.

"We're clear so far—no cops in this part of the garage." Bob leaned over and showed the display to Leon. A single dot appeared near the edge of the screen.

> Leon understood. The display showed sources of wireless network signals and estimated their distance. The Houston police department, like a few others around the country, had begun using wireless signals between their squad cars and repeater stations set on traffic signals. The resulting network gave them a high-speed data link back to their headquarters, so they could retrieve datalike lookups on license plates or pull up videos on certain public area surveillance cameras. The problem with the system was that they hadn't considered how easy it was to detect the wireless signal. Even though it was encrypted, it still warned of their presence. Even when they went on silent runs, they were emitting a Wi-Fi networking signal (p. 84).

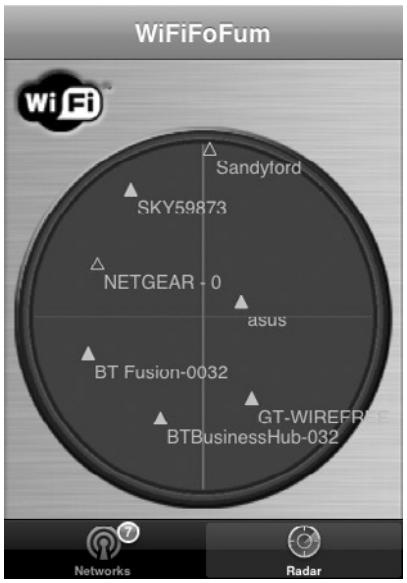


FIGURE 12.10
WiFiFoFum for the Apple iPhone

Since the local police departments are now using Wi-Fi, people like Bob can track them when they are nearby. Bob uses a very simple program called WiFiFoFum, as shown in Figure 12.10 to track Wi-Fi signals in the area. This technology is not new and many company's like Chrysler have enabled civilian vehicles for becoming Wi-Fi capable, as shown in Figure 12.11.

FIGURE 12.11
Chrysler car turns into Wi-Fi hotspot

PUBLIC RECORD ON TAP: CHP and Wi-Fi

Metro-Scale Wi-Fi for San Mateo Police Department

By Tropos Networks Inc.

Scenario

FIGURE 12.12

The California Highway Patrol (CHP) is engaged in a high-speed pursuit along Highway 101, a major north/south corridor in the San Francisco Bay Area. The pursued vehicle, attempting to evade capture, exits the highway in San Mateo, California. In the congested traffic of this Silicon Valley city with a population of over 90,000, the perpetrator quickly realizes he will not be able to outrun or outmaneuver the law enforcement presence behind him. He hastily abandons his vehicle and flees on foot, hoping to quickly disappear among the many pedestrians in the downtown shopping district.

In most cities and suburbs, this is where the story would have ended. The perpetrator would have eluded his pursuers and moved on anonymously, working on his alibi, possibly reporting the car stolen and absolving himself of any responsibility for the pursuit. Unfortunately for this runner, he didn't exit the highway in just any city. He tried to make his break in San Mateo. The police in this city have in-vehicle laptop computers equipped with broadband Wi-Fi data access, which provides patrol officers unprecedented access to high-bandwidth, data and applications once only accessible at a headquarters location.

Directly after the vehicular pursuit ended, a San Mateo Police Department (SMPD) vehicle arrived on scene to assist the CHP. An immediate inquiry to the state's Department of Motor Vehicle (DMV) records using the Wi-Fi-enabled in-vehicle computer provided the officers with information on the vehicle's registered owner, including a high-resolution driver's license photo and fingerprints. Previously, this information would have been unavailable to field officers limited by low-bandwdith mobile data radio and cellular data technologies. With Wi-Fi, the pursuing CHP officer instantly provided a positive identification that the driver of the pursued vehicle was in fact the registered owner. The SMPD officer then quickly broadcasts this photo information to all other SMPD vehicles in the Wi-Fi coverage area. As a result of an identification made from the DMV photo, the perpetrator was apprehended in less than 10 minutes after the pursuit ended.

Deployment

The metro-scale Wi-Fi mesh network infrastructure from Tropos Networks delivered to the SMPD officers a true carrier-class broadband solution quickly and economically. Data rates of 1–5 Mbps are consistently delivered to the SMPD vehicles throughout the Wi-Fi coverage area.

The SMPD, already equipped with Panasonic Toughbooks in their patrol cars and PDAs for motorcycle and bicycle patrols, needed no client device modification or equipment addition to provide all officers access to the network. The Tropos solution is based on the 802.11b standard, allowing client access via any standard 802.11b/g client card. This fact alone saved the department significant dollars as they were not forced to perform hardware upgrades on the client devices in any of their 35 patrol cars or the additional client devices used by the more than 110 police officers.

FIGURE 12.13

The Tropos 5320 outdoor MetroMeh router

The Tropos 5320 Wi-Fi router is built for outdoor use, with extreme temperature, high wind, and lightning strike survivability. Additionally, the Tropos 5320 is specially designed for mounting on municipally owned street lamps, and can utilize the various power options available on these structures. The unit can be installed by a city worker in a bucket or lift truck in under 15 minutes and does not require any specific technology training for installers. The Tropos 5320 Wi-Fi routers, once connected to power (usually taken from the photocell socket), are self-discovering and self-configuring, instantly extending the network range upon power-up.

Because of Tropos' Predictive Wireless Routing Protocol (PWRP), over 80% traditional wired backhaul is eliminated and replaced with a scalable wireless metro-scale Wi-Fi mesh network PWRP also ensures maximum bandwidth to each user and dynamically routes around interference and failures seamless to end-users. The result is a true broadband (>1Mbps) network with superb coverage outdoors. In addition, PWRP enables fast network deployment. In general, a city-wide network can be deployed in under 30 days with relatively little maintenance required thereafter.

To read more, visit: http://www.tropos.com/pdf/case_studies/tropos_casestudy_smpd.pdf.

FICTIONAL STORY DISSECTED: Lock Bumping

> Bob knelt on one knee and began to rummage through his backpack. "I've been playing with bumping locks and I'm getting pretty good at it" (p. 97).

Being a hacker like Bob, you have to not only know how to hack computers and networks but also locks on doors. Bob uses a technique called "lock bumping." Lock-bumping is a lock-picking technique for opening a pin tumbler lock using a

specially-crafted bump key, as shown in Figure 12.14. One bump key, will work for all locks of the same type. For detailed key and lock nomenclature, see Figure 12.15.

When bumping a lock, the key is initially inserted into the keyway one notch (pin) short of full insertion. Bumping the key inward forces it deeper into the keyway. The specially-designed teeth of the bump key transmit a slight impact force to all of the bottom pins in the lock. The key pins transmit this force to the driver pins; the key pins stay in place. This physics action can be visualized by observing the same effect on the desktop toy: Newton's Cradle. Because the pin movements are highly elastic, the driver pins "jump" from the key pins for a fraction of a second, moving higher than the cylinder (shear line of the tumbler), then are pushed normally back by the spring to sit against the key pins once again. Even though this separation only lasts a split second, if a light rotational force is continuously applied to the key during the slight impact, the cylinder will turn during the short separation time of the key and driver pins, and the lock can be opened while the driver pins are elevated above the keyway. Lock bumping takes only an instant to open the lock. The lock is not damaged in any way. Certain clicking and vibrating tools designed for bumping can also be used. These allow for rapid repetition of bumping against locks that have advertised "bump proof" features. Only a rare, few key-pin locks cannot be bumped. Electronic locks that have a key backup are obviously completely susceptible to this method.

FIGURE 12.14

Bump key

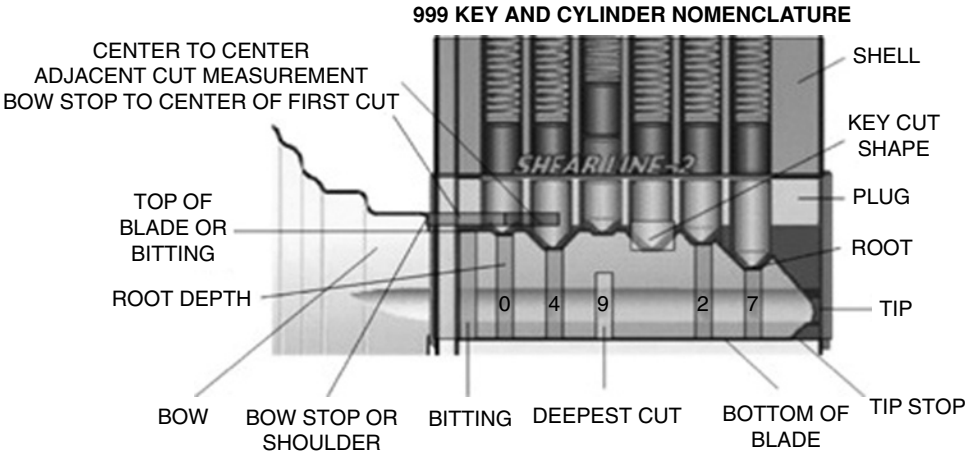


FIGURE 12.15

Key and Lock terms

PUBLIC RECORD ON TAP: Locked, But Not Secure

The Lockdown: Locked, but not secure (Part I)

The Bump Key: A new old threat to the security of mechanical locks

By Marc Weber Tobias, posted Aug 24th 2006

The most popular locking mechanism in the world utilizes the pin tumbler design, first developed 4000 years ago in Egypt and then rediscovered and perfected a century and a half ago by Linus Yale. There are billions of these locks in the world and they come in all sizes, configurations, and security ratings. Some are secure; most are not, and even some high-security rated cylinders can be easily compromised. All that is required to open many times of pin tumbler cylinders—the kind of lock that probably keeps the bad guys out of your home—is a bump key and a tool for creating a bit of force. The bump key shown above opens an extremely popular five pin lock, and the plastic bumping tool is produced by Peterson manufacturing, although many others are now being offered for sale. With these two cheap implements, anyone—and I do mean anyone—can get into your home or business in a matter of seconds.

In 2004, this relatively old technique of opening locks was rediscovered by the European locksmith community in Germany and other countries. As the word spread as to the ease with which certain locks could be bypassed, several sports lock picking clubs and notably the members of TOOOL began to examine the issue more closely. Subsequently, tests were conducted by the prestigious consumer research organization in the Netherlands in 2006 and published last March. In early April, we issued a security alert on security.org with regard to the vulnerability of United States Postal Service and Mail Boxes Etc. locks. Two White Papers were also posted, dealing with the security threat and legal issues involving bumping: A detailed technical analysis of bumping and Bumping of Locks: Legal issues in the United States.

To view a video of lock bumping, visit:
http://www.engadget.com/videos/lockdown/lockdown_defcon.wmv

To read more, visit:
http://www.engadget.com/2006/08/24/the-lockdown-locked-but-not-secure-part-i/

FICTIONAL STORY DISSECTED: 36 Stratagems

> "A hacker doesn't care about traffic that's forbidden. Systems are configured to block out what administrators think is bad. But a hacker knows the only interesting traffic is trusted traffic. If you can abuse a trust, you can own a network. Funny how this is just more of what you can read about in ancient Chinese war texts" (p. 42).

The Chinese war text that Bob is referring to is the 36 Stratagems (traditional Chinese: 三十六計; simplified Chinese: 三十六; pinyin: Sānshíliù Jì), which is a Chinese essay used to illustrate a series of stratagems used in politics, war, as well as in civil interaction, often through unorthodox or deceptive means. They were first published in the Western world by the Swiss scholar Harro von Senger after he heard the Chinese proverb, "If all else fails, retreat" at Taipei University.[15] The Stratagems are often misnamed as strategies; however, stratagem (synonymous with ruse) has nothing to do with strategy (being a long-term plan or outline).

PUBLIC RECORD ON TAP: The 36 Stratagems

China's 36 stratagems

By Yang Jiaqing from Beijing Review

According to the treatise *36 Stratagems: The Secret Book of the Art of War* (Sanshiliu Ji: Miben Bingfa) from circa AD 1500

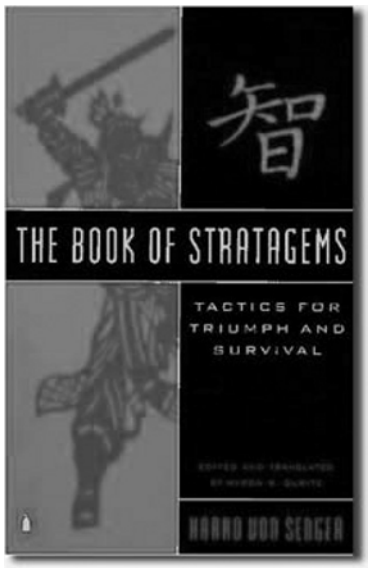


FIGURE 12.16

1. Deceiving the emperor [by inviting him to a house by the sea that is really a disguised ship] and [thus cause him to] cross the sea
2. Besieging [the undefended capital of the country of] Wei to rescue Zhao [the country that has been attacked by the Wei forces]
3. Killing with a borrowed knife
4. Awaiting at one's ease the exhausted enemy
5. Taking advantage of a fire to commit robbery
6. Clamor in the east, attack in the west
7. Creating something out of nothing
8. Openly repairing the [burned wooden] walkway, in secret [before completing the repairs] marching to Chencang [to attack the enemy]
9. Observing the fire burning on the opposite shore [seemingly uninvolved]
10. Hiding the dagger behind a smile

[15]Harro von Senger and His 36 Stratagems: http://www.bjreview.com.cn/exclusive/txt/2006-12/21/content_51557.htm

11. Letting the plum tree wither in place of the preach tree

12. [Quick-wittedly] leading away the sheep [that unexpectedly crosses one's path]

13. Beating the grass to startle the snakes

14. Borrowing a corpse for the soul's return

15. Luring the tiger down from the mountain [onto the plain]

16. If one wishes to catch something, one has first to let it go

17. Tossing out a brick to attract jade

18. Catching the bandits by first catching the ringleader

19. Removing the firewood from under the cauldron

20. Clouding the water to catch the fish [robbed of their clear sight]

21. The cicada casts off its skin of gleaming gold

22. Shutting the door to capture the thief

23. Befriending a distant enemy to attack an enemy nearby

24. Borrowing a route [through the country of Yu] for an attack against [its neighboring country of] Guo [in order to capture Yu after the conquest of Guo]

25. Stealing the beams and replacing the pillars [change on the inside, while leaving the façade of the house unchanged]

26. Cursing the acacia, [while] pointing at the mulberry tree

27. Feigning madness without losing the balance

28. Removing the ladder after [the opponent] has climbed onto the roof

29. Decorating a [barren] tree with [artificial] flowers

30. Turning [the role of] the guest into [that of] the host

31. The stratagem of the beautiful man/woman

32. The stratagem of opening the gates [of a city that is unprepared for self-defense]

33. The special agent stratagem/the stratagem of sowing discord

34. The stratagem of the suffering flesh

35. The linking stratagem/stratagem-linking

36. [When the situation is growing hopeless] running away [in good time] is the best stratagem

To read more, visit http://www.bjreview.com.cn/exclusive/txt/2006-12/21/content_51557.html

PUBLIC RECORD ON TAP: Sun Tzu

Sun Tzu (traditional Chinese: 孫子; simplified Chinese: 孙子.

Sun is his family name, and Tzu is an honorific in classic Chinese, roughly equivalent to Sir, or the Learned Gentleman. His given name is Wu (武). His style name is Changqing (長卿).Sun Tzu is traditionally believed to be the author of *The Art of War*, sometimes called the *Sun Tzu*, an influential ancient Chinese book on military strategy considered to be a prime example of Taoist strategy. Sun has had a significant impact on Chinese and Asian history and culture, both as an author of the *Art of War* and as a legendary figure. During the 19th and 20th centuries, Sun's *The Art of War* grew in popularity and saw practical use in Western society, and his work has continued to influence both Asian and Western culture and politics. Historians have questioned whether or not Sun was an authentic historical figure. Traditional accounts place him in the Spring and Autumn Period of China (722–481 BCE) as a heroic general of the King of Wu who lived c. 544–496 BCE. Scholars accepting his historicity place his supposed writing *The Art of War* in the Warring States Period (476–221 BCE), based on the descriptions of warfare in the text. Traditional accounts state that his descendant, Sun Bin, also wrote a master treatise on military tactics.

FIGURE 12.17
Statue of Sun Tzu in Yurihama, Tottori, Japan

The Art of War is attributed to Sun, and it was originally called the Sun Tzu Bing Fa (Pinyin: Sunzi Bingfa), or simply the Sun Tzu. It presents a philosophy of war for managing conflicts and winning battles. Contrary to popular belief, it contains not only the writings of the original author, but also commentary and clarifications from later military philosophers, such as Li Quan and Du Mu. It is accepted as a masterpiece on strategy and often referenced by generals and theorists throughout history.[16] Of the texts written before the unification of China in the 2nd century BCE, six major works survived, including *The Art of War*. During the Song Dynasty in the early 1st millenium CE, the six works were combined with a Tang Dynasty text into a collection called the Seven Military Classics. As a central part of that compilation, *The Art of War* formed the foundations of orthodox military theory in China. Illustrating this point, the book was required reading to pass the tests needed for imperial appointment to military positions.[17] In the book, Sun uses language that may be unusual in a Western text on warfare and strategy. For example, the 11th chapter states that a leader must be "serene and inscrutable" and capable of comprehending "unfathomable plans". The text contains similar remarks that have confused Western readers. The meaning of such statements is clearer when interpreted in the context of Taoist thought and practice. Sun viewed the

[16]http://en.wikipedia.org/wiki/Sun_Tzu#CITEREFMcNeilly2001
[17]http://en.wikipedia.org/wiki/Sun_Tzu#CITEREFSawyer1994

FIGURE 12.18
A bamboo version of *The Art of War*

ideal general as an enlightened Taoist master,[18] which has led to *The Art of War* being considered a prime example of Taoist strategy.[19] *The Art of War* is distinguished from similar Western works, such as Prussian general Carl von Clausewitz's On War, by this spiritual dimension. Awareness of the Taoist viewpoint in *The Art of War* is essential to understanding its intended meaning.[18] The book is not only popular among military theorists, but it has also become increasingly popular among political leaders and those in business management. Despite its title, *The Art of War* addresses strategy in a broad fashion, touching upon public administration and planning. The text outlines theories of battle but also advocates diplomacy and cultivating relationships with other nations as essential to the health of a state.[16] In the early 1970s, scholars uncovered a collection of ancient texts written on unusually well-preserved bamboo slips. Among them were *The Art of War* and Sun Bin's Military Methods. Although Han Dynasty bibliographies noted the latter publication as extant and written by a descendant of Sun, it had since been lost. The finding of Sun Bin's work was therefore considered to be extremely important, because of Sun Bin's relationship to Sun, and the work's illustration of military thought in late Chinese antiquity. The discovery as a whole expanded the total known Chinese military works by hundreds. However, Sun Bin's treatise is the only known additional text surviving from the ancient period or bearing a close association with Sun Tzu.[20]

BOOKS

The Book of IRC: The Ultimate Guide to Internet Relay Chat

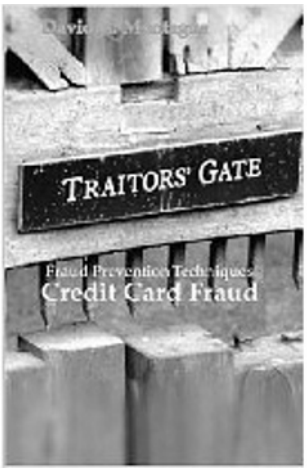
By Alex Charalabidis

Publisher: No Starch Press

ISBN-10: 1886411298

ISBN-13: 978-1886411296

[18]http://en.wikipedia.org/wiki/Sun_Tzu#CITEREFHanzhang_.26_Wilkinson1998
[19]http://en.wikipedia.org/wiki/Sun_Tzu#CITEREFSimpkins_.26_Simpkins1999
[20]http://en.wikipedia.org/wiki/Sun_Tzu#CITEREFSawyer1994



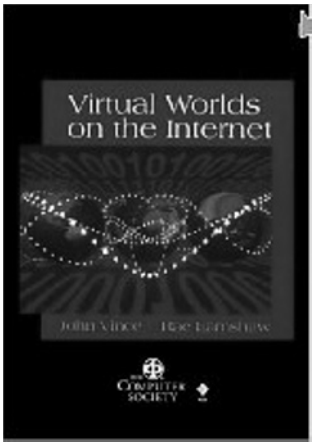
Fraud Prevention Techniques for Credit Card Fraud

By David A. Montague

Publisher: Trafford Publishing

ISBN-10: 1412014603

ISBN-13: 978-1412014601



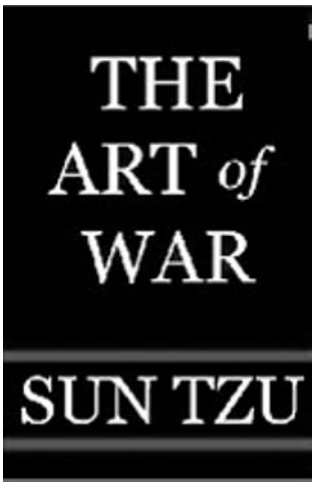
Virtual Worlds on the Internet

By John Vince and Rae Earnshaw

Publisher: Wiley-IEEE Computer Society Press

ISBN-10: 0818687002

ISBN-13: 978-0818687006



The Art of War

By Sun Tzu

Publisher: Filiquarian

ISBN-10: 1599869772

ISBN-13: 978-1599869773

Index

F

G

H

I

V

W

X

Y

Z

This page intentionally left blank