Contents

Hide and Sneak—Ido Dubrawsky

If you want to hack into someone else's network, the week
between Christmas and New Year's Day is the best time. I love that
time of year. No one is around, and most places are running on a
skeleton crew at best. If you're good, and you do it right, you
won't be noticed even by the automated systems. And that was a
perfect time of year to hit these guys with their nice e-commerce
site—plenty of credit card numbers, I figured.

The people who ran this site had ticked me off. I bought some
computer hardware from them, and they took forever to ship it to
me. On top of that, when the stuff finally arrived, it was damaged.
I called their support line and asked for a return or an exchange,
but they said that they wouldn't take the card back because it was a
closeout. Their site didn't say that the card was a closeout! I told
the support drones that, but they wouldn't listen. They said, "policy
is policy," and "didn't you read the fine print?" Well, if they're
going to take that position…. Look, they were okay guys on the
whole. They just needed a bit of a lesson. That's all.

The Worm Turns—Ryan Russell and Tim Mullen

After a few hours, I've got a tool that seems to work. Geeze, 4:30 A.M. I mail it to the list for people to check out and try.

Heh, it's tempting to use the root.exe and make the infected boxes TFTP down my tool and fix themselves. Maybe by putting it out there some idiot will volunteer himself. Otherwise the tool won't do much good, the damage is done. I'm showing like 14,000 unique IPs in my logs so far. Based on previous worms, that usually means there are at least 10 times as many infected. At least. My little home range is only 5 IP addresses.

I decide to hack up a little script that someone can use to remotely install my fix program, using the root.exe hole. That way, if someone wants to fix some of their internal boxes, they won't have to run around to the consoles. Then I go ahead and change it to do a whole range of IP addresses, so admins can use it on their whole internal network at once. When everyone gets to work tomorrow, they're going to need all the help they can get. I do it in C so I can compile it to a .exe, since most people won't have the Windows perl installed.

Just Another Day at the Office —Joe Grand

I can't disclose much about my location. Let's just say it's damp and cold. But it's much better to be here than in jail, or dead. I thought I had it made—simple hacks into insecure systems for tax-free dollars. And then the ultimate heist: breaking into a sensitive lab to steal one of the most important weapons the U.S. had been developing. And now it's over. I'm in a country I know nothing about, with a new identity, doing chump work for a guy who's fresh out

of school. Each day goes by having to deal with meaningless corporate policies and watching employees who can't think for themselves, just blindly following orders. And now I'm one of them. I guess it's just another day at the office.

h3X's Adventures in Networkland—FX

h3X is a hacker, or to be more precise, she is a *hackse* (from *hexe*, the German word for witch). Currently, h3X is on the lookout for some printers. Printers are the best places to hide files and share them with other folks anonymously. And since not too many people know about that, h3X likes to store exploit codes and other kinky stuff on printers, and point her buddies to the Web servers that actually run on these printers. She has done this before.

The Thief No One Saw—Paul Craig

My eyes slowly open to the shrill sound of my phone and the blinking LED in my dimly lit room. I answer the phone.

"Hmm … Hello?"

"Yo, Dex, it's Silver Surfer. Look, I got a title I need you to get for me. You cool for a bit of work?"

Silver Surfer and I go way back. He was the first person to get me into hacking for profit. I've been working with him for almost two years. Although I trust him, we don't know each other's real names. My mind slowly engages. I was up till 5:00 A.M., and it's only 10:00 A.M. now. I still feel a little mushy.

"Sure, but what's the target? And when is it due out?"

"Digital Designer v3 by Denizeit. It was announced being final today and shipping by the end of the week, Mr. Chou asked for this title personally. It's good money if you can get it to us before

it's in the stores. There's been a fair bit of demand for it on the street already."

"Okay, I'll see what I can do once I get some damn coffee."

"Thanks dude. I owe you." There's a click as he hangs up.

Flying the Friendly Skies—Joe Grand

Not only am I connected to the private wireless network, I can also access the Internet. Once I'm on the network, the underlying wireless protocol is transparent, and I can operate just as I would on a standard wired network. From a hacker's point of view, this is great. Someone could just walk into a Starbucks, hop onto their wireless network, and attack other systems on the Internet, with hardly any possibility of detection. Public wireless networks are perfect for retaining your anonymity.

Thirty minutes later, I've finished checking my e-mail using a secure Web mail client, read up on the news, and placed some bids on eBay for a couple rare 1950's baseball cards I've been looking for. I'm bored again, and there is still half an hour before we'll start boarding the plane.

dis-card—Mark Burnett

One of my favorite pastimes is to let unsuspecting people do the dirty work for me. The key here is the knowledge that you can obtain through what I call social reverse-engineering, which is nothing more than the analysis of people. What can you do with social reverse-engineering? By watching how people deal with computer technology, you'll quickly realize how consistent people really are. You'll see patterns that you can use as a roadmap for human behavior.

Humans are incredibly predictable. As a teenager, I used to watch a late-night TV program featuring a well-known mentalist. I watched as he consistently guessed social security numbers of audience members. I wasn't too impressed at first—how hard would it be for him to place his own people in the audience to play along? It was what he did next that intrigued me: He got the TV-viewing audience involved. He asked everyone at home to think of a vegetable. I thought to myself, carrot. To my surprise, the word *CARROT* suddenly appeared on my TV screen. Still, that could have been a lucky guess.

Social (In)Security—Ken Pfeil

While I'm not normally a guy prone to revenge, I guess some things just rub me the wrong way. When that happens, I rub back—only harder. When they told me they were giving me walking papers, all I could see was red. Just who did they think they were dealing with anyway? I gave these clowns seven years of sweat, weekends, and three-in-the-morning handholding. And for what? A lousy week's severance? I built that IT organization, and then they turn around and say I'm no longer needed. They said they've decided to "outsource" all of their IT to ICBM Global Services.

The unemployment checks are about to stop, and after spending damn near a year trying to find another gig in this economy, I think it's payback time. Maybe I've lost a step or two technically over the years, but I still know enough to hurt these bastards. I'm sure I can get some information that's worth selling to a competitor, or maybe to get hired on with them. And can you

imagine the looks on their faces when they find out they were hacked? If only I could be a fly on the wall.

Chapter 9 211

BabelNet—Dan Kaminsky

Black Hat Defense: Know Your Network Better Than The Enemy Can Afford To…

SMB—short for Server Message Block, was ultimately the protocol behind NBT(NetBIOS over TCP/IP), the prehistoric IBM LAN Manager, and its modern n-th generation clone, Windows File Sharing. Elena laughed as chunkage like `ECFDEECACACACACA-CACACACACACACACA` spewed across the display. Once upon a time, a particularly twisted IBM engineer decided that "First Level Encoding" might be a rational way to write the name "BSD". Humanly readable? Not unless you were the good Luke Kenneth Casson Leighton, whose ability to fully grok raw SMB from hex-dumps was famed across the land, a postmodern incarnation of sword swallowing.

Chapter 10 235

The Art of Tracking—Mark Burnett

It's strange how hackers think. You'd think that white hat hackers would be on one end of the spectrum and black hat hackers on the other. On the contrary, they are both at the same end of the spectrum, the rest of the world on the other end. There really is no difference between responsible hacking and evil hacking. Either way it's hacking. The only difference is the content. Perhaps that is why it is so natural for a black hat to go legit, and why it is so easy for a white hat to go black. The line between the two is fine, mostly defined by ethics and law. To the hacker, ethics and laws have holes just like anything else.

Many security companies like to hire reformed hackers. The truth is that there is no such thing as a reformed hacker. They may have their focus redirected and their rewards changed, but they are never reformed. Getting paid to hack doesn't make them any less of a hacker.

Hackers are kind of like artists. An artist will learn to paint by painting whatever they want. They could paint mountains, animals, or perhaps nudes. They can use any medium, any canvas, and any colors they wish. If the artist some day gets a job doing art, he becomes a commercial artist. The only difference is that they now paint what other people want.

Appendix 269

The Laws of Security—Ryan Russell

This book contains a series of fictional short stories demonstrating criminal hacking techniques that are used every day. While these stories are fictional, the dangers are obviously real. As such, we've included this appendix, which discusses how to mitigate many of the attacks detailed in this book. While not a complete reference, these security laws can provide you with a foundation of knowl-edge prevent criminal hackers from *stealing your network*.