

Foreword

The first book in this series *Stealing the Network: How to Own the Box* created a new genre of “Cyber-Thrillers,” that told fictional stories about individual hackers using real technologies. This second book in the series *Stealing the Network: How to Own a Continent* (or *STC* for short) introduces the concept of hacker groups, and the damage they can inflict through a concerted, orchestrated string of malicious attacks. The “Stealing” books are unique in both the fiction and computer book categories. They combine accounts that are fictional with technology that is very real. While none of these specific events have happened, there is no reason why they could not. You could argue it provides a roadmap for criminal hackers, but I say it does something else: It provides a glimpse into the creative minds of some of today’s best hackers, and even the best hackers will tell you that the game is a mental one. The phrase “Root is a state of mind,” coined by K0resh and printed on shirts from DEF CON, sums this up nicely. While you may have the skills, if you lack the mental fortitude, you will never reach the top. This is what separates the truly elite hackers from the wannabe hackers.

When I say hackers, I don’t mean criminals. There has been a lot of confusion surrounding this terminology, ever since the mass media started reporting computer break-ins. Originally, it was a compliment applied to technically adept computer programmers and system administrators. If you had a problem with your system and you needed it fixed quickly, you got your best hacker on the job. They might “hack up” the source code to fix things, because they knew the big picture. While other people may know how different parts of the system work, hackers have the big picture in mind while working on the smallest details. This perspective gives them great flexibility when approaching a problem, because they don’t expect the first thing they try to work.

xxii Foreword

The book *Hackers: Heroes of the Computer Revolution*, by Steven Levy (1984), really captured the early ethic of hackers and laid the foundation for what was to come. Since then, the term *hacker* has been co-opted through media hype and marketing campaigns to mean something evil. It was a convenient term already in use, and so instead of simply saying someone was a *criminal hacker*, the media just called him a *hacker*. You would not describe a criminal auto mechanic as simply a mechanic, and you shouldn't do the same with a hacker, either.

When the first Web site defacement took place in 1995 for the movie *Hackers*, the race was on. Web defacement teams sprung up over night. Groups battled to outdo each other in both quantity and quality of the sites broken into. No one was safe, including *The New York Times* and the White House. Since then, the large majority of criminal hacking online is performed by "script-kiddies"—those who have the tools but not the knowledge. This vast legion creates the background noise that security professionals must deal with when defending their networks. How can you tell if the attack against you is a simple script or just the beginning of a sophisticated campaign to break in? Many times you can't. My logs are full of attempted break-ins, but I couldn't tell you which ones were a serious attempt and which ones were some automated bulk vulnerability scan. I simply don't have the time or the resources to determine which threats are real, and neither does the rest of the world. Many attackers count on this fact.

How do the attackers do this? Generally, there are three types of attacks. Purely technical attacks rely on software, protocol, or configuration weaknesses exhibited by your systems, and these are exploited to gain access. These attacks can come from any place on the planet, and they are usually chained through many systems to obscure their ultimate source. The vast majority of attacks in the world today are mostly this type, because they can be automated easily. They are also the easiest to defend against.

Physical attacks rely on weaknesses surrounding your system. These may take the form of dumpster diving for discarded password and configuration information or secretly applying a keystroke-logging device to your computer system. In the past, people have physically tapped into fax phone lines to record documents, tapped into phone systems to listen to voice calls, and picked their way through locks into phone company central offices. These attacks bypass your information security precautions and go straight to the target. They work because people think of physical security as separate from information security.

To perform a physical attack, you need to be where the information is, something that greatly reduces my risk, since not many hackers in India are likely to hop a jet to come attack my network in Seattle. These attacks are harder to defend against but less likely to occur.

Social engineering (SE) attacks rely on trust. By convincing someone to trust you, on the phone or in person, you can learn all kinds of secrets. By calling a company's help desk and pretending to be a new employee, you might learn about the phone numbers to the dial-up modem bank, how you should configure your software, and if you think the technical people defending the system have the skills to keep you out. These attacks are generally performed over the phone after substantial research has been done on the target. They are hard to defend against in a large company because everyone generally wants to help each other out, and the right hand usually doesn't know what the left is up to. Because these attacks are voice-oriented, they can be performed from anyplace in the world where a phone line is available. Just like the technical attack, skilled SE attackers will chain their voice call through many hops to hide their location.

When criminals combine these attacks, they can truly be scary. Only the most paranoid can defend against them, and the cost of being paranoid is often prohibitive to even the largest company. For example, in 1989, when Kevin Poulson wanted to know if Pac Bell was onto his phone phreaking, he decided to find out. What better way than to dress up as a phone company employee and go look? With his extensive knowledge of phone company lingo, he was able to talk to the talk, and with the right clothes, he was able to walk the walk. His feet took him right into the Security department's offices in San Francisco, and after reading about himself in the company's file cabinets, he knew that they were after him.

While working for Ernst & Young, I was hired to break into the corporate headquarters of a regional bank. By hiding in the bank building until the cleaners arrived, I was able to walk into the Loan department with two other people dressed in suits. We pretended we knew what we were doing. When questioned by the last employee in that department, we said that we were with the auditors. That was enough to make that employee leave us in silence; after all, banks are always being audited by someone. From there, it was up to the executive level. With a combination of keyboard loggers on the secretary's computer and lock picking our way into the president's offices, we were able to

xxiv Foreword

establish a foothold in the bank's systems. Once we started attacking that network from the inside, it was pretty much game over.

The criminal hacker group in *STC* led by mastermind Bob Knuth, deftly combines these various types of attacks in an attempt to compromise the security of financial institutions across an entire continent, and stealing hundreds of millions of dollars in the process. Hacking is not easy. Some of the best hackers spend months working on one exploit. At the end of all that work, the exploit may turn out to not be reliable or to not function at all! Breaking into a site is the same way. Hackers may spend weeks performing reconnaissance on a site, only to find out there is no practical way in, so it's back to the drawing board. *STC* takes you inside the minds of the hackers as they research and develop their attacks, and then provides realistic, technical details on how such attacks could possibly be carried out.

In movies, Hollywood tends to gloss over this fact about the time involved in hacking. Who wants to watch while a hacker does research and tests bugs for weeks? It's not a visual activity like watching bank robbers in action, and it's not something the public has experience with and can relate to. In the movie *Hackers*, the director tried to get around this by using a visual montage and some time-lapse effects. In *Swordfish*, hacking is portrayed by drinking wine to become inspired to visually build a virus in one night. This is why the *Stealing* books are very different from anything you have ever read or seen. These books are written by some of the world's most accomplished cyber-security specialists, and they spare no details in demonstrating the techniques used by motivated, criminal hackers.

There have always been both individual hackers, and groups of hackers like the one portrayed in *STC*. From the earliest days of the '414' BBS hackers to modern hacking groups, there is always mystery surrounding the most successful teams. While the lone hacker is easy to understand, the groups are always more complicated due to internal politics and the manner in which they evolve over time. Groups usually are created when a bunch of like minded people working on a similar problem decide to combine forces. Groups are also formed when these individuals share a common enemy. When the problem gets solved or the enemy goes away, these groups are usually set adrift with no real purpose. The original purpose over, they now become more like a social group. Some members leave; others join; they fracture, and very seldom do they survive the test of time. Old groups such as the Legion of Doom (LOD) went

through almost three complete sets of members before they finally retired the name. It might have had something to do with their long-standing battle with a rival group, the Masters of Destruction (MOD) and run ins with the FBI. But, who really knows for sure other than the members themselves?

The ability of some of these now defunct groups is legendary in the underworld. Groups such as the LOD, The PhoneMasters, the MOD, and BELL-CORE had excellent hacking skills and were capable of executing extremely sophisticated attacks. Their skills ranged from purely technical to social engineering and physical attacks. This ability to cross disciplines is what makes some groups so powerful when they set themselves to a task. BELLCORE got a back-door installed in an operating system that shipped to the public, and some of its members monitored bank transfers over the X.25 network. Through a combination of hacking and social engineering, the PhoneMasters obtained tens of thousands of phone calling cards, located and used unlisted White House phone numbers, re-routed 911 calls to a Dominos Pizza, and had access to the National Crime Information Center (NCIC) database. They were even able to access information on who had their phone lines tapped.

There are documented reports of U.S. organized crime tricking unknowing hackers into doing work for them. What starts out looking like a friendly competition between hackers to break into a couple of Web sites can mask the intention of one of them to do so for financial gain. The other hackers have no idea of the bigger picture, and are unwitting accomplices.

One such incident occurred in Los Angeles when unsuspecting hackers helped Mexican gangs hack gas station credit cards, which allowed the gangs to operate over a larger area with no fuel costs. The hackers thought they were doing something cool, and sharing the how-to information with other locals who were a little more enterprising, shall we say.

This is the problem with the net. You can never be too paranoid, or too careful, because nothing may be as it seems. When your sole protection to being caught depends on keeping your identity and location secret, any information you share on-line could come back to haunt you. This creates a paradox for the illegal hacking group. You want to be in a group with people you trust and who have good skills, but you don't want anyone in the group to know anything about you. Many illegal hackers have been busted when it turns out their on-line friend is really an AFOSI or FBI informant! Hackers seem to be good at hacking, and bad at being organized criminals.



xxvi Foreword

So, what if you were part of a group, and didn't even know it? What if you made friends with someone on-line, and the two of you would work on a project together, not knowing the other person was using you to achieve their own goals that may be illegal? Now things get interesting! Motives, friendship, and trust all get blurred, and on-line identities become transient. STC shows you what can happen when talented hackers who are very motivated (for many different reasons) try to *Own a Continent!*

Jeff Moss
Black Hat, Inc.
www.blackhat.com
April, 2004

