A Closer Look at Ethical Hacking and Hackers

Marilyn Leathers

East Carolina University

ICTN 6865

Abstract

Due to the advance technology of the Internet, the government, private industry and the everyday computer user have fears of their data or private information being comprised by a criminal hacker. C.C. Palmer (2001), who manages the Network Security and Cryptography department at the IBM Thomas J. Watson Research Center writes, "they are afraid that some hacker will break into their Web server and replace their logo with pornography, read their e-mail, steal their credit card number from an on-line shopping site, or implant software that will secretly transmit their organization's secrets to the open Internet" (p. 1). This hacking is not only widespread, but is being executed so flawlessly that the attackers compromise a system, steal everything of value and completely erase their tracks within 20 minutes (EC-Council [ECC], p. 2). Because of criminal hackers, ethical hacking is rapidly becoming an accepted business practice. This paper will define ethical hacking, list some of the commonly use terms for attackers, provide a list of the standard services offered via ethical hacking to combat attackers, discuss the three common group of hackers and the top 10 most famous hackers, and finally discuss legal implications of hacking.

A Closer Look at Ethical Hacking and Hackers

One of the most significant current discussions in the information technology community is ethical hacking. The topic of discussion varies from “why is ethical hacking so popular” to “can hacking be ethical”.

Why is ethical hacking so popular? Author James Tiller (2004), a security services expert, states his opinion of why ethical hacking is so popular as “Several reasons can be attributed to the frenzy we’re seeing, but for me one seems to stand out. Based on hundreds of conversations with companies throughout the United States and most of Europe, many feel they are practicing sound security and have tamed the beast. Now all that is left for them is to test what was implemented and apply a patch or two”(p. 10).

Can hacking be ethical? According to author Kimberly Graves (2007), the answer is “Yes! Ethical hackers are usually security professionals or network penetration testers who use their hacking skills and toolsets for defensive and protective purposes”(p. 7).

Ethical Hacking Defined

What is ethical hacking? Ethical hacking is the controversial practice of employing the tools and tactics of hackers to test the security precautions protecting a network (Livermore, 2007, p.1). Ethical hacking is also called “penetration testing” and “intrusion testing” or “red teaming,” a term used when the U.S. government began hacking its own systems in the 1970s. In the 1980s, telecommunications companies – a frequent target of budding cybervandals who could gain street credibility by messing with the local phone company – began using ethical hacking as well. Banks caught on in the 1990s, and later in that decade, most e-commerce firms depended on ethical hacking as a critical security measure, since a single interruption or intrusion could cause massive financial problems (Coffin, 2003, p.1). Consequently, a company main goal in hiring ethical hackers is to test for vulnerabilities and mitigate them or defend against them.

Who Are the Attackers?

Ethical hackers are up against several individuals in the battle to secure the network. The following list presents some of the more commonly used terms for these attackers (Immortal, 2008):

- *Phreakers* – The original hackers. These individuals hacked telecommunication and PBX systems to explore the capabilities and make free phone calls. Their activities include physical theft, stolen calling cards, access to telecommunication services, reprogramming of telecommunications equipment, and compromising userids and passwords to gain unauthorized use of facilities, such as phone systems and voice mail.
- *Script/Click Kiddies* – A term used to describe often younger attackers who use widely available freeware vulnerability assessment tools and hacking tools that are designed for attacking purposes only. These attackers typically do not have any programming or hacking skills and, given the technique used by most of these tools, can be defended against with the proper security controls and risk mitigation strategies.
- *Disgruntled employee* – Employees who have lost respect and integrity for the employer. These individuals might or might not have more skills than the script kiddies. Many times, their rage and anger blind them. They rank as a potentially high risk because they have insider status, especially if access rights and privileges were provided or managed by the individual.
- *Whackers* – Whackers are typically newbie who focus their limited skills and abilities on attacking wireless LANs and WANs.

- *Software Cracker/Hacker* – Individuals who have skills in reverse engineering software programs and, in particular, licensing registration keys used by software vendors when installing software onto workstations or servers. Although many individuals are eager to partake of their services, anyone who downloads programs with cracked registration keys are breaking the law and can be a greater potential risk and subject to malicious code and malicious software threats that might have been injected into the code.
- *Cyber-Terrorists/Cyber-Criminals* – An increasing category of threat that can be used to describe individuals or groups of individuals who are typically funded to conduct clandestine or espionage activities on governments, corporations, and individuals in an unlawful manner. These individuals are typically engaged in sponsored acts of defacement; DoS/DDoS attacks identify theft, financial theft, or worse, compromising critical infrastructures in countries, such as nuclear power plants, electric plants, water plants, and so on.
- *System Cracker/Hacker* – Elite hackers who have specific expertise in attacking vulnerabilities of systems and networks by targeting operating systems. These individuals get the most attention and media coverage because of the globally affected viruses, worms, and Trojans that are created by System Crackers/Hackers. System Cracker/Hackers perform interactive probing activities to exploit security defects and security flaws in network operating systems and protocols (p.10).

Standard Services Offered to Combat the Attackers

Because of the onslaught of hacker attacks, companies offer ethical hacking services to combat the attackers. Bill Coffin (2003), in his article *IT takes a thief: Ethical hackers test your defenses,* points out that "what goes into ethical hacking depends on the range of services required, the size of the client and how much that client is willing to pay. Typical services offered to combat attackers include the following:

- *External network hacking*. This includes scanning the target's Web server, firewall and routers for vulnerabilities from an external source. This is the most commonly provided ethical hacking service.
- *Internal network hacking*. This involves deploying a team to the target site, where they conduct penetration testing on the company's servers and routers, using its own equipment. This is a good test for defending against disgruntled employees, industrial saboteurs (although uncommon) or anyone else who might try to intrude upon a company's network from within.
- *Application testing*. A growing arena for the ethical hacking industry, application testing is aimed specifically at clients who have developed their own software, such as custom Web-based voting and polling programs or online stores and payment programs. Just about any software that is not delivered shrink-wrapped falls under the custom application category. Comparatively, scanning Web servers for vulnerabilities are fairly easy since they are all relatively uniform. When scanning custom applications, however, the ethical hacker must reverse engineer the program and analyze every line of code.
- *Wireless Lan Assessment*. This is another increasingly common service because many firms employ wireless networks within their facilities. Such networks enable laptop users to move their computers from office to office while remaining connected to the local network. The downside is passersby outside the facility can use that same wireless technology to log in to the company's network without the company knowing it. The

most common way to perform a wireless LAN assessment is to conduct "war driving" – physically traveling around the target facility in search of wireless access points.

- *War Dialing*. This is an old hacking technique where a hacker breaks into a network by calling phone numbers in the hopes of hitting an unsecured modem that the target has accidentally left active or forgotten. Automated programs enable hackers to dial thousands of number in a matter of moments. The technique almost always works and is one of the tests ethical hackers run that usually turns up an intrusion alert.
- *Social engineering*. Like war dialing, social engineering is a simple but effective technique. An intruder calls someone within the target company and convinces him or her to give up sensitive IT information over the phone. Ethical hackers test against this vulnerability by performing social engineering of their own to highlight what ruses the client's personnel will fall for—and what it needs to educate itself against.
- *Thrashing.* This is another old hacker trick in which intruders comb through the garbage of a target company in search of documents that contain important IT data, such as access numbers and passwords. Not all ethical hackers perform trash testing, which borders on breaking into the client's facilities. Many firms choose to stick exclusively with technology testing. Since some companies (such as financial institutions) employ armed guards, trashing carries with it the possibility of a tragic misunderstanding between the ethical hacker and his or her client's security personnel. Those ethical hacking firms that do "trash" their clients often use subcontractors for the job and coordinate extensively with the client company so that security guards do not mistake an intrusion test for something more sinister" (p.1).

Three Common Group of Hackers

Hackers can be divided into three groups: white hats, black hats, and grey hats. According to author Kimberley Graves (2007), “Ethical hackers usually fall into the white-hat category, but sometimes they’re former gray hats who have become security professionals and who use their skills in an ethical manner.” Graves offers the following description for the three groups of hackers:

- ***White Hats*** are the good guys, the ethical hackers who use their hacking skills for protective purposes. White-hat hackers are usually security professionals with knowledge of hacking and the hacker toolset and who use this knowledge to locate weaknesses and implement countermeasures (p. 6).
- ***Black Hats*** are considered the bad guys: the malicious hackers or *crackers* use their skills for illegal or malicious purposes. They break into or otherwise violate the system integrity of remote machines, with malicious intent. Having gained unauthorized access, black-hat hackers destroy vital data, deny legitimate users service, and basically cause problems for their targets (p. 7).
- ***Grey Hats*** are hackers who may work offensively or defensively, depending on the situation. This is the dividing line between hacker and cracker. Both are powerful forces on the Internet, and both will remain permanently. And some individuals qualify for both categories. The existence of such individuals further clouds the division between these two groups of people (p.7).

Top 10 Most Famous Hackers of All Times

An article titled, *Top 10 Most Famous Hackers of All Time,* provides the following profile of the top 10 most famous hackers of all times (IT Security, 2007, p. 1):

Top 5 White Hack Hackers

- ***Stephen Wozniak:*** "Woz" is famous for being the "other Steve" of Apple. Wozniak, along with current Apple CEO Steve Jobs, co-founded Apple computer. Woz got his start in hacking making blue boxes, devices that bypass telephone-switching mechanisms to make free long-distance calls. After reading an article about phone phreaking in Esquire, Wozniak called up his buddy Jobs. The pair did research on frequencies, then built and sold blue boxes to their classmates in college. Wozniak even used a blue box to call the Pope while pretending to be Henry Kissinger.
- ***Tim Berners-Lee*** is famed as the inventor of the World Wide Web, the system that we use to access sites, documents and files on the Internet. While a student at Oxford University, Berners-Lee was caught hacking access with a friend and subsequently banned from University computers. w3.org reports, "Whilst [at Oxford], he built his first computer with a soldering iron, TTL gates, an M6800 processor and an old television."
- ***Linus Torvalds*** fathered Linux, the very popular Unix-based operating system. He calls himself "an engineer," and has said that his aspirations are simple, "I just want to have fun making the best damn operating system I can." Torvalds hacks included "an assembler and a text editor…as well as a few games."
- ***Richard Stallman*** fame derives form the GNU Project, which he founded to develop a free operating system. Stallman got his start hacking at MIT. He worked as a "staff hacker" on the Emacs project and others. He was a critic of restricted computer access in the lab. When a password system was installed, Stallman broke it down, resetting passwords to null strings, and then sent user messages informing them of the removal of the password system.

- ***Tsutomu Shimomura*** reached famed in an unfortunate manner: he was hacked by Kevin Mitnick. Following this personal attack, he made it his cause to help the FBI capture him. Shimomura's work to catch Mitnick is commendable, but he is not without his own dark side. Author Bruce Sterling recalls: "He pulls out this AT&T cellphone, pulls it out of the shrinkwrap, finger-hacks it, and starts monitoring phone calls going up and down Capitol Hill while an FBI agent is standing at his shoulder, listening to him." Shimomura out-hacked Mitnick to bring him down. Shortly after finding out about the intrusion, he rallied a team and got to work finding Mitnick. Using Mitnick's cell phone, they tracked him near Raleigh-Durham International Airport. Shimomura used a cellular frequency direction-finding antenna hooked up to a laptop to narrow the search to an apartment complex. Mitnick was arrested shortly thereafter. Following the pursuit, Shimomura wrote a book about the incident with journalist John Markoff, which was later turned into a movie.

Top 5 Black Hat Hackers

- ***Johnathan James*** gained notoriety when he became the first juvenile to be sent to prison for hacking. He was sentenced at 16 years old. In an anonymous PBS interview, he professes, "I was just looking around, playing around. What was fun for me was a challenge to see what I could pull off." James's major intrusions targeted high-profile organizations. He installed a backdoor into Defense Threat Reduction Agency server. The DTRA is an agency of the Department of Dense charged with reducing the threat to the U.S. and its allies from nuclear, biological, chemical, conventional and special weapons. The backdoor he created enabled him to view sensitive emails and capture employee usernames and passwords. James also cracked into NASA computers, stealing software worth approximately $1.7 million. NASA was forced to shut down its computer systems, ultimately racking up a $41,000 cost. James explained that he downloaded the code to supplement his studies on C programming, but contended, “The code itself was crappy … certainly not worth $1.7 million like the claimed.” If James, also know as “c0mrade,” had been an adult he likely would have served at least 10 years, instead he was banned from recreational computer use and was slated to serve a six-month sentence under hose arrest with probation.

- ***Adrian Lamo’s*** claim to fame is his break-ins at major organizations like The New York Times and Microsoft. Dubbed the “homeless hacker,” he used internet connections at Kinko’s, coffee shops and libraries to do his intrusions. Lamo’s intrusions consisted mainly of penetration testing, in which he found flaws in security, exploited them and then informed companies of their shortcomings. His hits include Yahoo!, Bank of America, Citigroup and Cingular. When he broke into The New York Times’ Intranet, things got serious. He added himself to a list of experts and viewed personal information on contributors, including Social Security numbers. For his intrusion at The New York Times, Lamo was ordered to pay approximately $65,000 in restitution. He was also sentenced to six months of home confinement and two years of probation, which expired January 16, 2007. Lamo is currently working as an award-winning journalist and public speaker.
- ***Kevin Mitnick*** is a self-proclamied “hacker poster boy.” Mitnick went through a highly publicized pursuit by authorizes. His mischief was hyped by the media but his actual offenses may be less notable than his notoriety suggests. The Department of Justice describes him as “the most wanted computer criminal in the United States history.” His

exploits were detailed in two movies: Freedom Downtime and Takedown. Mitnick had a bit of hacking experience before committing the offenses that made him famous. He started out exploiting the Los Angeles bus punch card system to get free rides. Then, like Apple co-founder Steve Wozniak, dabbled in phone phreaking. Although there were numerous offenses, Mitnick was ultimately convicted for breaking into the Digital Equipment Corporation's computer network and stealing software. Mitnick's mischief got serious when he went on a two and a half year "coast-to-coast hacking spree." Today, Mitnick has been able to move past his role as a black hat hacker and become a productive member of society. He served five years, about 8 months of it in solitary confinement, and is now a computer security consultant, author and speaker.

- ***Kevin Poulsen*** who is also known as Dark Dante, gained recognition for his hack of LA radio's KIIS-FM phone lines, which earned him a brand new Porsche, among other items. Law enforcement dubbed him "the Hannibal Lecter of computer crime." Authorities began to pursue Poulsen after he hacked into a federal investigation database. During this pursuit, he further drew the ire of the FBI by hacking into federal computers for wiretap information. His hacking specialty, however, revolved around telephones. Poulsen's most famous hack, KIIS-FM, was accomplished by taking over all of the station's phone lines. In a related feat, Poulsen also "reactivated old Yellow Page escort telephone numbers for an acquaintance who then ran a virtual escort agency." Ultimately, Poulsen was captured in a supermarket and served a sentence of five years. Since serving time, Poulsen has worked as a journalist. He is now a senior editor for Wired News. His most prominent article details his work on identifying 744 sex offenders with MySpace profiles.

- ***Robert Tappan Morris,*** son of former National Security Agency scientist Robert Morris, is known as the creator of the Morris Worm, the first computer worm to be unleashed on the Internet. As a result of this crime, he was the first person prosecuted under the 1986 Computer Fraud and Abuse Act. Morris wrote the code for the worm while he was a student at Cornell. He asserts that he intended to use it to see how large the Internet was. The worm, however, replicated itself excessively, slowing computers down so that they were no longer usable. It is not possible to know exactly how many computers were affected, but experts estimate an impact of 6,000 machines. He was sentenced to three years' probation, 400 hours of community service and a fine of $10500. Morris is currently working as a tenured professor at the MIT Computer Science and Artificial Intelligence Laboratory. He principally researches computer network architectures including distributed has tables such as Chord and wireless mesh networks such as Roofnet.

Legal Implications of Hacking

What are the legal implications of hacking? Ethical hackers should know the laws and penalties of unauthorized hacking into a system. No ethical hacking activities associated with a network-penetration test or security audit should begin until a signed legal document giving the ethical hacker express permission to perform the hacking activities is received from the target organization (Graves, 2007, p.13).

Hacking is covered under law Title 18: Crimes and Criminal Procedure: Part 1: Crimes: Chapter 47: Fraud and False Statements: Section 1029 and 1030. Each is described here (Immortal, 2008, p.21):

Section 1029 Fraud and related activity with access devices.

This law gives the U.S. Federal government the power to prosecute hackers that knowingly and with intent to defraud, produce, use, or traffic in one or more counterfeit access devices. Access devices can be an application or hardware that is created specifically to generate any type of access credentials, including passwords, credit card numbers, long distance telephone service access codes, PINs, and so on for the purpose of unauthorized access.

Section 1030 Fraud and related activity in connection with computers.
The law covers just about any computer or device connected to a network or Internet. It mandates penalties for anyone who accesses a computer in an unauthorized manner or exceeds one's access rights. This is a powerful law because companies can use it to prosecute employees when they use the rights the companies have given them to carry out fraudulent activities.

Other federal laws that address hacking include the following:

Computer Fraud and Abuse Act of 1984
The Computer Fraud and Abuse Act (CFAA) of 1984 protect certain types of information that the government maintains as sensitive. The Act defines the term "classified computer," and imposes punishment for unauthorized or misused access into one of these protected computers or systems. The Act also mandates fines and jail time for those who commit specific computer – related actions, such as trafficking in passwords or extortion by threatening a computer. In 1992, Congress amended the CFAA to include malicious code, which was not included in the original Act.

The Cyber Security Enhancement Act of 2002
This Act mandates that hackers who carry out certain computer crimes might now get life sentences in jail if the crime could result in another's bodily harm or possible death. This means that if hackers disrupt a 911 system, they could spend the rest of their days in jail.

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001
Originally passed because of the World Trade Center attack on September 11, 2001. Strengthens computer crime laws and has been the subject of some controversy. This Act gives the U.S. government extreme latitude in pursuing criminals. The Act permits the U.S. government to monitor hackers without a warrant and perform sneak and peek searches.

Conclusion

One of the most significant findings to emerge from this research is that ethical hacking can be beneficial in identifying vulnerabilities before they are exploited. Ethical hacking is legal and performed with the target's permission. It is part of an overall information risk management program that allows for ongoing security improvements (Beaver, 2005, p. 10). Finally, according to Ed Skoudis, Vice President of Security Strategy for Predictive Systems' Global

Integrity consulting practice, “ethical hacking has continued to grow in an otherwise lackluster IT industry, and is becoming increasingly common outside the government and technology sectors where it began” (SearchSecurity, 2007, p. 1).

References

Beaver, K. (2005). *Hacking for Dummies*. Hoboken, NJ: John Wiley & Sons Inc..

Coffin, B. (2003, July 1). *IT takes a thief: Ethical hackers test your defenses.* Retrieved November 10, 2008, from http://findarticles.com/p/articles/mi_qa5332/is_/ai_n29015644

EC-Council (n.d.). *Ethical Hacking and Countermeasures.* Retrieved November 10, 2008, from http://www.eccouncil.org/ipdf/EthicalHacker.pdf

Graves, K. (2007). *CEH Official Certified Ethical Hacker Review Guide* (1st ed.). Indianapolis, In: Wiley Publishing, Inc..

I. (2008, July 7). *Ethical Hacking Basics Class part 1.* Retrieved November 10, 2008, from http://www.go4expert.com/forums/showthread.php?t=11925

IT Security (2007, April 24). *Top 10 Most Famous Hackers of All Time.* Retrieved November 10, 2008, from http://www.itsecurity.com/features/top-10-famous-hackers-042407/

Livermore, J. (2007, June 4). *What Are Faculty Attitudes Toward Teaching Ethical Hacking and Penetration Testing?.* Retrieved November 10, 2008, from http://www.cisse.info/colloquia/cisse11/proceedings11/PDFs/Papers/S07P01.pdf

Palmer, C. C. (2001, April 13). *Ethical Hacking.* Retrieved November 10, 2008, from http://www.research.ibm.com/journal/sj/403/palmer.html

SearchSecurity (2007, June 5). *Ethical Hacker.* Retrieved November 15, 2008, from http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci921117,00.html#

Tiller, J. S. (2004). *The Ethical Hack: A Framework for Business Value Penetration Testing* . Portland, OR: Book News, Inc..