International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 11 Issue 2 –NOVEMBER 2014.

Ethical Hacking and Types of Hackers

S. TULASI PRASAD

Assistant Professor, Department of MCA, KBN College, Vijayawada

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". Many university programs have increased the course offerings and the depth of computer security programs, as the ethics of teaching hacking as an ongoing professional development tool is certainly an issue in today's digital age. If you want to catch a criminal, you have to be able to think like one. 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]). 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.

Keywords: ethical hacking, information security, faculty attitudes, education and training, teaching hacking

I. INTRODUCTION

According to Pashel (2006) the practice of "ethical hacking" has received worldwide attention. Many co rporations are advocates of teaching employees how hackers think and work in an effort to determine whether a corporate network has been hacked, as well as to determine potential weaknesses and prevent future hacking. Moreover, consulting firms exist whose purpose is to instruct information technology professionals on the practices of ethical hacking (Pashel, 2006). Proponents of ethical hacking have also introduced the concept of teaching university level future information technology professionals how to hack as well as the legal and ethical implications of such practices.

Bratus, Shubina&Locasto (2010) explained information security and assurance holds an increasingly important place in the education of Computer and Information System students, many of whom will be asked to deal with new security and control challenges. To meet the challenges of modern computer security practice, students must be able to switch from their traditional computer science and software engineering curricula to the attacker's way of thinking (Bratus, Shubina&Locasto, 2010). In order to be meaningful and practical, the computer security curriculum must include both "defender" and "attack er" perspectives. According to Livermore (2007) to meet the demand for trained security professionals with attack and defense skills, colleges and universities are teaching "ethical hacking" and penetration skills as part of their Information Assurance (IA) programs.

II. HACKING

The term hacker is defined as a person who accesses computers and information stored on computers without obtaining permission. Logan and Clarkson (2005) decribed hacking as accessing a system that one is either not authorized to access, or who accesses a system at a level beyond their authorization. Hackers are divided into several categories, some are ethical and others are unethical. "White hat" hackers are those who use their ability in a manner that most would clearly define as ethical. On the other hand the "Black Hats" are those individuals who are highly skilled, however they use their skills in criminal and other activities (Pashel, 2006).

III. ETHICAL HACKING DEFINED:

What is ethical hacking? Ethical hacking is the controversial practice of employing the tools and tactics of hacker's 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 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".

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. 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. 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).

IV. 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):

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 weuse 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. Hecalls 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 from the GNU Project, which he founded to develop afree operating system. Stallman got his start hacking at MIT. break-ins at major organizations like The New YorkTimes 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 Mitnickis 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 Poulsenwho is also known as Dark Dante, gained recognition for his hack of LAradio'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).

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism

V. 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 lacklustre IT industry, and is becoming increasingly common outside the government and technology sectors where it began" (Search Security, 2007, p.)

VI. REFERENCES

[1] 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. RetrievedNovember 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

[2] 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 102008,fromhttp://www.go4expert.com/forums/showthread.php?t=11925

[3] 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).

[4] National Strategy to Secure Cyberspace: The White House, "National Strategy to Secure Cyberspace. Retrieved from: http://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

[5] (2006). Teaching Students to Hack: Ethical Implicatios in Teaching Students to Hack at the University Level. InfoSecCD Conference'06, September 22-23, 2006