Teaching Students to Hack: Ethical Implications in Teaching Students to Hack at the University Level

Brian A. Pashel
Kennesaw State University
1000 Chastain Rd
Kennesaw, GA 30144
678-687-2595
bphunter1001@yahoo.com

ABSTRACT

Hacking has become a widespread problem with the onset of the digital age and the nearly universal access to the internet and other digital media. It is important for individuals, corporations, and the government to protect themselves from being vulnerable to such attacks. The purpose of this paper is to provide detailed information regarding the practices of hacking and ethical hacking, as well as to discuss the ethical nature of teaching computer students how to hack in an attempt to strengthen their skills in the field of information systems security.

Categories and Subject Descriptors

K.4.1 **[Computers and Society**]: Public Policy Issues – *Ethics*

General Terms

Management, legal aspects, security, standardization.

Keywords

Hacking, ethical hacking, teaching hacking, student misuse.

1. INTRODUCTION

The practice of hacking has become a widespread issue in the world today. Hackers can be anyone from a curious middle school student to a malicious criminal. They hack for a variety of reasons from testing their computer skills to committing fraudulent and harmful acts. It is important for individuals and corporations to protect themselves, their personal information, and their computers from hackers.

In recent years, the practice of "ethical" hacking has received much attention. Many corporations are proponents of teaching employees how hackers think and work in an effort to determine whether a network has been hacked as well as to determine potential weakness and prevent future hacking. Consulting firms exist whose purpose is to instruct information technology professionals in the practices of ethical hacking, however these services tend to be rather costly. 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.

The purpose of this paper is to explore the idea of teaching students to hack at the university level. The first sections will define and provide information on the practices of hacking and ethical hacking before exploring the ethics of teaching students to hack at the university level and outlining ways in which university computer security programs can help prevent the misuse of information and skills acquired in their programs.

2. HACKING

Before one can clearly understand what it means to be an ethical hacker, the concept of hacking must be defined. Originally, a hacker was thought of as a person with extreme technological talent (Falk, 2005). In recent years, however, the term has taken on a more negative definition and is used most typically to describe a person who accesses computers and information stored on computers without first obtaining permission. Logan and Clarkson (2005) support that definition in describing hacking as accessing a system that one is either not authorized to access or who accesses a system at a level beyond their authorization. "It includes the application of computer skills to find vulnerable systems, penetrate systems, and to remove evidence of access to a system" (Logan & Clarkson, 2005 p. 157). Hackers can be categorized in to a number of groups some of which are clearly ethical, others are clearly unethical, and still others exist in a gray area of sorts and whose ethics can be debated.

"White Hats" are those hackers who use their ability in a manner that most would clearly define as ethical. Examples are employees who, with permission, attack a company's network in order to determine weaknesses and law enforcement and intelligence agents who use their skill in the name of national security or to investigate and solve crimes. "It is a part of their duty to use their knowledge in such a way as to benefit other people" (Falk, 2005, p. 5).

"Black Hats" are those individuals who are highly skilled, however they use their skills in criminal and other less than ethical ways. Such individuals include members of organized

InfoSecCD Conference'06, September 22-23, 2006, Kennesaw, GA, USA. Copyright 2006 ACM 1-59593-437-5/00/0006…$5.00.

crime units who use their talent for extortion and fraudulent acts as well as other criminals who illegally access information stored on computer for the express purpose of committing a crime.

The ethical nature of a “Gray Hat’s” activity is, as the name implies, a more questionable gray area. Gray Hat hackers include vigilantes (individuals who use computers to investigate and or attempt to punish supposed criminals. It is important to note that vigilantes operate outside of legal authority and without the consent of citizens) and “hacktivists” (individuals who use computers and the internet to convey political messages), among others (Hartley, 2006; Falk, 2005).

Norfolk (2001) identifies several ways in which individuals typically conduct hacking activities: passive information gathering, active information gathering, vulnerability mapping, and the practical exploit. A rather significant amount of company information can be accessed through public websites and documents, a practice known as passive information gathering. While the average person would choose not to exploit this availability, a hacker may in fact use perfectly legal means of gathering information to use in negative ways.

For example, by reviewing the source code of a company website, a hacker may come across such information as naming conventions, names and email addresses of staff, and IP addresses of host machines found behind a company’s firewall. In some cases, a hacker could even determine the name of an individual in tech support through mapping email addresses then make a simple phone call, claiming that the tech support employee asked the hacker to call for password information in order to fix a “problem.” Many individuals would provide password information without a second thought after being provided with just the name of a company employee (Norfolk, 2001).

Active information gathering results in more information for the hacker, however it also places him at greater risk of being discovered. “Dumpster diving”, or browsing waste bins in an attempt to discover information such as user names and addresses, is an active information gathering method that is less likely to draw attention. Another method is to scan a host’s ports in an attempt to find an open one. Sending malformed packets to a host in order to analyze the information sent back can allow a hacker to determine the operating system used by a given company (Norfolk, 2001).

Vulnerability mapping involves creating a map of a particular network that includes host names, operating system, IP addresses, operating version, and the services being used in an attempt to discover vulnerabilities. Unfortunately, there are a variety of ways in which hackers can access information regarding broad ranging and typical vulnerabilities including advisories sent by software companies, public access information on past and successful attacks, and secret hacker groups that discuss in detail past attacks and methods which may be factual or may be fiction in an attempt to show greater skill than the competition. Companies can correct these vulnerabilities through a few simple steps including the proper configuration of new software, proper programming practices, and improved security culture (Norfolk, 2001).

The practical exploit involves the exploitation of poor programming and poor security practice within a company. For example, a programmer who programs past a buffer allows a weakness by which a hacker can exploit a network and install a relatively undetectable back door. The hacker can then use that back door to determine other network vulnerabilities after which he has the ability to erase any trace of his actions. A less skilled hacker may actually, unintentionally, crash a system and destroy data in his attempts to install and use a backdoor. Many hackers will post their “successes” on hacker newsgroups thereby providing information about companies with weak security and enticing other hackers to exploit the same system (Norfolk, 2001).

3. ETHICAL HACKING

Ethics in computing pose a somewhat more complex, complicated philosophical issue than do ethics in other areas. Johnson (2004) poses several parameters which describe behavior as ethical or not. According to him, if an action does at least one of the following it can be thought of as ethical: “promote the general health of society, maintain or increase individual rights and freedoms, protect individuals from harm, treat all human beings as having an inherent value and accord those beings respect, [and] uphold religious, social, cultural, and government laws and mores” (Johnson, 2004 p. 2).

Essentially, those actions that do not damage an individual or society can be thought of as ethical. Computer ethics, however, are not so cut and dry as so called “real world” ethics. The general population does not thoroughly understand computers and the damage that can be caused by the unethical use of them. Therefore, it is the obligation of computer professionals to prevent and defend against their misuse. It is the argument of this paper that the practice of ethical hacking is a useful means of doing so.

Ethical hacking can be defined as the practice of hacking without malicious intent. “Ethical hackers…employ the same tools and techniques as the intruders, but they…neither damage the target systems nor steal information. Instead, they…evaluate the target systems’ security and report back to owners with the vulnerabilities they found and instructions for how to remedy them” (Palmer, 2004 as quoted by Greene). An example of ethical hacking is the use of penetration testing, or purposefully attempting to gain “illegal access” to a network in order to determine the depth of a network’s security (Hartley, 2006). This concept of “breaking” an item in order to test it is not new as demonstrated by the use of crash-testing a car to determine its safety levels or testing the amount weight a beam can hold before mass producing it for use in the construction of homes (Greene, 2004).

Training in computer security is intended to improve information security in general as well as to educate professionals. An increasing number of corporations are implementing practices of ethical hacking in order to identify and correct security flaws. There are a number of private consulting firms including who provide such services. Recently, however, the cost efficiency of training internal employees in this security skill has become apparent and companies have started training a select number of computer security personnel in the practices of ethical hacking. Additionally, many university programs have broadened the course offerings and the depth of computer security programs. While the ethics of teaching hacking as an ongoing professional development tool is certainly an issue in today's digital age, that topic is beyond the scope of this paper and the next section will focus solely on the ethics of teaching students how to hack at the university level.

4. THE ETHICS OF TEACHING STUDENTS TO HACK AT THE UNIVERSITY LEVEL

The concept of teaching individuals how to hack in graduate and undergraduate computing programs has received much attention in recent years. At the university level, the idea behind hacking as a means of training is a method of teaching students how to protect the data assets of a future employer (Logan & Clarkson, 2005). A debate exists as to whether teaching a student how to hack so that he may, in turn, utilize that skill in order to strengthen the network security of an employer or other reasons that benefit the greater good outweighs the risk of potentially teaching students skills that will be used in a negative or illegal manner (Hartley, 2006). The stance of this paper is that, given the proper training in ethics and law, students who learn traditionally illegal computer skills in the course of studying computer security will use those skills for the greater good far more often than they will use them illegally and immorally. After all, "the goal of the educator is to instill the knowledge that they have about any given subject into their students so that they not only understand the material but also know how to apply it" (Poteat, 2004, p. 225).

The purpose of teaching a student how to hack can be more clearly understood when explained in correlation with the skills of an auditor. With such skills, a student will be able to test the systems of a future employer in order to pinpoint flaws in system designs as well as security issues. By understanding how to hack, a student not only knows how a system might be breached but can identify the signs of a breach and can determine where in a system a hacker might attempt an attack. By possessing the same skills as the criminal a student can better protect a system (Logan & Clarkson, 2005). The key to effectively teaching students how to hack so that they may use these skills in their future profession is in teaching them the ethical and legal implications of their skill, and the ramifications of misusing their skill.

5. PREVENTING STUDENT MISUSE

Just as young children learn best through behavior modeled by adults, computing students can learn ethical behavior best through modeling of professors and other professionals as opposed to learning it in the classroom. By providing students access to real networks with real skills and modeling proper use of those skills they can not only strengthen the depth of their understanding of computer security but appreciate the power of their skill and the necessity of using that skill in an ethical manner (Greene, 2004). While demonstrating ethical practice can certainly aid in the enhancement of ethical behavior among students, documentation of guidelines and punishment for inappropriate computer behavior, among other items, is still necessary. Logan and Clarkson (2004) identified five areas on which universities should focus attention as they develop and/or strengthen security programs in an attempt to prevent student misuse and abuse of acquired skill. Attention to these areas would, ideally, prevent students from using their skill in an unethical manner as well as demonstrate to the larger population, the skeptics in particular, the ethicality and utility of teaching students to "hack, write malicious code, or use forensic tool sets" (Logan & Clarkson, 2005, p. 157).

First, few universities have programs in computer security. Administrative officials in those that do tend to not be concerned with hands on experiences of security students. Logan and Clarkson (2004) argue that structured courses with plenty of opportunity for hands on learning experiences combined with an understanding of the potential for misuse of university resources and learned skills would strengthen security programs. While many would argue that formally teaching students how to write viruses and break in to systems only increases the likelihood that some would use these skills in malevolent ways, others would argue that most computer sciences already posses these skills. As such, a main focus of courses that teach hacking should be on understanding these practices and preventing such malevolent acts (Logan & Clarkson, 2004).

Another issue that must be considered is the fact that certain tools installed on a university network that will aid in the instruction and practice of security students could pose a risk to the network or possibly violate computer law. University networks also tend to be less secure in general, so it is important that strict regulations and a clear understanding of those regulations exists within computing departments (Logan & Clarkson, 2004).

An essential aspect of any computing program that teaches forensic and hacking skills must be coursework in ethics. At present, few computing students are required to take ethics and law classes. It is unrealistic to expect these students to understand the full ramifications of their potentially illegal behavior if they are not schooled in these areas. Universities cannot assume that students are inherently ethical or knowledgeable and the likelihood that a student will use his newly acquired skills to commit a malevolent act will likely decrease dramatically when required to take computer ethics and law courses. "…a casual warning about legal/university consequences in a syllabus or brief comment about ethics in an introductory course will [not] be sufficient against rouge activity" (Logan & Clarkson, 2004 p. 68).

Logan and Clarkson acknowledge that many fields of study require strict background investigations and students must pass certain psychological tests before being allowed in the field. They question why such a practice does not exist in the field of computer science considering the fact that basic computer knowledge in the hands of a malicious or unstable person could produce catastrophic results. A criminal background check, the requirement of some sort of professional certification, and student interviews are a few measures that could potentially weed out several, if not all, students with potential malevolent intentions (Logan & Clarkson, 2004).

Finally, by giving more attention to not only the discovery of students misusing their skill and university systems but actually reacting to these discoveries university officials can send a message that computer crime is a serious campus infraction that will be punished. At present, many universities not only make little effort to publish computer policy and infraction penalties, they rarely punish the infractions that are discovered. As such, many students either do not realize that their actions are illegal, or they simply do not care. When university guidelines are published before infractions occur, they can work as a preventative measure against computer crime. Other guidelines more specific to computer security students could target their newly acquired skills, and when fully explained, prevent many students from using their knowledge in negative ways while still allowing opportunities to strengthen skills (Logan & Clarkson, 2004).

6. CONCLUSION

As is evidenced by the information provided, teaching university level students how to hack is a legitimate means of identifying company network weaknesses and preventing malicious attacks can be an effective component of computer security programs. This skill will provide students with an important skill as they move in to the professional arena where network security is vital to many companies. As with many skill sets, it is not unlikely that a handful of students would use their newfound skills in a malicious way rather than for the intended purpose. Therefore, it is important to school students in the ethical and legal implications of the misuse of their skills. Overall, however, instruction in ethical hacking would be a useful and critical component of computer security programs at universities.

7. BIBLIOGRAPHY

[1] Greene, Tim (2004). *Training Ethical Hackers: Training the Enemy?* Retrieved June 20, 2006 from http://www.infosecwriters.com/texts.php?op=display&id=185.

[2] Hartley, Regina D. (2006). Ethical Hacking: Teaching Students to Hack. (Doctoral Dissertation, East Carolina University, 2006).

[3] Johnson, Doug (2004). *Teaching Students Right from Wrong in the Digital Age*. Ohio: Linworth Publishing.

[4] Logan, Patricia & Clarkson, Allen (2005, February). *Teaching Students to Hack: Curriculum Issues in Information Security*. Paper presented at the Special Interest Group on Computer Science Education Symposium, St. Louis, MO.

[5] Logan, Patricia & Clarkson, Allen (2004, June). *Is it Safe? Information Security Education: Are We Teaching a Dangerous Subject?* Proceedings of the 8th Colloquium for Information Systems Security Education, West Point, NY.

[6] Norfolk, David (2001). *Understanding Ethical Hacking*. PC Network Advisor. 128 7-12.

[7] Poteat, Vance E. (2004, October). *Classroom Ethics: Hacking and Cracking*. Paper presented at the Consortium for Computing Sciences in Colleges Annual Conference, Orem, UT.