Ethical Hacking as a risk management technique

Syed A. Saleem
MSIS Student, Kennesaw State University
134 Parkmont Way, Dallas GA 30132
404-316-1441
syedsaleem@gmail.com

ABSTRACT
The rapid growth of the Internet has brought many constructive and valued solutions for our lives such as e-commerce, electronic communication, and new areas for research and information sharing. However, like many other technological advancements, there is also an issue of growing number of criminal hackers. Businesses are scared of computer experts who will penetrate into their web server and change their logo, steal their private emails or credit card numbers, or put in software that will quietly transmit their organization's data to somebody in another country. The need is to train our computer science students with ethical hacking techniques, so that they can fight against criminal hackers. Also, organizations should hire experts with hacking expertise to combat above mentioned problems. Hence, this paper will discuss ethical hackers; their expertise, attitude, how they assist their customers and their pros and cons.

Categories and Subject Descriptors
C.2.0 [Computer-Communication Networks]: Security, General-Security and protection
C.4 [Performance of systems]: Reliability, availability, and serviceability, fault tolerance

General Terms
Security, Management, Reliability

Keywords
Ethical hacker, White hat hacker, Network Security, Computer Security, System Security, Information Security

1. INTRODUCTION
Hackers are commonly known as bad or terrible people in our society. They are also known as crackers or black hats. The reason is that majority of computer users are somehow victim of malicious activities by other users who are expert in computers. The important thing to understand is not all the hackers are bad as some people are doing penetration of a system in the limits of

ethical standards to understand the vulnerabilities in their system or their clients system, also called white hat hackers. Ethics (from Greek word ethos meaning "custom") is a branch of philosophy, which attempts to understand the nature of morality; in order to distinguish right or wrong (Wikipedia, 2006).

Morality is influenced by one's internal or external environment. For example, if you are Hindu, it is wrong to eat beef. If you are Muslim or Jewish it's considered wrong to eat pork but Christians probably eat both (Informit, 2006). Although there is a difference between ethics and religion, but above example is used to explain how different people have different perception of right or wrong, depending on their religion, culture or society. The term "hacker" has a double usage in the computer industry (Palmer, 2001). Originally, the term was defined as:

1. A person who learns the particular details of computer systems and the possible ways to extend their abilities, unlike the most users of computers, who are learning only the minimum skills necessary.
2. A person who programs devotedly or who enjoys programming instead of only theorizing about programming.

This flattering description was frequently extended to the verb form "hacking," intended to explain the rapid creation of a new programs or the making changes to existing complex programs (Palmer, 2001).

2. BACKGROUND
The definition of ethical hacking (SecuritySearch, 2006) is "a computer or network expert who attacks a system on behalf of its owners, seeking vulnerabilities that a malicious hacker can exploit". Ethical hacking is one of the growing areas of ethics and Information Security. The term "ethical hacker" has become popularized by corporations hiring security professionals to test their systems for vulnerabilities and describing these individuals as "ethical hackers".

Since computers became available in universities and schools, all the groups of people have been using them. Everybody wanted to use them, especially students involved in research. Some of these computer systems were so expensive that access to them was restricted. Users with limited access tried to use their expertise to decode a system or steal a password just so that they can have the full access. As network or system administrators found out about the intrusions, they made their systems more secure, and some of the computer users (experts) had started reacting because they were not able to access the protected systems anymore. Once successful in their intrusion to more secure systems, some of them have started damaging the systems for fun or profits. Also, the media recognized the act of

InfoSecCD Conference'06, September 22-23, 2006, Kennesaw, GA, USA.

unauthorized access in the past, by printing stories of people involved in the hacking activities (Palmer, 2001).

3. EDUCATION AND TRAINING

As the ethical hacker will have the keys to the front door and probably will have the access to crucial business information, he should be:

- Trustworthy
- Aware of when to stop before the system get damage
- Expert in Risk Management (recovery to original situation if anything goes wrong)
- Expert of his field

They should be trustworthy as they will have the access to the critical business secrets. It can be a disaster for an organization if their trade secrets or security issues in their systems get published on the internet. Ethical hackers should be experts in risk management and incident response to any outside or inside criminal attacks. Usually they are people with the most expertise in computer hardware and software. They typically are expert in programming, networking skills and have been in computer field for several years. In other words they should be better in skills and intelligence than any other black hat hacker in order to protect the system.

As Information security courses are being added into the curriculum of computer science, many instructors are designing labs exercises that cover information system auditing or ethical hacking. The practice first emerged within the U.S. intelligence community and military where "tiger teams" would simulate attacks against government IT assets to determine vulnerabilities. The teams would employ the same tools and techniques as malevolent intruders but would cause no harm (Greene, 2004).

A question remains about the legality of teaching students to hack, in order to improve their intrusion detection skills. The same question was asked last year when the University of Calgary announced plans to offer a virus writing course with the stated goal of improving the understanding of virus mechanisms. Opponents of virus writing course argue that formal instruction in writing viruses only encourages more illegal activity. Dr. Ken Barker, chair of the Department of Computer Sciences at the university, contends that "most computer-science graduates today already have the technical knowledge to create a virus" and that the focus of the course is understanding and prevention (Brandt, 2006).

Besides teaching students or computer professionals how to hack a system, it's as much necessary to give them awareness about ethical values in computing activities. Students with major in computer science normally don't take courses in law and ethics. A survey of a graduate class at Marshall University found that not a single student had read the University's Accepted Use Policy. Many students don't know that there are laws against unauthorized access to mp3 files or networks (Logan & Clarkson, 2006). There should be a method to test the students or trainees of ethical hacking courses to make sure they understand the legal and unethical sides of hacking. The formal methods can be surveys, Q&A and discussions.

4. GUIDELINES FOR ETHICAL HACKING

New challenges in the area of information security are arising with time. If computer experts will try to follow the old techniques, they can be fooled by others. Kevin Beaver who is an expert in information security mentioned ten lessons, for ethical hackers, from his own experience. First, make sure everything is in writing and approved. It can happen that you as a computer professional perform a task with an outcome as a crash of a system or loss of a data. There should be a complete documentation which should identify assets, stakeholders and responsible management team with signatures. If you have approval from upper management you will be safe, otherwise it can be a nightmare for yourself and your lawyers. Second, identify your goals, why you want to do this? What is the required output? Which systems and which information needs protection etc. For example, an ethical hacker goal is to investigate a Microsoft Windows base, server and find its vulnerabilities, so that he can replace the system with UNIX based server.

Third, don't try to test all the system at once, prioritize and test only the critical components of the system. Fourth, unimportant components need be tested too, as most of the time ordinary components like workstations with no confidential information become a threat. Fifth, think like criminal hackers, only regular system checks with sophisticated tools are not enough. Try to look at the system from different angles and look for manual hacking techniques too. Six, It's important to have the right tools which will make the job easier. Seventh rule is that ethical hacker should make sure that he is performing the tasks at the slow times or night times when there is less traffic. Hacking tools are usually complex and they can crash the systems if the network is overloaded with traffic. Ninth, if the ethical hacker is unable to penetrate in the system, it doesn't mean that system is secure as there can be a view of the system which he overlooked. Finally, prioritize your tasks; attack the vulnerabilities which are most important in terms of high impact, if exploited, and high likely hood of being exploited. These ten rules or guidelines give an ethical hacker or security professional, a framework to succeed at his task (Kevin, 2003).

5. ADVANTAGES AND DISADVANTAGES

Hiring an expert to hack the system and then fixing the vulnerabilities, sounds a very simple task but it is very complex one. It can cost an organization a good amount of money to find the weaknesses in a system and it is possible that the result will be useless information. Sometimes, security holes are needed in a system because of the way it works, e.g. access to vendors so that they can easily communicate with our system (Bernard, 2004). On the other hand, if you hire an ethical hacker and do nothing else, it can be useless. On the day the hacker will complete the penetration in the system, the system will be at the same level as it was before penetration. The reason is that the ethical hacking only gives you a big picture of the weaknesses in the system which can be changed with little changes in the system, destroying the effort of the ethical hacker.

The benefits of training ethical hackers far out weigh the risks associated with it. It is imperative that all trainers teach the countermeasures to each attack strategy. New laws are continually being written and old ones are being brought up to

date to deal with people that have weak morals. After completing a hacking course, a student should be aware of how difficult it is to successfully remain invisible online, after post September 11 Attacks. Unfortunately, following policies are the situations where we drop the ball. Policies that aren't up-to-date often miss the threat that new technologies like USB flash drives exist. Some of these "memory sticks" look like an ink pen, which makes it difficult to recognize the person who has them. After completing "hacker" training, a student may have the mind set and abilities to use a device like this to readily steal information or execute security tools in order to attack a resource, possibly undetected. Every effort should be made to properly draft and regulate good security policies. If a student's sense of right and wrong fails, fear often will provide guidance (Greene, 2004).

CONCLUSION

The method of testing the system reliability by trying to damage it is not new. Whether an automobile company is testing cars by crashing the cars in a controlled environment, or an individual is testing his skills at an army training camp by sparring with another people, is generally accepted as reasonable. Identification of vulnerabilities is useless without regular auditing, persistent intrusion detection, high-quality system administration practice, and computer security knowledge. A simple breakdown can expose an organization to cyber attacks, loss of income or mind share, or even something worse. Every new technology has its advantages and its risks. Ethical hackers can only assist their clients in better understanding and identifying of their security needs, it is the responsibility of the clients who decide whether to address them or not.

REFERENCES

1. Beaver, Kevin, CISSP (2003). Ethical hacking: Ten crucial lessons. Retrieved on June 21, 2006. http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci941500,00.html

2. Bernard, Allen (January, 2004). The Pros & Cons of ethical hacking. Retrieved on June 25, 2006. http://www.cioupdate.com/trends/article.php/3303001.

3. Brandt, Andrew (2003). Class on virus creation Draws Industry Ire. Retrieved on July 15, 2006. http://www.pcworld.com/resource/printable/article/0,aid,110938,00.asp.

4. Clarkson, Logan (2006). Teaching Students to hack: Curriculum issues in Information Security, ACM Library. Informit Network (2006). Ethics, hacking and religion. Retrieved on July 1, 2006 from http://www.informit.com/guides/content.asp?g=security&seqNum=191&rl=1

5. Palmer, Charles (April, 2001). Ethical Hacking. Retrieved on June 20, 2006 from http://www.research.ibm.com/journal/sj/403/palmer.html.

6. Greene, Tim (July 2004). Training Ethical Hackers: Training the Enemy? Accessed July 5, 2006 www.ebcvg.com/articles.php?id=241

7. Regina, Hartly (2006). Teaching Students to hack Retrieved on June 26, 2006 from http://www.infosecwriters.com/text_resources/pdf/Ethical_Hacking_RHartley.pdf