Proceedings of the 11th Colloquium for Information Systems Security Education
Boston University
Boston, MA June 4-7, 2007

What Are Faculty Attitudes Toward Teaching Ethical Hacking and Penetration Testing?

Jeffrey Livermore, *Walsh College, Member, IEEE Computer Society*

Abstract – Ethical hacking is the controversial practice of employing the tools and tactics of hackers to test the security precautions protecting a network. Ethical hacking is becoming an accepted business practice and a number of schools are including ethical hacking in their Information Assurance (IA) curriculum. Some educators feel that it is necessary to know how to attack a network to truly understand how to defend a network. Schools that teach ethical hacking provide instruction to students along with the hardware and software tools they need to conduct ethical hacking exploits. Schools with Information Assurance or Information Security programs need to address the ethical, legal, and practical issues surrounding teaching ethical hacking. These issues include liability for damages caused by attacks, security lab design, and curriculum design. Schools that provide access to the hardware and software necessary to hack into outside systems must accept the legal and ethical responsibility for the actions of their students using these computing resources. This research project consisted of a literature review to identify the ethical issues involved with ethical hacking followed by a survey of IA faculty members to determine their attitudes toward these issues. The surveyed faculty members agreed that ethical hacking and penetration testing should be taught along with a course on ethics. The faculty did not feel that incoming students should be screened for criminal backgrounds or that teaching penetration skills should be limited to law enforcement personnel. The faculty did agree that student should be made to sign a student code of conduct before being allowed to access IA computer labs and that those labs should be multi-platform labs that can be isolated from other networks.

Index terms – faculty attitudes, ethical hacking, penetration testing

I. Introduction

Internet crime has steadily increased in recent years. System attacks are becoming more and more sophisticated. Expert system administrators and IT managers need to continually develop more effective defenses. Many industry experts feel that in order to develop effective defenses, system administrators must understand how the attacks are developed and deployed [1]. 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. These schools compete with commercial training firms that offer the Certified Ethical Hacker certification [2].

Ethical hackers attempt to break into systems and networks to find weaknesses that might be exploited by criminals [3; 1]. Companies have been hiring ethical hackers for years to conduct security analyses [4; 5]. Major firms such as Visa and MasterCard utilize ethical hackers to test their defenses [6]. The Ace Group and other insurance companies that insure IT systems, may require that the system be tested by ethical hackers before providing a quote [6].

Not everyone is convinced that teaching college students how to attack systems is an ethical or wise course of action [7]. Some educators are concerned that teaching dangerous skills to immature and unqualified students may be socially irresponsible. Some educators are willing to teach ethical hacking and penetration skills but only under controlled circumstances and to screened students.

II. Justification for Teaching Ethical Hacking

One of the earliest examples of ethical hacking was when the United States Air Force evaluated the security controls of the Multics Operating system [8]. The Air Force formed "tiger teams" that tried to break into the Multics system. The teams performed their penetration under realistic circumstances. Ethical hacking emerged in the mainstream when the Security Analysis Tool for Auditing Networks (SATAN) was posted to Usenet by Dan Farmer [3].

Many academics and industry practitioners feel that the best way to prepare system defenses is to understand the attacks that the systems will face [9]. The people who attack systems are typically programmers while the defenders are not [9]. These different backgrounds affect the design of attacks and defenses. Defenders need to understand how attacks are designed and launched.

Students with hacking skills will be better prepared to work as network administrators with better chances of landing jobs than students without these skills [1]. The same tools used to attack systems are also used to develop defenses to protect them [10]. Deloitte, Ernst & Young,

ISBN 1-933510-96-7/$15.00

IBM, and KPMG all provide ethical hacking services and need to hire students with ethical hacking skills [6].

Colleges are including ethical hacking and penetration testing in their IA and Computer Science programs. The University of North Carolina (UNC) at Charlotte's College of Information Sciences is offering a course called Vulnerability Assessment and System Assurance [11]. UNC's course is modeled after courses taught at military institutes. The course will be taught by ethical hackers and cover the ethical as well as technical implications of ethical hacking. There will be lab component to the course, which will teach case studies of ethical hacking. The University of Abertay Dundee in Scotland will also be offering a course in ethical hacking [12]. The university announced that it was offering this course to meet market demand.

III. Problems Associated with Ethical Hacking

There are benefits to teaching ethical hacking but there are problems that lead some to question this practice. Schools may be teaching dangerous skills to students that are unable to make correct decisions on how to use these skills. Some students with criminal backgrounds or troubled backgrounds may not be good candidates for admission to IA programs and ethical hacking classes. Schools may also be held liable for their students' actions using the school's hacking tools and computer labs.

3.1 Ethical Issues

One of the concerns about teaching ethical hacking is that the wrong people may be taught very dangerous skills. Traditionally, hacking skills were acquired by many hours of practice or intense tutoring from another hacker [1]. University programs and commercial training classes are providing a new way for aspiring hackers to learn how to penetrate systems.

Teaching students how to attack systems without providing ethical training may be teaching criminals and terrorists how to pursue their illegal activities [1]. Wulf [10] compares teaching ethical hacking to undergraduate students to handing them a loaded gun. The use of many hacking tools outside of an isolated test network may be illegal [10].

3.2 Legal liability

Adding ethical hacking to the curriculum raises a variety of legal issues. Schools and individual faculty members may be held liable for the actions of their students [13]. Unmonitored penetration testing may be a breach of the law and violate a school's software licensing agreements [1]. The United States versus Morris decision determined that the Computer Fraud and Misuse Act (18 USC 1030) applies and that an individual is liable for the accidental release of malware [14]. Schools that facilitated the creation of malware would be liable for damages from malware released from their labs.

3.3 Forcing Services and Information on Organizations and Society

Ethical hackers test the security of networks, Web sites, and applications without the permission or knowledge of their owners. The rationale for this testing is that they are only testing security and do not intend to cause damage or compromise any individual's privacy [1; 15]. Ethical hackers can uncover information about Web sites and applications that the owners of these sites and applications do not want uncovered. Schneier [15] compares it to finding a note on your refrigerator informing you that "I was testing the security of back doors in the neighborhood and found yours unlocked. I just looked around. I didn't take anything. You should fix your lock." When Nathaniel Heatwole tested airline security by smuggling in a box cutter, faux explosives, and bleach on to airliners he stated that he was only testing security precautions but was prosecuted for his actions [15]. Neither the airlines or the government had asked Mr. Heatwole to test their security precautions.

Randal Schwartz, an Intel employee, was also prosecuted for testing security precautions [10]. Mr. Schwartz discovered that a fellow employee was using a weak password. Mr. Schwartz then copied the password database from the server and executed a password cracking program. When Mr. Schwartz's activities were discovered by Intel, he was terminated and prosecuted even though he had no criminal intent. Intel had not asked Mr. Schwartz to test their security precautions.

Hole, Moen, and Tjostheim [16] studied consumer authentication at Norwegian Internet banks. They discovered that customer authentication was weak and presented a vulnerability to criminals. Hackers would have been able to access accounts and also conduct an effective denial of service attacks against the banks. These three researchers presented their findings to the banks and the government agency that regulates them. A similar vulnerability was found in the Norwegian Public Service Pension Fund's Web applications. The researchers were surprised that the banks and the government did not react and took their findings to the press. The researchers felt justified in publishing information about the vulnerabilities to force changes in the Norwegian banking industry.

IV. Potential Solutions

There are a number of problems with teaching ethical hacking but there are also a number of steps that schools can take to reduce their liability and prevent teaching

dangerous skills to the wrong students. Schools can teach ethics in their curriculum, screen students, have students sign a code of conduct, and construct computer labs that minimize the chances of accidental or intentional abuse. Schools that take these steps improve the chances of having a successful IA program that includes ethical hacking and penetration testing.

4.1 Teaching ethics

Teaching ethics can be traced back to Plato and Aristotle [17]. These ancient Greek philosophers felt it was important to teach ethics as part of the curriculum taught to all students. The principles behind ethical decision have not changed over the years and including them in IA curriculum makes sense by preparing students to make sound ethical decisions. Vartiainen [18] documented the need for teaching ethics to students by presenting them with case studies. In a case study of coding a virus, only 70% of the students found the virus creation to be ethically unacceptable. Similarly, 37% of the students found it ethically acceptable to access students' records through a loophole in their school's security system.

Some schools have chosen to dedicate an entire course to the ethics of ethical hacking [19]. For example, The West Chester University of Pennsylvania has a course dedicated to ethics and security. Their course covers privacy, ethics, legal issues, information warfare, malware, and defenses. Logan and Clarkson [1] conducted a study on how many of the National Security Agency designated Academic Centers of Excellence require a course on ethics in their Information Assurance programs. These researchers found that 62% of the Centers of Excellence offered an ethics course but only 34% require students to take it.

Some schools include ethics in all of their IA courses. For example, The University of Houston includes ethics in all four of their Information Security courses [20]. Every lab exercise includes a "reflective observation" on what the goals of the lab exercise are. Ethical issues are intertwined with the technical issues and can be discussed as each technical issue is addressed [19]. Harris [21] agreed that students should be reminded of their and the school's ethical responsibilities throughout their curriculum. Poteat [7] states that students will naturally bring up ethical questions when discussing networking and assembly programming.

Plymouth State University and Armstrong Atlantic State University require students to develop a security policy for the school as one of their assignments [22;23]. Developing a solid security policy requires the students to understand the school's security needs, vulnerabilities, and the threats to their computing assets. The students enjoyed and benefited from this assignment and it has been made a permanent part of the curriculum.

4.2 Screening applicants

Endicott-Popovsky [17] recommends screening applicants to IA programs before admission and forcing the accepted students to participate in an orientation that explains the issues at participating in an IA program. Some schools will only teach some IA topics to law enforcement personnel [24]. Some schools, such as the University of Calgary, do not believe in screening applicants and will provide the knowledge to anyone who seeks it [25].

In colleges and universities, undergraduate students are typically taught to experiment and try to apply new methods in different situations [10]. This can be dangerous when presenting undergraduate students with hacking tools in IA courses. These courses should be offered later in the curriculum that will be taken by older students and only after completing adequate prerequisites [25; 21; 1].

4.3 Student Code of Conduct and Computer Usage Agreement

Schools that provide access to computer hardware and software should consider having a student code of conduct that the students sign [17]. The code of conduct should clearly state that improper forms of hacking are both unethical and illegal [1]. Having a carefully written code of conduct that spells out boundaries for student behavior and the consequences for unacceptable behavior may help limit the school's liability [13]. The code of conduct should be signed by the student [21; 13]. The George Washington University (GWU) requires faculty to make certain that their students have read and understand their student code of conduct [13]. GWU students are required to sign the code and agree to adhere to the school's ethical code. This signed agreement can be used in court to demonstrate that the school and faculty made a good faith effort to explain the consequences of the student's behavior.

4.4 Licensing and Professional Certification

Towell and Thompson [26] conducted a study on teaching ethics in software engineering curriculum. They discovered that 46% of the respondents felt that software engineering should be a licensed profession. Academics held this opinion more strongly than practitioners. Most industry association memberships and certifications require agreement to their ethical code of standards. Losing licensure or certification would cost the abuser their legitimate livelihood. The issue of licensing and certification raised more comments from the survey

participants than any of the other topics in the survey instrument.

4.5 Security Lab design and Isolation

To teach Information Assurance, schools need to have labs equipped with software and hardware tools to reinforce the material presented in texts and lectures [20]. For example, the University of Houston has equipped their labs with scanners, sniffers, firewalls, and intrusion detection tools [20].

Schools that construct computer labs for teaching ethical hacking and penetration in their information assurance programs must take precautions to ensure that their labs are not used to harm outside organizations. Information assurance labs should be able to be isolated from all networks outside of the classroom [14; 10]. Having a security lab partitioned off by firewalls for student use does not completely solve the liability issues [21]. Students can still create malware in the security lab and transfer it to outside networks via alternative channels.

Many schools have trouble justifying the expense of having computer labs dedicated to security [14]. Designing and building labs that are adaptable for a variety of uses encourages inter-departmental collaboration [27]. Crowley [20] recommends configuring the labs with a variety of operating systems including Windows and Linux. Plymouth State University accomplished this by installing a second hard drive in each of the lab computers [23]. The operating systems that are attacked and destroyed by student activities should be installed via imaging solutions (King, et al.).

V. Research Methodology

A survey instrument was developed to solicit faculty opinions on the issues identified during the literature review conducted for this paper. The instrument presents twelve statements about teaching ethical hacking that the faculty members are asked to indicate whether they agree with, disagree with, or have no opinion about. The survey instrument was distributed to 137 faculty members at 29 NSA designated Academic Centers of Excellence. All of these faculty members had their e-mail addresses available on their school's Web site. The 29 schools selected were the Centers of Excellence that either received or had their NSA CAE designations renewed in 2006.

The survey instrument was distributed via e-mail between January 23 and February 4, 2007. Responses were accepted until February 13, 2007. A total of 32 surveys were returned from faculty at 14 different schools for a 23.3% return rate.

VI. Results

The survey data shows that IA faculty is in agreement on the issues surrounding ethical hacking. The results were not always unanimous but with one exception, they always showed an overwhelming majority. More than 71% of the faculty members agreed that schools should be teaching ethical hacking and 62.5% of those faculty members agreed that it should not be restricted to undergraduate students. Despite the recommendations of some faculty and lawyers, 53% of the faculty members do not want to screen students for criminal backgrounds prior to admission to an IT program. A significant number of faculty members (15.6%) are undecided on this issue.

There is a correlation between the answers on these first three statements. Fifty percent of the faculty members agreed with one or more of these restrictions. One half of the faculty members who agreed with one of the restrictions agreed with one or more of the other restrictions. It is important to note that one half of the faculty members did not want to restrict teaching ethical hacking to anyone.

Three fourths of the faculty members felt that their schools should require an ethics course as part of the IA curriculum. A similar number of faculty members feel that ethics should be part of every IA course in the curriculum.

All but one of the faculty members agreed that students should be required to sign a lab usage agreement prior to being allowed to access school computing labs. The faculty was unanimous in their opinion that the school's IA labs should be multi-platform to allow student to attack and defend a variety of computing platforms. The majority of faculty members (75%) felt that the IA should be taught in a lab that can be isolated from other networks.

The faculty was also unanimous in their opinion that students should not be allowed to scan networks without the permission of the network owner. A large majority of the faculty (90%) felt that students should not be allowed to scan the school's network.

The faculty members surveyed were also asked to identify any other issues that they associated with teaching ethical hacking and penetration testing. The only issue raised by more than one faculty member was the pejorative effect of using the terms ethical hacking and penetration testing.

Faculty members typically provided a definite agreement or disagreement to the statements. The exception was the statement that IA professionals should be required to maintain a professional license or certification. More

than a third of the respondents did not have an opinion on this issue. The remaining responses were split between agreement and disagreement with one more faculty member disagreeing with the need for licensure or certification than agreeing.

The survey instrument was flawed and incomplete. Several of the respondents documented their objections to the terms "ethical hacking" and "penetration testing" that were used in the questions one and two. These terms can be pejorative and prejudice anyone who is taking the survey. Alternative terms and definitions provided at the beginning of the survey would have greatly improved the survey instrument. The results of the survey are illustrated in Table 1.

Table 1: Survey Responses

Statement	Agree	No Opinion	Disagree
1- We should not teach ethical hacking or penetration testing	8		23
2- We should not teach ethical hacking or penetration testing to undergraduates	9	2	20
3- We should screen applicants	8	5	17
4- We should require an ethics course	24	4	3
5- We should include ethics in every IA course	23	3	4
6- All students should sign a lab agreement	30	1	
7- We should teach in an isolated lab	24	2	5
8- We should have a multi-platform lab	31		
9- Students should not scan without permission	31		
10-Students should not access school network	29		2
11- IA professionals should be certified	9	12	10
12-Only teach forensics to law enforcement	2	1	28

VII. Conclusion and Recommendations

The surveyed faculty made it clear that their schools need to require students to sign lab usage agreements and not scan any network without the permission of the network owner. Faculty members would also like to have access to multi-platform computer labs to teach in. These labs should have the ability to be isolated from other networks so students cannot access the school network.

The data collected in this research project has value to the administrators that are responsible for Information Assurance programs at any school. Faculty opinions on lab design and configuration will affect the curriculum that can be taught in the labs. There are issues that faculty members agree on and there are issues where there is disagreement. Faculty members are concerned about the ethical implications of their work. Roughly a third of faculty members do not believe that undergraduates are equipped to handle certain skills and that we should not be teaching them how to penetrate systems. The author and a minority of faculty are concerned about teaching certain skills to students without regard to their background or situation in life. The ethical consideration should be considered when designing curriculum along with mapping curriculum to national standards. Administrators may wish to survey their faculty to determine which issues need to be addressed at their schools.

Reference List

[1] Logan, P., & Clarkson, A. (2005). Teaching students to hack: Curriculum issues in information security. *Proceedings of the 36th SIGSE Technical Symposium on Computer Science Education*. (pp. 157-161). St. Louis, MO.

[2] Schoenberger, C. (2003, September 15). A week at hacker camp (Intense school course in ethical hacking). *Forbes*. 172(5), 199.

[3] Langley, N. (2005, July 26).Hot skills as criminal IT activity increases, security skills are in demand: Ethical hacking is challenging and lucrative but training is expensive. *Computer Weekly*. (pp. 44).

[4] Mohan, S. (1999). Ethical hacking finds network holes. *InfoWorld*. 21(8), (pp. 45, 51).

[5] Sisk, M. (2003). Betting students will be drawn to ethical hacking. *US Banker*. 113(6), 12.

[6] Pesola, M. (2005, June 17). Computer crime victims seek ethical hacker's aid. *Financial Times*. p. 3).

[7] Poteat, V. (2005). Classroom ethics: hacking and cracking. *Journal of Computing Sciences in Colleges*. 20(3), 225-231.

[8] Palmer, C. C. (2001). Ethical hacking. *IBM Systems Journal*. 40(3), 769-780.

[9] Arce, I. & McGraw, G. (2004). Why attacking systems is a good idea. *IEEE Security & Privacy*. 2(4), 17-19.

[10] Wulf, T. (2003). Teaching ethics in undergraduate network security courses: The cautionary tale of Randal Schwartz. *Journal of Computing Sciences in Colleges*. 19(1), 90-93.

[11] Teaching Ethical Hacking (2005). *BizEd*. 4(2), 49.

[12] Shifrin, T. (2006, June 27) Dundee to teach ethical hacking MSc. *Computer Weekly*.
[13] Ryan, J., & Ryan, D. (2002) Institutional and Professional Liability in Information Assurance Education. Retrieved October 26, 2006 from: http://www.danjryan.com/Institutional%20and%20Professional%20Liability%20in%20Information%20Assurance%20Education.doc.
[14] Caltagirone, S., Ortman, P., Melton, S., Manz, D., King, K., & Oman, P. (2006). Design and implementation of a multi-use attack-defend Computer security lab. *Proceedings of the 39th Annual Hawaii International Conference on System Sciences* (pp. 220-226). Kauai, HI.
[15] Schneier, B. (2003). Airplane hackers. *IEEE Security & Privacy*. 1(6), 92.
[16] Hole, K., Moen, V., & Tjostheim, T. (2006). Case study: Online banking security. *IEEE Security & Privacy*. 4(2), 14-20.
[17] Endicott-Popovsky, B. (2003). Ethics and teaching information assurance. *IEEE Security & Privacy*. 1(4), 65-67.
[18] Vartiainen, T. (2003). A study of computer science student's ethical attitudes and its implications to small group discussion in computer ethics education. *ACM SIGCAS Computers and Society*. 32(6), 3.
[19] Epstein, R. G. (2006). An ethics and security course for students in computer science and information technology. *Proceedings of the 37th SIGCSE Technical Symposium on Computer Science Education*. (pp. 535-537). Houston, TX.
[20] Crowley, E. (2004). Experiential learning and security lab design. *Proceedings of the 5th Conference on Information Technology Education*. (pp. 169-176). Salt Lake City, UT.
[21] Harris, J. (2005). Maintaining ethical standards for a computer security curriculum. *Proceedings of the 1st Annual Conference on Information Security Curriculum Development*. (pp. 46-48). Kennesaw, GA.
[22] Katz, F. (2005). The effect of a university information security survey on instruction methods in information security. *Proceedings of the Information Security Curriculum Development Conference*. (pp. 43-48). Kennesaw, GA.
[23] LeBlanc, C., & Stiller, E. (2004). Teaching computer security at a small college. *Proceedings of the 35th SIGCSE Technical Symposium on Computer Science Education.* (pp. 407-411). Norfolk, VA
[24] Gottschalk, L. Liu, J., Dathan, B., Fitzgerald, S., & Stein, M. (2005). Computer forensics programs in higher education: A preliminary study. *Proceedings of SIGSCE*. (pp. 147-151). Retrieved November 18, 2006 from ACM Digital Portal database.
[25] Aycock, J. & Barker, K. (2005). Viruses 101. *Proceedings of SIGSCE '05*. (pp. 152-156). St. Louis, MO.
[26] Towell, E., & Thompson, J. B. (2004). A further exploration of teaching ethics in the software engineering curriculum. *Proceedings of the 17th Conference on Software Engineering Education and Training*. (pp. 39-44). Norfolk, VA.
[27] King, K., Manz, D., Ortman, P., Shikashio, D., & Oman, P. (2006). A rapidly reconfigurable computer lab for software engineering security experiments and exercises. *Proceedings of the 19th Conference on Software Engineering Education and Training Workshops*.

.