International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 11 Issue 4 –NOVEMBER 2014.

ETHICAL HACKING AND LEGAL SYSTEMS

Dr. V SUBHASHINI

HOD, Department of Zoology, KBNCOLLEGE

Subhashin_vsn@yahoo.co.in

Abstract— This paper deals with faculty attitudes toward teaching ethical hacking to Computer and Information Systems undergraduate students. The authors examine issues that should be considered when designing information security curriculum. Furthermore, the paper discusses issues involved when faculty teach students how to hack and explores the issues involved in designing and information security course with laboratory components that can involve destructive actions. 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. Finally, this paper will provide university administrators with an idea of the issues encountered when designing an information assurance curriculum, and at the same time demystify the term of hacking or ethical hacking between faculties. More research should be done on how to integrate the concept of ethics, not in just an isolated course but across the information assurance curriculum.

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 corporations 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 "attacker" 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. However, not everyone is convinced that teaching college students how to attack systems is an ethical or wise course of action (Poteat, 2005). Moreover, some educators are concerned that teaching dangerous skills to immature and unqualified students may be socially irresponsible. Other educators are willing to teach ethical hacking and penetration skills but only under controlled circumstances and to screened students (Livermore, 2007).

1.1 HACKING

The term hacker is defined as a person who accesses computers and information stored on computers without obtaining permission. Logan and Clarkson (2005) described 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).

1.2 ETHICAL HACKING AND PENTESTING

Ethical hacking is defined as the practice of hacking without malicious intent. According to Palmer (2004, as quoted by Pashel, 2006): "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". Moreover, 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). An increasing number of corporations are implementing practices of ethical hacking in order to identify and correct security flaws. One of the more effective ways of testing network security is penetration testing or ethical hacking. Penetration testing is often done to help monitor, identify, track, and diagnose any faults within

the system as well as to assess the number of vulnerabilities present. Witman and Mattford (2003) declared "Penetration testing involves security personnel simulating or performing specific and controlled attacks to compromise or disrupt their own systems by exploiting documented vulnerabilities. Security personnel attempt to exploit vulnerabilities in the system from the attacker's viewpoint and are commonly referred to as white hat hackers or ethical hackers" (p. 455).

Additionally, many university programs have increased 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. If you want to catch a criminal, you have to be able to think like one.

1.3 JUSTIFYING INFOSEC COURSES: TEACHING ETHICAL HACKING According to the US Government document: "The National Strategy to Secure Cyberspace", "Education and outreach play an important role in making users and operators of cyberspace sensitive to security needs. These activities are an important part of the solution for almost all of the issues discussed in the National Strategy to Secure Cyberspace". Therefore, there is a need for security that transcends the implementation of a single course, but instead should be integrated throughout a program of study in Information Systems or Computer Science.

Moreover, information security prepares IT students to recognize and combat information system threats and vulnerabilities. There is a wide range of educational opportunities existing for individuals interested in pursuing information security education. Many of these opportunities are being offered in the public sector within community colleges and universities. It is interesting to note that while many schools offer such education and training, a number of professionals express concern about teaching hacking techniques. This apprehension stems from a fear that students may use the information unethically. Educational institutions counteract this assumption by offering concepts within an ethical framework (Sanders, 2003).

Moreover, some important college and university programs offer a variety of intensity and content in ethical hacking courses. For example, Syracuse University offered a Cyber Security Boot Camp to prepare future technology security professionals. The list of topics include cyber security, cryptography, steganography, digital forensics, network security, and wireless security. However, there are stringent rules for entry into the program, and the Boot Camp ends with "Hack fest" which is a hands-on event putting into practice the theoretical concepts covered within the course (Carnevale, 2005). To help government and businesses minimize security risk, colleges and universities are increasingly offering courses and security training programs.

Polytechnic University of Puerto Rico started to offer security courses at the undergraduate level since 2008. The four courses offered were: Ethical Hacking, Network Security, Computer Forensics, and Reverse Engineering & Software Protection. These course have become very popular, especially the Ethical Hacking course, that has always had an enrolment of more than 20 students when offered. The course on Reverse Engineering &Software Protection teaches students to use reverse engineering to learn about the function of malicious software, such as viruses, Trojans, and spyware, and create solutions that counteract that malware through detection, elimination, and prevention. Our experience has been that students that take these courses become highly attractive to the NSA and National labs such as Oak Ridge and Lawrence Livermore for internships and coops.

1.4 ISSUES ASSOCIATED WITH ETHICAL HACKING Hartley (2006) stated that the problem of teaching students to hack is still a very serious issue to face today; course leaders feel that this will teach students how to improve intrusion. To understand the true intentions of students is very hard to identify, and the reason why ethical hacking should be used is very much a debate. Teaching a student to hack and later discover that knowledge was used to commit crimes will definitely have an impact on society. Why were they allowed to understand how to hack in the first place? We cannot simply pinpoint the argument to say that it was the fault of the course leaders that allowed him to undertake the course.

Livermore (2007) declared that there are benefits to teaching ethical hacking but there are also problems. Universities may be teaching dangerous skills to students that are unable to make correct decisions on how to use ethical hacking skills. Moreover, some students with criminal backgrounds or troubled backgrounds may not be good candidates for admission to Information Assurance programs and ethical hacking classes.

Therefore, universities and colleges may also be held liable for their students' actions using hacking tools and computer labs.

Moreover, Logan and Clarkson (2005) stated that a question remains about the legitimistic of teaching students to hack in order to improve their intrusion detection skills. According to PCWorld.com (2004), as cited by Logan and Clarkson (2005), the University of Calgary offered a virus writing course with the stated goal of improving the understanding of virus mechanisms. Many opponents argued that formal instruction in writing viruses only encourages more illegal activity, but Dr. Ken Barker, chair of the Department of Computer Sciences at the university of Calgary 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.

1.4.1.1 ETHICAL BEHAVIOR IN COMPUTING

Logan and Clarkson (2005) manifested that one of the concerns about teaching ethical hacking is that the wrong people may be taught very dangerous skills. Teaching students how to attack systems without providing ethical training may be teaching criminals and terrorists how to pursue their illegal activities. Many students do not often take courses in ethics

and law, which are more usually offered in the social science or the business curriculum. As a consequence, students are not often taught the law with respect to computing and electronic transmission. (Logan & Clarkson, 2005). Furthermore, Pashel (2006) declared that just as young children learn best through behaviour modelled by adults, computing students can learn ethical behaviour best through modelling of professors and other professionals as opposed to learning it in the classroom. Moreover, demonstrating ethical practice can certainly aid in the enhancement of ethical behaviour among students, documentation of guidelines and punishment for inappropriate computer behaviour, among other items, is still necessary (Pashel, 2006). When a computer science and information system curriculum does not require a course in ethics and law, a course in information security should emphasize the ethical responsibility of the security professional who is entrusted to protect data assets (Logan & Clarkson, 2005). Moreover, training students to attack systems without the ethical or legal constructs to understand their actions carries the risk of training future security professional and hacker's side-by-side.

The intent of information security training is to improve information security and to educate future security professionals.

Training students to be ethical professionals should begin with an instructor (Logan & Clarkson, 2005). Universities and Colleges that provide access to computer hardware and software should consider having a student code of conduct that students must sign before any ethical hacking course (Endicott-Popovsky, 2003). The code of conduct should clearly state that improper forms of hacking are both unethical and illegal. Having a carefully written code of conduct that spells out boundaries for student behaviour (and the consequences for unacceptable behaviour) may help limit the school's liability (Ryan & Ryan, 2002).

1.4.2 LEGAL LIABILITY

Many universities and colleges must be aware of the risk and legal issues of adding ethical hacking courses to the curriculum. In addition faculty members may be held liable for the actions of their students. Legal issues have to be considered when conducting penetration tests, in order to protect the universities' data; colleges must take measures to guarantee the availability, confidentiality and integrity of data or to ensure access for authorized persons only. Livermore (2007) stated unmonitored penetration testing may be a breach of the law and violate a school's software licensing agreements. In addition, schools that facilitated the creation of malware would be liable for damages from malware released from their laboratories. 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.

1.4.3 SCREENING STUDENTS

Logan and Clarkson (2004) stated that once a student acquires new hacking skills they may use them for good or even for bad intentions. However, certain policies need to be applied at the university level to address issues about students conducting malicious acts. These issues can be rectified by universities applying security checks on individuals for certain courses such as ethical hacking. A criminal background check (required for some professional certifications), and student interviews, are a few measures that could potentially weed out several, if not all, students with potential malevolent intentions. Moreover, Jamil and Ali Khan (2011) presented that the idea of corruption can be seen as a major issue in ethical hacking. Additionally, Logan and Clarkson (2004) acknowledged that many fields of study require strict background investigations and students must pass certain psychological tests before being allowed in the field of cyber security.

1.4.4 DESIGN AND USE OF SECURITY LAB

To teach Information Assurance, universities need to have laboratories equipped with software and hardware tools to reinforce the material presented in texts and lectures.

According to Livermore (2007) universities that construct computer laboratories 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 isolated from all networks outside of the classroom.

According to Gephart and Kuperman (2010) it is difficult for colleges to implement hands-on security exercises for students. Moreover, Yang, Yue, et. al (n.d) stated that computer science educators who are interested in teaching computer security in a "realistic" context are thus faced with a unique challenge: for Setting up 'realworld'computer in security laboratories and assignments without negatively impacting the rest of the campus network.

II. RESEARCH METHODOLOGY

An online survey instrument was developed to assess faculty attitudes toward teaching ethical hacking to computer and information systems undergraduates' students. The instrument presented nine statements about teaching ethical hacking and faculty members are asked to indicate whether they agree with or disagree with it. In addition, faculty were asked to complete one open question in which they have to describe their opinion of teaching ethical hacking to undergraduate's students. The online survey instrument was distributed into two different faculty groups, one group from a public and the other from a private university. Two emails reminder were sent to complete the online survey for a total of 13 completed surveys.

III. RESULTS

In general, the online survey data (please see Table 1) showed that faculty from public and private universities agree

that institutions should teach ethical hacking (100%, public, 87% private) at the same time they are agreed that institutions should teach hacking to undergraduates students (100% public, 87% private).

However, despite the recommendations of some faculty and lawyers, 75% of the faculty (from public) and 85% of the faculty (from private) universities do not want to screen students for criminal backgrounds prior to admission to an IT program. On the contrary, 25% of the faculty (public) and 14.29% of the faculty (private) agreed on screening students before teaching them how to hack.

Moreover, faculty members felt that their schools should require an ethics course as part of the information assurance curriculum, 80% faculty (public) strongly agreed and 75% faculty (public) agreed and strongly agreed. Contrary of what is expected a number of faculty members feel that ethics should NOT be part of every information assurance curriculum (20% public and 25% private).

A tremendous amount of faculty members agreed, and strongly agreed (100% public and private), that students should sign a laboratory liability agreement. When faculties where asked if the information security courses should be taught in and isolated laboratory, 80% of the faculty (public) and 85% of the faculty (private) agreed or strongly agreed. However, 20 % of the faculty (public) and 14.29% of the faculty (private) disagreed that courses should be taught in and isolated laboratory.

For the most part faculty from public and private institutions agreed all security courses should have a multiplatform laboratory (100% public, 100% private). Having a multiplatform allows student to attack and defend a variety of computing platforms.

The faculty was also unanimous in their opinion that students should not be allowed to scan networks without the permission of the network owner Likewise, faculty members surveyed were also asked to describe in an open question their opinion of teaching ethical hacking to undergraduate's students. Some of their comments were:

Faculty (Public):

1. I like the idea very much because it gives students more opportunities for employment

2. It is fine and encouraged as long as you put boundaries and controls into the infrastructure used for testing and training. It should not be an invitation to try and break down the university system or any other system without prior authorization and strict terms of non-disclosure.

3. I believe it is appropriate, however, students must be aware of responsibilities and held accountable for their acts. Faculty (Private) It seems like it would make a good special topics course for undergraduates.

2. I think that ethics is a very important subject that should be taught not only in graduate and sub-graduate level but in High School too [sic.]. The sooner the better.

3. It is a must to teach Ethical Hacking

IV. CONCLUSION AND RECOMMENDATIONS

In general the online survey results showed that faculty agreed to teach ethical hacking skills to undergraduate students. In addition, faculty agreed on the requirement for students to sign laboratory usage agreements and also agreed that students should not scan any network without the permission of the network owner. Moreover, faculty did not agree on background checks before enrolling students in any information assurance course. However, ethics was a topic of great concern principally because faculty members agreed ethics should be part of the hacking curriculum. In terms of school liability, all participants agreed that the university and user could be held as responsible for misconduct behaviour. Therefore, schools who are teaching how to hack need to have policies and guidelines for manage any liability issues.

In a July, 2012 conference, National Security Agency Director General Keith B. Alexander addressed the attendees of the Defcon hacker conference in Las Vegas and asked for their help to secure cyberspace. "This is the world's best cyber security community," said Gen. Alexander, who also heads the U.S. Cyber Command. "In this room right here is the talent our nation needs to secure cyberspace." Hackers can and must be part, together with the government and the private industry, of a collaborative approach to secure cyberspace, he said. Hackers can help educate other people who don't understand cyber security as well as they does, the NSA chief said. "You know that we can protect networks and have civil liberties and privacy; and you can help us get there." Certificates for graduate and undergraduate students should be offered in more colleges and universities in the security field of Ethical Hacking. A typical curriculum for an Ethical Hacking certificate may be composed of the following courses: Ethical Hacking, Advanced Ethical Hacking Tools, Reverse Engineering & Software Protection, Computer Forensics, and Network Security.

ACKNOWLEDGEMENT

This material is based upon work supported by, or in part by, the U. S. Army Research Laboratory and the U. S. Army Research Office under contract/grantnumber W911NF1110174.

V. REFERENCES

[1] Carnevale, D. (2005). Basic Training for Anti-Hackers: An intensive summer program drills students on cybersecutity skills. Chronicle of Higher Education, 52(5), pp. 41-41.

[2] Endicott-Popovsky, B. (2003). Ethics and teaching information assurance. IEEE Security & Privacy .1(4), 65-67.

[3] Gephart, N., and Kuperman, B. (2010). Design of a virtual computer Lab environment for hands-on information securityexercises. Retrived from:

[4] http://www.cs.oberlin.edu/~kuperman/research/papers/xenlabs2010ccsc-mw.pdf

[5] Livermore (2007) what are Faculty Attitudes toward Teaching Ethical Hacking and PenetrationTesting?Proceedings of the 11th Colloquium for Information System Security Education, Boston, MA.

[6] Logan, P., & Clarkson, A. (2004). 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.

[7] Logan, P., & Clarkson, A. (2005). Teaching students to hack: Curriculum issues in information security