Teaching Students to Hack: Curriculum Issues in Information Security

Patricia Y. Logan Ph.D.
Associate Professor
Marshall University Graduate College
Charleston, West Virginia 25303-1600
(304) 746-1951
Loganp@marshall.edu

Allen Clarkson, M.S., MCSE
Independent Consultant
San Antonio, Texas
(210) 863-0610
allen@espressodonkey.com

ABSTRACT
Teaching "hacking" as a legitimate means of training students in how to protect a future employer's data assets has been introduced into courses with increasing frequency. The introduction of "red teaming" and attack-based exercises into information security courses presents a potential ethical problem. This paper explores the issues involved in designing an information security course with lab components that involve destructive actions.

Categories and Subject Descriptors
Security

General Terms
Security

Keywords
Information security, education, computer security, computer science education, hacking, information assurance, ethics and computers

1. INTRODUCTION
With the introduction of information security courses into the computer science curriculum has come content that includes labs and exercises that emphasize a form of internal security auditing known as "ethical hacking." Instructors have begun to construct labs and develop exercises that teach students how to employ the tactics and exploits of hackers.[1] 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. [2] 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". C.C. Palmer in the IBM Systems Journal says, "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." [3] Farmer and Venema advocated an approach to improving security that included breaking into one's own system using the argument that they were "trying to help systems administrators to make informed decisions on how to secure their site." [4]

At its simplest, hacking is accessing a system without authority or beyond one's authority. It includes the application of computer skills to find vulnerable systems, penetrate systems, and to remove evidence of access to a system. These skills most often are acquired from diligent practice, or through directed assistance from experienced hackers (possibly via chat rooms, web resources, black hat groups). With the introduction of information security courses, both proprietary and academic, these skills can now be acquired with less effort. Additionally, vendors have introduced the idea of ethical hacking certification such as the CEH (Certified Ethical Hacker) offered by the EC-Council. [5] Arguments in favor of "ethical hacking" as an important security practice are: 1) that hacking skills are equivalent to audit skills as both are designed to discover flaws in the protection of data and secure operation of a system. Just as auditors test systems for security or operational flaws, hackers "test" systems through attack; 2) knowledge of hacking skills and practice in attacking secured systems improves security by informing network administrators of how an exploit can be executed; and 3) to provide the best security defense, a systems administrator must possess the same skills as the attacker. These arguments in favor of "ethical hacking" have been lifted up as justification for including these skills in information security courses at both the undergraduate and graduate levels. Courses have been designed to teach students to hack, with the implication that it is a necessary security practice and that it will improve employability as a network administrator charged with protecting valuable corporate assets.

This paper deals with the implementation of courses in information security with a lab component that includes exercises in hacking. The authors examine some curriculum issues that should be considered when designing information security curriculum. The paper discusses four issues for universities and CS departments that arise from students learning to hack, write malicious code, or use forensic tool sets. These areas are:

SIGCSE'05, February 23-27, 2005, St. Louis, Missouri, USA.

1. Appropriate hands-on course content for security and forensics classes
2. The design and use of security labs
3. Student awareness of ethical behavior in computing
4. University response to student attacks

2. Appropriate Hands-On Course Content for Security and Forensics Classes

It can be argued that hacking tools, methods, and other types of security course content are readily available on the Internet; a Google™ search reveals hacker web sites and tool sets with instructions and chat rooms for personal assistance. Within CS departments, however, there has been a quiet inclusion of this same content within the context of a course of study in information security without much discussion of the potential for misuse or abuse by students. Courses that include hacking often state that they are providing practical knowledge in identifying, detecting, and responding to intrusions. Students are theoretically being equipped to interpret the output of intrusion sensors, identify whether a system has been compromised, learn to contain the intrusion and perform necessary actions to eliminate the source of the intrusion and return affected systems to secure operation. The problem is that anyone can hack a network and describe the results of a scan but network administrators will need to put the results into a business context in order to manage an intrusion. They must describe to management the nature of the security risk as well as the remedies that will mitigate the risk. Any hack performed on a network should be part of a larger security audit process designed to reveal vulnerabilities and improve security policies and procedures. Professionals in security assessment believe that hacking a network will only give a snapshot in time [6] but an organized security audit is designed to provide an on-going assessment of vulnerability. Students that perform a single exercise perform the actions of hacking and not of defense. Students should learn to protect their networks from common intruder methods of attack but should also be able to perform vulnerability assessments on the entire spectrum of data assets: applications, policies, procedures, and physical infrastructure.

Universities that include undergraduate or graduate majors in information security and offer courses in network or computer forensics often have been designated by the National Security Administration as Centers of Academic Excellence in Information Assurance (CAE). Using the published list (2004) of NSA Centers of Academic Excellence in Information Assurance (CAE) there are 59 U.S. universities that have these courses and offer a major or emphasis in information security at the undergraduate or graduate level. Implementing these courses often means approval by university curriculum committees. At that level, questions are seldom raised about the content of hands-on exercises or the security of the lab facilities. Course developers may offer reassurances that the content would not be dangerous or that the risk is necessary in pursuit of guiding students to be effective network administrators.

Many universities offer information security courses with labs only at the graduate level. Allowing these courses only at the graduate level possibly ensures that students are more mature, gainfully employed, and therefore, less likely to use course content for malicious experimentation. These assumptions are not supported by the history of on-campus hacking cases which involve both undergraduate and graduate students. Some universities avoid the issue altogether by not teaching hands-on content or having separate labs away from general student access to practice their skills. Book and lecture-based instruction is not always as effective in demonstrating concepts as hands-on experience. Separate labs help reduce malicious activity initiated from within their confines, but that solution alone does nothing to protect the wider network from experimentation on other nodes. A question remains about the legitimacy 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 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. [7]

The authors reviewed the web sites for the CAE schools and where available examined the on-line syllabi for evidence that a course included lab instruction or activities in hacking. Most of the schools had received funding for a specialized computer lab that enabled testing of security precautions. These labs were described as set-up to facilitate the testing of systems through attempts at penetration. The syllabi for information security courses that contained a lab component revealed the following types of activities required of their students: writing port scanners, writing a propagating virus, writing an exploit program, creating a shell to gain root privilege, packet sniffing, injecting a packet, war games competitions, and attack teams hacking a "secure network". The course content in any of these courses did not appear to include recovery activities, intensive vulnerability assessments of a simulated corporate network, network forensic investigations. As systems administrators will reveal, their job is seldom fighting hackers in computer-to-computer combat. Most systems attacked have security applied, including some high-profile systems with better than average security (Microsoft). The most devastating hacks are often exploits that do not include strong technical knowledge (i.e., password guessing, social engineering, using Google). A recent report from the financial industry the *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector* [8] compiled by the U.S. Secret Service and the CERT/CC at Carnegie Mellon showed that 87 percent of the attacks were from insiders who exploited non-technical vulnerabilities (business rules, organization processes, procedures) and were carried out by those with little technical skill. A number of questions should be asked about the appropriate content for courses in information security: How should students be taught to implement network and desktop security? Is hacking and virus-writing a pre-requisite for developing strong technical skills in detecting malicious activity? What course content (if any) should be off-limits? Should courses follow the content for CISSP certification or SANs technical seminars for GIAC certification? Does it necessarily follow that hacking skills for future network administrators will improve security and their employability?

A starting point for designing information security courses is to establish what skills will add the most value to the security of the enterprise. Faculty should examine the value of exercises that attack a system, and assignments that encourage the creation of

malicious programs. No research has yet shown a direct positive benefit between the special knowledge of hacking and the subsequent improved security of a network. Red team exercises and attack competitions carried out as events isolated from the over-all responsibilities for security will focus student-attention and their knowledge retention on the "thrill" of the hunt (or attack) rather than on a security message.

In advance of developing assignments and exercises that include the creation of malicious code, attacks on secure networks or the use of tools to find network vulnerabilities, faculty should determine if these activities can be justified within the context of the learning goals of the course. These courses should include assignments that mimic the job responsibilities of security administrators. Students need to be taught methods of detecting attacks from inside that do not use traditional hacker's methods. Recent study shows that 28% of attacks were from existing employees and 21% from former employees. Hacker tools sets and skills do nothing to protect a company from this threat. An over-emphasis on attack scenarios may do a disservice to students as they will believe they possess the total skill set to protect a company from attack focusing on the perimeter and not what is inside the network. [9]

Courses in information security with a lab component should include activities that present the greatest challenges to information security in the enterprise. These include: restoration of a hacked system to full operation, creation of an enterprise security plan, collecting evidence of a network attack for law enforcement, and the skills to perform a proper security audit (meaning people, policies, and technology). Assignments that are weighted heavily toward red team exercises and attack-defense labs present an unrealistic view of the skill sets needed to be an effective information security professional. Students should not assume that technology or policies will insure success: as good security planning includes the plan for an inevitable failure.

Summary: CS departments need to be practicing, considering, and justifying the methods used to train students in information security. Course developers should consider that systems administrators seldom spend their days waiting to respond to an intrusion. The reality of administering a secure network is that it is often practicing to fail. Systems administrators will need to have a variety of skill sets to effectively implement security, not just the skill to hack a system. These skills include the ability to perform security audits, maintaining a secure network, recovering from intrusion, and planning for disaster recovery and business continuity. Course content needs to cover the entire spectrum of security management and not just the exercise in attack and defense or the creation of malicious code.

3. The Design and Use of Security Labs

Universities have received funding for "cyber battlefield" labs that simulate a corporate network and enable students to attack a system in a controlled environment. The lab can simulate a broad range of real-world cyber-threats and enable students to perform vulnerability assessments, test defenses, and implement tool sets. These specialized labs can give instructors an opportunity to provide "hands-on" exercises that provide an "in the trenches perspective and understanding of how the various technologies work." [10]

The configuration of these specialized security labs and their connection to the university network should be carefully considered. University CS departments often depend on university computing services to maintain labs and install software. What happens when security and forensics courses require installation of tools that if connected to a university network would potentially do damage and violate computer law? Where computer science departments use a general purpose university lab for computer science students, who protects against the improper use of the tools? Should departments assume the risk and configure and manage labs for high security to prevent potential rogue activity? What happens when universities, such as Marshall University, West Virginia house the state's digital evidence lab for the state police, as well as student computer forensic training labs? If computing services require additional tools to effectively manage these unique labs, who will pay for them if they are not part of an existing effort to manage security? In at least one course reviewed by the authors, it was obvious that the instructor was using a lab that was not disconnected from the wider university network as the instructions explicitly said, "Do not attack beyond xxx.xxx.xxx.xxx." The list of universities that have been attacked by students (most recently UC Berkeley) would indicate that university resources are not always well-protected. Improperly configured security labs that allow access to the wider university network (whether by mishap or design) may place the university assets in a vulnerable position as well as expose the university to legal liability. Unmonitored penetration testing of a class network that is connected to other networks and systems may be a potential breach of law and licensing restrictions of software. [11] Instructors typically allow students to attack without approving the specific actions that will be used. One instructor stated in such an exercise that any student able to secure the root password, by any means automatically earned an A in the course. In several syllabi, students had assignments that simply requested that a student find a hacking tool, test it, and demonstrate it to the class.

A university and campus computing services has a legitimate interest in knowing about these exercises and making sure that students are properly guided in their actions. Computing services departments have a better understanding of the technical relationships among student labs, administrative databases, university data services, email, and the systems and controls that link them all together. In part, computing services can offer expertise in isolating CS students in these courses, but also they can help identify potential flaws in a lab's design that can lead to security breaches.

Summary: The design of information security labs should involve careful planning and include consultation with computing services. Including computing services in the design of security labs and curriculum can prevent complicating security further by stemming one potential source of intrusion.

4. Student Awareness of Ethical Behavior in Computing

CS students do not often take courses in ethics and law, which are more usually offered in the social science or the business curriculum. Students are not often taught the law with respect to computing and electronic transmission. A survey of a graduate computer security class at Marshall University found that no students had read the university's Acceptable Use Policies (AUP). Most students are surprised to find that there are laws against

copying MP3 files and unapproved wireless access to networks on campus. Each year at least one instructor can give an example of students that have managed to find their way into the instructor's network drive, WebCT or other network services that compromise grading or tests. Given the ethical lapses of Enron and Anderson, it appears that business schools were doing an inadequate job of describing to MBA students ethics and the law that resulted in flagrant violations. Universities should never assume that students learn ethical behavior, the laws on illegal network/computer access, outside (or before) their time at the university.

In order to determine whether universities were requiring their CS students to take a course in ethics and computer law, we reviewed computer science major requirements from the websites of the institutions listed on the NSA website as CAEs. These schools were chosen as a representative sample of those that place a high priority on information security curriculum. The statistics represented in Figure 1 ***do not*** reflect an opinion on CAE programs or course offerings, but instead they represent CS programs at these same institutions. No inference should be drawn from this study regarding the individual CAEs. The integration of the CAE varies widely – some integrate directly into student CS curricula, while others are purely research centers, and still others offer their own academic programs entirely separate from the CS tracks.

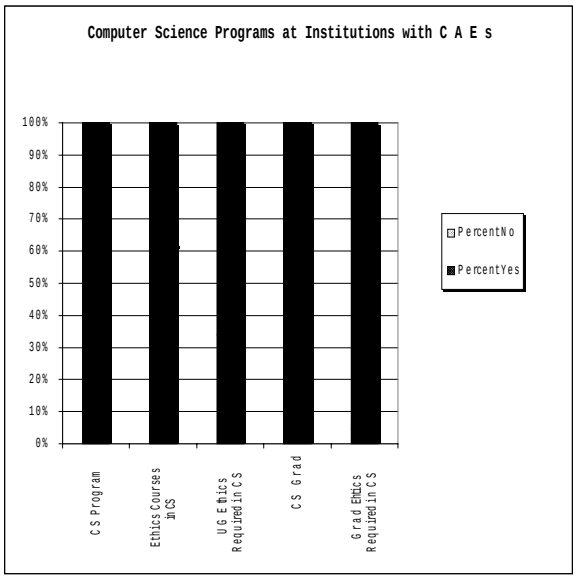

Figure 1.

The statistics show that while a solid majority (62%) have ethics courses in their CS program, an even larger percentage (66%) do not *require* undergraduate students to study ethical and/or legal issues as part of a degree program (includes both those institutions that do and do not *offer* ethics or legal issues courses). Further, 95% of all such institutions with graduate studies programs do not require ethics courses. These same universities often have international students that may be unfamiliar with the legal restrictions on computing activities in the United States. It is evident from these percentages that formal instruction in ethical and/or legal issues of computing is not a universal priority in CS curricula even in those institutions with a focus on security. The authors found in examining the syllabi for a variety of courses in security at CAEs that ethics about the use of computer facilities was not generally covered but unethical behavior with respect to cheating was fully explained in every syllabus. When a CS curriculum does not require a course in ethics and the law, a course in information security should emphasize the ethical responsibility of the security professional who is entrusted to protect data assets.

Could it be that we are training both the "good guys" – security professionals – and the "bad guys" – those with knowledge of techniques and tools but without exposure to ethical and legal issues – at the university level? The statistics from this study show that there may be a disconnect between the study of security and the translation of lessons learned to the rest of the computer-oriented curriculum. Reviewing the CAE schools, the pattern for offering these courses becomes clear: strong technical content and the absence of an ethics and computer law course. Many offer a single course in ethics and law as an elective. What student in this area would by-pass a technical course in order to take a course in ethics? It is apparent that instructors believe that a casual warning about legal/university consequences in a syllabus or brief comment about ethics in an introductory course will be sufficient warning against rogue activity.

Training students to attack systems without the ethical or legal constructs to understand their actions carries the risk of training future security professional and hackers side-by-side. The intent of information security training is to improve information security and to educate future security professionals. The idea of testing the security of a system by breaking it is not new. Is breaking into a system really the best way to teach students how to protect a company's data assets? Training students to be ethical professionals should begin with an instructor that models the behavior of an ethical security professional. Any exercises should include not only the technology but the soft attacks like social engineering, and malware from email attachments. Students should be steered toward the development of tools to assist in detection and strengthen systems to focus attention on their contribution to security. "Ethics do not replace good policies. Promoting ethical principles can instill positive behavior …but policies …provide clear and mandatory guidelines for acceptable conduct. Simply trusting the student to behave in an ethical manner is not enough". Class policies should exist to dissuade students with weak ethics. These policies should clearly present improper forms of hacking as illegal and unethical. All activities should be represented as right or wrong and not neutral or described as "ethical hacking …" [12] Each course should emphasize the role of the systems administrator in applying countermeasures. Proper security training should instill in students a strong ethical sense of what they should and should not do as security professionals.

Summary: As the role of information technology continues to increase in importance to business and critical infrastructures, additional consideration needs to be given to ethics awareness. Other professions, such as medicine, pharmacology and civil engineering, require that students be exposed to ethical and legal issues in their respective fields. Computer-oriented curricula need to include the same focus for those who will be operating modern infrastructure.

What should we teach in a course on ethics and law? Possible topics include: Cases from the CCIPS web site on FBI investigations and convictions of cyber-criminals, which includes some virus writers and improper access; a review of investigative

processes and the specifics of the laws on monitoring, search and seizure, and illegal access of protected data; ethical duties owed to employers and for those who are in the field of computing, the ACM code of ethics.

5. University reaction to student attacks

Universities have crafted Acceptable Use Policies (AUPs) to respond to the necessity of maintaining and securing computing facilities. Universities enforce AUPs with banners at logon that students quickly bypass reading. Students involved in security courses with hacking exercises do not usually provide a separate and trackable ID that allows network administrators to monitor their activities. In the absence of strong network security and an awareness of the need for creating monitored accounts, should a university worry about downstream liability? Can a university be held responsible for a student's malicious efforts aimed at a corporation or business? A principle tool in protecting the university is the AUP, but it can be most effective only when introduced to students *before* a violation occurs, as a preventative measure, rather than after the fact as a justification for prosecution. Students need to be made aware of AUPs as a regular practice in CS courses. It seems contradictory to give students tools and knowledge that may damage the university system, not explaining the necessary restrictions on their use, and then punishing students for violations.

Universities have seldom prosecuted students involved in malicious or unethical use of campus networks. Given the knowledge that many students possess from their own education in hacking, and exposure to information about campus network configuration from their security course lab, it is reasonable to assume that some students may cross the line at a moment of temptation or revenge. Students should understand the legal consequences for moving across the legal line and that their university is prepared to prosecute them for their actions. In the authors experience, computer science students that have performed their own network vulnerability scans on university networks and collected data from unauthorized sniffing have been caught and warned rather than prosecuted. This lenient treatment for a criminal act does not reinforce the seriousness of the offense and may reinforce the view that hacking is a trivial activity.

Summary: Most students are unaware of the university acceptable use policies and any restrictions they might impose. Students in security courses may need accounts that work only under monitoring, signed statements of an understanding of their responsibilities in learning security material, and actual dismissal if involved in misuse. CS departments should consider creating course-level AUPs to augment the university's general use policies that clearly delineate what is being explored for instructional purposes and what is expected of students in their extra-curricular application of the knowledge.

6. CONCLUSION

University CS departments are moving quickly into information assurance courses at both graduate and undergraduate levels with the current popularity of the major magnified by the large number of job opportunities available in security, access to large amounts of federal funding (NSF scholarship for service or instructional enhancement), and increased focus on the issues by society at large. Students are being trained to use tools and investigative procedures that provide knowledge of hacking and avoidance of detection. Instructors should carefully consider the design of all "red team" exercises that use tools and techniques that mimic criminal intrusion methods. The ethics of computing activities and the legal issues need to be included in the study of security techniques and tools.

REFERENCES

[1] http://thewhir.com/king/ethical-hacking.cfm, last accessed November 30, 2004.

[2] Greene, Tim, Training Ethical Hackers: Training the Enemy?, www.ebcvg.com/articles.php?id=241, last accessed October 14, 2004.

[3] C.C. Palmer,Ethical Hacking, IBM Systems Journal, www.research.ibm.com/journal/sj/403/palmer.html, last accessed November 30, 2004.

[4] D. Farmer and W. Venema, "Improving the Security of Your Site by Hacking Into It," www.deter.com/unix/papers/improve_by_breakin.html, last accessed November 28, 2004.

[5] http://www.eccouncil.org/CEH.htm, last accessed November 29, 2004.

[6] Bernard, Allen, The Pros and Cons of Ethical Hacking, www.cioupdate.com/trends/article.php/3303001, last accessed September 14, 2004.

[7] http://www.pcworld.com/resource/printable/article/0,aid,110938,00.asp last accessed February 25, 2004.

[8] *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector* http://www.cert.org/archive/pdf/bankfin040820.pdf

[9] The State of Information Security, 2004, L.C. Ware, CSO Research Reports, http://www.csoonline.com/csoresearch/report75.html, last accessed November 30, 2004.

[10] http://news.com.com/2102-1001_3-898084.html?tag=st_util_print last accessed February 25, 2004.

[11] Appreciating the Art of the Hack, D. Phillips, Legal Times, 02-06-2002

[12] http://news.com.com/2102-1001_3-898084.html?tag=st_util_print last accessed February 25, 2004