Journal of International Technology and Information Management

Volume 24 | Issue 4 Article 6

2015

Ethical Hacking Pedagogy: An Analysis and Overview of Teaching Students to Hack

Regina D. Hartley
Appalachian State University

Ethical Hacking Pedagogy: An Analysis and Overview of Teaching Students to Hack

Regina D. Hartley
Appalachian State University
USA

ABSTRACT

An area that is being scrutinized as a more effective method of educating and preparing security professionals is that of ethical hacking. The purpose of this research is to examine a more proactive approach to adequately prepare future information security professionals. Future careers in security may require that professionals be equipped with the necessary skill sets to combat an ever-growing presence of unwanted activity throughout the Internet. Many argue that future information security professionals need to have the same skill sets as attackers in order to adequately recognize and defend networks from intrusion. This research defines ethical hacking and examines the pros and cons of ethical hacking pedagogy as a viable approach for teaching network security to future professionals. The analysis includes the concept of ethical hacking education with an emphasis on ethical and legal concerns associated with ethical hacking pedagogy. The research concludes with an overview of existing best practices in ethical hacking education highlighting a hands-on approach as well as the inclusion of soft skills needed to complement the technical hard skills for future information security professionals.

Keywords**:** Ethical hacking, information security instruction, ethical hacking pedagogy

INTRODUCTION

The prominence of information technologies and increasing dependence on technological infrastructures continues to infiltrate all of society. It may be argued that some concern stems from the apparent lack of security inherent within information technologies and systems. Of particular importance is our growing reliance on the Internet and networking capabilities. The Internet has provided vast opportunities in a wide array of areas not possible in prior years. Today we are able to access massive amounts of information, and connect in unprecedented ways.

Along with the positive capabilities provided by the Internet and networking, unpleasant aspects also infiltrate in unexpected ways. While various crimes have existed for many years, the Internet and information technology have brought computer crime into our homes and businesses in unimaginable ways. Criminals of today have a new platform for conducting activities, and many individuals are so bewildered at the subsequent onslaught from these endeavors that in many cases only reactive measures may be implemented.

The purpose of this research is to analyze the use of an ethical hacking pedagogical approach to improve information security instruction. A hacking methodology appears to be a more offensive and proactive approach for information security instruction. This approach may be effective to better prepare future information security professionals to combat unethical hacker intrusions associated with the Internet and computer networks. Future information security professionals

  ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

would be better equipped to combat intrusions if equipped with the knowledge and skill sets currently used by attackers. In order to equip those professionals, students must be prepared to fight the ever-growing challenges associated with effectively securing computer networks.

This research defines ethical hacking pedagogy followed by an overview of this approach in information security instruction. The ethical and legal implications are addressed regarding teaching students how to hack. Finally, a review of best practices in the field are examined featuring components necessary to use ethical hacking as a viable approach for teaching network security to students.

A qualitative study was conducted focusing on the research question underlining the analysis of an ethical hacking pedagogical approach to improve information security instruction. Information was acquired utilizing the Belk Library and Information Commons at Appalachian State University. Searches were conducted in the databases and journals at the university. The databases are organized by subject matter, and "computer information systems" provided the majority of the literature. Two of the major databases utilized in this research were ACM Digital Library and the IEEE Computer Society Journals. General searches were also conducted with a basic search engine, which assisted in providing additional materials.

ETHICAL HACKING

This research examines ethical hacking by defining what it is along with the effectiveness of using an ethical hacking pedagogical approach to instruct future information security professionals. Based upon a review of the literature, there appear to be two primary approaches concerning computer security instruction. One method focuses on the instruction of the theoretical concepts alone, and the other includes a hands-on laboratory component to reinforce the theoretical concepts. One approach that appears to be effective in computer security instruction is that of ethical hacking.

Ethical hacking may be thought of as a methodology for assisting computer professionals and administrators in their efforts to secure networks. As such this topic will be reviewed in light of its effectiveness for instructing proactive offensive measures to students in computer security courses.

The basic assumption associated with ethical hacking is merely that of a different approach to security. Ethical hacking is primarily penetration testing and includes penetrating the "system like a hacker but for benign purposes" (Oriyano, 2014). It is felt by many that students need to experience first hand what the attacker will be doing and what tools will be used (Ethical Hacking: Student courseware).

Ethical hacking may be further defined as the "methodology adopted by ethical hackers to discover the vulnerabilities existing in information systems' operating environments" (Ethical Hacking: Student courseware). Finally, it may be defined as someone with the same skill sets as an attacker, but differs in the fact that permission has been granted from the owner to test the security system of the target (Oriyano, 2014).

ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

There are a number of classes of hackers such as Black Hats who are highly skilled, but have malicious and destructive intent. They are also the ones whose actions fall outside of what is considered legal. White Hats, in contrast, are hackers who use their expertise for defensive security analyses, and who have permission to perform the tasks. Gray Hats hack for different reasons either ethically or unethically depending on the situation, and they may perform offensively as well as defensively (Ethical Hacking: Student courseware; Oriyano, 2014).

A hacker may be defined as a ”person who enjoys learning the details of computer systems and how to stretch their capabilities...One who programs enthusiastically or who enjoys programming rather than just theorizing about programming” (Ethical Hacking: Student courseware)**.** Originally hackers, or enthusiasts, were people who were merely curious and passionate about whatever technology was new at the time (Oriyano, 2014).

Greene (2004) suggests, “Ethical hackers and malicious hackers both attack computers, only their intent differs.” Pashel (2006) further elaborates that “Ethical hacking can be defined as the practice of hacking without malicious intent.”

Floyd, Harrington, and Hivale (2007) believe that it is important to determine how a hacker started and for what reasons. They suggest that there are two types of hackers, one that does it more out of curiosity and the “autotelic” thrill. Those are the ones that would make good ethical hackers. In contrast, some individuals may have been prone to unethical or illegal actions and have later turned to computers to assist with the crime.

Ethical hacking, or penetration testing is similar in concept to hiring external auditors. Organizations are increasingly using this methodology to evaluate the effectiveness of information security. These activities are used to identify and exploit security vulnerabilities thereby providing the organization with the necessary information to implement corrective measures (Using an Ethical Hacking Technique).

Logan and Clarkson (2005) propose that information security is a type of “audit” for computer systems. As such, hackings skills may be viewed as something similar to auditing skills as both attempt to uncover issues. They go on to suggest “Just as auditors test systems for security or operational flaws, hackers ‘test’ systems through attack” (Logan, & Clarkson, 2005).
Greene (2004) offers that testing of computer system is similar to “crash-testing cars.” In both examples, as an audit or crash-test, the objective is to make something better.

Yurcik and Doss (2001) offer that the "security of the Internet is broken and 'ethical hacking' has evolved as part of the potential solution." They go on to suggest that "'ethical hacking' may be one of the most effective ways to proactively plug rampant security holes" (Yurcik, & Doss, 2001). An increasing number of security professionals are advising companies to elicit the assistance of white hat hackers or ethical hackers for testing and consulting purposes (Using an Ethical Hacking Technique).

As noted earlier in the discussion, there appear to be two basic approaches in information security instruction. One focuses on theoretical concepts only, while the other highlights the concepts with a hands-on component. Trabelsi and McCoey (2016) feel strongly that covering only “theoretical

aspects of information security may not prepare students for overcoming the difficulties associated with the efficient protection of complex computer systems and information assets." They maintain that students must have opportunities to "experiment and practice with security technologies" in order to be equipped for contributions in the field of computer security.

ETHICAL HACKING EDUCATION

With the culmination of the definition of ethical hacking the conversation will now offer an overview of ethical hacking education to train future security professionals. Teaching students how to hack ethically may be seen as a worthy endeavor, and most researchers agree that it is critical for security professionals. Pashel (2006) proposes that the ability to determine weaknesses in computer systems can assist security professionals in preventing attacks. He goes on to offer that ethical hacking may be deemed a crucial element in a security program (Pashel, 2006).

An increasing number of researchers feel that it is important that computer administrators have comparable knowledge and skills as the attackers. It is important to determine what skill sets are needed by security professionals and help educate those skills (Logan, & Clarkson, 2005). Another researcher goes on to suggest, "As quickly as the field of Information Security is changing, the 'good guys' need all of the information and help that they can get" (Greene, 2004).

Many of the skills used in ethical hacking may be viewed as more proactive rather than reactive in nature. Security educators feel that teaching "offensive methods" produces better security professionals than teaching "defensive techniques" (Trabelsi, 2011).

A number of researchers and educators agree that practicing ethical hacking skills are crucial in developing necessary skill sets for computer security professionals. Trabelsi (2011) states that students should receive instruction to prepare them for robust research and development in their career. He goes on to propose, "One cannot perfectly design or build defenses for attacks that one has not truly experienced, first-hand" (Trabelsi, 2011).

In another study, Trabelsi (2012) argues that by not providing information and knowledge gleaned from hacking, computer security professionals are not adequately being prepared for their career. He goes on to suggest that teaching attacks is considered a necessary element of security education. Finally, Trabelsi and Alketbi (2013) state that techniques of ethical hacking should be included in a curriculum to better prepare security professionals.

ETHICAL AND LEGAL CONCERNS OF ETHICAL HACKING EDUCATION

After the review of ethical hacking education, ethical and legal implications of this approach to prepare security professionals must be addressed in light of concerns of educators and researchers within the field. The discussion will also address the use of a computer ethics policy as a means of reducing or prevented inappropriate behavior as a result of ethical hacking instruction.

Teaching ethical hacking may be viewed with skepticism concerning the ethics of providing students with a knowledge that may cause them to behave poorly. Still others argue that teaching hacking techniques could cause institutions to be faced with ethical and legal dilemmas.

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 prevail over this assumption by offering concepts within an ethical framework (Sanders, 2003).

A large number of those in favor of ethical hacking for teaching computer security also highly favor ethical and legal instruction. Pashel (2006) suggests that while some students may use their newly acquired skills to perform unethical activities, they should all receive the same instruction in ethical and legal implications that may result. Security instruction should assist students in developing ethics and what is expected as security professionals (Greene, 2004).

The majority of researchers studied were emphatic about legal and ethical instruction to accompany ethical hacking. It appears that some educators have felt that a hands-on course in ethical hacking is unethical, and that there is a potential for students to use "tools and techniques in an irresponsible manner" (Trabelsi, 2011).

Most researchers recognize and identify the necessity of offering ethical and legal information and training along with teaching hacking techniques to students. Logan and Clarkson (2005) feel there is a lack of ethical and legal instruction relating to computing and networking. They go on to suggest "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" (Logan & Clarkson, 2005).

Others offer legitimate concerns regarding what students will do with their newly acquired skill sets in computer hacking. One researcher poses the possibility of educating ethical hackers as well as "malicious hackers" at the same time (Greene, 2004). Still another argues that some question the "legality of teaching students to hack, in order to improve their intrusion detection skills" (Saleem, 2006).

As concerns about teaching students to hack abound, some studies have shown the apprehension to be a valid one. In one study, students apparently used their new hacking skills in unethical applications. According to Trabelsi (2011) there was "a major ethical concern" that became apparent when they studied logs from the university's intrusion detection system. Apparently students decided to use their new skills in activities outside of the classroom.

Another study by the same educator found that a "Number of injected malicious traffic targeting the university switches' CAM tables, increased considerably each time the students experiment the DoS attack" (Trabelsi, 2012). Seeking to validate concerns, the professor administered an anonymous questionnaire to the students. Alarmingly 88% of the students admitted to deliberately attempt to "sniff " the network of the university, and 70% confessed they tried to "hack" into faculty computers (Trabelsi, 2014).

In a more recent study, Trabelsi and McCoey (2016) once again found concerning statistics from an anonymous survey. Though the numbers were slightly lower, 85% of the students admitted to repeating the lab activity outside of the isolated classroom network. Only this time, it appeared

that the web and email servers were the targets of their attempts. On a more positive note, 89% of the students admitted that they did not have "malicious intent" in their efforts (Trabelsi & McCoey, 2016).

Computer use policy

One major step in deterring unwanted behavior in the instruction of ethical hacking instruction is the use of a computer ethics policy. Many argue that institutions must have a policy to assist in the process of instilling ethical behavior relating to new hacking skills. Greene (2004) argues that educational institutions need a policy to encourage ethical actions and to "dissuade students with weak ethics."

While policies are only one component, they are crucial in assisting institutions with creating an environment of ethical behavior. Greene (2004) goes on to offer that computer use policies can help regulate a sense of ethics and permitted behavior. He concludes by suggesting that educators must stress legal implications and information concerning the punishment for crimes. It is hoped that once students understand the legal aspects of unwanted behavior relating to ethical hacking instruction, that they will have second thoughts about acting unethically.

Logan and Clarkson (2005) also contend with the importance of computer use policies in institutions of higher education. They further recommend that, "CS departments should consider creating course-level AUPs to augment the university's general use polices" (Logan & Clarkson, 2005). They go on to offer that the tools and techniques used within the classroom be combined with instruction in ethics and legal issues (Logan & Clarkson, 2005).

While the use of a computer ethics policy contributes in reduction of unethical behavior by students in ethical hacking preparation, it is critical that they know of its existence and content. Saleem (2006) conducted a survey of students in a security class, and found that they had not read the university's computer policy. It is particularly important for educators to make students aware the institution's computer use policy in content and in practical application.

BEST PRACTICES IN ETHICAL HACKING EDUCATION

With the ethical and legal implications of ethical hacking now addressed, the attention will be placed upon the best practices currently being offered to prepare future security professionals. As shown in the literature, some of the best practices emphasize a hands-on approach and the incorporation of soft skills.

The curriculum for teaching ethical hacking techniques should adequately prepare students for a career in security. Bratus, Shubina, and Locasto (2010) offer that educators may refer to the "Hacker Curriculum" to access quality content to assist in the development of ethical hacking instruction. Trabelsi (2014) states that "a security education curriculum that does not give the students the opportunity to experiment in practice with security techniques" could potentially cause students to be inadequately prepared for a future career. He goes on to offer that students need to have the skills to feel confident in their ability to combat an attacker.

ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

In a more recent study, Trabelsi and McCoey (2016) found that if students have not had the opportunity to experiment with "real hacking" they might be found inadequately prepared. In particular, when it becomes necessary for them to "design and implement architecturally sound and efficient security solutions to thwart future attacks, especially with the quickly evolving threats" (Trabelsi, & McCoey, 2016).

The researchers go on to argue that students need to be able to identify an attacker and have a similar mindset when combating them. As a result, it is highly recommended that educators shift from a traditional approach to an "attacker's way of thinking" (Bratus, Shubina, & Locasto, 2010). They conclude by suggesting that educational offerings within the security curriculum should address both a "defender" and "attacker" perspective.

Still other researchers agree with preparing students to understand the mindset of attackers better prepares them to adequately defend a network as well as web applications in general. Saleem (2006) offers that computer students should be prepared with ethical hacking techniques to be able to fight attackers. Wu (2014) goes on to suggest that "thinking like a hacker and acting like an ethical hacker" is a critical skill for a successful career in security for web applications.

Continuing along with the defender and attacker approach, Lancor and Workman (2007) suggest that a "good defense" begins with understanding the opponent's offense. The educators offered Google hacking as a tool within a web security course. Students were exposed to a powerful approach in defending networks by using Google to perform attacks. The educators felt it critical to teach students how to protect against such Google attacks by intruders. They conclude by maintaining that the exercise worked perfectly in achieving the learning outcomes of being aware of security threats and how to protect networks (Lancor, & Workman, 2007).

Hands on Approach

The review of the literature concerning best practices appears to indicate that ethical hacking preparation demands a hands-on approach. Logan and Clarkson (2005) argue that training in ethical hacking should be conducted with a "hands-on" approach. The researchers go on to suggest that a "book and lecture-based instruction is not always as effective in demonstrating concepts as hands-on experience" (Logan & Clarkson, 2005).

Another researcher also agrees with the necessity of having a hands-on approach in teaching future professionals security concepts. Weiss and Mache (2011) offer that there should be "hands-on security in all core classes." They go on to propose that teaching security is critical in the curriculum, and that students learn best with a hands on approach. Trabelsi (2011) advises that a security curriculum with only theoretical components is not nearly as effective as a hands-on approach. He further suggests that students need experience and practice to contribute to "research and development in the computer security field" (Trabelsi, 2011).

Most agree that the quality of the instruction is critical to the success of the educational offering. Along with the importance of actually performing the hacking, the tools should be the effective in conducting the assignment. Greene (2004) argues, "Training students to use crippled or bogus

tools discounts the students their experience and may lead them to have a limited view of a real malicious attacker's power."

Students need to see that ethical hacking is only one component in a security plan. Logan and Clarkson (2005) offer that ethical hacking should be part of a larger plan. In addition to hacking there should be the vulnerability assessments that continue to monitor the network. The goal would be to perform the process as an ongoing basis to improve the overall security of the network. They go on to suggest that labs should provide "careful planning and include consultation with computing services" (Logan & Clarkson, 2005).

When students were anonymously surveyed concerning the hands-on lab instruction, 85% felt that the applications were useful and helped them to understand the theoretical concepts in the class. Moreover, 87% of the students indicated that they would like further hands-on lab instruction, and 86% felt they would recommend the lab activities to others (Trabelsi, & McCoey, 2016).

Soft Skills

A second area of best practices, as shown in the literature, indicates that soft skills should not be overlooked in ethical hacking education. Dimkov, Pieters, and Hartel (2011) propose that "teaching students only the technical side of information security leads to a generation of students that emphasize digital solutions, but ignore the physical and social aspects of security." It may be argued that often, when examining computer systems, a practice or instruction lacks the human component.

Some researchers favor soft skills that enhance awareness of a potential security threat in the form of the social engineering. Dimkov, Pieters, and Hartel (2011) state that social components increase security awareness for students and relates to social engineering. They go on to offer that security courses typically focus on digital components, which "provides an unrealistic view of the security requirements of an organization..." (Dimkov, Pieters, & Hartel, 2011). Greene (2004) also argues in favor of offering social engineering practice with a security curriculum.

Additional researchers had similar findings concerning the need for soft skills and social engineering. Bratus and Masone (2007) found that activities such as social engineering and understanding user preferences assisted students in understanding some of the aspects of computer behavior. Trabelsi and McCoey (2016) also discovered that students need "soft" skills such as social engineering, an enhanced understanding of security, and an understanding of an attacker's way of thinking to be successful in the field.

Upon the conclusion of the review of best practices in instruction of ethical hacking to prepare future security professionals, it must be noted that most educators and researchers agree that the pros outweigh the cons. Trabelisi offers that the ethical concerns relating to teaching hacking are small compared to the benefits realized for students (Trabelsi, 2011, 2012, 2013, 2014).

ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

CONCLUSION

The prominence of information technologies and networking permeate all aspects of our lives and society. Security concerns relating to attackers and intruders are causing many security professionals to examine and explore more proactive approaches to securing networks.

This research defines ethical hacking pedagogy, suggests ethical hacking as a computer security instruction methodology, and illustrates the ethical and legal consequences of teaching students to hack. Best practices in ethical hacking pedagogy were reviewed as well as suggestions and recommendations of the components for ethical hacking instruction, which may be needed to effectively instruct and prepare future information security professionals.

This research demonstrates that not only will future information security professionals need to be equipped with skill sets currently used by attackers, but students will also need skill sets to combat the persistent future advances and challenges imposed by attackers. In addition, future information security professionals will need similar hacker mindsets and skill sets to effectively secure networks from intruders. This research suggests that instruction in information security utilizing an ethical hacking methodology creates a better learning model to combat the destructive issues associated with the activities of attackers on the Internet and computer networks.

REFERENCES

Bratus, S., Shubina, A., & Locasto, M. (2010). Teaching the principles of the hacker curriculum to undergraduates. *Proceedings of the 41st ACM Technical Symposium on Computer Science Education – SIGCSE '10.*

Dimkov, T., Pieters, W., & Hartel, P. (2011). Training students to steal: A practical assignment in computer security education. *Proceedings of the 42nd ACM Technical Symposium on Computer Science Education – SIGCSE '11.*

Ethical Hacking: Student courseware. Ec-Council. (2005, March). Retrieved from www.eccouncil.org.

Floyd, K., Harrington, S., & Hivale, P. (2007). The autotelic propensity of types of hackers. *Proceedings of the 4th Annual Conference on Information Security Curriculum Development - InfoSecCD '07.*

Greene, Tim (2004, July 22). Training ethical hackers: Training the enemy? Retrieved from https://defcon.org/html/links/dc_press/archives/12/ebcvg_training_ethical_hackers.htm.

Lancor, L., & Workman, R. (2007). Using Google hacking to enhance defense strategies. *Proceedings of the 38th SIGCSE Technical Symposium on Computer Science Education – SIGCSE '07.*

Logan, P. Y. (2002). Crafting an undergraduate information security emphasis within information technology. *Journal of Information Systems Education,* 13(3), 177-182.

Logan, P., & Clarkson, A. (2005). Teaching students to hack. *SIGCSE Bull. ACM SIGCSE Bulletin*, 157-157.

Oriyano, S. (2014). *CEHv8 Certified Ethical Hacker version 8: Study guide.* Indianapolis: Sybex.

Pashel, B. A. (2006). Teaching students to hack. *Proceedings of the 3rd Annual Conference on Information Security Curriculum Development - InfoSecCD '06*.

Saleem, S. A. (2006). Ethical hacking as a risk management technique. *Proceedings of the 3rd Annual Conference on Information Security Curriculum Development – InfoSecCD '06.*

Sanders, A. (2003). Utilizing simple hacking techniques to teach system security and hacker identification. *Journal of Information Systems Education,* 14(1), 5.

Trabelsi, Z. (2011). Hands-on lab exercises implementation of DoS and MiM attacks using ARP cache poisoning. *Proceedings of the 2011 Information Security Curriculum Development Conference on - InfoSecCD '11*.

Trabelsi, Z. (2012). Switch's CAM table poisoning attack: *Hands-on lab exercises for network security education. Proceedings of the Fourteenth Australasian Computing Education Conference (ACE2012), Melbourne, Australia.*

Trabelsi, Z., & Alketbi, L. (2013). Using network packet generators and snort rules for teaching denial of service attacks. *Proceedings of the* 18th ACM conference on Innovation and technology in computer science education - ITiCSE '13.

Trabelsi, Z. (2014). Enhancing the comprehension of network sniffing attack in information security education using a hands-on lab approach. *Proceedings of the 15th Annual Conference on Information Technology Education – SIGITE '14.*

Trabelsi, Z., & McCoey, M. (2016). Ethical hacking in Information Security curricula. *International Journal of Information and Communication Technology Education*, 12(1), 1-10.

Using an ethical hacking technique to assess information security risk. (2003). The Canadian Institute of Chartered Accountants. Retrieved from http://docplayer.net/6744254-Using-an-ethical-hacking-technique-to-assess-information-security-risk.html.

Weiss, R., & Mache, J. (2011). Teaching security labs with web applications, buffer overflows and firewall configurations. *Journal of Computing Sciences in Colleges,* 27(1), 163-170.

Wu, A. (2014). Project development for ethical hacking practice in a website security course. *Proceedings of the Western Canadian Conference on Computing Education – WCCCE '14.*

Yurcik, B., & Doss, D. (2001). Ethical hacking: The security justification. *Paper presented at Ethics of Electronic Information in the 21st Century Symposium. University of Memphis: Memphis, TN.*