ISSN: 2473-3857
v3 n4341

Ethical Hacking: Educating Future Cybersecurity Professionals

Regina Hartley
hartleyrd@appstate.edu

Dawn Medlin
medlinbd@appstate.edu

Zach Houlik
houlikzj@appstate.edu

Appalachian State University
Computer Information Systems and Supply Chain
Boone, NC 28608

Abstract

Businesses, governments, and individuals are all aware how important information security is today, and unfortunately, that fact may be due in part to their financial losses, damage to their brand, loss of customer trust, and personal consequences of fraudulent activities. Due to the severity of these actions, it is incumbent for students interested in information security to obtain an education that will allow them to communicate with the entire user community. Ethical hacking education can provide future professionals with the knowledge and skills to combat current and future cybersecurity issues. This research will define ethical hacking, current information security trends, offer pedagogical methods, an overview of information security instruction, and lastly, best practices in the field are examined.

Keywords: Ethical hacking education, information security instruction, ethical hacking pedagogy.

1. INTRODUCTION

The prominence of information technologies and increasing dependence on technological infrastructures continues to infiltrate all of the society. It may be argued that some concern stems from the apparent lack of security inherent in 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, as well as the need to educate individuals on topics related to this expansive growth.

Along with the positive capabilities provided by the Internet and the networking of global computing devices, unpleasant aspects have also produced unexpected results such as ransomware and DYN DDoS Attacks, as well as other highly politicized and publicized hacks. While various crimes have existed for many years, the Internet and information technology have brought computer crime into our societies in unthinkable ways. Criminals 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 paper 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 would be better equipped to combat intrusions if equipped with the knowledge and skill sets currently used by attackers, and those that can only be imaged by security professionals. In order to equip security/cyber professionals, students must be prepared to fight the ever-growing challenges associated with effectively securing computer networks.

Following the brief review of the history of hacking, this research will examine more recent trends and concerns related to cybersecurity. By examining current events, it becomes very apparent that incidents and breaches are occurring more rapidly. As attackers create new methods of attack, future information security professionals will need to be better prepared and better equipped to handle the increasing and ever present number of attacks and intrusions.

2. LITERATURE REVIEW

To better understand the need for proactive measures relating to the education of future security professionals, attention will briefly focus on the history of hacking. Hacking began for the most part in the 1960s and originated on the campuses of Massachusetts Institute of Technology (MIT) and Stanford University. At that time, the word "hack" referred to programming shortcuts and was considered a better way to complete anything more efficiently. These original "old school hackers" were not interested in malicious intent, but rather simply enjoyed technology (Slatalla, 2005).

Through the passage of time hackers have lost their romantic appeal to the public as the Internet has evolved and become more widely utilized (Slatalla, 2005). Though newer groups are emerging with the title of "suicide hackers," older categories and titles have remained such as "script kiddies and coders." The new suicide hackers are known as individuals who attack to prove a point, but unlike "hacktivists" they do not cover their tracks and are not concerned if they get caught (Oriyano, 2014).

Recent cybersecurity events are quite disturbing and offer evidence that security measures implemented by today's cybersecurity professionals require a more proactive approach. While there are increasing cybersecurity events there are several prominent attacks addressed in the headlines within the past year that have required advanced technical knowledge. As an example, the Democratic National Convention hack of 2016-2017 (DNC Hack) caused tremendous upheaval concerning the possibility of Russian sponsored hackers trying to influence the 2016 Presidential election. The hack appeared to be the work of two Russian groups known as Cozy Bear and Fancy Bear based on their methods and tactics (Greene, 2016; van Der Walt, 2017). Many have suggested that the alleged hack into the system is not the important issue at hand. The outcome of the hack by alleged Russian hackers caused many Americans to lose trust in the political system within the United States (van Der Walt, 2017).

A second significant attack in 2017 identified as a Dyn DDoS Attack affected thousands of Internet of Things (IoT) devices. The attack was used as a "botnet" to carry out the attack. As more and more devices are connected to the Internet, an attack of this type no longer requires regular computer machines as was in the case in the past.

Another major attack occurred in 2016, when the Shadow Brokers hacked into the Equation Group, stole their tools for exploiting software vulnerabilities, and then essentially offered them online for free (van Der Walt, 2017). It is believed that the Shadow Brokers have connections to Russia, and the Equation Group have connections to the NSA (National Security Agency). Some have theorized that Russia wanted to expose NSA tools to embarrass them and weaken the U.S. response to the alleged hack of the DNC (Greene, 2016). As a result of the NSA Shadow Brokers leak, attackers were able to utilize the tools to target vulnerabilities in computer systems worldwide. Almost 100 countries were hit with the largest ransomware attack in history. "Cyberattackers took over the computers, encrypted the information on them and then demanded payment of $300 or more from users to unlock the devices" (Scott & Wingfield, 2017). This attack was significant, because it is believed to be the first in the usage of "a cyberweapon developed by the NSA," and to be used by attackers on a global scale (Scott & Wingfield, 2017). The attack was particularly successful because cybercriminals could target "large institutions with a track record of not keeping their technology systems up-to-date" (Scott & Wingfield, 2017).

3. 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 on 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.

McMaster University's Department of Computing and Software defines ethical hacking as "the controversial act of locating weaknesses and vulnerabilities of computer and information systems by duplicating the intent and actions of malicious hackers" (Jaskolka, 2009). Ethical hacking is also commonly referred to as red teaming, intrusion testing, and penetration testing (Jaskolka, 2009).

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 information 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 researchers, that students need to experience first-hand what the attacker will be doing and what tools will be used (Ethical Hacking: Student courseware, 2005).

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, 2005). 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).

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, 2005; Oriyano, 2014).

A hacker may be defined as a "person who enjoys learning the details of computer systems and how to stretch their capabilities" (Ethical hacking: Student courseware, 2005). 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 (Sheoran, P., & Singh, S. 2014).

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 a computer system is similar to the example of crash-testing cars. In both examples, as an audit or crash-test, the objective is to make something better by

identifying the weaknesses within a system. As taunted by many researchers, humans are the weakest link in computer security.

Ideas and definitions of information security have varied over the last few decades, however, a contemporary definition was proposed by Lundin in 2013. "Information security, or InfoSec, is the practice of protecting information from unauthorized use, disclosure, access, modification, or destruction. This term is applied to all information regardless of the form it takes and is comprised of two major categories: information assurance, which is the ability to ensure data is not lost to a breakdown in system security, due to theft, natural disasters, or technological malfunction; and IT (information technology) security, which is the security applied to computer networks."

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 (Sheoran, P., & Singh, S., 2014).

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 further maintain that students must have an opportunity to be engaged with security technologies in order to acquire the knowledge and skillset that is needed to be successful in the field of computer security.

4. 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 that of the attackers. It is important to determine what skillsets are needed by security professionals in order to help educate students appropriately (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 prepared 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 skillsets 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 are considered a necessary element of security education. A 2013 book, titled *Hands-On Ethical Hacking and Network Defense*, suggests an overview of an ethical hacking curricula. The author's reason that the specific role of penetration testers should be constructed, propose different models for penetration testing, observe what can be done legally and illegally, separate federal and state laws through case study analysis, and examine different ethical hacking certifications (Simpson, et al., 2013). Finally, Trabelsi and Alketbi (2013) state that techniques of ethical hacking should be included in a curriculum to better prepare security professionals.

5. ETHICAL AND LEGAL CONCERNS REGARDING 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. Our discussion will 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 like the cybercriminals they are attempting to catch. Additionally, others contend that teaching hacking techniques could cause institutions to be faced with ethical and legal dilemmas.

It is interesting to note that while many colleges and universities offer such education and training, a number of security professionals express concern about teaching hands on hacking techniques. This apprehension may stem from a fear that students may use the knowledge of "how to" 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 the 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 attempting to "sniff" the network of the university, and 70% confessed they had 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" to their efforts (Trabelsi & McCoey, 2016).

6. 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.

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 to thwart future attacks.

Other 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.

According to Pawlowski & Yoonhyk (2015), "As information systems (IS) educators, we are responsible for preparing our students to be aware of the risks in cyberspace, to see potential threats and to make good decisions in their professional and personal lives." The authors close their research by stating that
"today security education and training is considered essential in order to prepare students for future roles," in employment and society.

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.

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 receiving 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 security concepts to future security professionals. 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 that if students do not use good hacking tools within their course work, that their experiences may lead them to have a more limited view of the knowledge of real attacker's skills and their malicious behaviors.

The educational models proposed by Simpson et al. focus on the amount of information given to students and are broken into three categories: White Box, Black Box, and Gray Box (2013). The White Box Model is where students are provided "network diagrams, showing all the company's routers, switches, firewalls, and intrusion detection systems or…a floor plan detailing the location of computer systems and the Oss running on these systems" (Simpson et al., 2013). In the Black Box Model, the students are not provided any information and employees are not notified of

a potential attack. Simpson et al. noted that "This model also helps management see whether the company's security personnel can detect an attack" (2013). Finally, "the gray box model is a hybrid of the white and black box models. In this model, the company gives the tester only partial information. For example, the tester might get information about which Oss are used but not get any network diagrams" (Simpson et al., 2013).

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 on 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

The 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 relate to social engineering. They additionally suggest that organizational security requirements may appear unrealistic (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 & 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 the 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).

7. CONCLUSIONS

As individuals, organizations, and societies become more adept at using computers and more reliant upon them, the possibility of fraud or crime continues to grow. Educating students through the practices and knowledge of ethical hacking can provide them with the skills necessary to address and develop specific security policies and procedures, as well as provide the needed administrative support that may be required to combat cybercrimes. Technical expertise is necessary to implement the details of a security operation that will include both a defensive and offensive action. Whatever the responsibility of the security professional, students must learn how to perform the job functions that focus on protecting the organization's information system or the individual's information from attacks.

6. 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.*

Bratus, S., & Masone, C. (2007). Hacker Curriculum: How We Can Use It in Teaching]. *IEEE Distributed Systems Online, 8*(11), 1-5. doi:10.1109/mdso.2007.61.

Dimkov, T., Pieters, W., & Hartel, P. (2011). Training students to steal: A practical assignment in computer security education.

ISSN: 2473-3857
v3 n4341

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, T (2004, July 22). Training ethical hackers: Training the enemy? Retrieved December 10, 2015.

Jaskolka, J. (2009, April 7). *Ethical Hacking*. Retrieved June 8, 2017.

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

Lundin, L. (2013). *Information security*. Ipswich, MA: Salem Press Encyclopedia.

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*.

Pawlowski, S. D., & Jung, Y. (2015). Social Representations of Cybersecurity by University Students and Implications for Instructional Design. *Journal of Information Systems Education*, *26*(4), 281.

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), p. 5.*

Scott, M., & Wingfield, N. (2017, May 13). Hacking Attack Has Security Experts Scrambling to Contain Fallout. Retrieved June 14, 2017.

Sheoran, P., & Singh, S. (2014). Applications of Ethical Hacking. *International Journal of Enhanced Research in Science Technology & Engineering*, *3*(5), 112-114.

Simpson, M. T., Backman, K., & Corley, J. E. (2013). *Hands-on ethical hacking and network defense. Boston, MA: Cengage Technology*.

Slatalla, M. A brief history of hacking. Retrieved November 5, 2005.

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.*

Van der Walt, C. (2017, April). The impact of nation-state hacking on commercial cyber-security. Retrieved June 14, 2017.

Weiss, R., & Mache, J. (2011). Teaching security labs with web applications, buffer overflows,

ISSN: 2473-3857
v3 n4341

and firewall configurations. *Journal of Computing Sciences in Colleges, 27(1), pp163-170.*

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

.

ISSN: 2473-3857
v3 n4341