IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

# Ethical Hacking & Cybersecurity Future

**Divyansh Jain[1], Arsh Kumar[2], Chahat[3] Dr. Suman Madan[4]**

[1,2,3](Student, Department of IT, Jagan Institute of Management Studies, Sector-5 Rohini, Delhi, India)

[4](Associate professor, Department of IT, Jagan Institute of Management Studies, Sector-5 Rohini, Delhi, India)

## Abstract

Because of financial losses, brand harm, consumer confidence loss, and personal effects of fraudulent activities, businesses, governments, and individuals are all aware of the value of information security today. Because of the gravity of these acts, students interested in information security should obtain a degree that will enable them to interact with the entire user community. Ethical hacking education will help potential professionals develop the awareness and skills they need to combat current and future cybersecurity threats. This research will identify ethical hacking, address current information security patterns, present pedagogical approaches, provide an overview of information security training, and conclude with best practises in the field.

**Keywords---** Ethical hacking knowledge, information security instruction, ethical hacking teaching and learning.

## I. Introduction

The importance of information technologies, as well as our increasing reliance on technological infrastructures, is pervasive throughout society. Some concern could be attributed to Information technology and applications seem to have a security flaw. The importance of our increasing dependence on the Internet and networking capabilities cannot be overstated. The Internet has opened up previously unattainable possibilities in a number of fields., as well as the need to educate people about topics related to this rapid expansion. Along with the positive capabilities offered by the Internet and the networking of global computing devices, unintended consequences such as ransomware and DYN DDoS attacks, as well as other highly politicised and publicised hacks, have emerged. While different types of crimes have existed for a long time, the Internet and information technology have brought computer crime into our societies in previously unimaginable ways. Criminals now have a new platform to conduct their activities on, and many people are so perplexed by the onslaught that only reactive measures can be taken in many cases. The aim of this paper is to examine how a pedagogical approach to ethical hacking can be used to improve information security training. A hacking technique tends to be a more offensive and pragmatic approach to information security preparation. This method could aid aspiring information security professionals in better preparing for unethical hacker intrusions into computer networks and the Internet. Future information security practitioners would be better prepared to deter intrusions if they had access to attackers' existing capabilities and skill sets, as well as those that can only be imagined by security professionals. Students must be prepared to face the ever-increasing challenges associated with effectively protecting computer networks in order to equip security/cyber professionals. Following a brief overview of hacking's past, this study will focus on more recent cybersecurity developments and concerns. When current events are examined, it becomes clear that incidents and breaches are occurring at a faster rate. Future information security professionals will need to be better prepared and equipped to deal with the increasing and ever-present number of attacks and intrusions as attackers develop new methods of attack.

## II. Literature review

The history of hacking will be briefly discussed in order to better understand the need for constructive steps relating to the education of potential security professionals. Hacking started in the 1960s, mostly on the campuses of the Massachusetts Institute of Technology (MIT) and Stanford University. At the time, the term "hack" applied to code shortcuts and was thought to be a more effective way to complete tasks. These original "old school hackers" were not motivated by malice, but rather by a desire to learn new things (Slatalla, 2005).

As the Internet has grown and become more commonly used, hackers have lost their romantic appeal to the general public (Slatalla, 2005). Older types and names, such as "plot kiddies and coders," have persisted, despite the emergence of newer groups with the moniker "suicide hackers." Individuals who attack to make a point are classified as new suicide hackers, but unlike "hacktivists," they do not cover their tracks and are unconcerned if they are captured (Oriyano, 2014).

Recent cybersecurity incidents are alarming, and they demonstrate that today's cybersecurity practitioners must take a more proactive approach to protection. Although there are more cybersecurity incidents on the rise, there have been some high-profile attacks in the news in the last year that necessitated advanced technological expertise. The 2016-2017 Democratic National Convention hack (DNC Hack), for example, ignited public outrage about Russian-backed hackers attempting to sway 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 people have stated that the alleged computer hack isn't the most pressing issue. As a result of the alleged Russian hack, many Americans have lost confidence in the US political system (van Der Walt, 2017). Thousands of Internet of Things (IoT) devices were impacted by a second major attack in 2017, dubbed the Dyn DDoS Attack. The assault was carried out with the help of a "botnet." When more devices become connected to the Internet, an assault of this nature no longer necessitates the use of traditional computer machines, as was the case previously.

In 2016, the Shadow Brokers hacked into the Equation Community, stole their tools for manipulating software vulnerabilities, and then basically gave them away for free on the internet (van Der Walt, 2017). The Shadow Brokers are thought to have ties to Russia, while the Equation Group is thought to have ties to the NSA (National Security Agency). Some hypothesized that Russia was attempting to embarrass the NSA and weaken the US response to the alleged DNC hack by leaking NSA resources (Greene, 2016). As a result of the NSA Shadow Brokers leak, attackers were able to use the tools to exploit vulnerabilities in computer systems all over the world. Nearly 100 countries were hit by the world's largest ransomware attack. “Cybercriminals took control of the computers, encrypting the data on them, and then charging users $300 or more to decrypt the devices” (Scott & Wingfield, 2017). This attack was noteworthy because it is believed to be the first-time attackers used "a cyberweapon designed by the NSA" on a global scale (Scott & Wingfield, 2017). The attack was particularly successful because cybercriminals were able to target "large organizations with a track record of not keeping their technology systems up to date" (Scott & Wingfield, 2017).

## Ethical Hacking

This study looks at ethical hacking by defining it and evaluating the effectiveness of teaching future information security practitioners using an ethical hacking pedagogical approach. According to a review of the literature, there tend to be two distinct approaches to computer security instruction. One approach emphasizes theoretical concepts only, while the other includes a hands-on laboratory component to reinforce theoretical concepts. One strategy that tends to be useful in computer security education is ethical hacking.

"The contentious act of discovering computer and information system weaknesses and vulnerabilities by duplicating the intent and actions of malicious hackers," according to McMaster University's Department of Computing and Software (Jaskolka, 2009). Ethical hacking is referred to by a variety of names, including red teaming, intrusion testing, and penetration testing (Jaskolka, 2009).

Ethical hacking is a technique for assisting network managers and technical experts in protecting networks. As a result, the effectiveness of this subject in teaching students in information security courses proactive offensive measures will be evaluated.

Ethical hacking's basic idea is that it takes a particular approach to protection. Breaking into a computer "like a hacker but for benevolent motives" is what ethical hacking, also known as penetration testing, entails (Oriyano, 2014). Many experts agree that students can see what an attacker can do and what tactics will be used first hand (Ethical Hacking: Student courseware, 2005).

Ethical hacking is also known as the "methodology used by ethical hackers to find flaws in information system operating environments" (Ethical Hacking: Student Courseware, 2005). Finally, it can be defined as someone of the same ability sets as an intruder, with the exception that the target's security mechanism has been tested with approval from the owner (Oriyano, 2014).

There are several different types of hackers, including Black Hats, who are highly skilled but have a malicious and destructive intent. They're still the ones that do things that aren't exactly legal. White Hats, on the other hand, are hackers who have permission to use their expertise for defensive security research. Gray Hat hackers hack for a number of reasons, both ethically and unethically depending on the situation, and they can both attack and protect (Ethical Hacking: Courseware, 2005; Oriyano, 2014).

A hacker is a person who enjoys learning about computer systems and how to test them (Ethical hacking: Student courseware, 2005). Initially, hackers and gamers were mostly interested in and excited about whatever cutting-edge technology was available at the time (Oriyano, 2014).

“Both ethical and malicious hackers attack machines, but their goals are different,” Greene writes (2004). According to Pashel, "ethical hacking" is "the practice of hacking without malicious intent" (2006).

It's important to find out how and why a hacker got started, according to Floyd, Harrington, and Hivale (2007). They suggest that there are two types of hackers: those who hack for the “autotelic” thrill and those who hack for the sake of curiosity. Those are the individuals who would succeed as ethical hackers. Others, on the other hand, may have been prone to unethical or unlawful behaviour and sought assistance from computers.

Ethical hacking, also known as penetration testing, is similar to hiring external auditors in terms of definition. Organizations are continually using this method to measure the effectiveness of information security. These procedures are used to identify and exploit security flaws, providing the organization with the information it requires to take corrective action (Sheoran, P., & Singh, S. 2014).

According to Logan and Clarkson (2005), information security is a type of computer system "audit." As a consequence, hacking skills and auditing skills are similar in that both seek to find issues. “Hackers 'test' systems by targeting them in the same way that auditors review systems for security or organizational vulnerabilities,” they add (Logan, & Clarkson, 2005).

Greene (2004) compares the crash-testing of vehicles to the testing of electronic devices. In any case, the aim of an audit or a crash-test is to improve things by identifying weaknesses in a system. Humans are the weakest link in computer security, as many researchers have pointed out.

While ideas and principles about information security have evolved over the decades, Lundin introduced a new definition in 2013. “Information security, or InfoSec, is the practice of protecting data from unauthorized access, disclosure, modification, or destruction. Information assurance refers to the ability to ensure that data is not lost due to a loss of system security, such as fraud, natural disasters, or technological malfunction, and IT (information technology) security refers to the protection given to computer networks.”

"The Internet's security is broken," Yurcik and Doss (2001) write, "and 'ethical hacking' has emerged as part of the potential solution." They go on to state that ethical hacking may be one of the most effective ways to prevent security vulnerabilities from spreading" (Yurcik, & Doss, 2001). An increasing number of security experts are advising companies to hire white hat hackers or ethical hackers for research and consultancy purposes (Sheoran, P., & Singh, S., 2014).

As discussed earlier in this discussion, there are two basic approaches to information security training. One is primarily concerned with theoretical ideals, while the other is more practical. Focusing exclusively on "theoretical aspects of information security," according to Trabelsi and McCoey (2016), does not sufficiently prepare students to deal with the complexities of defending complex computer systems and data resources. They also agree that in order to learn the knowledge and skills needed to excel in the field of computer security, students should be able to work with security technologies.

## III. Ethical Hacking Education

After we've covered the basics of ethical hacking, we'll move on to an outline of ethical hacking education for aspiring security professionals. It's a worthwhile endeavour to teach students ethical hacking tactics, and most researchers believe that it's important for security professionals. Security professionals would be able to stop attacks if they can find vulnerabilities in computer systems, according to Pashel (2006). He goes on to suggest that ethical hacking may be an essential part of a security strategy (Pashel, 2006).

Software managers, according to an increasing number of experts, should have the same level of experience and skills as attackers. It's important to find out what skillset security professionals need so that students can get the training they need (Logan, & Clarkson, 2005). “With the rapid evolution of information security, the 'good guys' need all of the information and resources they can get,” another researcher adds (Greene, 2004).

Rather than being reactive, many ethical hacking skills are proactive. According to security instructors, teaching "violent techniques" rather than "defensive methods" produces better qualified security professionals (Trabelsi, 2011).

A number of experts and educators agree that learning ethical hacking skills is essential for computer security professionals to acquire the necessary skills. Trabelsi (2011) believes that students should be directed in order to prepare them for a career requiring comprehensive research and development. “One cannot perfectly prepare or build defences for attacks that one has not first-hand experienced,” he continues (Trabelsi, 2011).

Trabelsi (2012) believes that computer security professionals are under-trained for their jobs because they are not provided with knowledge and experience obtained from hacking. He goes on to say that teaching attacks is an important component of security training. The 2013 book Hands-On Ethical Hacking and Network Défense provides an outline of an ethical hacking curriculum.

The author proposes that a specific role for penetration testers be established, that different models for penetration testing be suggested, that what can be done legally and illegally be observed, that federal and state laws be divided through case study analysis, and that various ethical hacking certifications be examined (Simpson, et al., 2013). Finally, ethical hacking techniques should be included in a curriculum to help train security professionals, according to Trabelsi and Alketbi (2013).

## IV. ETHICAL AND LEGAL CONCERNS REGARDING ETHICAL HACKING EDUCATION

The ethical and legal implications of this approach to training security professionals must be addressed following a review of ethical hacking education, taking into account educators' and researchers' concerns. Our discussion will focus on the use of a computer ethics policy to mitigate or discourage unethical behaviour as a result of ethical hacking instruction. Because of the ethical consequences of providing students with knowledge that could lead them to behave like the cybercriminals they are attempting to arrest, teaching ethical hacking could be viewed with scepticism.

Others argue that teaching hacking techniques could place businesses in a legal and ethical bind. Although several colleges and universities provide such education and training, a number of security experts have expressed reservations about teaching hands-on hacking techniques. This anxiety will arise from a concern that students would use their “how to” information unethically. Educational organisations defeat this belief by providing principles that are ethically sound (Sanders, 2003).

Many of those who advocate for ethical hacking as a means of teaching information security often advocate for ethical and legal training. While some students may use their newly acquired skills to participate in unethical behaviour, Pashel (2006) maintains that all students should be educated on the ethical and legal implications of their actions. Students should participate in security training to learn about ethics and what is expected of them as security professionals (Greene, 2004).

When it came to ethical hacking, the bulk of the researchers polled were adamant about the need for legal and ethical guidelines. Some educators conclude that a hands-on course in ethical hacking is unethical because it exposes students to the risk of using "tools and techniques in a reckless manner" (Trabelsi, 2011).

The value of providing ethical and legal information and training, as well as teaching students hacking techniques, is recognized by the majority of researchers. According to Logan and Clarkson (2005), there is a lack of ethical and legal guidelines in the field of computing and networking. “Training future security professionals and hackers’ side-by-side by preparing students to target networks without the ethical or legal constructs to understand their behaviour,” they add (Logan & Clarkson, 2005).

Others raise legitimate concerns about what students can do with their newly acquired hacking skills. According to one scholar, ethical and "malicious hackers" can be educated at the same time (Greene, 2004). According to another person, several people are debating the "legality of teaching students to hack in order to improve their intrusion detection skills" (Saleem, 2006).

While there are many concerns about teaching students to hack, some research has shown that these concerns are well-founded. Students seemed to be using their newly learned hacking skills for unethical reasons in one report. According to Trabelsi (2011), they discovered "a big ethical problem" when reviewing logs from the university's intrusion detection system. Students seemed to want to use their new skills outside of the classroom.

According to another study by the same professor, the amount of inserted malicious traffic targeting the university switches' CAM tables increased dramatically each time the students experimented with the DoS attack (Trabelsi, 2012). In order to validate their questions, the professor circulated an anonymous questionnaire to the students. Alarmingly, 88 percent of students admitted to attempting to “sniff” the university network on purpose, and 70% admitted to attempting to “hack” faculty computers (Trabelsi, 2014).

In a more recent study, Trabelsi and McCoey (2016) discovered startling statistics from an anonymous survey. Despite the fact that the numbers were slightly smaller, 85 percent of students admitted to repeating the lab task outside of the isolated classroom network. This time, however, it appeared that their attacks were aimed at web and email servers. On a more upbeat note, 89 percent of students admitted that they were not motivated by "malicious intent" in their efforts (Trabelsi & McCoey, 2016).

## V. BEST PRACTICES IN ETHICAL HACKING EDUCATION

The emphasis will now turn to the new best practices being offered to train future security practitioners, now that the ethical and legal implications of ethical hacking have been addressed. According to the literature, some of the best practices emphasize a hands-on approach and the implementation of soft skills.

Students should be taught ethical hacking strategies in a way that properly prepares them for a career in defence. According to Bratus, Shubina, and Locasto, educators may use the "Hacker Curriculum" to access quality content to help in the development of ethical hacking instruction (2010). "A security education program that does not give students the opportunity to experiment in practice with security strategies," according to Trabelsi (2014), will leave students unprepared for future careers. He continues, "Students must feel confident in their ability to protect themselves against an intruder."

In a more recent study, Trabelsi and McCoey (2016) found that students who have not had the opportunity to experiment with "real hacking" might be unprepared to thwart possible attacks.

Others argue that students must be able to identify intruders and battle them with the same mindset. As a result, educators are strongly urged to embrace an "attacker's approach" (Bratus, Shubina, & Locasto, 2010). They conclude by recommending that educational offerings in the defence curriculum provide both "defender" and "attacker" viewpoints.

According to Pawlowski and Yoonhyk, “as information systems (IS) educators, we are responsible for teaching our students to be aware of the risks in cyberspace, to recognize potential challenges, and to make good decisions in their professional and personal lives” (2015). The authors conclude that “security education and training is now deemed appropriate in order to prepare students for future roles” in employment and society.

Others, on the other hand, suggest that teaching students how to think like attackers will help them learn how to defend networks and web applications in general. Saleem (2006) proposes arming computer students with ethical hacking strategies to defeat attackers. “Thinking like a hacker and acting like an ethical hacker,” according to Wu (2014), is a necessary skill for a successful career in web application security.

Lancor and Workman (2007) suggest that learning the opponent's offense is the first step toward a "good defence," based on the defender and attacker model.

**Hands-on Approach**

Ethical hacking teaching, according to a review of the literature on best practices, requires a hands-on approach. Ethical hacking school, according to Logan and Clarkson (2005), should be done "hands-on." The researchers go on to say that "book and lecture-based teaching is not always as effective in illustrating concepts as hands-on practice" (Logan & Clarkson, 2005).

Another researcher argues that security concepts should be taught by a hands-on approach to future security practitioners. All core groups, according to Weiss and Mache (2011), should have "hands-on defence." They go on to say that teaching safety is critical in the curriculum and that hands-on experiences are the most effective way for students to learn. According to Trabelsi (2011), a security curriculum that is solely theoretical is not nearly as effective as a hands-on approach. He goes on to say that in order to contribute to "computer security research and development," students need training and practice (Trabelsi, 2011).

The majority of people agree that the efficacy of an educational program is determined by the quality of its instruction. In addition to the value of actually hacking, the techniques used to carry out the assignment must be precise. According to Greene (2004), if students do not use good hacking strategies in their coursework, their experiences will restrict their understanding of real-world attackers' skills and malicious behaviour.

Based on the amount of information offered to students, Simpson et al instructional models are divided into three categories: White Box, Black Box, and Gray Box (2013). The White Box Model provides students with "network diagrams, showing all of the company's routers, switches, firewalls, and intrusion detection systems, or...a floor map detailing the position of computer systems and the Oss running on these systems" (Simpson et al., 2013). In the Black Box Model, students are not given any information, and employees are not aware of a potential assault. According to Simpson et al., "this model also allows management to see whether the company's security personnel can detect an attack" (2013). Finally, the "grey box model" is a hybrid of white and black box designs. The organization only offers a small amount of experience to the tester in this model. The tester, for example, can obtain details about which Oss is being used but no network diagrams" (Simpson et al., 2013).

Students must realize that ethical hacking is just one component of a broader security plan. Ethical hacking, according to Logan and Clarkson (2005), should be part of a larger plan. In addition to hacking, there should be security checks that continue to monitor the network. The aim is to replicate the process on a regular basis in order to improve the overall security of the network. Logan and Clarkson (2005) go on to state that labs should have "careful planning and have consultation with computing facilities," according to Logan and Clarkson (2005).

When students were polled about the hands-on lab instruction, 85 percent said the applications helped them understand the theoretical concepts in class. In addition, 87% of students said they'd like more hands-on lab instruction, and 86% said they'd recommend the lab activities to others (Trabelsi, & McCoey, 2016).

**Soft Skills**

The second area of best practices, according to the literature, is that soft skills should not be overlooked in ethical hacking education. According to Dimkov, Pieters, and Hartel, "teaching students only the technical aspect of information security leads to a generation of students who prioritize digital solutions while ignoring the physical and social aspects of security" (2011). It could be argued that when it comes to computer systems, a process or instruction still lacks the human element.

Some researchers favour soft skills that improve awareness of a potential security hazard in the sense of social engineering. Social elements, according to Dimkov, Pieters, and Hartel (2011), raise students' security awareness and are linked to social engineering. Organizational security requirements, according to Dimkov, Pieters, and Hartel (2011), may seem unrealistic. Greene (2004) also believes that social engineering experience should be included in a safety curriculum.

Other researchers have also discovered the importance of soft skills and social engineering. Tasks like social engineering and understanding user preferences, according to Bratus and Masone (2007), helped students comprehend some aspects of computer operation. According to Trabelsi & McCoey (2016), students need "soft" skills like social engineering, a better understanding of protection, and an understanding of how an attacker thinks in order to be successful in the field.

After evaluating ethical hacking preparation best practices for future security practitioners, it's important to note that most educators and analysts agree that the benefits outweigh the drawbacks. According to Trabelisi (Trabelsi, 2011, 2012, 2013, 2014), the ethical concerns about teaching hacking pale in comparison to the benefits realized for students.

## VI. Conclusion

When individuals, organizations, and societies become more adept at using computers and more reliant on them, the risk of fraud or crime increases. By training them responsible hacking practices and experience, students would be equipped with the skills required to manage and improve applicable security policies and procedures, as well as provide the administrative support needed to combat cybercrime. Technical experience is needed to carry out the details of a security activity that will include both defensive and offensive activities. Regardless of the security professional's duties, students must learn how to perform job functions that focus on protecting the organization's information system or an individual's information from attacks.

## References

**[1]** 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.

**[2]** 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.

**[3]** 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.

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

**[5]** 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.

**[6]** Greene, T (2004, July 22). Training ethical hackers: Training the enemy? Retrieved December 10, 2015.

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

**[8]** 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.

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

**[10]** Van der Walt, C. (2017, April). The impact of nation-state hacking on commercial cybersecurity. Retrieved June 14, 2017.

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

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

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