International Refereed Journal of Engineering and Science (IRJES)
ISSN (Online) 2319-183X, (Print) 2319-1821
Volume 12, Issue 4 (Jul.-Aug. 2023), PP. 24-29

Ethical Hacking: Skills to Fight Cyber security

Deepak Kumar Biswal[1] Sudhir Kumar Das[2] Riyazuddin Khan[3]
Department of Computer Science & Engineering, Einstein Academy of Technology & Management, Bhubaneswar, Odisha

Abstract
Ethical hacking education equips future information security professionals with the necessary skills to combat cyber security threats. This proactive approach, unlike most defensive technologies, is used by malicious hackers, making it a double-edged sword for businesses, schools, and individuals are all becoming reliant on the Internet and Internet of Things (IoT) devices.
Keyword*: Malicious hackers, Ethical hackers, Firewalls, Vulnerabilities*

I. Introduction

The internet and its importance are expanding at an incredible rate. Schools, businesses, governments, and individuals are all becoming reliant on the Internet and Internet of Things (IoT) devices. IoT devices can include but are not limited to desktops, laptops, smart phones, smart watches, etc. With so many institutions relying on the Internet and devices connected to the Internet, their security from outside threats becomes the owner's highest priority. The rise of information technology and the Internet have brought cybercrime to the forefront of everyday life. Information technology has created a new, seemingly anonymous, avenue for criminals to operate and cause damage. Malicious users find new ways to penetrate IoT devices nearly every day, allowing many security measures to only be reactive in nature. Ethical hacking is one security measure that provides an exception to these reactive measures and is viewed as a proactive one. These hackers use the same skills and tools as malicious hackers; however, there are many strict guidelines they must follow, and a certification must be obtained to become a legally recognized ethical hacker. Therefore, it is important for instructors to correctly inform their students about the repercussions of malicious hacking to help encourage them to complete their program and become a certified ethical hacker.

Organizations, schools, governments, etc. have historically used a defensive approach to secure networks, systems, and data. This approach leveraged technologies such as firewalls, antivirus/antimalware software, network segmentation, and access control lists to defend against unauthorized access (Thomas et al., 2018). It is important to note that these technologies, for the most part, cannot stop an active breach into a system. Sometimes they can prevent a breach from happening but only if it is through a known vulnerability. Thus, the importance of ethical hacking becomes evident. No organization wants to fall victim to a data breach from a malicious hacker just to discover a vulnerability in their computer security. Ethical hackers discover these risks and vulnerabilities in a system or network from within a controlled environment, with no intention to cause damage to or steal data from the owners of the system/network. However, ethical hackers and their instruction raise important questions about their implications such as "Is teaching students how to hack worsening the problem of malicious hackers?" and "If a student uses the information provided to him by an institution to commit a crime, who is at fault?". Ethical hacking is performed by trained/certified individuals who carry out actions like that of malicious hackers in hopes of finding vulnerabilities in a system or network before a hacker has the chance to exploit it. Hartley defines ethical hacking as penetrating a system as a hacker but with benign intentions (Hartley et al., 2017). Not only must ethical hackers adhere to a strict code of ethics, but they must also be conscious of the law while performing their job. For an individual to become an ethical hacker they must be taught the strategies and methods of malicious hackers; therefore, teaching students these tactics has the potential to compound, rather than fix, the problem of the increasing number of malevolent hackers. Ultimately, it is the students' decision whether to use their newfound skills in an ethical or malicious way; however, it is important for instructors and instructing institutions to provide the students with not only the proper skills but a strong moral standing as well. The purpose of this paper is to analyze ethical hacking, its use in information security, and the implications that occur from teaching individuals ethical hacking. To do this, a brief history of hacking will be provided, and a basic understanding of what hacking must be reached. This paper will discuss the different classifications of hackers along with what side of legality they are placed. The actions of some are not always black and white in terms of the law. Then it will delve into ethical hacking itself. This will include the significance of ethical hacking, the code of ethics these hackers must follow, and an ethical hacker's methodology on the job. Next it will discuss the implications of teaching ethical hacking to students and some good practices that can be employed to not only protect the instructing institution but the students as

well. Finally, this paper will call attention to some common laws for hackers to be aware of along with some recent data breaches caused by malicious hackers.

The remainder of this paper will be organized as follows: Section 2 introduces relevant background information on hacking. This information will include a short history on hacking, the three main classifications hackers are put under, and what classification ethical hackers are considered a part of. Section 3 will analyze ethical hacking in depth. This section will evaluate the significance of ethical hacking with information security, present the code of ethics that ethical hackers must adhere to, and discuss the methodology used by ethical hackers on the job. The analysis section will also discuss the benefits and implications ethical hacking has on society. Further, in Section 3, possible solutions will be analyzed that may alleviate the impact of the ethical hacking implications brought forward in the analysis section. Finally, Section 3 will conclude with call attention drawn to federal laws that both malicious and ethical hackers should be aware of when they decide to use their skills.

II. Background

This section describes the history of hacking, the types of hackers and at what category the ethical hackers fall into.

2.1 Origin of Hacking

The origin of hacking can be traced to college campuses such as Stanford University and Massachusetts Institute of Technology in the 1960s; however, the term hack or verb hacking was a reference to methods or actions taken as shortcuts to finish tasks in an efficient manner. Despite hacking's connotation today, original hackers enjoyed and explored new technology without malicious intent (Hartley et al., 2017). Though hacking began innocently, some hackers quickly learned they could use their skills and knowledge to exploit companies. In the 1970s, Steve Jobs and Steve Wozniak, the future founders of Apple Computer, made and sold devices known as a "blue box". These devices utilized a whistle, obtained from a Cap'n Crunch cereal box, that allowed users to make free phone calls through AT&T (Farsole et al., 2010). In the early 1980s some of the first known hacker groups were formed which further caused havoc through an online battle to jam phone lines. The actions of these groups lead to a governmental response with the Computer Fraud and Abuse Act passed in 1986, which made breaking into computer systems a federal crime (Farsole et al., 2010). This could be viewed as the beginning of the negative connotation that hacking is known for now. After the Computer Fraud and Abuse Act was passed; the first computer worm was made and unleashed, a hacker's manifesto was published, and hacking groups have attacked government and college websites (Farsole et al., 2010) (Peacock,2013).

2.2 Types of Hackers

Hackers have been classified into three overarching categories. The three categories are White Hat, Black Hat, and Gray Hat hackers. These categories and the hackers placed in them were determined from the intentions and actions of those that exist within them. The two most common categories are white and black hat hackers because these two categories were formulated from the hacker's intentions and whether they were good or bad. However, the third category, gray hat hacker, was created for those that did not fit cleanly within black or white hat (Peacock, 2013). The terms "white hat" and "black hat" are derived from old western movies in which the good guy wore a white hat, and the bad guy wore a black hat (Peacock, 2013) (Pace & Jagnarine, 2005). A white hat hacker is typically an information security professional that possesses a hacker's toolset that uses this toolset to determine where weaknesses occur in a system and either deploy or recommend countermeasures (Peacock, 2013). White hat hackers will obtain proper authorization from the person or organization that owns the rights to the system they will break into. They work in a strutted environment that the owner of the system is fully aware of at the time of the attempted hack. In contrast to white hat hackers, black hats are viewed as the stereotypical bad guy. These hackers have malicious intentions. Though the two main categories of hackers use the same or similar tools to access the system, the primary thing that separates the two is their intentions. They use their skills to disrupt, damage, and steal from computer systems and their owners. Black hat hackers are seeking personal gain from their actions which can range from selling stolen data to destroying data to cause problems for the authorized user later. Not only do their intentions separate them from white hat hackers but their lack of authorization to access a system also separates them (Pace & Jagnarine, 2005). Gray hat hackers exist in a moral gray area. For the most part they act illegally and do not acquire formal or correct authorization to access a computer system. However, their intentions are not completely malicious. Many gray hats begin as black hats and later utilize their skills for their perception of good (Thomas et al., 2018). Hackers that work for the government are considered gray hat hackers. These hackers are performing their duties as a government employee to ensure national security through hacking foreign governments (Thomas et al., 2018). A common occurrence for nongovernmental gray hats is breaking into a website or

company computer system without permission and afterwards contacting the company for compensation in return for details on the security flaw. Though their actions might have good intentions, they are still considered illegal because permission was never granted.

2.3 Who are Ethical Hackers

Ethical hackers will typically fall under the category of white hat hackers. These hackers possess a certification from the EC-Council, which requires them to have experience in information security and to pass an exam. Ethical hackers are hired by organizations to test and validate their security controls (Thomas et al., 2018). Organizations that hire ethical hackers are typically inquiring into the safety and security of sensitive data and if the hired ethical hacker obtains access to this information/data they must be trusted to not steal or utilize the data for personal gain. What separates ethical hackers from white hats is the code of ethics they must follow to remain an ethical hacker. This code of ethics grants them more trust and credibility than regular white hat hackers. Though an ethical hacker must follow the EC Council's code of ethics it is also important for them to stay informed on new penetration methods. However, in doing so their professional ethics might come in question. Resulting in the creation of larger implications for ethical hackers and ethical hacking as a whole (Thomas et al., 2018). A certified ethical hacker's trustworthiness directly relates to the possibility of employment and if their ethics ever come into question, it may cost them their career.

III. Analysis

This section will take a more in-depth look at ethical hackers. The code of ethics formulated by EC Council will be addressed and evaluated on how feasible it is for all certified ethical hackers to follow. Then both the benefits and implications of ethical hacking within education will be discussed. Following the implications, potential solutions will be given to ease the impact of these implications. Finally, a brief overview of the most significant federal laws that affect malicious and ethical hackers alike will be presented. 3.1 Code of Ethics To become an ethical hacker, an information security professional must pass a certification exam conducted by the EC-Council. However, to maintain possession of their certification, ethical hackers must follow the EC-Council's code of ethics. Though most of these rules rely on common sense and are black and white, a few remain ambiguous and may vary in meaning in different situations. It is this ambiguity in an ethical hacker's code of ethics that can call into question their professional ethics. Many of the individual rules within the EC Council's code of ethics overlap with professional ethics. These common ones are do not steal or damage client information, do not involve yourself in deceptive financial practices, and obtain proper authorization before accessing a system or network, to name a few (EC-Council, 2021). Although, as stated previously, ethical hackers use methods and tools that are extremely similar, if not the same, as malicious hackers. Therefore, when the EC Council's code of ethics requires ethical hackers to avoid contact and affiliation with any black hacker

The EC-Council provides only one avenue to become a certified ethical hacker and one code of ethics they require these certified hackers to follow. There are several other professionally recognized information security organizations and communities that possess their own form of ethics. These organizations include CREST, ISC2, and ISACA to list a few (Thomas et al., 2018)

3.2 Benefits of Ethical Hacking

It has become more and more apparent over the last decade that information security professionals are always on the defensive. Many times, they are only able to employ preventative measures to hinder malicious hackers and when a malicious user gains access to a restricted system or network, information security professionals play the role of damage control. Ethical hackers provide an opportunity for security professionals to play a more offensive role in protecting their client's systems and networks (Hartley et al., 2017). Thus, as the Internet of Things continues to increase in size, the threat of users with malicious intent increases along with it. In a 2013 study performed by Ronald Pike, 206 cyber security professionals were asked their beliefs on the best way to prevent malicious hackers and they unanimously replied with the inclusion of instructional hacking at schools and universities (Pike, 2013). It is important for most cyber security professionals to understand hacking in some fashion to efficiently protect their systems against it. While most organizations nowadays have full- time cyber security professionals working for them, certified ethical hackers can be viewed as an extra measure of security or as cyber security auditors. Auditors' objective is to improve upon the system's/network's security, not to damage or steal from the company that hired them (Hartley et al., 2017). It has become common practice for organizations and corporations to hire white hat/ethical hackers to infiltrate their systems. These hacks or penetration tests are viewed as baseline security that these organizations must have to deter or fully prevent common hacking methods used by malicious hackers (Pace & Jagnarine, 2005). White hat's will relay any security risks or vulnerabilities found along with their severity to the hiring organization and provide potential solutions they can employ to eliminate or reduce these risks.

3.3 Implications of Ethical Hacking

Permissions abuse is categorized by software re-questing permissions not essential to the functionality of the program or application, specifically with intentions to use device resources and collect information about the user. For instance, over the years there has been controversy about the permissions required by apps like Face book and Messenger, including the ability to change the state of network connectivity, send outgoing calls, read text messages, read call logs, contact data, and more. Although these permissions are indicative of features on the app, it is also possible that they can be abused without the knowledge of the user in a worst-case scenario. While one may deduce legitimate reasons for such data collection, it seems increasingly unnecessary as the list goes on, and some such apps have been found to save this in-formation in persistent records. While apps like this at least inform the user of the range of permissions, others access devices without giving such notice. One study on real-time security monitoring on smart phones found that countless apps access location, device ID, network status, and more without ever informing the user (Enck et al., 2019). Without the user having a way to detect this, their security is breached, and malicious attackers can exploit their devices.

3.4 Federal Laws Affecting the Action of Hacking

There are several significant federal laws that directly affect the action of hacking. As stated previously in the background section of this paper, the Computer Fraud and Abuse Act (CFAA) was enacted in 1986. The CFAA prohibits unauthorized access to a separate party's computer system. If this law is violated, a hacker could face up to ten years in prison depending on the computer system infiltrated and the information that was compromised (Marshall Jarrett et al., 2015). A second federal law that hackers should be aware of is the Stored Communications Act (SCA) which was enacted in 1986. The SCA provides protection for the customers of network service providers. It also prohibits the interception of communications whether they be oral, wired, or electronic. While the punishment for violating the SCA may not be as lengthy as the CFAA violating the SCA can lead to two years imprisonment on the first offense. The Electronic Communications Privacy Act (ECPA) is directly related to the SCA and was enacted at the same time with the SCA being Title II of the ECPA. Where the SCA addresses intercepted communications, the ECPA focuses on stored electronic communications and protects civilians from governmental wiretaps. These three laws are only a select few of many that cyber security professionals should be aware of and do not include the many different state laws that could affect malicious and ethical hackers. Therefore, it is important that before an ethical hacker act while working that they review what laws they may come into conflict with.

3.5 Ethical Hacking Resources Misuse

In a study performed by Ronald Pike, he identified several propositions for educational institutions to employ to combat increasing the number of malicious hackers while attempting to train ethical hackers. Pike found that groups of hackers whether they be malicious or ethical, create ethical frameworks that guide activities and discipline (Pike, 2013). Ethical frameworks work like group morals. If a white-hat hacker peer would not perform an action, then the white-hat pondering that action will most likely not act on it. These frameworks are created through social interaction and the formation of peer groups. It is proposed that hacking instructors should encourage the formation of peer groups that support white hat hacking methods and practices. The second proposition that Pike presents is directed toward competition. Students should be exposed to hacking competitions because it provides real-world scenarios and rewards students that utilize white hat methods. Competitions also create an opportunity for students to expand their social network and in turn their ethical framework. The second and third proposition are closely related in that the third proposition relates to rewarding students for their hacking methods. If a peer group is rewarded and provided recognition for white hat hacking methods those methods are more likely to be reinforced over black hat methods. These three propositions will not completely solve malicious hacker numbers increasing due to ethical hacking education, but they should lead to a decrease in the overall number of malicious hackers created through formal education. Another possible solution to decrease malicious hacking is to teach the viewpoints of hacking and ethics during such instructions and resources documentations. The resources that are meant for white hat hackers, are now used by malicious hackers (Islam et al., 2021). There are ethical hacker forums where many threads have malicious intent. The online marketplace and online information intended for benign purpose are now also used by malicious hackers. The intent of hackers is becoming so malicious that in many articles, "hackers" are implicitly means malicious hackers, rather white hat hackers. For example, the author of (Islam et al., 2021) used hacker to mean malicious hacker for most of their work. There is an example of hackers who started his carrier as a hacker but later took hacking to an extreme level (Hamid, 2018). He used online available resources to train himself initially, before joining the terror group. He started hacking since his teenage and became a hacktivist.

3.6 Interdisciplinary Research as a Measure Against Malicious Hacking

There are interdisciplinary concepts that can be applied to minimize or harden the activities of hackers. For example, feature selection method used for reducing feature dimensions of cyber security dataset (Ahsan et al., 2021), can be used to select mal features of emails (against social engineering attack). Computational trust can be used trust the activity of another connecting device and malicious user (M. Chowdhury & Nygard, 2018) (M. M. Chowdhury et al., 2018) (M. M. Chowdhury & Nygard, 2017) (Md Minhaz Chowdhury, 2017) (Krishna Kambhampaty, Maryam Alruwaythi, Md Minhaz Chowdhury, 2019) (Nygard et al., 2017) (Kendall E. Nygard, Md Minhaz Chowdhury, Ahmed Bugalwi, 2017). State-of-the-art methods of securing cloud data can be used to secure data on cloud (Mayerski & Chowdhury, 2021) (John Hanley, Md Minhaz Chowdhury, Mike Jochen, n.d.) and methods of securing mobile devices can be used as individual or business best practices (A. Mos & Chowdhury, 2020) (Helm & Chowdhury, 2021) (Khan & Chowdhury, 2021) (Atanassov & Chowdhury, 2021). Clients and employees can be trained to follow the best practices against social engineering attack by hackers and how to automatedly trust a user (Mattera & Chowdhury, 2021) (Krishna Kambhampaty, Maryam A Maryam Alruwaythi, Md Minhaz Chowdhury, 2019). State-of the-art defense against malwares can be practices, example defense against ransomware (M. A. Mos & Chowdhury, 2020). Device hardening is a good way to discourage attackers (Rae et al., 2019). The harder the mobile device will be to attack, the less interest a hacker will get. In the worst-case scenario, such techniques can keep out the script kiddies hackers or low skilled hackers.

IV. Conclusion

The article presented the relation between intentions and the methods used for ethical hacking. The article also presented a tying discussion on hacking with the current laws used for preventing. The Internet and the Internet of Things are expanding at an exponential rate, and it is becoming increasingly important to ensure computer systems and networks are sufficiently secure from malicious hackers. Ethical hacking is becoming an integral part of the cyber security field; however, its practice and education result in significant implications. The use of hacking as a cyber security tool allows information security professionals to seek out vulnerabilities along with the opportunity to identify any future problems. These implications consist of increasing the number of malicious hackers through the education of future ethical hackers, the possibility of ethical hackers to break contract with employers, and whether hacking is ever actually ethical. Possibly the greatest concern that surrounds ethical hacking, is its instruction to college students. Cyber security professionals and businesses worry that they are increasing the number of malicious hackers through teaching students how to use the same methods as black hat hackers. Therefore, it is important for institutions and instructors to instill correct knowledge of laws concerning hacking and their repercussions. Studies have also shown that the more socially involved and the more students feel rewarded for their actions while learning ethical hacking, the less likely it is that these students will turn to black hat hacking. It is important for certified ethical hackers to follow the EC-Council's code of ethics. They must adhere to this code not only to remain certified through EC-Council, but also to remain trusted by past, present, and future employers. However, for ethical hackers to remain up to date on methods of malicious hackers their adherence to their code of ethics and their professional ethics may be called into question.

References

[1]. Ahsan, M., Gomes, R., Chowdhury, M. M., & Nygard, K. E. (2021). Enhancing Machine Learning Prediction in Cyber security Using Dynamic Feature Selector. Journal of Cyber security and Privacy, 1(1), 199–218. https://doi.org/10.3390/jcp1010011

[2]. Atanassov, N., & Chowdhury, M. M. (2021). Mobile Device Threat: Malware. IEEE International Conference on Electro Information Technology, 2021-May, 7–13. https://doi.org/10.1109/EIT51626.2021.9491845

[3]. Chowdhury, M. M., & Nygard, K. E. (2017). Deception in cyberspace: An empirical study on a con man attack. IEEE International Conference on Electro Information Technology, 410–415. https://doi.org/10.1109/EIT.2017.8053396

[4]. Chowdhury, M. M., Nygard, K. E., Kambhampaty, K., & Alruwaythi, M. (2018). Deception in Cyberspace: Performance Focused Con Resistant Trust Algorithm. Proceedings - 2017 International Conference on Computational Science and Computational Intelligence, CSCI 2017, 25–30. https://doi.org/10.1109/CSCI.2017.5

[5]. Chowdhury, M., & Nygard, K. E. (2018). Machine learning within a con resistant trust model. Proceedings of the 33rd International Conference on Computers and Their Applications, CATA 2018, 2018-March.

[6]. Dvorak, R., Dillon, H., Ralston, N., & Welch, J. M. (2020). Exploring ethical hacking from multiple viewpoints. ASEE Annual Conference and Exposition, Conference Proceedings, 2020-June. https://doi.org/10.18260/1-2--34640

[7]. EC-Council. (2021). Code Of Ethics - EC-Council. EC-Council. https://www.eccouncil.org/code-ofethics

[8]. Enck, W., Gilbert, P., Chun, B. G., Cox, L. P., Jung, J., McDaniel, P., & Sheth, A. N. (2019). Taint Droid: An information-flow tracking system for real time privacy monitoring on smart phones. Proceedings of the 9th USENIX Symposium on Operating Systems Design and Implementation, OSDI 2010, 393–407.

[9]. Farsole, A. A., Kashikar, A. G., & Zunzunwala, A. (2010). Ethical Hacking. International Journal of Computer Applications, 1(10), 14–20. https://doi.org/10.5120/229-380

[10]. Hamid, N. (2018). The British Hacker Who Became the Islamic State's Chief Terror Cyber coach: A Profile of Junaid Hussain – Combating Terrorism Center at West Point. Combating Terrorism Center, 11(4), 30–37. https://www.academia.edu/36582618/A_Profile_of_Junaid_Hussain_The_British_Hacker_Who_Became_the_Islamic_States_Chief_Terror_Cyber coach

[11]. Hartley, R., Medlin, D., & Houlik, Z. (2017). Ethical Hacking: Educating Future Cyber security Professionals. Proceedings of the EDSIG Conference, October, 1–10. http://proc.iscap.info 2017/pdf/4341.pdf%0Ahttp://iscap.com
[12]. Helm,G., & Chowdhury, M. M. (2021). Security Issues of Mobile Devices: A Survey. IEEE international Conference on Electro Information Technology, 2021-May, 14–20.