Impact Factor: 9.9
ISSN-L: 2544-980X

Is Ethical Hacking Ethical?

Shohjakhon Jonuzokov
AI & Robotics Student
New Uzbekistan University

Abstract: This paper examines the ethicality of ethical hacking as a security countermeasure. It defines and examines ethical hacking as a safety practice before considering arguments both in favor of and against its implementation. Critical reflection is then offered on potential implications for organizations choosing either to implement or omit ethical hacking as part of their broader security efforts. Ultimately, this paper concludes that it is possible for ethical hacking to be considered an ethically defensible strategy provided certain conditions are met; namely, that it meets all applicable regulations (including those related to privacy and data protection laws).

Keywords: Hacking, Cyber Security, Malicious Software, Penetration Testing

1. Introduction

Ethical hacking is the practice of Cyber Security that uses the same techniques and tools as malicious hackers but intends to expose and fix vulnerabilities in a system or network. Ethical hacking is also known as **Penetration Testing** and **White Hat Hacking**. Ethical hacking aims to identify and prevent potential threats before malicious hackers can exploit them (Bhawana et al., 2014). It is highly valued in each organization as it is the era of digitalizing every single piece of data. Thereby, they have a high demand for ethical hackers unless they ignore the privacy of users and data. However, the implication of ethical hacking has been a hot topic of debate for decades. Is it ethical to use the same tools as malicious hackers to protect the system? Is it ethical to breach the system to identify potential vulnerabilities? How can we teach students ethical hacking and assure that they will use their skills only for security purposes? This research will discuss the questions debated among security professionals and examine the pros and cons of this practice. In addition, the research will explore how organizations can implement ethical hacking to protect their systems and the potential risks associated with it.

2. Methodology

The current study used a mixed-method approach to investigate the ethical question of whether or not ethical hacking is ethical. Firstly, several research papers were collected from databases like Google Scholar, core.co.uk, and Research Gate because of the authenticity of each research paper. Moreover, these databases are peer-reviewed which prevents research papers from being outdated, plagiarized, fake, and untrustworthy. 5 research papers were carefully chosen taking into consideration the credibility of the author and working experience in this field. Articles were chosen with the following keywords: cyber security, ethical hacking, ethics of cyber security, and teaching methods of ethical hacking. As this field of cybersecurity is relatively new, it still needs more discoveries and work. On account of this, the number of research in this field is very limited.

In addition to the existing data, I also conducted 2 interviews with experts in the fields of either information security or computer science. The semi-structured interviews were taken online in text and audio formats and then transcribed verbatim. Analyzed using a content analysis approach. The objective was to gain insight into professional perspectives on the subject as well as to uncover any potential arguments or ideas that had not been previously addressed in the literature.

3. Results

3.1 Is it ethical to use the same tools as malicious hackers to protect the system?

The rapid growth and prevalence of the Internet gave access to e-commerce, e-mail, and easy ways of communication. However, it also brought potential threats of being stolen and blackmailed by criminal hackers. These types of hackers are called black hat hackers. Therefore, to overcome this issue, another category of hackers came into existence which is termed ethical hackers or white hat hackers. Ethical hackers utilize the same tools as intruders, however, they neither steal the information nor damage the system. Their purpose is to explore vulnerabilities and report them to the owner with evaluation and instructions on how to remedy them. Ethical hacking can be categorized as a security assessment, a type of training, and a test for the security of the information technology environment (Bayo, 2018). Ethical hacking demonstrates the risks that the system could face and the actions that could mitigate the problem as much as possible. Therefore, it is considered as the most appropriate way of testing available unauthorized backdoors.

3.2 Is it ethical to breach the system to identify potential vulnerabilities?

The driving force of hackers was initially to enhance the security of the system, renovate the existing code, and make it more efficient. Not all forms of hacking are prohibited. Some hacking techniques are comparable to what happens when a car owner accidentally locks his car key inside the car and tries to unlock the door using a different method. He may do this by using force or a strategic approach. Likewise, burglars (malicious hackers) have the same options (Bhawan, 2014).

3.3 How can we teach students ethical hacking and assure that they will use their skills only for security purposes?

There are several key strategies for teaching ethical hacking and ensuring that students use their skills ethically. First, it is important to emphasize the ethical and legal implications of hacking. Students need to understand that there are consequences for unethical behavior, both in terms of legal penalties and damage to their professional reputation. Second, it is important to provide students with a strong ethical framework. This includes teaching the principles of responsible disclosure, which emphasizes responsible reporting of vulnerabilities to the affected organizations. Third, students should be given opportunities to practice their skills in a controlled environment. Finally, it is important to encourage students to pursue certifications in ethical hacking. These certifications demonstrate that students have the knowledge and skills necessary to use ethical hacking techniques in a responsible manner (Ronald, 2013).

4. Discussion

4.1 Is it ethical to use the same tools as malicious hackers to protect the system?

It is even better to use more sophisticated devices when it comes to protecting the system because the purpose of ethical hacking is to test the immunity of the system to either intentional or breaks. These tools can be used to identify security weaknesses and vulnerabilities in the system, which can then be addressed to ensure that the system is secure. Additionally, using the same tools as malicious hackers can help security professionals to better understand the malicious techniques and tactics used by attackers.

From the side of the software development lifecycle, it can be referred to as “testing and evaluating”. Testing the system to assure that it meets certain criteria. Looking from the perspective of software engineering standards, the company is creating a product that is in the interest of the public (IEEE Code of Ethics), as the users now know that the system is secure, private, and tested (Prabhat, 2020).

4.2 Is it ethical to breach the system to identify potential vulnerabilities?

The question of whether it is ethical to breach a system in order to identify potential vulnerabilities is a complex and nuanced one. On the one hand, breaching a system can help to identify potential vulnerabilities that would otherwise go undetected, potentially preventing serious security breaches or attacks. On the other hand, such an action, especially if done without prior permission, can be viewed as unethical, as it involves intentionally bypassing security protocols and potentially causing harm to the system or those using it.

In order to determine whether breaching a system is ethical or not, it is necessary to consider several factors, such as the purpose of the breach and the potential consequences of such an action. If the breach is intended to identify potential vulnerabilities in order to strengthen security protocols, then it could be argued that the action is ethical, as it is done in the interest of protecting the system and its users. However, if the breach is done for malicious purposes, then it is likely to be considered unethical (Divyansh, Arsh, et al, 2021).

According to Divyansh, it is also important to consider the potential consequences of a breach. If the breach is done without permission, it could result in legal repercussions, depending on the jurisdiction. Additionally, a breach could cause serious harm to the system or those using it and could lead to data loss or other damages. Thus, it is important to weigh the potential risks and benefits of a breach before taking such an action.

4.3 How can we teach students ethical hacking and assure that they will use their skills only for security purposes?

Teaching ethical hacking is essential to the future of cybersecurity. However, it is important to ensure that students use their skills ethically and responsibly. The strategies outlined in this paper can help to achieve this goal. By emphasizing the ethical and legal implications of hacking, providing a strong ethical framework, providing opportunities for practice in a controlled environment, and encouraging certification, we can ensure that students use their skills only for security purposes.

References

1. Jain, D. Kumar, A. Suman, C. (2021). Ethical hacking & Cybersecurity future, (IJCRT) International Journal of Creative Research Thoughts, Volume 9, Issue 5.
2. Jamil, D. Numan, M. (2011). ‘Is ethical hacking ethical?’, International Journal of Engineering Science and Technology (IJEST), Volume 3, Issue 5.

3. Kumar, P. Acharya, B. (2020). A review paper on ethical hacking, International Journal of Advanced Research in Engineering and Technology (IJARET), Volume 11, Issue 12.
4. Omoyiola, B. (2018). The legality of ethical hacking, IOSR Journal of Computer Engineering (IOSR-JCE), Volume 20, Issue 1.
5. Pike, R. (2013). The "ethics" of teaching ethical hacking, Journal of International Technology and Information Management, Volume 22, Issue 4.
6. Sahare, B. Naik, A. Khandey, S. (2014). Study of Ethical Hacking, (IJCSIT) International Journal of Computer Science and Information Technologies, Volume 2, Issue 6.