

Anthony Gomez-Reyes

Prof. Diwakar Yalpi

CYSE201S

23 November 2023

Ethical Hacking and Social Science

Introduction

In the rapidly evolving landscape of cybersecurity, professionals face the ongoing challenge of defending digital assets against an array of threats. Ethical hackers, in particular, are tasked with proactively identifying vulnerabilities in systems to prevent malicious exploitation. This paper explores how ethical hackers rely on social science research and principles, demonstrating the practical application of concepts learned in class and addressing broader societal implications, especially those related to marginalized groups.

Overview of Ethical Hacking

An ethical hacker, also known as a "white hat," (What Is Ethical Hacking and How Does It Work?) is described as a "security expert that performs security assessments" (What Is Ethical Hacking and How Does It Work?) with the aim of improving an organization's security posture. The key concepts of ethical hacking involve staying legal, defining the scope, reporting vulnerabilities, and respecting data sensitivity. According to the text, ethical hackers differ from malicious hackers as they "use their knowledge to secure and improve the technology of organizations," (What Is Ethical Hacking and How Does It Work?) providing a valuable service by identifying vulnerabilities and offering remediation advice with the organization's consent. The skills required for ethical hackers include "expertise in scripting languages, proficiency in operating systems, knowledge of networking, and a solid foundation in the principles of

information security," (What Is Ethical Hacking and How Does It Work?) as highlighted in the text. Certifications such as "Certified Ethical Hacking Certification, Offensive Security Certified Professional (OSCP) Certification, CompTIA Security+, Cisco's CCNA Security, and SANS GIAC" (What Is Ethical Hacking and How Does It Work?) are mentioned as common in the field. Ethical hacking aims to identify vulnerabilities through reconnaissance and testing, with the ethical hacker providing a detailed report on compromised vulnerabilities and mitigation steps, as outlined in the text. However, ethical hacking has limitations such as a "defined scope," "resource constraints," and "restricted methods," (What Is Ethical Hacking and How Does It Work?) including avoiding test cases that may lead to server crashes.

Social Science in Ethical Hacking

Social science research is frequently used by ethical hackers to comprehend the psychological components of cyberthreats. Studies on social engineering strategies, for instance, assist professionals in anticipating and countering deceptive tactics employed by malevolent actors. Furthermore, user behavior research helps ethical hackers create security awareness campaigns that work well for businesses. "Over 99% of cyberattacks require human interaction because, in most cases, it's much easier to trick a person than it is to trick a computer." (Poston). This underscores the significance of understanding human psychology and motivations, a core focus of social science research. "Social engineering exercises are a vital aspect of ethical hacking engagements," (Poston) highlighting the indispensable role of social science in identifying and addressing human vulnerabilities. The emphasis on knowing the target, simplifying information acquisition, and keeping social engineering subtle aligns with social science principles that explore how individuals respond to various stimuli and communication strategies. In essence, the integration of social science research in ethical hacking ensures a

comprehensive approach that recognizes and addresses the human element in cybersecurity, making it an indispensable tool for ethical hackers in their efforts to fortify systems against cyber threats.

Social Science Principles in Daily Routines

Ethical hackers use fundamental ideas from social science. The adherence to ethical and social principles is paramount in daily routines. "Ethical issues are the most important and prevalent issues that must be addressed in our society." (Jain). This underscores the foundational role of ethics in guiding actions. The set of values and principles delineated serves as a compass for decision-making, defining how to act in various situations: "It is the set of values and principles which define how to act in a particular situation." (Jain). Emphasizing the overarching goal of ethical issues, stating, "The main aim of ethical issues is to protect the rights of individuals and groups by defending them against unfair or unjust treatment." (Jain). This principle aligns with the ethical hacker's responsibility to safeguard against potential harm or injustice in their activities. Moreover, the acknowledgment of "ethical hacking challenges in social and cultural ethics" (Jain) recognizes the intersection of technology and societal values. In the broader context, the ethical hacker is called to navigate and address prevalent social and ethical issues, such as social inequality, discrimination, and environmental degradation, mirroring the multifaceted nature of ethical considerations. By recognizing the psychological aspects of cyberattacks, experts can develop focused security plans that highlight the role of people within the larger cybersecurity framework.

Relationship with Marginalized Groups and Societal Impact of Ethical Hacking

Ethical hacking promotes inclusivity by considering the diverse perspectives of marginalized groups. Professionals in this field actively work towards ensuring that

cybersecurity measures are accessible and effective for everyone, irrespective of their background. This inclusivity extends to addressing potential biases in algorithms and ensuring fair representation in cybersecurity discourse. (Kozhuharova et al.). While strengthening digital defenses against cyber-attacks is one way that the ethical hacking profession significantly contributes to social well-being. Experts in this domain contribute to the security of vital infrastructure in addition to safeguarding private enterprises. In the realm of education, challenges arise as students, intrigued by the allure of hacking, may not fully comprehend the ethical implications. In the text, "the major problem is that the students really don't know the importance and impacts of hacking." (Society impacts of ethical hacking). However, it emphasizes the imperative of instilling ethical considerations in hacking education. In the business sphere, the digital landscape's ubiquity has led to an increase in electronic transactions, providing ethical hackers with opportunities to uncover vulnerabilities. A safer and more robust digital civilization is achieved by ethical hackers by staying ahead of growing cyber dangers. (Society impacts of ethical hacking)

Conclusion

In conclusion, ethical hacking is a field in cybersecurity that carefully combines social science theories and research. Understanding human behavior, cultural sensitivity, and ethical considerations are among the ideas that ethical hackers have learnt. These ideas are essential to their everyday work. Through the application of these principles, ethical hackers address the concerns of marginalized groups and society at large, while also improving the security of digital systems and fostering a more inclusive and ethical cybersecurity landscape.

Works Cited

Jain, Aditi. "Ethical Hacking Issues: Professional, Legal, Social & Cultural." KnowledgeHut, www.knowledgehut.com/blog/security/ethical-hacking-issues.

Kozhuharova, Denitsa, et al. "Ethics in Cybersecurity. What Are the Challenges We Need to Be Aware of and How to Handle Them?" *SpringerLink*, Springer International Publishing, 1 Jan. 1970, link.springer.com/chapter/10.1007/978-3-031-04036-8_9.

Poston, Howard. "Ethical Hacking: Social Engineering Basics." *Infosec*, Infosec, resources.infosecinstitute.com/topics/hacking/ethical-hacking-social-engineering-basics/. "Society Impacts of Ethical Hacking." *LinkedIn*, MIE-Modern International Education , 17 Apr. 2022, www.linkedin.com/pulse/society-impacts-ethical-hacking-mie-modern-international-education.

"What Is Ethical Hacking and How Does It Work?" *Synopsys*, Synopsys, www.synopsys.com/glossary/what-is-ethical-hacking.html#:~:text=Ethical%20hackers%20use%20their%20knowledge,identified%20vulnerabilities%20to%20the%20organization.