Chad Ward

Professor Diwakar Yalpi

CYSE201S

7 April 2024

Cybersecurity Career Professional Paper

Introduction

Social engineering plays on sociology by posing something unauthentic as being legitimate to people that will be curious and vulnerable enough to fall victim to. Ethical hackers take advantage of the number one social engineering tactic known as phishing defined as an attack that aims to obtain sensitive information by posing as a real email or website that the user is known to use (GeeksforGeeks, 2024). Once the ethical hacker has conducted a phishing test, they will be able to report metrics to their organization which could indicate which employees may need user training of Cyber awareness. Humans are prone to fall victim to these ploys and emotional responses are typical in Cyber victims. Those that deal in Cyber victimization have feelings of self-blame, anger, shame, fear, and sadness when victimized in Cybercrime (Canadian Resource Centre for Victims of Crime, n.d.).

Ethical hackers are the good guys and are aiming to educate through simulated attacks whilst avoiding the consequences that come from real attacks. These white hat hackers help society by stabilizing, growing the economy of organizations by providing a great return of investment. As of 2023, organizational data breaches in the United States are estimated to be a loss of an average 9.48 million dollars (Statista, 2024). Ethical hackers help ensure that these breaches are less likely to occur by testing systems and making the weak areas known to organizations, providing recommendations to bolster security. Ethical hackers in the United States make a yearly salary that averages around $82,000 which can be a motivating factor into why career (Scheldt, 2022).

Consent to traverse in the digital environment to find vulnerabilities is important for ethical hackers to consider along with the data privacy implications within the field. When working in this career it is important to treat users and their data as you would approach humans and their personal belongings in the real physical world. However, digital ramifications and consequences are just as serious as real-world privacy as customer data can contain sensitive information such as PII (Personal Identifiable Information) like an SSN (Social Security Number). Thus, it is important to work with care when dealing with systems and accounts that are not your own, the hacker must perform operations properly and uphold trust with given consent or they could face consequences such as being fired or serious lawsuits, legality battles (Johansen, 2023). The Code of Ethics is shaped through rules created by society to act morally and is the law of the land for these hackers.

Conclusion

Ethical hacker is one of the most sought-after Cybersecurity career positions typically requiring one to “pentest” systems with permission to find and exploit vulnerabilities. Once this white hat hacker (ethical) conducts their work, they will then report their helpful findings to an organization or customer to bring awareness of what a black hat hacker (unethical) could take advantage of. Social science and ethical hacking relate through the interdisciplinary research of the two disciplines, the hypothetical questions asked, ethical problems that arise and social engineering approaches that a pentester use to create exploitable vulnerabilities. “Ways that ethical hacking benefits society” could prompt the use of an interdisciplinary approach with collaboration between social scientist and ethical hacker while a question could be “what motivates a person to become an ethical hacker?” Ethical topics such as data privacy, access consent are issues that an ethical hacker must consider while conducting work in a social environment and social engineering tactics such as phishing emails can create an entry point for ethical hackers to leverage against users that are the weak links of any network thus making them victims.

References

Canadian Resource Centre for Victims of Crime. (n.d.). The Impact of Victimization. https://www.crcvc.ca/docs/victimization.pdf

Cost of a data breach in the U.S. 2023. Statista. (2024, March 22). https://www.statista.com/statistics/273575/us-average-cost-incurred-by-a-data-breach/#:~:text=As%20of%202023%2C%20the%20average,million%20U.S.%20dollars%20in%202023.

GeeksforGeeks. (2024, March 20). Phishing in Ethical Hacking. GeeksforGeeks. https://www.geeksforgeeks.org/phishing-in-ethical-hacking/

Johansen, R. (2023, October 13). Ethical Hacking Code of Ethics: Security, Risk & Issues. Panmore Institute. https://panmore.com/ethical-hacking-code-of-ethics-security-risk-issues#:~:text=The%20legal%20risks%20of%20ethical,it%20is%20not%20performed%20properly.

Scheldt, A. (2022, August 15). How Much Can You Earn as an Ethical Hacker. CompTIA. https://www.comptia.org/blog/how-much-can-ethical-hacker-earn