Cybersecurity Professional Career Paper: Penetration Testing and Ethical Hacking.

Student Name: Matthew Fox

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Diwakar Yalpi

Date: 11 / 14 / 2025

Introduction

The career this paper will be focusing on is ethical hacking. An ethical hacker is hired to attempt a penetration test to see if there are any vulnerabilities in a company's systems. These hackers are also known as white-hat hackers. Fashoto et al. (2018) explain that “Penetration testing uses the same principles as crackers or hackers to penetrate computer network infrastructure, thereby verifying the presence of flaws and vulnerabilities, and help to confirm the security measures.” Angel and Sarala (2011) go further into why penetration tests are important: “ If vulnerability is utilized by an unauthorized individual to access company resources, company resources can be compromised.” We need these types of hackers because it is difficult to predict where a malicious hacker might strike if you do not have a solid understanding of your system's weak points. Cybersecurity is generally very important; in the modern day, many activities are online. Unfortunately, that does not guarantee the safety of things like your finances or identity. What this paper will cover is how ethical hackers use the social sciences to pinpoint where a hacker may most likely attack a company.

Social science principles

As stated in the introduction, ethical hackers simulate how a real hacker may think in order to gain access to something. Using the motivations that people have when they are hacking, you may be able to infer where a hacker might strike. For example, if the cyber criminal is in need of financial gain, he may strike the bank account or a person with access to the finances rather than trying to completely shut down a company's systems. Ethical hackers may use parsimony to help pinpoint a company where their issues may be. There may be situations where someone gains access through a complicated and detailed method, explaining that it may

be an issue for those less experienced. So keeping it as simplistic as possible will help the company patch up its vulnerabilities quicker and more efficiently. Coming back to motivations, they are a significant way to help boost the defenses of a system. A coordinated attack by a malicious hacker will be full of motivations, examining where the attackers strike, and then hiring an ethical hacker to penetrate your system after the incident can significantly help prevent hackers with the same motivations in the future from striking your systems.

Application of Key Concepts

In the hacker subculture, there is an assumption that every hacker has experience with handling a computer and using it. Cangea (2018) states that " The word *hacker* was initially used to describe an exceptional computer expert, capable of developing complex reasoning for studies of software programs…". By taking this assumption, ethical hackers are able to use any means necessary to gain access to a system. The CIA triad also has importance too. A corporation always wants to have Confidentiality, Integrity, and Availability at all times; if a malicious hacker can compromise one of these, then the corporation could be damaged. One may hire an ethical hacker to attempt and take down one part of the triad, an example is Integrity. If a criminal gains access to important documents, they may tamper with them and potentially spread disinformation, which in turn blocks the company from accessing the correct information. A hacker has different ways to get into a system. They may use tactics like phishing, where they mimic someone in a higher position and ask for personal information, or they may use identity theft to impersonate and access the information the victim has. Ethical hackers may use these strategies to see if it's not just the system that has issues, it is the people who work there. Some ethical hackers may use tools like "John the Ripper" or "Libcrack" to gain access to an

employee's account. This relates to the company's practices with cyber hygiene and how it can be exploited if they do not train and help educate their employees about staying safe on the internet.

Marginalization

Some companies do not put much effort into their cybersecurity practices, which leaves them at risk of an unauthorized person infiltrating their systems and causing a lot of potential damage. Newer organizations may also be susceptible to these issues, as they may not have the financial resources to fulfill the necessary requirements to keep their systems safe. To address these issues, ethical hackers are tasked with analyzing the systems. What these white-hat hackers may do when they're hired is to give the companies the boost they need to help fix their systems and prevent them from being attacked.

Career Connection to Society and Conclusion

White-Hat Hackers contribute to society by going into the minds of an actual hacker and testing the vulnerabilities that may have future consequences. Every department will be affected by a hacker attempt, so it would be efficient to make sure there are no weak points. Even outside of hacking, penetration testing in cybersecurity is important. An example would be a social engineer trying to walk into a physical building and hack from the inside. One of the best ways to defend against hackers is to simulate an actual hacking attempt. It gives you the best information on the weakest places.

To conclude, we need ethical hackers in cybersecurity because they provide us with a behavioral perspective that simply responding to a threat can’t give. It uses many social science tactics to gain a good scope on how hackers may react to being counterattacked, too. They use

the same tools that any hacker may use too, which gives better insight as to not only how the tool may affect the company, but also how you are able to counter it.

Scholarly Journal Articles

- **Ethical hacking solution to defeat cyber attacks**: The methods of penetration testing described here help show how certain vulnerabilities may be detrimental to a company.
- **A study on Penetration Testing**: Penetration tests help guide someone on the thought process of an attacker, which gives the defender the upper hand for future cyber attacks.
- **Evaluation of Network and Systems Security using Penetration Testing in A Simulation Environment**: These sources help differentiate the difference between the types of motivations that an ethical hacker, or a more malicious one, may have while trying to penetrate a system.

References

Angel, S., & Sarala, S. (2011). A study on Penetration Testing. *International Journal of Advanced Research in Computer Science*, *2*(5), 396–398.

Cangea, O. (2018). Ethical Hacking Solution to Defeat Cyber Attacks. *Petroleum - Gas University of Ploiesti Bulletin, Technical Series*, *70*(2), 29–36.

Fashoto, S. G., Ogunleye, G. O., & Adabara, I. (2018). Evaluation of Network and Systems Security Using Penetration Testing in a Simulation Environment. *Computer Science & Telecommunications*, *55*(3), 3–12.