Cybersecurity Professional Career Paper: Penetration Tester (Social Engineering)

Student Name: Daija Brown

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Diwakar Yalpi

Date: 4/13/2026

Introduction

Penetration testers are ethical hackers who operate with explicit written permission from the organization they are testing. They exploit an organization's physical and digital vulnerabilities by conducting real-time tests. This can vary from piggybacking, phishing, or obtaining access to sensitive or "locked down" areas of the network via lateral movement. Penetration testers are important because they turn an organization's expected level of security into a reality.

In this paper, I will describe the differences between a penetration tester and a standard hacker. I will also relate the job role to the principles of social sciences, psychological theories, explain the methodologies these professionals use, and outline their connection to society.

Social science principles

Penetration testers have to understand the "human factors" side of social sciences. There have been multiple studies that outline what vulnerabilities are associated with human behaviors, and what factors and skills improve compliance overall. The Penetration tester utilizes human weaknesses to define areas of improvement from a security perspective. The key difference between the standard hacker and the penetration tester is that a penetration tester has explicit written authorization to hack an organization.

After the penetration test is conducted, a report is generated. This report is used to create an After Action Report (AAR) or lessons learned presentation. This presentation identifies vulnerabilities in the network and areas of improvement that need to be made. These metrics can then be used to create refined security awareness training.

Application of Key Concepts

There are notable psychological theories in the penetration testing field. One of note is the Personality theory. A white hat hacker, also known as an ethical hacker, displays a dominant personality trait of agreeableness. Another psychological theory is the behavioral theory. While deviant peer association is linked to hacking, it's a behavior that is linked to

ethical hacking as well. Penetration testing is also closely related to social engineering. Social engineering preys on the human factors of cybersecurity. The reality is, the "human firewall" may be strong one day, but it's not without its vulnerabilities. Finally, Penetration testers use ethics and the principle of parsimony to conduct their work.

Penetration testers lean on human weaknesses to successfully perform social engineering attacks. Humans value convenience, so they may often use repeated passwords or write them down. The principle of parsimony in this case could relate to the simplicity of humans and their desire for convenience, making password cracking easier for a penetration tester. In some cases, penetration testers may use kindness or look vulnerable to piggyback or bypass security checks. It's important to note the boundaries of what a penetration tester can do. While they may find vulnerabilities outside the scope of their work. They must follow what has been written down and signed by senior leadership. This boundary is what keeps their testing legal and ethical.

Common tools utilized for password cracking are John the Ripper and Hydra. They may also use one of many databases or websites available that have commonly used passwords for the current year. After a penetration tester obtains the right credentials, they can use them to perform a lateral movement in the network. This could potentially provide access to sensitive data on the network.

Marginalization

Cybersecurity as a career path consists primarily of white males. The barrier to entry is significantly impactful for minorities such as women and people of color. The issue becomes exacerbated when considering intersectionality (black women). This is partially due to the lack of resources available to obtain the skills to begin hacking at a young age. Another aspect that

marginalized groups face is the feeling of not belonging in cybersecurity, especially in a difficult field like penetration testing. To become a penetration tester, certain certifications are desired, but they can cost upwards of a thousand dollars for an attempt. Unless the aspiring penetration tester's organization pays for the certification, they may face affordability issues.

Many organizations have introduced incentives for minorities and women to encourage them to join cybersecurity careers, including penetration testing. This is because diversity in the cybersecurity workspace creates an opportunity to expand knowledge bases and provide new perspectives in an evolving field. "Why is it crucial to encourage more women to consider careers in the cybersecurity sector? Primarily, diversity fosters creativity and innovation" (Fortra, 2024).

Career Connection to Society

Penetration testers identify vulnerabilities and exploit them in a controlled environment, so organizations know what they need to improve. Critical infrastructures utilize penetration testing as a method to keep their organization operational. By identifying the gaps in security, critical infrastructures can keep the lights on and water flowing.

Penetration testing has grown due to the introduction of "bug bounty" programs. This creates an environment where freelancers can improve the security posture for organizations and receive monetary rewards. "Bug bounty advocates have argued that they are a cost-effective means for companies of all types to shore up their security posture" (Sridhar & Ng, 2021, 1).

Conclusion

In conclusion, penetration testers contribute to the security of society. While the field is lacking diversity, many organizations are remedying this gap by creating equal opportunities for

minorities. Finally, penetration testers identify vulnerabilities and close the gap between perceived security and actual security.

Scholarly Journal Articles

- This Scholarly article outlines the standard penetration testing process and explores the benefits of automating penetration testing.
    - https://airccj.org/CSCP/vol8/csit88610.pdf.
- This article describes the penetration testing process as a whole and highlights the ethics behind penetration testing.
    - https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4402456.
- This article describes the vulnerability management aspect of penetration testing and identifies the gaps that could lead to data loss.
    - https://link.springer.com/article/10.1007/s11416-014-0231-x

References

Fortra. (2024, May 20). *Closing the Skills Gap for Women in Cybersecurity*. Fortra. https://www.tripwire.com/state-of-security/closing-skills-gap-women-cybersecurity

Sridhar, K., & Ng, M. (2021). Hacking for good: Leveraging HackerOne data to develop an economic model of Bug Bounties. *Journal of Cybersecurity*, *7*(1), 1. https://academic.oup.com/cybersecurity/article/7/1/tyab007/6168453?login=false