

Cybersecurity Professional Career Paper: Pen Tester

Obi Oputa

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Professor Diwakar Yalpi

4/14/26

Introduction

The career this paper will focus on is penetration testing. A penetration tester, or pen tester for short, is an individual who is authorized to perform simulated cyberattacks on the systems, networks, and people within an organization to find weaknesses in their security that malicious actors may take advantage of. This paper explores how penetration testers apply social science principles in their daily work, how the profession interacts with marginalized groups, and how this career connects to society as a whole (Hatfield, 2019).

Relation to Social Science Principles

Penetration testing is deeply rooted in social science principles, mainly the principles of empiricism, ethical neutrality, and relativism. Penetration testers require the understanding of the empiricism principle because they need to base their findings on data from the penetration test rather than assumptions and opinions. The ethical neutrality principle is also required of penetration testers because testers must navigate an ethical line between manipulating and deceiving the participants of a penetration test and doing so in a way that does not stray too far from ethical behavior (Hatfield, 2019). The relativism principle requires penetration testers to understand that all systems are connected and one change to a system will affect other systems. Penetration testers must have an understanding of the systems and the human elements involved in the system in some way (KM, 2024). penetration testing requires both technical and social science knowledge to be successful.

Application of Key Concepts

There are many easily identifiable key concepts from this course that relate directly to the work of a penetration tester. The first being the human factor, which refers to how human capabilities and limitations affect interactions with technology. Pen testers must constantly understand human factors, as social engineering attacks exploit psychological vulnerabilities like trust, authority, fear, and reciprocity to manipulate individuals into giving up sensitive information (K M, 2024). Understanding these vulnerabilities is what allows pen testers to simulate realistic attacks and expose where an organization is weakest in their security. The second of the concepts is social engineering, which is also referred to as the art of human hacking. Social engineers study human psychology to find vulnerabilities in individuals that they can take advantage of to access the information that they require. Steinmetz et al. (2021) studied 37 social engineers to determine the techniques that they used to succeed in their crimes, finding that they relied upon careful research, rapport building, and exploiting social norms to make individuals feel as though they were legitimate.

Marginalization

The penetration testing intersects with many marginalized groups. Women and minorities significantly underrepresent themselves within the field itself. The lack of diversity within the industry contributes to challenges because individuals in a homogeneous group tend to approach problems from similar perspectives. K M (2024) states that diversity and cultural sensitivity are two essential considerations in the security testing of a system due to the fact that different cultures interact with technology in different ways. Attackers also use social stereotypes tied to race, gender, and class, making awareness of these biases important for effective security testing (Steinmetz et al., 2021).

Career Connection to Society

Penetration testers play a critical role in protecting the digital infrastructure that a majority of society depends on. Financial institutions, hospitals, government agencies, and schools all rely on secure networks, and a successful cyberattack on any of them carries serious consequences for the public. Many social engineering tactics are deeply embedded in social structures and human interaction, requiring pen testers to understand sociology just as much as technical security (Steinmetz et al., 2021). From a structural perspective, pen testers help maintain societal stability by keeping critical organizations secure. From a conflict theory perspective, their work also highlights the inequality that exists between organizations that can afford penetration testing and those that cannot.

Conclusion

In conclusion, penetration testing is a career that sits between technology and social sciences. Penetration testers must apply principles from the social sciences to their work in the field. The concepts of human factors, social engineering, determinism, and cybersecurity culture are essential to the work that penetration testers do on a daily basis. Penetration testers have responsibilities to observe, interact with, and protect organizations from bad actors looking to cause harm.

References

- Hatfield, J. M. (2019). Virtuous Human Hacking: The Ethics of Social Engineering in Cybersecurity. *Computers & Security*, 83, 1477.
<https://doi.org/10.1016/j.cose.2019.02.012>
- K M, J. (2024). Social Engineering and Human Factors in Penetration Testing. *International Journal for Multidisciplinary Research*, 6(3).
<https://doi.org/10.36948/ijfmr.2024.v06i03.21496>
- Steinmetz, K. F., Pimentel, A., & Goe, W. R. (2021). Performing social engineering: A qualitative study of information security deceptions. *Computers in Human Behavior*, 124, 106930. <https://doi.org/10.1016/j.chb.2021.106930>