Cybersecurity Professional Career Paper: What do Penetration Testers Do?

Student Name: Labib Khan

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Diwakar Yalpi

Date: 11/14/2025

Introduction

Penetration testers, who are more commonly known as pen testers, are cybersecurity professionals who simulate attacks to identify weaknesses in an organization's digital environment. Their work is crucial to prevent data breaches, strengthen resilience in the face of adversity, and ensure that governments and businesses remain protected in a world where cyber threats are continuously evolving. This paper explores how penetration testers utilize social science principles, how key concepts from our class are used in their daily lives, and how this job interacts with marginalized groups and society.

Social Science Principles as Related to the Career

Penetration testers rely heavily on social science research in order for them to understand human behavior, motivations for hacking, and the psychological factors that lead individuals to fall for social engineering attacks. Psychology principles help these testers design simulated cyberattacks based on cognitive biases such as urgency, authority, and fear. Sociological insights allow them to analyze workplace cultures that might encourage risky or unsafe practices or that discourage reporting suspicious activity. Through human-computer interactions, penetration testers can evaluate how UI design and usability influence user behaviors that can introduce vulnerabilities. These social science principles help ethical hackers develop more realistic tests, create effective awareness training, and recommend behavioral changes that strengthen an organization's overall security posture.

Application of Key Concepts as Related to the Career

Key CYSE 201S concepts like risk management, rational choice theory, deterrence, and human factors directly influence the work of penetration testers as they mimic attacker behavior

and prioritize testing activities. Risk assessments help penetration testers identify which systems require more evaluation. Rational choice theory allows them to anticipate which targets attackers would most likely pursue based on perceived reward and low probability of detection. Human factors guide the design of these social engineering scenarios and the analysis of user errors that can contribute to security failures. Penetration testers apply these concepts through practical use cases, like network reconnaissance, vulnerability scanning, etc. This ensures that their efforts closely align with legal, ethical, and compliance standards.

Marginalization

Penetration testing intersects with issues of marginalization by exposing how certain populations face greater cybersecurity risks due to little to no access to technology, lower levels of digital literacy, and increased vulnerability to targeted social engineering attacks. Marginalized groups, which include immigrants, senior citizens, and low-income individuals often become primary attack targets for scams, phishing campaigns, and identity theft because they lack access to security education and advanced protections. Penetration testers help address these issues by advocating for accessible security design, testing systems that serve vulnerable populations, and promoting inclusive cybersecurity practices within organizations and communities. Their work also supports initiatives aimed at diversifying the cybersecurity workforce.

Career Connection to Society

Penetration testers play a critical role in protecting social infrastructure. These include financial institutions, healthcare networks, government systems, and other essential services from potentially devastating cyberattacks. Their work reduces the likelihood of data breaches,

service outages, and large-scale disruptions that could impact millions of people. This demonstrates how cybersecurity supports societal stability and public trust. These testers also operate within the framework of cybersecurity laws and public policies, like data protection regulations and federal information security standards, which all shape the legal and ethical context of their work.

Scholarly Journal Articles

1. Montañez, R., Golob, E., & Xu, S. (2020). In their study "Human cognition through the lens of social engineering cyberattacks, Montañez et al. (2020) examine how attackers exploit cognitive vulnerabilities, like biases in trust, attention, and decision-making to carry out social engineering attacks. They identify specific mental shortcuts and heuristics (for example, how urgency or authority can affect decision making) that make people more susceptible to manipulation. This is extremely relevant to a penetration tester's role because it provides empirical evidence for psychological factors that social engineers rely on, which enables testers to design more realistic cyberattack simulations and human targeted attack scenarios.
2. Siddiqi, M.A., Pak, W., & Siddiqi, M.A. (2022). In "A study on the psychology of social engineering-based cyberattacks and existing countermeasures", Siddiqi et al. (2022) explore the psychological foundations of social engineering attacks (e.g. persuasion techniques, cognitive biases) and review countermeasures like training, policies, and technical defenses. Their findings support the analysis of social science principles in cybersecurity: they show how awareness training behavior-based interventions can reduce falling for cyberattacks. This aligns with penetration testers

using social science to make ethical assessments and deliver effective security education.

3. Zhu, H., et al. (2021). The article “Social engineering in cybersecurity: a domain ontology and knowledge graph application examples” by Zhu et al. (2021) develops an ontology (a set of concepts) and knowledge graph that models numerous types of social engineering attacks, their relationships, and common tactics. This representation helps penetration testers by giving them a systematic way to classify and communicate threat patterns to businesses. From a career connection perspective, the ontology supports the penetration testers’ risk modeling, threat assessment, and reporting. All of these are key parts of their role in helping organizations understand where they are most vulnerable and how the should prioritize their defenses.

Cited Sources

Montañez, R., Golob, E., & Xu, S. (2020). Human Cognition Through the Lens of Social Engineering Cyberattacks. *Frontiers in Psychology*, *11*(1). https://doi.org/10.3389/fpsyg.2020.01755

Siddiqi, M. A., Pak, W., & Siddiqi, M. A. (2022). A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures. *Applied Sciences*, *12*(12), 6042. https://doi.org/10.3390/app12126042

Wang, Z., Zhu, H., Liu, P., & Sun, L. (2021). Social engineering in cybersecurity: a domain ontology and knowledge graph application examples. *Cybersecurity*, *4*(1). https://doi.org/10.1186/s42400-021-00094-6