Cybersecurity Professional Career Paper: Penetration Testing

Kyle Dunker

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Professor Yalpi

12/6/2025

Introduction

In modern times, cybersecurity has become more and more popular as a major and career path for students. Organizations are relying on cybersecurity roles to help protect their data against ever-growing threats and data breaches. One of the most important roles within cybersecurity is penetration testing. Penetration testers— or "pen-testers" for short— are also known as ethical hackers. Ethical hacking is defined as "the practice of legally probing computer systems and networks to identify and fix security vulnerabilities before malicious attackers employ them." The role of a pen-tester is heavily technical but also requires social science research and practices. With insider attacks being a common attack vector, a pen-tester must understand human behaviors and also be able to communicate effectively with employees and owners of the organizations they are hired to work for. The purpose of this paper is to show how pen-testers rely on social science concepts and principles in their work and how they contribute to society as a whole.

Social Science Principles

Psychology and sociology are both important social sciences used in pen-testing. They use psychology to help understand human behaviors and interactions between technology and human manipulation. Social engineering has become one of, if not the most, common methods used by threat actors in recent years. Social engineering is the practice of exploring human emotions such as trust, fear, curiosity, and urgency (Hadnagy, 2018). Many psychological concepts such as authority bias and decision fatigue are part of social engineering tactics that

lead to data breaches. Pen-testers use these concepts in things like phishing emails when designing their campaigns for testing the security of an organization.

A second social science that is used within the role of pen-testing is sociology. One thing that is very important within a company is organizational culture. This includes things like group behaviors, social norms, and employee training. Weak security practices and training lead to employees falling victim to phishing scams, sharing passwords with other employees that should not have access, using personal devices to access company emails and databases, and ignoring things like setting up 2-FA for company accounts. Pen-testers analyze the social structures of the organization they are testing to see what impact it has on security (Hadnagy, 2018).

Application of Key Concepts

Several key concepts from the material we have gone over in this class directly apply to the daily work of penetration testers. These concepts include social engineering, trust, privacy, and risk perception. They are all central to how testers evaluate security vulnerabilities within a system. When designing and then simulating real-world attacks, these social science concepts are used by pen-testers. This shows how it is not only technical concepts but also human elements used to target the security of a system. For example, phishing campaigns are used to see how employees react and respond to malicious communications. After an employee falls victim to a phishing email, pen-testers then measure how quickly the IT team responds to and fixes the incident.

Some tools used by pen-tests are purely technical (vulnerability scanners and password cracking software), but they also rely on social science methods to interpret results. After testing

the security of a network, they prepare detailed reports that recommend security improvements. A lot of these recommendations are heavily based on things such as organizational culture and employee training (NIST, 2023).

Marginalization

Penetration testing also ensures that sensitive data belonging to vulnerable populations is safeguarded. These groups include low-income populations and the elderly, as these groups generally have less training on security practices. When testing organizations in healthcare, government, and financial institutions, extra precautions must be taken to avoid exposing personal information. The cybersecurity industry as a whole has begun addressing marginalization through diversity initiatives, digital literacy programs, and community outreach. These efforts are extremely important as they help improve equal access to security practices to disadvantaged groups (Pew Research Center, 2022).

Career Connection to Society

Penetration testers play a very important role in society's safety and stability by guarding critical infrastructure such as financial institutions, healthcare networks, and government communications/databases. They use a proactive approach to help prevent financial fraud, protect sensitive records and documents, and ensure the reliability of public services. By identifying and patching vulnerabilities before malicious actors can exploit them, penetration testers contribute to national security and economic stability. There are laws within the practice of penetration testing which govern data privacy and system authorization. This ensures that the

practice of ethical hacking is conducted responsibly and legally. The work of pen-testers helps in building public trust in digital systems and ensures that society can continue to rely on secure online services (Verizon, 2024).

Scholarly Journal Articles

Source 1: Hadnagy (2018) explains how social engineering works by taking advantage of basic human emotions like trust, fear, curiosity, and urgency. His work shows why cybersecurity professionals such as pen-testers need to understand how humans think and react to situations. Being able to predict and recognize human error is very important.

Source 2: Pew Research Center (2022) discusses how digital security risks disproportionately affect marginalized communities. This scholarly journal shows the disparities when it comes to accessing security resources and digital literacy. This supports the paper's discussion of how pen-testers must apply social science principles.

Source 3: The Verizon Data Breach Investigations Report (2024) provides large-scale empirical evidence that human error remains one of the leading causes of cybersecurity incidents. This contributes to understanding how cybersecurity careers like pen-testing relate to broader social behavior patterns and organizational culture.

References

GeeksforGeeks. (2019, September 5). *Introduction to Ethical Hacking*. GeeksforGeeks. https://www.geeksforgeeks.org/ethical-hacking/introduction-to-ethical-hacking/

Hadnagy, C. (2018). Social Engineering: The Science of Human Hacking. 2nd Edition, Wiley. https://doi.org/10.1002/9781119433729

National Institute of Standards and Technology. (2023). NIST Special Publication 800-53: Security and privacy controls for information systems and organizations. U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-53r5

Pew Research Center. (2022). How Americans View Data Privacy. https://www.pewresearch.org/wp-content/uploads/sites/20/2023/10/PI_2023.10.18_Data-Privacy_FINAL.pdf

Verizon. (2024). Data breach investigations report. Verizon Enterprise.