Cybersecurity Professional Career Paper: Penetration Tester

Asher Embry

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Professor Diwakar Yalpi

November 14, 2025

Introduction

As society advances within the digital age, the field of cybersecurity has expanded beyond defense. An important part of current defense strategy is to proactively find weaknesses before an attacker does. This is the role of a penetration tester, or pen tester for short, often used interchangeably with the term ethical hacker. IBM describes the practice as looking for vulnerabilities in a simulated attack against a company's computer systems, which can include hardware, software, or even human weaknesses. The U.S. Bureau of Labor Statistics (BLS) groups the role under Information Security Analysts, noting that they "plan and carry out security measures" (U.S. Bureau of Labor Statistics, 2025) by simulating cyberattacks to test for vulnerabilities. While this career is highly technical, requiring strong knowledge in networking, applications, and coding, it also involves a strong application of social sciences. The goal is not just to find a flaw in a network's security, but to understand and mimic how an attacker would behave, which relies on principles of psychology, sociology, and criminology.

Social Science in Penetration Testing

Daily duties of a pen tester is a form of applied behavioral research. They must use an attacker's mindset, which is less about technology and more about understanding a person's motivation, behavior, and weaknesses. Understanding an attacker's motivations integrates cyberpsychological, psychological, criminological, and sociological theories to determine the motives and actions of a cybercriminal (Martineau, Spiridon, & Aiken, 2024). Cybersecurity Guide reinforces this idea by noting that pen tester provides the best possible security by "offensively attacking computer systems like a real life hacker would" (Cybersecurity Guide Contributors, 2025). This is an application of psychology and criminology, understanding intent, methodology, and motivation. The most significant and often successful vector for a pen tester is

not a complex exploit, but rather social engineering, psychologically manipulating people into performing a desired action or providing sensitive information. IBM notes that personnel pen testing can involve using phishing attacks, or even test a building's physical security (IBM, 2025), both are forms of social engineering. This requires a practical understanding of social science, as well as what motivates a person to click a link, trust the voice of a stranger on the phone, or hold the door for someone.

Application of Key Concepts

Some techniques that a pen tester might use are direct applications of social science concepts. One of these is the psychological theories of persuasion. A pen tester's toolkit when testing personnel is built on principals of influence such as authority, urgency, and scarcity. The use of social engineering to "leverage psychological aspects" (Veitaitė, 2024) is a very effective method of compromising a network. A common action is running a phishing or vishing (voice phishing) campaign. To do this, the pen tester uses authority by impersonating the CEO or an IT administrator. They then apply urgency by warning that the user's account will be locked, or scarcity by offering a bonus if the user acts immediately. These skills are not technical, they are weaponized uses of behavioral psychology intended to make a target skip out on rational thoughts.

Another key concept, taken from criminology and sociology, is rational choice theory and understanding an attacker's motivation. To effectively simulate an attack, a pen tester must know how the attacker must act. By placing themselves in the place of an attacker, they can identify vulnerabilities to exploit, because if it is used by a pen tester, an attacker can do the same (IBM, 2025). The pen tester must ask, is the potential attacker a nation-state group looking to disrupt infrastructure? A hacker group motivated by financial gain? Something else? The

Cybersecurity and Infrastructure Security Agency (CISA) warns organizations about social engineering tactics like impersonation, where an attacker pretends to be a trustworthy organization to obtain information (Cybersecurity and Infrastructure Security Agency, 2021). A pen tester needs to build a credible phishing message, like posing as a new product vendor, to gain trust and physical access to an organization. This requires a sociological understanding of organizational norms, trust, and how to blend in to a specific environment.

Interaction with Marginalized Groups and Society

Using a social science lens is imporatnt when a pen tester considers their targets. Malicious actors often disproportionately target marginialized or vulnerable populations because they are seen as a softer target. This perception is rooted in sociological reality; research demonstrates that socioeconomic and digital inequalities directly correlate with a higher risk of victimization. For example, Khan, Ikram, & Saleem (2024), found that "individuals with lower socioeconomic status and who are digitally less connected are at a greater risk of falling victims to cyber-threats" (Khan, Ikram, & Saleem, 2024) Because of these vulnerabilities, scammers may target the elderly with tech support scams, immigrants with offical-looking fake governmnent emails, or low-income individuals with fraudulent financial aid offers. A pen tester's job is to demonstrate risks posed to an organization, including risks faced by marginalized groups. By simulating these methods, they force their organization to implement more resilient and inclusive defenses that protect all of its customers and employees, not just the tech-literate ones.

Additionally, a pen tester must also be aware of any internal biases they may have. There could be an unconsious bias to use social engineering attacks to target low level employees like receptionists or support staff who may come from more diverse demographic groups than

executive management. While this may be a valuable vector to utilize, a targeted form of phishing known as whaling can be used to target a high-level executive within an organization, which can be multitudes more devastating than going after a receptionist. This requires nuance and a sociological understanding of the organization's internal hierarchy and structure. All vulnerabilities must be ethically identified, from the front desk to the boardroom.

Conclusion

The career of a penetration tester, while is largely a technical role, is a strong example of social sciences being applied to real-world situations. The most successful pen testers are not simply programmers or network engineers, they are human analysts as well. They combine technical skills with applied principles of psychology, criminology, and sociology to both behave like an attacker, and exploit human vulnerabilities that technology cannot patch. Their daily work utilizes behavioral experiments to test the resilience of an organization. By doing this, they provide critical defense to protect digital infrastructure before an attacker can exploit a potentially dangerous vulnerability.

References

Cybersecurity and Infrastructure Security Agency. (2021, February 01). *Avoiding Social Engineering and Phishing Attacks*. From Cybersecurity and Infrastructure Security Agency: https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks

Cybersecurity Guide Contributors. (2025, September 10). *Become a pen tester: The essential guide*. From Cybersecurity Guide: https://cybersecurityguide.org/careers/penetration-tester/

IBM. (2025, September 16). *What is penetration testing?* From IBM: https://www.ibm.com/think/topics/penetration-testing

Khan, N. F., Ikram, N., & Saleem, S. (2024). Effects of socioeconomic and digital inequalities on cybersecurity in a developing country. *Security Journal, 37*, 214-244. doi:https://doi.org/10.1057/s41284-023-00375-4

Martineau, M., Spiridon, E., & Aiken, M. (2024). Pathways to Criminal Hacking: Connecting Lived Experiences with Theoretical Explanations. *Forensic Sciences, 4*(4), 647-668. doi:https://doi.org/10.3390/forensicsci4040045

U.S. Bureau of Labor Statistics. (2025, August 28). *Information Security Analysts*. From U.S. Bureau of Labor Statistics: https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

Veitaitė, I. (2024). CHALLENGES OF CYBER SECURITY IN MODERN SOCIETY: THE IMPACT OF SOCIAL ENGINEERING. *Scientific and Practical Cyber Security Journal, 8(4)*, 139-148. From https://journal.scsa.ge/papers/challenges-of-cyber-security-in-modern-society-the-impact-of-social-engineering/