The Role of Social Sciences in Penetration Testing

Samantha Riggs

11/24/2024

Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Dr. Diwakar Yalpi

Introduction:

Penetration testing is defined by Cloudflare, a prominent company in the cybersecurity sphere, as “a security exercise where a cyber-security expert attempts to find and exploit vulnerabilities in a computer system.” These tests are often done by pen testing experts by simulating a cybersecurity attack to evaluate and strengthen a company’s security protocols and identify vulnerabilities in a system. This particular career has been growing as technology has advanced, leading to more vulnerabilities and opportunities for malicious attackers to attempt to gain access to different systems.

This career is often viewed in a mostly technical light in terms of programming and computing. However, there are many ways the social sciences can relate back to this career path. Fields like psychology, sociology, and ethics provide insight into human behavior, and therefore risk assessment.

Social Science Concepts:

Perhaps the largest and most prominent social science in the cybersecurity field is psychology and sociology. The human factor is often the weakest link when it comes to cybersecurity and attack prevention. Social engineering tactics are often involved in phishing and other baiting attacks. Principles such as persuasion, trust, and manipulation are often used to create these attacks. A pen tester must hold an understanding of psychology to examine human behavior and how psychological vulnerabilities might be exposed within an organization.

In the penetration testing career specifically, ethics and moral responsibility plays a large role. The act of penetration testing at its base level involves action that simulate cybercrimes

such as gaining unauthorized access to a system. Those in the career must be sure that their actions follow legal frameworks and general moral guidelines. Since the methods used are most often the exact same as a malicious attacker, pen testers must understand and uphold a moral responsibility. Understanding ethics and the ethical implications of penetration testing is paramount in this field.

Applying Social Science Concepts to the Daily Routine of a Penetration Tester:

The daily tasks and routines of a pen tester involve a blend of technical execution with interpersonal and ethical considerations. Everyday tasks such as network scanning, vulnerability assessments, and exploiting, or making the attempt to exploit, system weaknesses. These tasks also are accompanied by the need to consider human behavior and the need to hold a strong, general understanding of social sciences as a whole. Consumer mistrust is a growing concern in wake of increasing information and data breaches globally.

Social science theories influence the strategies pen testers often use in identifying and mitigating risks. Sociological principles can help them navigate and gain an understanding of organizational hierarchies and other factors that may affect the effectiveness of current and future security policies.

Impact on Society as a Whole:

At a societal level, the work of penetration tests contributes to the protection of personal privacy and corporate assets. Identifying and mitigating vulnerabilities before malicious attackers can exploit them helps maintain public trust in digital systems as a whole.

Penetration testing also includes a social responsibility when it comes to addressing systemic issues. Many communities, particularly those in developing regions, lack access to the same level of cybersecurity measures that other areas have. This is referred to as “technological inequality”. Pen testers working in terms of national or even global contexts must be aware of and consider these disparities when designing their tests and creating their recommendations for addressing vulnerabilities.

Conclusion:

Penetration testing, while driven mainly by technical skill and knowledge, is deeply influenced by the social sciences. Understanding human behavior, social structures, and ethical considerations is paramount for the success of a penetration tester in their daily routine and career as a whole. The integration of social science concepts allows penetration tests to navigate complex social dynamics and ensure their practices are ethically sound. As cybersecurity as a field continues to evolve, the blend of technology and society will be increasingly important, and the role of social sciences will remain crucial.

References:

1. What is penetration testing? | what is pen testing? | cloudflare. (n.d.). https://www.cloudflare.com/learning/security/glossary/what-is-penetration-testing/

2. Loveland, J. (2021, February 25). *What is the social impact of cyber security attacks?*. Verizon Enterprise. https://www.verizon.com/business/resources/articles/s/the-social-impact-of-cyber-security-attacks/

3. *Technological inequality – scholars for society*. Scholars for Society – We create free, accessible resources about the world's most pressing issues. (2023, December 13). https://scholarsforsociety.org/topics/technological-risks/technological-inequality/#:~:text=Technological%20inequality%20broadly%20refers%20to,wider%20economy%20of%20that%20country.