Ethan Lawson

Exploring the Social Dimension of Penetration Testing

Introduction:

A penetration tester is responsible for identifying vulnerabilities in systems and networks that could be exploited. The human factors influence on exposing a network's security cannot be understated with over 80% of cyber incidents resulting from human error (Chamorro-Premuzic, 2023). This statistic stresses the need to include social engineering tactics in penetration tests, which are often skipped. Furthermore, this means that penetration testers should be familiar with social science research and principles to be most effective. Penetration testers protect the data of vulnerable and marginalized groups which breaches, surveillance, and cyber exploitation disproportionately affect. They keep society at large safe by ensuring that the systems and networks of organizations that the public use are not susceptible to incidents that could expose their data.

How Career Relies on Social Science Research and Principles:

Cybersecurity is an interdisciplinary field and many jobs within it require knowledge in both technical expertise and social science fields. Besides needing technical expertise, penetration testers also need to incorporate social science research and principles from fields like psychology, sociology, behavioral science, economics, and law. Besides the technical infrastructure, "a penetration test can also test the organizational and personnel infrastructure, to monitor escalation procedures" (Shravan et al., 2014). For penetration testers to carry out social engineering techniques effectively, an understanding of behavior, sociology, and psychology is needed. Common psychological principles used for social engineering include authority bias, urgency, and trust. Also, penetration testers need an understanding of sociological concepts like group dynamics and power hierarchies to understand how personnel interact. They must also be aware of how their actions affect the economics of the organization they are testing and any legalities that might follow from identifying vulnerabilities or failing to do so. Penetration testing also relies on behavioral science to predict incidents and how individuals will respond to specific stimuli which can be used to improve simulation. Understanding psychology, sociology, behavioral science, and economics can also help them understand an attacker's motives, giving a slight advantage.

How Class Key Concepts are Applied in Career and Daily Routines:

Insider threats represent one of the greatest vulnerabilities to a network, making it essential to educate employees about the associated risk. In addition to organizational training to improve awareness on social engineering tactics, it is important to incorporate a variety of potential risk scenarios during a penetration test. Social engineering and physical penetration testing use deceptive methods which organizations might not want to subject their employees to (Dimkov et al., 2010). Nothing compares to the essential risk-based experience this can give, and the gaps in training it can identify. The risk triangle gives an understanding of security risks and helps evaluate a system on its protection, ensure that information is accurate, and remains accessible. Perceptions of safety are challenged by a penetration test and makes employee's true exposure obvious which can encourage safe practices. Understanding the information flow of a specific organization for penetration testers is a necessary step. This allows them to identify the informal flow of information so it can be remediated. Liability is an important concept to penetration testers because they must operate within strict legal and ethical boundaries. Their findings might get an organization into trouble or result in lower cyber insurance premiums.

How Career Interacts with Marginalized Groups and Society at Large:

Penetration tests are needed for many organizations to remain compliant with governmental standards. Smaller organizations might not have the financial means to ensure their networks meet standards or hire a penetration tester. Careful coordination and preparation are needed to avoid unintentional harm that could disrupt business functions, especially for critical services such as public health. A disruption of services can disproportionately impact low-income individuals that have limited alternatives available. Many penetration testing methodologies are generalized and might not consider unique risks faced by marginalized users. Furthermore, the entirety of the cybersecurity industry needs more diversity to expand perspectives and identify cultural and contextual factors that influence risk. Relativism reminds penetration testers that ethical standards and privacy standards vary, making it essential to approach systems with an open mind. Penetration tests are necessary to protect organizations that work with sensitive data and do not understand complex communication structures (Bertoglio & Zorzo, 2017).
Penetration testing simulates real world attacks and intersects with society by raising awareness of the ethical and legal implications. Its very existence emphasizes the importance of protecting personal and organizational data in this interconnected world.

Conclusion:

Penetration testing needs more than technical skills, requiring a broad understanding of social sciences and how people behave to effectively perform their job and comprehend the broader impact of their work. An overwhelming majority of cyber incidents are rooted in human error, making it clear that the integration of social engineering techniques is needed. Penetration testing, being a job within the interdisciplinary field of cybersecurity, requires an understanding of research and principles in social science fields such as psychology, sociology, economics, law, and behavioral science. A penetration tester's work embodies an intersection of technology and social science allowing them to translate complex risk into remediating actions. Their work directly impacts society by protecting personal and organizational data that a loss of would disproportionately affect marginalized groups. Ultimately, penetration requires a deep understanding of human behavior, societal needs, and organizational structures in conjunction with technical expertise.

References

Chamorro-Premuzic, T. (2023, May 3). *Human error drives most cyber incidents. could AI help?*. Harvard Business Review. https://hbr.org/2023/05/human-error-drives-most-cyber-incidents-could-ai-help

Dalalana Bertoglio, D., & Zorzo, A. F. (2017). Overview and open issues on penetration test. *Journal of the Brazilian Computer Society*, *23*, 1-16.

Dimkov, T., Van Cleeff, A., Pieters, W., & Hartel, P. (2010, December). Two methodologies for physical penetration testing using social engineering. In *Proceedings of the 26th annual computer security applications conference* (pp. 399-408).

Shravan, K., Neha, B., & Pawan, B. (2014). Penetration Testing: A Review. *Compusoft*, *3*(4), 752.