Examining the Relationship between Physical Penetration Testing and the Social Sciences

Bailey Williams

Department of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Prof. Diwakar Yalpi

December 2, 2024

Physical penetration testing is a career in cybersecurity that involves simulating physical attacks on an organization to identify weaknesses in its physical infrastructure and employees. Various attack methods are used in physical penetration testing, including social engineering, physical or technical bypasses, destructive or nondestructive testing, and advanced persistent threats (*Physical Penetration Testing*, 2023).

Relation to Social Science Principles

Physical penetration testing relates to each social science principle, relativism, objectivity, parsimony, empiricism, ethical neutrality, determinism, and skepticism.

Relativism is the understanding that all things are related, including the relationship between the social system and behaviors driven by technology (Yalpi, n.d.-a, p. 4). In physical penetration testing, particularly when conducting social engineering attacks, practitioners must deeply understand how people will react in different situations to manipulate the surrounding social system to gain the most information.

Objectivity is the idea that researchers conduct research in a value-free manner (Yalpi, n.d.-a, p. 7). While physical penetration testers do not routinely conduct scientific research as part of their job, they must remain objective in how they conduct their testing, regardless of their personal feelings about the organization they are testing.

Parsimony is the idea that scientists should make their explanations as simple as possible (Yalpi, n.d.-a, p. 8). Simple explanations are critical in physical penetration testing because the final step of any test is to compile a report that details all of the information the tester collected and any vulnerabilities they found and exploited (*Physical Penetration Testing*, 2023). If the report is not written in language that is easy for the organization to understand, it may not be able to address all the stated vulnerabilities adequately.

Empiricism is the concept that social scientists only research what is real to the senses, meaning that one cannot rely on hunches or opinions in their research (Yalpi, n.d.-a, p. 10).

Physical penetration testers cannot simply state that a vulnerability exists, they must attempt to exploit the vulnerability and document the process and results to prove that it exists.

Similar to objectivity, ethical neutrality means scientists must obey ethical standards while conducting research (Yalpi, n.d.-a, p. 11). For physical penetration testers, practicing ethical neutrality means they should not agree to testing jobs if they feel that their personal biases towards the organization may interfere with their work.

Determinism is the principle that behavior is influenced by preceding events (Yalpi, n.d.-a, p. 12). Each step of the physical penetration testing process, from information gathering with OSINT and surveillance, to reconnaissance, to exploitation and data collection, builds on the previous steps in the process (*Physical Penetration Testing*, 2023).

Finally, skepticism is the idea that ideas should be critically reviewed, rather than accepted at face value (Yalpi, n.d.-a, p. 15). Similarly to empiricism, this means that physical penetration testers must do their due diligence to exploit any suspected vulnerabilities rather than reporting their hunches.

Application to Class Concepts

Many of the concepts discussed in class are applicable to careers in physical penetration testing, including social engineering, human factors, personality theories, and developing a cybersecurity culture.

As mentioned above, social engineering is one of the primary attacks used in physical penetration testing. Social engineering in physical penetration tests is more intense than in digital penetration testing because the penetration tester is face-to-face with their target, rather than interacting behind screens (Dimkov et al., 2010, p. 1). This means that physical penetration testers must have a solid understanding of social engineering and psychological principles, which will be covered in more detail in the following paragraphs.

Human factors in cybersecurity, also known as human centered cybersecurity, is an area of research that works to reduce human errors contributing to cybersecurity violations (Yalpi,

n.d., p. 15). Physical penetration testers must be familiar with human factors assessments, as these assessments will point to different vulnerabilities in the human space that they may be able to exploit during testing.

Continuing with the theme of understanding human behavior, it is also important for physical penetration testers to know different personality theories. There are many different psychological principles involved in social engineering attacks, including authority, scarcity, reciprocity, and consensus (K M, 2024, pp. 3–4). These principles are directly related to personality theories, including the Big Five Personality Trait model. By understanding which job roles are predisposed to different personality traits, penetration testers can tailor their social engineering attacks to feature different psychological principles.

Finally, developing a cybersecurity culture is also directly related to the physical penetration career. At the end of a physical penetration test, the tester will compile a report to present to the organization detailing the results of the test (*Physical Penetration Testing*, 2023). After reviewing the results, the organization should address any vulnerabilities as part of its cybersecurity culture, which will encourage employees to maintain a high level of security in their interactions with technology.

Relation to Marginalized Groups

Like any career, especially those in STEM fields, physical penetration testing presents both advantages and challenges to marginalized groups. Increased awareness of non-technology-focused careers in cybersecurity, including physical penetration testing, may encourage more women to enter the field. Studies have noted that girls perceive cybersecurity careers as involving a lot of coding and sitting alone at a desk, which discourages them from pursuing careers in the field (Jethwani et al., 2017). By showing cybersecurity careers that lack an emphasis on technology and programming, more girls may be encouraged to join the field.

Depending on the target organization, marginalized groups may have benefits or disadvantages as physical penetration testers. Women are often perceived as being less

threatening than men, which may help them exploit male employees of the target organization by presenting themselves as vulnerable and in need of help (Roberts, 2012). In contrast, organizations that are predominantly white and male may be harder for women and minorities to infiltrate than it is for white males.

Connection to Society

Overall, physical penetration testers contribute to society by strengthening the cybersecurity culture and bringing more awareness to physical cybersecurity threats. As mentioned in the *Application to Class Concepts* section, the reports presented at the end of physical penetration tests, if taken seriously, help to shape the cybersecurity culture at the organization. If the organization that underwent testing is a leader in its industry, its cybersecurity culture and practices will influence other organizations in the industry as well. Many employees may not realize how important their actions are to the overall cybersecurity health of the organization until a physical penetration test occurs. This revelation will go with them to future roles, furthering awareness of physical cybersecurity threats.

Conclusion

In conclusion, physical penetration testing, which simulates physical cyberattacks on the target organization and compiles reports on how to address vulnerabilities, is related to social science principles, concepts from class, concerns of marginalized groups, and contributes to society as a whole. Physical penetration testing is related to all seven social science principles: relativism, objectivity, parsimony, empiricism, ethical neutrality, determinism, and skepticism. In addition, it is related to many concepts from class, including social engineering, human factors, personality theories, and developing a cybersecurity culture. Physical penetration testing may encourage more women to pursue a career in cybersecurity by presenting a career path with limited programming requirements, and women may have more success in conducting physical penetration tests in some organizations. Marginalized groups may also face difficulties in conducting tests depending on the demographics of the target organization. Finally, physical

penetration testing contributes to society at large by strengthening security culture and promoting awareness of physical cybersecurity threats.

References

Dimkov, T., van Cleeff, A., Pieters, W., & Hartel, P. (2010). Two methodologies for physical penetration testing using social engineering. *Proceedings of the 26th Annual Computer Security Applications Conference*, 399–408. https://doi.org/10.1145/1920261.1920319

Jethwani, M. M., Memon, N., Seo, W., & Richer, A. (2017). "I can actually be a super sleuth": Promising practices for engaging adolescent girls in cybersecurity education. *Journal of Educational Computing Research*, *55*(1), 3–25. https://doi.org/10.1177/0735633116651971

K M, J. (2024). Social engineering and human factors in penetration testing. *International Journal For Multidisciplinary Research*, *6*(3), 21496. https://doi.org/10.36948/ijfmr.2024.v06i03.21496

Physical penetration testing: The most overlooked aspect of security. (2023, September 5). ISACA. https://www.isaca.org/resources/white-papers/2023/physical-penetration-testing

Roberts, P. (2012, May 21). *Forget 'Brogrammers,' Women Have The Edge In DEFCON Social Engineering Contest*. Threatpost. https://threatpost.com/forget-brogrammers-women-have-edge-defcon-social-engineering-contest-052112/76587/

Yalpi, D. (n.d.-a). *CYSE201S (Module 2): Principles of Social Sciences and Cybersecurity Diversity and Cybersecurity*.

Yalpi, D. (n.d.-b). *CYSE201S (Module 7): Cybersecurity and the Social Dimensions of Data Science*.