Mike Green

Professor Yalpi

04-07-2024

CYSE-201S

Penetration Testing and its Relation to Social Science

**Job Description/Daily Duties**

Penetration Testers are vital components of a good cybersecurity team; without them, attackers would have a much easier time finding potential exploits in pre-established or even newly established systems used in everyday operations as well as existing or new vulnerabilities in these same systems. A wide range/variety of knowledge and skills is required to be an effective penetration tester; according to the NICCS (National Initiative for Cybersecurity Careers and Studies), “knowledge of ethical hacking principles and techniques” and “skill in mimicking threat behaviors” (NICCS, 2024), are two of the many necessary skills required for this sort of job/profession. The daily duties of a Penetration Tester, in broad terms, revolve around the assessment of a system, or systems, the documentation of those findings, as well as the relaying of information to the corporation/party that required the pen testing.

**Social Science Concepts/Principles & Pen Testing**

While something referred to as a system sounds technology/network-based, and will be most of the time, it could also be referring to something physical, or even mental depending on the perspective. A network could be targeted for many reasons whether it be to gain information or for monetary reasons.

Social engineering, as defined by the CISA, is when “an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems” (CISA, 2021). This can be both physical and within a network, so it is important that Pen Testers make sure that all avenues get covered during their assessments. They may utilize social engineering techniques to test how susceptible the corporation/employees of the corporation are to these types of attacks. In this case, the importance of being able to mimic behaviors can stem from an understanding of cyber victimization; attackers who successfully use social engineering, depending on which type of attack they use, may already know who has access to what in a network, or how they could use what they know to make the attack as seamless as possible. Brief examples of how attackers may do this is with smishing and phishing attacks; smishing involves texting phishing involves emailing.

An attacker, or a Pen Tester assessing a system, could spoof a five-digit service number that is typically associated with authentication to text an individual then direct the individual to a fraudulent website to potentially capture login info. In turn, the attacker could gain access to what they otherwise should not be accessing. The same can be done with emails, but it’s a bit different because there are more errors to be made regarding the format and grammar of the email; that is if the sender’s email address isn’t noticeable incorrect already. It is critical that Pen Testers assess vulnerability to social engineering because these types of attacks tend to affect the most people in society i.e., people that are unaware of potential dangers in the cyberspace.

Ethics are a major factor in pen testing as “an unethical pen tester can use their skills and resources to exploit vulnerabilities in a system, sell sensitive data, or sabotage the organization” (WGU, 2021). Understanding principles of social sciences such as, ethical neutrality and objectivity is important for maintaining a good reputation in the industry as well as maintaining customer/client safety. Ethical neutrality involves the adherence to ethical standards when conducting research, and objectivity involves conducting research in a value-free manner. Without these two principles, bias may come into play when Pen Testers are assessing a system, and findings can then be misrepresented or downplayed both with the aforementioned bias as well as without it. Reputation will quickly diminish as well as ethics is one of the largest aspects/reliances in any career in cybersecurity and a negative display of ethics will drive away stakeholders or opportunities for cooperation.

**Conclusion**

All in all, the role of Penetration Testers is important for the success of any cybersecurity team and for a corporation that prioritizes the safety of their systems; having the necessary knowledge and skills in tandem with understanding social science principles/concepts to be an effective Pen Tester is crucial for safeguarding against potential exploits & vulnerabilities and keeping the trust of society in regard to all things digital.

References

National Initiative for Cybersecurity Careers and Studies. (n.d.). Vulnerability Assessment Analyst | NICCS. <https://niccs.cisa.gov/workforce-development/nice-framework/work-roles/vulnerability-assessment-analyst>

Cybersecurity & Infrastructure Security Agency. (2021, February 1). Avoiding Social Engineering and Phishing Attacks | CISA. Cybersecurity and Infrastructure Security Agency CISA. <https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks>

Western Governors University. (n.d.). What Is Penetration Testing? <https://www.wgu.edu/blog/what-is-penetration-testing2112.html>