Adeline Harris

School of Cybersecurity, Old Dominion University

CYSE201S: Cybersecurity and Social Science

Professor Umphlet

August 1, 2024

Vulnerability Assessment and Penetration testing (VAPT)

The profession of penetration testing (pentesting) is a discipline that focuses on finding vulnerabilities in systems, individuals, programs, etc., and reporting them so they can be fixed to prevent infiltration and manipulation by malicious attackers. The profession can be considered to be ethical hacking since it involves emulating the patterns of hackers without exploiting infiltrated systems. It is a career similar to most specialized and professional computer science fields in that there is no specific path to it. A degree in any computer science course, combined with certifications in networking, programming, and a few other fields, is enough to set a person on the path of pentesting (Brecht 2019). The pentester has to think like an actual malicious hacker and try to find all accessible vulnerabilities (Shah & Mehtre, 2016). After the assessment of the vulnerabilities, the pentester must think like a malicious attacker to be able to know the severity of the vulnerability and how exploitable it is. This usually involves flaws from the human factor since humans make mistakes, and hackers are always looking to exploit that.

Pentesters try to exploit vulnerabilities in networks, programs, and systems, but the most common flaw in these things is the human factor. Humans are prone to mistakes since we can get distracted and carried away. This is where social-engineering tactics come into play, which hackers use in cases where there are no vulnerabilities in the system itself. By exploiting human interest and desires, most hackers can find a way to create a backdoor into the system. According to the CYSE201s modules, tricks like socio-engineering are commonly used in exploiting systems. This is why it is essential for pentesters to identify vulnerable parties and their vulnerabilities so they can be properly protected and fixed. Pentesting requires the testers to be open to ideas and consider all options. They must remain

objective and not become too attached to clients and their struggles. Since it is a security protocol, there is little room for assumptions, so pentesters can make as few assumptions as possible and double-check every possible vulnerability. The work of a pentester becomes tedious when they need to understand and examine the vulnerabilities of individuals or employees of an organization without being unethical. They must reveal this information to the necessary parties so that these openings to malicious attackers can be closed. This underscores the need for a proper organizational cybersecurity culture, is very needed and advised (CYSE201s modules).

The full process of vulnerability assessment and pentesting consist of nine steps, each of which is crucial since the vulnerabilities should first be identified and tested. These steps are scoping, reconnaissance, vulnerability detection, information analysis and planning, penetration testing, privilege exploitation, result analysis, reporting and clean up (Goel & Mehtre, 2015). Each of these steps are vitally important and codependent because the subsequent step builds upon the findings of the previous one. Since pentesting involves exploiting a vulnerability as a malicious attacker would, it reveals the severity of the vulnerability and its potential impact. However, for pentesting to be performed the vulnerability must first be identified and assessed (Vercode, May 9, 2019). The value of pentesting is seen in how it relates to identifying and mitigating risk. If a vulnerability is not detected and is exploited, it can lead to many disadvantages for system owners and users. In this context, a cost- benefit analysis reveals that it is less costly and more efficient to conduct a full Vulnerability Assessment and Penetration Testing (VAPT) than to leave the system unchecked. As a final part of the VAPT process, security awareness and employee training are crucial since humans are often the most exploitable part of a system. Employees should be educated on online safe practices and security procedures to prevent vulnerabilities from being exploited.

The field of VAPT, like many other computer science and cybersecurity fields, has very few women involved, as it can be considered time-consuming and tedious. But in addition, marginalized demographics, such as those based on race and socio-economic status, are often used as access points for vulnerabilities. Due to their standing in society, these groups can be more easily socially engineered and exploited.

The job of vulnerability assessment and penetration testing is focused on protection by locating vulnerabilities, emulating malicious attackers to understand the severity of these vulnerabilities, and then fixing them. This involves many social science practices and principles. Nonetheless, it is a crucial aspect of protecting individuals and organizations.

References

- Goel, J. N., & Mehtre, B. M. (2015). Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology. Procedia Computer Science, 57, 710–715. https://doi.org/10.1016/j.procs.2015.07.458
- VeraCode. (2019, May 9). Vulnerability Assessment and Penetration Testing. Veracode. https://www.veracode.com/security/vulnerability-assessment-and-penetration-testing
- CYSE201s module
- Shah, S., & Mehtre, B. M. (2016). An overview of vulnerability assessment and penetration testing techniques. Journal of Computer Virology and Hacking Techniques, 11(1), 27–49. https://doi.org/10.1007/s11416-014-0231-x
- Master the Penetration Tester Career Path | Infosec. (n.d.). www.infosecinstitute.com. Retrieved July 24, 2024, from https://www.infosecinstitute.com/resources/penetration-tester/penetration-tester-career-path/