Option #1: Where the Vulnerabilities Are

Liam Bergerson

CSU - Global

ITS481-1

D. Morrill

8/6/23

Option #1: Where the Vulnerabilities Are

In an IT infrastructure, there is always the risk of a security breach occurring. Threat actors desire the sensitive data that is harbored within the repositories of organizations in order to sell it on the dark web for a profit. To lower the risk of a security breach occurring, methods to find vulnerabilities within the IT infrastructure can be implemented. One of these methods is penetration testing. The goal of penetration testing is to act out a security breach. A penetration tester will act as the threat actor trying to breach an organization. Once the tester breaches the organization, they will state what vulnerabilities were exploited, sensitve data that was accessed, and how long they remained undetected in the report.

Penetration Testing Methods

A penetration tester will use a variety of methods in order to attempt to breach the organization that is acting as the victim. There are typically five steps a penetration tester will utilize when performing a penetration test. These steps are: Planning and Reconnaissance, Scanning, Gaining Access, Maintaining Access, and Analysis (Stapel, 2023). In the planning and reconnaissance stage, the tester will definer the scope and goals of the test. Then they will gather intelligence such as networks, domain names, servers, etc. to better understand how the target works and potential vulnerabilities. In the scanning phase, the tester will perform commands towards applications to see how they respond. One practice that is typically used in this stage is port scanning. This is to see

what ports are open on an organization's network. In the gaining access phase, methods such as cross-site scripting, SQL injection, etc. are used to try and gain access to an account and escalate the privileges of that account. In the maintaining access phase, the vulnerability is tested to see if that access gained in the third phase can be maintained. Finally, in the analysis phase, the tester will compile all of their findings into a report that they will give to the organization so that they can implement better methods to secure their infrastructure. Information such as vulnerabilities exploited, sensitive data that was accessed, and how long they remained undetected are all included in the report.

Penetration Testing Tools

A variety of tools are used by penetration testers while performing a penetration test. Kali Linux is a prebuilt Linux distribution that has all of the necessary tools preinstalled that penetration testers typically use (Fruhlinger & Porup, 2023). Most, if not, all of the tools discussed are preinstalled into Kali Linux. Nmap is a widely known port scanning tool that is used in the scanning phase of a penetration test to discover what ports are open on a network. Metasploit is an incredibly useful tool that uses preconfigured exploits that have been gathered over the years by professionals to exploit a vulnerability within an organization's network. Wireshark is a packet-analyzing tool that can be used to analyze packets traversing the network for valuable information such as protocols used. John the Ripper is a password cracking tool that uses wordlists to crack passwords. Burp Suite is a web vulnerability scanner that identifies

vulnerabilities within websites. SQLMap is a SQL Injection tool that identifies and exploits websites that are vulnerable to SQL Injection. Finally, Aircrackng is a Wifi cracking tool that can exploit wireless security protocols such as WEP, WPA, and WPA2 to gain access to the Wifi network.

Conclusion

In order to reinforce existing security methods and implement new security methods, organizations hire penetration testers to attempt to breach their IT infrastructure. Using the seven phases discussed previously, the penetration tester utilizes a variety of tools to breach the organization. After the infrastructure has been successfully breached, the tester writes a report for the organization that illustrates what vulnerabilities were exploited, sensitve data accessed, and how long they remained undetected. The organization then implements security methods to patch those vulnerabilities.

References

Fruhlinger, J., & Porup, J. M. (2023). 11 penetration testing tools the pros use. *CSO Online*. https://www.csoonline.com/article/551957/11-penetration-testing-tools-the-pros-use.html

Stapel, G. (2023, March 14). *What is Penetration Testing | Step-By-Step Process & Methods | Imperva*. Learning Center. https://www.imperva.com/learn/application-security/penetration-testing/