Kobe Coleman

Professor Duvall

CYSE 368

7/5/2024

Reflection Paper 3

This 50-hour work period marked my first penetration test on a system. The initial stage of this test involved scheduling a meeting with the system's owner to determine what we may test. This is done to prevent Pen Testers from testing parts of the system that were not intended to be examined. We began by conducting passive reconnaissance on the system to see what we might locate and exploit before moving on to the hands-on portion of the test. For the second portion of the test, we scanned the system with Nmap which stands for Network Mapper. “It is an open-source Linux command-line utility that scans a network for IP addresses and ports as well as detects installed applications. Nmap allows network administrators to locate which devices are running on their network, discover open ports and services, and detect vulnerabilities" (FreeCodeCamp), and Nessus Scans, which is “Nessus is a widely used vulnerability scanning tool in the field of cyber security and security testing. Nessus is a platform developed by Tenable that scans for security vulnerabilities in devices, applications, operating systems, cloud services, and other network resources. It is a remote security scanning tool, which scans a computer and raises an alert if it discovers any vulnerabilities that malicious hackers could use to gain access to any computer, that you have connected with any network” (Greek for Greeks).

Work Cited

"Explain Nessus Tool in Security Testing." *GeeksforGeeks*, GeeksforGeeks, 11 Jan. 2024, www.geeksforgeeks.org/explain-nessus-tool-in-security-testing/.

Shivanandhan, Manish. "What Is Nmap and How to Use It – a Tutorial for the Greatest Scanning Tool of All Time." *freeCodeCamp.Org*, freeCodeCamp.org, 2 Oct. 2020, www.freecodecamp.org/news/what-is-nmap-and-how-to-use-it-a-tutorial-for-the-greatest-scanning-tool-of-all-time/.