Jason Hodge

Lab 04 – Scanning the Target for Vulnerabilities

November 8, 2023

## Active Discovery Use Literature Review

There are many ways to conduct port scanning with various tools and techniques. Port scanning can be used for both good and bad intensions to either locate and exploit vulnerabilities or to secure and maintain a security system. All the ports on a network or device serve a different purpose in the way a computer functions and the features it can have. It would be extremely bad if a hacker got ahold of sensitive information through an open port or backdoor entrance into a part of one's system. As time progresses, the way security precautions are maintained, and tools work will continue to evolve, which is why it is important to learn from them to make future long lasting improvements. Thus, port scanning and Wi-Fi scanning can be used for both good intensions and bad intensions.

Port scanning is a technique hackers and administrators can use to discover weak points and open ports in networks. Ports all have different purposes and services they are assigned to. Some common ones are port 25 Simple Mail Transfer Protocol (SMTP) and 80 Hypertext Transfer Protocol (HTTP), which provide email and internet services. The most popular port scanning cybersecurity penetration tool is one we utilized in this lab, Nmap. Port scanning is a vital technique that "leverages TCP/IP capabilities to identify computing systems within a network. As network protocols utilize distinct ports, a thorough scan of a broad range of ports is crucial for comprehensive information gathering (Pittman, J. M. pg. 2)." Each port has a job to do, and it is extremely important every port has the proper protections in place to prevent

unwanted intrusions. Port scanning “techniques play a pivotal role in systematically probing network ports, allowing administrators to pinpoint open ports, uncover unauthorized services, and scrutinize potential entry points for potential attackers (Abu Bakar, R., & Kijsirikul, B. pg. 1).” This sounds like the next steps after the Nmap scan we ran in the lab, which provided port numbers, states, and services for each port on the system.

Utilizing Wi-Fi penetration testing is not something I am too familiar with. There are three Wifi network encryption methods including, “WiFi Protected Setup (WPS) encryption mode, Wired Equivalent Privacy (WEP) encryption mode, and WiFi Protected Access (WPA) encryption mode (Lu, H.-J., & Yu, Y. pg. 2-3).” These encryption methods all operate a little differently as they have different encryption and decryption methods that are primarily used on passwords. These encryption methods utilize large data grabbing techniques and protocol packet handshakes in order to gain access to a target network. As cipher encryption methods and protocols age and get cracked standards and new methods will take their places to continue to maintain the CIA triad confidentiality, integrity, and availability.

## Resources

Abu Bakar, R., & Kijsirikul, B. (2023, August 30). *Enhancing network visibility and security with advanced port scanning techniques*. MDPI. https://www.mdpi.com/1424-8220/23/17/7541

Lu, H.-J., & Yu, Y. (2021, February 27). *Research on WIFI penetration testing with Kali Linux*. Complexity. https://www.hindawi.com/journals/complexity/2021/5570001/

Pittman, J. M. (2023, March 20). *A comparative analysis of Port Scanning Tool Efficacy*. arXiv.org. https://arxiv.org/abs/2303.11282