Julianna Russo

Network Security

Lab 04- Scanning the Target for Vulnerabilities

Professor Cannistra

11/7/2023

This lab focuses on different active discovery tools and how these tools are used to gain valuable information about a host of a network and expose possible vulnerabilities that can be exploited. It is important to have a secure network, by having a concise view of the information of hosts on a network, such as IP addresses, MAC addresses, devices, and domains these hosts have so that vulnerabilities can be found and minimized. There are three phases of the network reconnaissance procedure: passive scanning, net border analysis, and active scanning ("Title of the Source," n.d.). Active scanning and passive scanning are the first steps in penetration testing, while they do share similarities, active discovery differs from passive discovery because the target host is being sent packets to elicit a response, which doesn’t happen in passive discovery. Typically active discovery gathers information quickly and can be conducted from different networks. The disadvantage to using active discovery is that, unlike passive discovery, it doesn’t go unnoticed.

Network discovery tools acquire information in a few ways, but the two most popular ones are through sending packets and through scans. These scans gather information such as IP addresses, MAC addresses, hosts, OS systems, vendors, and possible vulnerabilities that can be exploited. Through sending packets to common port numbers, active discovery tools analyze information found in the ports and are able to identify the host, the operating system, the ports, and the states of those ports. Network discovery can detect unauthorized devices and actors in a network("Passive Discovery," n.d.). Tools like Nmap are especially useful for detecting unauthorized users in a network since they map out a network topology.

In a network device vulnerability assessment(McDaid, Furey, & Curran, n.d.), Nmap and Net Scan were used to scan for vulnerabilities in a given network. Nmap was able to scan all the devices on a network and test them against several different databases of known device security vulnerabilities and was able to effectively discover device IP addresses, MAC addresses, OS information, Vendor information, and the vulnerabilities it had. Net Scan was effective in finding Wi-Fi devices transmitting over the network, but wasn't effective at finding Bluetooth devices. This tool was also able to find open ports that could be exploited, IP and MAC addresses, and vendor information. In this lab, Nessus was also used. Nessus is an active discovery tool that displays vulnerabilities based on standard formats and exports them into a variety of different formats(Tenable SecurityCenter Continuous View v4.6,2013). This tool tests each port on a host, determining what service it runs, and then tests if there are any vulnerabilities. What is great about this tool is not only does it retrieves information quickly, but it formats the gathered information in a clear, easily understood format, clearly defining the critical vulnerabilities, and giving suggestions on how to fix them.

The use of active discovery tools for vulnerability scanning is vital for both protecting systems from malicious actors and for penetration testing, some of the most useful active discovery tools include Namp and Nessus, based on the information they are able to retrieve, the way they display that information, and how quickly they retrieve that data.

Citations

Al-Sabaawi, A., & Alrowidhan, T. A. (2022). Detecting Network Security Vulnerabilities and Proactive Strategies to Mitigate Potential Threats. *ArXiv.Org*. https://doi.org/10.48550/arxiv.2212.11449

Azodi, A., Cheng, F., & Meinel, C. (2017). Event Driven Network Topology Discovery and Inventory Listing Using REAMS. *Wireless Personal Communications*, *94*(3), 415–430. https://doi.org/10.1007/s11277-015-3061-3

Gvozdenovic, S., Becker, J. K., Mikulskis, J., & Starobinski, D. (2022). IoT-Scan: Network Reconnaissance for the Internet of Things. *ArXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2204.02538

Yang, X.-S., Sherratt, S., Dey, N., & Joshi, A. (2020). Automatically Determining a Network Reconnaissance Scope Using Passive Scanning Techniques. In *Advances in intelligent systems and computing* (Vol. 1027, pp. 117–127). Springer Singapore Pte. Limited. https://doi.org/10.1007/978-981-32-9343-4_11

Curran, K., McDaid, A., & Furey, E. (2021). Wireless Interference Analysis for Home IoT Security Vulnerability Detection. *International Journal of Wireless Networks and Broadband Technologies*, *10*(2), 55–77. https://doi.org/10.4018/IJWNBT.2021070104

McDaid, A., Furey, E., & Curran, K. (2021). Wireless Interference Analysis for Home IoT Security Vulnerability Detection. *International Journal of Wireless Networks and Broadband Technologies* [IJWNBT], *10*(2), NA. https://link.gale.com/apps/doc/A759457687/AONE?u=nysl_se_marist&sid=bookmark-AONE&xid=ccc8da2d

nCircle Releases Unified Scanning Appliance for Agentless Network Discovery and Assessment. (2007). In *Canada NewsWire* (pp. 1-). PR Newswire Association LLC.

Tenable SecurityCenter Continuous View v4.6. (2013). *SC Magazine*, *24*(2), 53-. SC Media.

Ritzkal, R., Kodarsyah, Puspa Putri Amalia, Mahmud, W., Ade Hendri Hendrawan, Bayu Adhi Prakoso, & Riawan, I. (2023). Security Vulnerability Analysis and Recommendations for Open Media Vault Cloud Server on Raspberry Pi. *Ingénierie des systèmes d'Information*, *28*(3), 711-. https://doi.org/10.18280/isi.280321

Kaur, G., & Kaur, N. (2017). Penetration Testing - Reconnaissance with NMAP Tool. *International Journal of Advanced Research in Computer Science*, *8*(3).

Geier, E. (2021). 5 free network-vulnerability scanners: These 5 tools can help automate the detection and remediation of vulnerabilities, and they're available at no cost, and some are upgradeable to more fully featured platforms. *Network World (Online),* Retrieved from https://marist.idm.oclc.org/login?url=https://www.proquest.com/trade-journals/5-free-network-vulnerability-scanners/docview/2499488303/se-2

Constantin, A., Bulut, M. F., Sow, D., Ocepek, S., Bedell, C., & Ngweta, L. (2022). Attack Techniques and Threat Identification for Vulnerabilities. *ArXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2206.11171

(N.d.). Retrieved from

https://www.sciencedirect.com/topics/computer-science/passive-discovery