Identify and run scans: Five Tools to Identify and Run Scans

Vincent Kiweesi

Capstone

May 20th, 2023

This is a description of 5 tools that will be used during this phase to find open ports and look into network activity on the target system. The goal is to find as many open ports as possible to prepare for the next phase because open ports are potential points of entry of an attack. I will use Nmap, Nmap Scripting Engine, Nessus, Wireshark, and Metasploit mainly because Metasploit has a deep customizability, open source, and continually updated pen testing tool. Wireshark is a free open-source program that analyses network traffic in real-time, Nessus specialises at doing vulnerability checks. With Nmap Scripting Engine (NSE) can automate a wide range of networking tasks, a robust and adaptable capability. Nmap is an effective tool for ethical hackers who wish to scan and examine network traffic and logs to find hosts, ports, services, vulnerabilities, and other details about their target network.

**Tool:** Nmap.

**Purpose:** Obtain information on hosts services, script scan and operating systems they are running.

**Commands:** nmap -sV -sC URL -p port number

**Tool**: Nmap Scripting Engine (NSE).

**Purpose:** Automate scanning and identify vulnerabilities on the target system.

**Commands:**

* nmap --script=default scanme.nmap.org
* nmap -sV -O --script=<scripts> <ip address>

**Tool:** Nessus.

**Purpose:** Automated vulnerability scanning and identification of vulnerabilities on the target system. **Commands:** nessus -T ip address -p port range

**Tool**: Wireshark.

**Purpose**: Capture network traffic and analyze it to gain insights into the network.

**Commands**: wireshark -i interface -f filter

**Tool:** Metasploit.

**Purpose:** Automate exploitation of identified vulnerabilities and gain access to the target system. **Commands:** msfconsole -x commands

All host finding and network enumeration tasks are taken care of by the selected tools.  
Nmap searches for hosts and services on networks (Shivanandhan, 2020).

System vulnerabilities are found, and automated scanning is performed using Nmap Scripting Engine (NSE). Numerous scans, including port scans, operating system detection, and service identification, can be carried out by it. The scanning procedure might be automated by the Nmap Scripting Engine (NSE), producing more precise and detailed findings (Tathagat, 2021).  
These tools require knowledge, which makes them challenging to use and understand, certainly utilities could operate slowly depending on the size of the network. Since some tools can't discover specific vulnerabilities, manual testing may be necessary. Some technologies could provide false positives, demanding cautious analysis, choosing the right tools for host detection and enumeration is important in any security audit or assessment.  
 Another excellent tool for finding and counting hosts is Nessus. Nessus scanner that might identify potential weaknesses in the system being scanned like out-of-date software, missing patches, and misconfigured services. Nessus can identify and report on a wide range of vulnerabilities, including outdated software, updates that are missing, and improperly configured services (Tech2020, 2021).

To capture and analyse network data, Wireshark is a highly developed network protocol analyzer. By locating hosts, services, and communication patterns, it can be used to gather information about the network. Then, using this information, potential security threats like unusual traffic or malicious activity may be identified (What is wireshark and how to use it: Cybersecurity: Comptia n.d).  
  
 The penetration testing framework Metasploit automates the use of found vulnerabilities to obtain access to the target system. It is an important security auditing tool since it can be used to exploit a wide range of systems and applications. Using these tools is not without challenges, some level of competence is needed to use the tools correctly and understand the results. Additionally, some of the tools may operate slowly depending on the size of the target network (Buckbee, 2022).

In Conclusion, some of the technologies might not be able to find certain kinds of vulnerabilities, requiring manual evaluations. Also, some technologies could produce false positives, needing a close evaluation of the data. Using the appropriate tools for host identification and enumeration is important in any security audit or assessment. Tools like Nmap, NSE, Nessus, Wireshark, and Metasploit can all be used to find potential vulnerabilities and break into a target system. However, applying these tools effectively is not easy and could lead to false positives. An in-depth analysis of the results is needed to guarantee accuracy.

Reference

Buckbee, M. (2022, February 24). *What is Metasploit? the beginner’s guide*. Varonis. https://www.varonis.com/blog/what-is-metasploit

Shivanandhan, M. (2020, October 2). *What is nmap and how to use it – a tutorial for the greatest scanning tool of all time*. freeCodeCamp.org. https://www.freecodecamp.org/news/what-is-nmap-and-how-to-use-it-a-tutorial-for-the-greatest-scanning-tool-of-all-time/

Tathagat. (2021, March 25). *Nmap and useful NSE scripts*. CYBERVIE. https://www.cybervie.com/blog/nmap-and-useful-nse-scripts/#:~:text=The%20Nmap%20Scripting%20Engine%20(NSE,efficiency%20you%20expect%20from%20Nmap.

Tech2020. (2021, January 18). *What is nessus and how does it work? - ITPERFECTION - network security*. ITperfection. https://www.itperfection.com/network-security/network-monitoring/what-is-nessus-and-how-does-it-work-network-munitoring-vulnerabilit-scaning-security-data-windows-unix-linux/

*What is wireshark and how to use it: Cybersecurity: Comptia*. Default. (n.d.). https://www.comptia.org/content/articles/what-is-wireshark-and-how-to-use-it#:~:text=Wireshark%20is%20a%20network%20protocol,packet%20sniffer%20in%20the%20world.