Activitity 2

Nmap Commands and Their Uses

Nmap (Network Mapper) is a powerful open-source tool used for network discovery and security auditing. It allows ethical hackers, network administrators, and penetration testers to scan networks, identify live hosts, detect open ports, determine running services, and even detect operating system versions.

This document lists 20 useful Nmap commands, explaining what they do, their example usage, and their implications.

S/N	Command	Description (What It Does)	Example Usage	Implications
1	nmap <target>	Performs a basic scan to detect open ports and services on the target.	nmap 192.168.1.1	Helps identify reachable hosts and their open ports.
2	nmap -sP <network>	Performs a ping sweep to discover live hosts in a network.	nmap -sP 192.168.1.0/24	Useful for network mapping and reconnaissance.
3	nmap -p <port> <target>	Scans a specific port to check if it is open or closed.	nmap -p 80 192.168.1.1	Helps determine if a service (e.g., HTTP) is running on the target.
4	nmap -p- <target>	Scans all 65,535 ports on the target system.	nmap -p- 192.168.1.1	Time-consuming but provides a comprehensive view of open ports.
5	nmap -sS <target>	Performs a stealthy SYN scan to identify open ports without completing the TCP handshake.	nmap -sS 192.168.1.1	Less likely to be detected by intrusion detection systems (IDS).
6	nmap -sU	Scans for open	nmap -sU	Useful for

	<target>	UDP ports instead of TCP.	192.168.1.1	detecting UDP services like DNS, SNMP, and DHCP.
7	nmap -O <target>	Attempts to determine the target's operating system using fingerprinting.	nmap -O 192.168.1.1	Can help tailor exploits or security measures for specific OS versions.
8	nmap -sV <target>	Detects the versions of services running on open ports.	nmap -sV 192.168.1.1	Useful for vulnerability assessment by identifying outdated software.
9	nmap -A <target>	Performs aggressive scanning, including OS detection, version detection, and script scanning.	nmap -A 192.168.1.1	Provides detailed information but is noisy and easily detectable.
10	nmap -T4 <target>	Uses a timing template to speed up scanning.	nmap -T4 192.168.1.1	Reduces scan time but increases detectability.
11	nmap -Pn <target>	Treats all hosts as online, skipping the ICMP ping check.	nmap -Pn 192.168.1.1	Useful when the target blocks ICMP requests.
12	nmap --script=<script> <target>	Uses the Nmap Scripting Engine (NSE) to run specific scripts.	nmap --script=vuln 192.168.1.1	Can be used for vulnerability scanning or advanced reconnaissance.
13	nmap -sC <target>	Runs the default set of NSE scripts for basic security scanning.	nmap -sC 192.168.1.1	Provides additional details about security risks on the target.
14	nmap -F <target>	Performs a fast scan, checking only common ports.	nmap -F 192.168.1.1	Quicker but may miss services running on uncommon ports.

15	nmap -D RND:5 <target>	Uses random decoys to obfuscate the source of the scan.	nmap -D RND:5 192.168.1.1	Can help evade detection by making it appear as if multiple hosts are scanning.
16	nmap -sN <target>	Performs a NULL scan, sending packets with no TCP flags set.	nmap -sN 192.168.1.1	Can bypass certain firewalls but is ineffective against Windows targets.
17	nmap -sX <target>	Performs an Xmas scan by setting FIN, PSH, and URG flags.	nmap -sX 192.168.1.1	Used for stealth scanning, but ineffective on modern OS.
18	nmap -sA <target>	Performs an ACK scan to determine if a firewall is present.	nmap -sA 192.168.1.1	Useful for detecting the presence of stateful firewalls.
19	nmap -oN output.txt <target>	Saves scan results to a file in normal format.	nmap -oN output.txt 192.168.1.1	Useful for documentation and later analysis.
20	nmap -iL targets.txt	Reads target hosts from a file and scans them.	nmap -iL targets.txt	Efficient for scanning multiple targets without manual entry.

gideon360giroh@gmail.com