Network Mapper

Nmap, short for Network Mapper, is a powerful open-source tool for network discovery and security auditing. Security professionals and network administrators widely use it to assess the security posture of a network. Nmap provides a range of features for scanning networks, discovering hosts, and identifying open ports and services.

Host Discovery:

Command: nmap -sn 192.168.1.0/24

Explanation: This command performs host discovery on the specified IP range (192.168.1.0 to 192.168.1.255) without actually scanning for open ports. It helps identify live hosts on the network.

Port Scanning:

Command: nmap -p 1-100 192.168.1.1

Explanation: Conducts a port scan on the target host (192.168.1.1) for ports ranging from 1 to 100. This helps identify which ports are open and potentially running services.

Service Version Detection:

Command: nmap -sV 192.168.1.1

Explanation: This command detects the version of services running on open ports of the target host (192.168.1.1). Knowing service versions is crucial for identifying potential vulnerabilities.

Operating System Detection:

Command: nmap -O 192.168.1.1

Explanation: Attempts to identify the operating system of the target host (192.168.1.1) based on characteristics such as TTL values and TCP/IP fingerprinting.

Scriptable Interaction (NSE):

Command: nmap --script vuln 192.168.1.1

Explanation: Utilizes the Nmap Scripting Engine (NSE) to execute custom scripts (in this case, vulnerability scripts) against the target host (192.168.1.1).

Output Formats:

Command: nmap -oX scan_result.xml 192.168.1.1

Explanation: Specifies the output format as XML and saves the scan results for the target host (192.168.1.1) in a file named scan_result.xml. Nmap supports various output formats, including plain text and grepable formats.