BARI ANKIT (56)

Exp 8: Download and install nmap. Use it with different options to scan open ports, perform OS fingerprinting, do a ping scan, tcp port scan, udp port scan, etc.

Download and Install Nmap

Nmap (Network Mapper) is a powerful open-source tool used for network discovery and security auditing. It is widely used for tasks such as:

- **Scanning open ports on a network**
- **Performing OS fingerprinting (identifying the operating system of a device)**
- **Conducting ping sweeps**
- **Scanning for open TCP/UDP ports**
- **Detecting network vulnerabilities**

Here's how to download, install, and use Nmap for different types of scans.

---

1. Download and Install Nmap

On Linux (Ubuntu/Debian):

1. **Open a terminal.**
2. **Install Nmap using the following command:**

sudo apt update

sudo apt install nmap

On macOS (using Homebrew):

1. **If you don't have Homebrew installed, you can install it by running:**

/bin/bash -c "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/HEAD/install.sh)"

2. **Install Nmap using Homebrew:**

brew install nmap

On Windows:

1. **Go to the Nmap download page.**
2. **Download the Nmap Installer for Windows.**
3. **Run the installer and follow the prompts to complete the installation.**

After installation, you can verify Nmap is installed by running the following command in your terminal (or command prompt on Windows):

nmap --version

---

2. Using Nmap for Different Scans

Once installed, Nmap can be used with various options to perform a wide range of scans. Below are some of the most common use cases:

---

a. Scanning Open Ports

To scan the open ports of a target machine, use the following command:

nmap <target_ip_or_domain>

For example, to scan the open ports of a target with IP address 192.168.1.1:

nmap 192.168.1.1

Nmap will scan the 1,000 most common ports by default.

---

b. Scanning Specific Ports

You can specify the port range to scan, like scanning ports 80 and 443 for HTTP/HTTPS:

nmap -p 80,443 192.168.1.1

Or, to scan a range of ports (e.g., 20-80):

nmap -p 20-80 192.168.1.1

---

c. OS Fingerprinting

To perform OS fingerprinting (detecting the operating system of a target system), use the following command:

nmap -O 192.168.1.1

This will attempt to determine the OS and other relevant information about the target machine by analyzing the TCP/IP stack.

---

d. Ping Scan (Discovery Scan)

A ping scan can be used to determine which hosts are up on a network. This scan sends ICMP echo requests (pings) without port scanning. To perform a ping scan on a network:

nmap -sn 192.168.1.0/24

This will scan all the IP addresses in the subnet 192.168.1.0/24 and show which hosts are alive. It doesn't scan open ports, just checks if the hosts are responding.

---

e. TCP Port Scan

To scan TCP ports (default scan type for Nmap), use:

nmap -sT 192.168.1.1

This is a TCP Connect Scan where Nmap attempts to make a full TCP connection with the target system's ports.

If you need to scan a specific port range using TCP, you can use:

nmap -sT -p 1-1000 192.168.1.1

This command will scan TCP ports 1-1000 on the target.

---

f. UDP Port Scan

To scan UDP ports, use the following command:

nmap -sU 192.168.1.1

This will scan UDP ports instead of the default TCP. You can specify a port range just like for TCP:

nmap -sU -p 53,161,162 192.168.1.1

This scans for UDP ports 53 (DNS) and 161, 162 (SNMP).

---

g. Stealth Scan (SYN Scan)

A SYN Scan is considered stealthier because it doesn't complete the TCP handshake (half-open scan). It’s often used by penetration testers to avoid detection by intrusion detection systems (IDS).

To perform a SYN scan, use the following command:

nmap -sS 192.168.1.1

This scan sends SYN packets to ports and waits for responses without establishing a full TCP connection, making it less likely to be logged.

---

h. Version Detection

To detect the version of the services running on open ports (e.g., HTTP version, SSH version), use:

nmap -sV 192.168.1.1

This will scan the open ports and attempt to determine the software version of the services running on those ports.

---

i. Aggressive Scan (Combining Multiple Options)

For a thorough scan that combines multiple features (port scan, OS detection, version detection, script scanning), use the aggressive scan option -A:

nmap -A 192.168.1.1

This will perform:

- **OS fingerprinting**

- **Service version detection**
- **Script scanning (using Nmap's NSE scripts)**
- **Traceroute**

It provides a comprehensive view of the target system but can take longer to complete.

---

j. Save Scan Results to a File

You can save the scan results to a file using the -oN option for normal output:

nmap -oN scan_results.txt 192.168.1.1

You can also save the results in XML format:

nmap -oX scan_results.xml 192.168.1.1