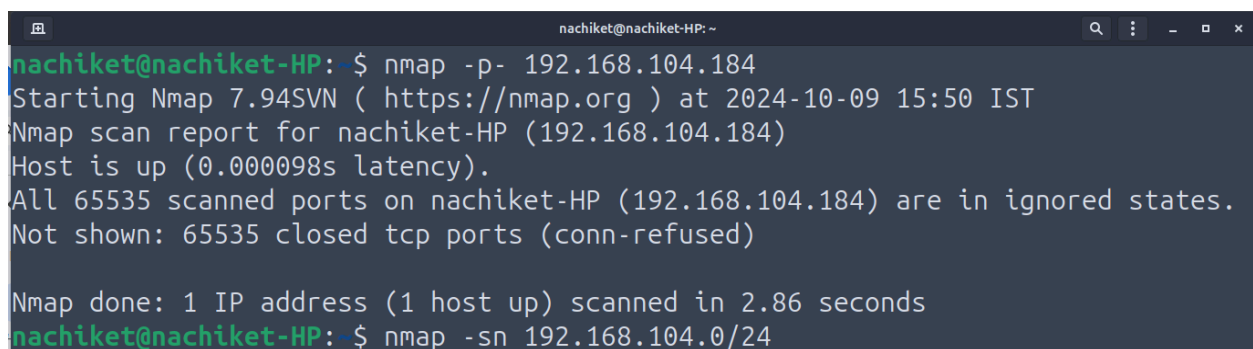


Assignment 7: Using Nmap for Network Scanning

Introduction: Nmap (Network Mapper) is a powerful open-source tool used for network discovery, security auditing, and more. It allows users to identify open ports, detect live hosts, discover the version of operating systems, and obtain information about software running on target systems. In this assignment, we will explore several key features of Nmap that are essential for network administration and penetration testing.

1) Find Open Ports On A System

In networking, ports are virtual communication endpoints that allow different services to interact over the network. Each service (like HTTP, FTP, etc.) listens on a specific port number. Nmap can be used to scan systems for open ports, which are often entry points for attackers if not properly secured. By identifying open ports, network administrators can detect potential vulnerabilities and close unnecessary or risky services.

A terminal window titled 'nachiket@nachiket-HP: ~' showing the execution of Nmap. The user enters the command 'nmap -p- 192.168.104.184'. The output shows the scan starting at 2024-10-09 15:50 IST, reports the host is up with 0.000098s latency, and states that all 65535 scanned ports are in ignored states (closed TCP ports). The scan is completed in 2.86 seconds. The user then enters the command 'nmap -sn 192.168.104.0/24'.

This command scans all 65,535 TCP ports on the target system to find which ones are open.

2) Find The Machines Which Are Active

Before interacting with devices on a network, it is important to identify which machines are currently active or "up." Nmap uses ICMP (Internet Control Message Protocol) echo requests (pings) to detect if a host is active. Other methods like ARP requests can also

be used to find live hosts within a network range. This technique is useful for network mapping and discovery.

```
nachiket@nachiket-HP: $ nmap -sn 192.168.104.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-09 15:51 IST
Nmap scan report for _gateway (192.168.104.167)
Host is up (0.0036s latency).
Nmap scan report for nachiket-HP (192.168.104.184)
Host is up (0.00028s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 14.38 seconds
```

This command sends a ping to each IP address within the specified network range to determine which devices are active.

3)Find The Version Of Remote Os On Other Systems

Operating system (OS) detection is crucial in penetration testing as it helps identify potential vulnerabilities specific to the OS version. Nmap performs OS detection by analyzing characteristics of the network packets, such as the TCP/IP stack fingerprint, to guess the OS running on the target machine. With OS fingerprinting, you can gather information like the OS family (Windows, Linux, etc.) and sometimes even the specific version.

```
nachiket@nachiket-HP: $ sudo nmap -O 192.168.104.184
[sudo] password for nachiket:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-09 15:51 IST
Nmap scan report for nachiket-HP (192.168.104.184)
Host is up (0.000055s latency).
All 1000 scanned ports on nachiket-HP (192.168.104.184) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.63 seconds
```

This command attempts to detect the operating system on the target machine.

4)Find The Version Of s/W Installed On Other System

In addition to OS detection, it's often necessary to determine the versions of services running on open ports. This is known as version detection or service fingerprinting. By identifying the exact versions of software running on a system, administrators can identify outdated versions and patch vulnerabilities. Attackers often target older versions of software with known exploits, so staying updated is key to security.

```
nachiket@nachiket-HP: ~$ nmap -sV 192.168.104.184
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-09 15:52 IST
Nmap scan report for nachiket-HP (192.168.104.184)
Host is up (0.00013s latency).
All 1000 scanned ports on nachiket-HP (192.168.104.184) are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.43 seconds
nachiket@nachiket-HP: ~$
```

This command identifies the version of software running on open ports of the target machine.

Conclusion:

Nmap is an essential tool for network administrators and security professionals. By scanning for open ports, identifying active machines, detecting the remote OS, and finding software versions, Nmap helps in securing networks and identifying potential vulnerabilities. Understanding how to utilize these features effectively can prevent unauthorized access and improve network security.