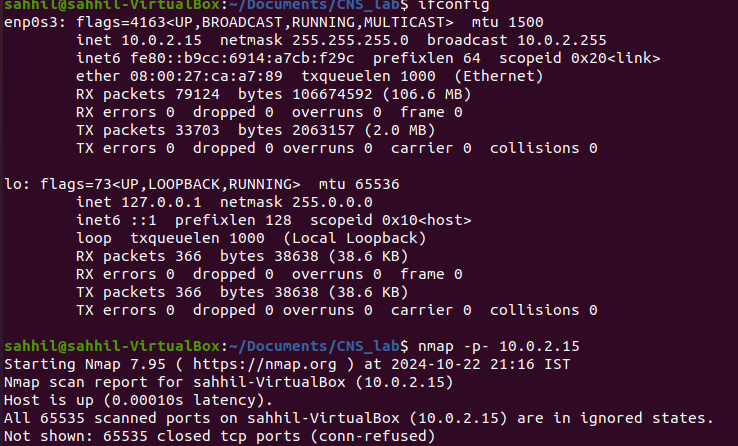
Assignment 6: Network Scanning with Nmap

1. Find Open Ports on a System



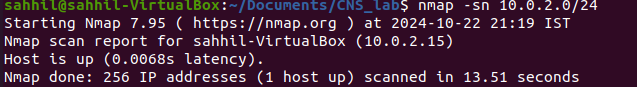
Conclusion:

**The nmap -p- 10.0.2.15 command in your screenshot is used to scan all 65,535 TCP ports on the target host (10.0.2.15). The result indicates that:**

* **The host is up and responsive, with a very low latency (0.00010s).**
* **All 65,535 ports are closed (connection refused).**

**This means that there are no open ports on the scanned IP address (10.0.2.15) that could accept incoming connections.**

1. Find the Machines Which Are Active



Conclusion:

* **Host is up**: This line confirms that the host at 10.0.2.15 is online
* **256 IP addresses (1 host up)**: Nmap scanned 256 possible IPs on the subnet and found that only one host is up.
* **Scanned in 13.51 seconds**: The scan took 13.51 seconds to complete.

1. Find The Version Of Remote OS On Other Systems

sahhil@sahhil-VirtualBox:~/Documents/CNS\_lab $ sudo nmap -0 192.168.104.184

[sudo] password for sahhil:

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-09 15:51 IST

Nmap scan report for sahhil (192.168.104.184)

Host is up (0.000055s latency).

All 1000 scanned ports on sahhil (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

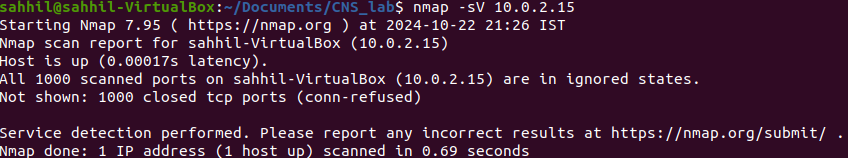
Network Distance: 0 hops

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

1. Find The Version Of S/W(s) Installed On Other System



Output:

1. **Nmap Version and Time**:

* Nmap 7.95 is the version of Nmap being used.
* The scan started at 2024-10-22 21:26 IST (Indian Standard Time).

2. **Scan Report for sahhil-VirtualBox (10.0.2.15)**:

* The target machine is sahhil-VirtualBox with the IP address 10.0.2.15.
* The host is **up** with a very low latency (0.00017s), indicating quick response time from the target machine.

3. **Port Scanning Results**:

* All 1000 TCP ports that were scanned are in the **ignored states**. This typically means these ports are either closed or filtered.
* The note "Not shown: 1000 closed tcp ports (conn-refused)" indicates that none of the ports responded with an open state, and they all returned a "connection refused" message, meaning no service is actively listening on any of these ports.

4. **Service Detection**:

* Even though no open ports were found, Nmap performed service detection (-sV) on the host.
* Since all ports were closed, there is no further information about any running services.

5. **Scan Summary**:

* Nmap scanned 1 IP address in 0.69 seconds, and the scan is complete

Conclusion:

* The scan result shows **"Not shown: 1000 closed tcp ports (conn-refused)"**, meaning **no open ports** were found.
* Since no ports are open, **no software services** were detected on the target system.
* Therefore, **the answer to the question** "Find the version of software(s) installed on the other system" would be:

**No software versions were found** because all scanned ports were closed, and no services were detected running on the system at 10.0.2.15.

If there were any open ports, Nmap would have displayed the version of the software or services running on those ports.

