WEEK-1

Asad Muhammad Channar

DHC-56

TASK-3:

Explore a Security Tool:

Required:

- Choose a Tool:*Pick a basic security tool (e.g., Wireshark, Nmap).
- Task: Perform a simple task with the tool, such as capturing network traffic or running a basic network scan. Write a short report (1 page) on what you did and learned.

Nmap

Nmap is short for Network Mapper. It is an open-source Linux command-line tool that is used to scan IP addresses and ports in a network and to detect installed applications. Nmap allows network admins to find which devices are running on their network, discover open ports and services, and detect vulnerabilities.

Switches:

Nmap uses a number of switches during scanning to provide additional information regarding the scan.

Some most famous switches are as follows:

- **-v(Verbose Mode):**

Nmap prints many extra informational notes when in verbose mode. For example, it prints out the time when each port scan is started along with the number of hosts and ports scanned.

- **-A**

By using –A switch , nmap performs OS detection , version detection and script scanning.

- **-Pn**

When using –Pn switch , nmap scans the system despite system is up or not.

- **-sn**

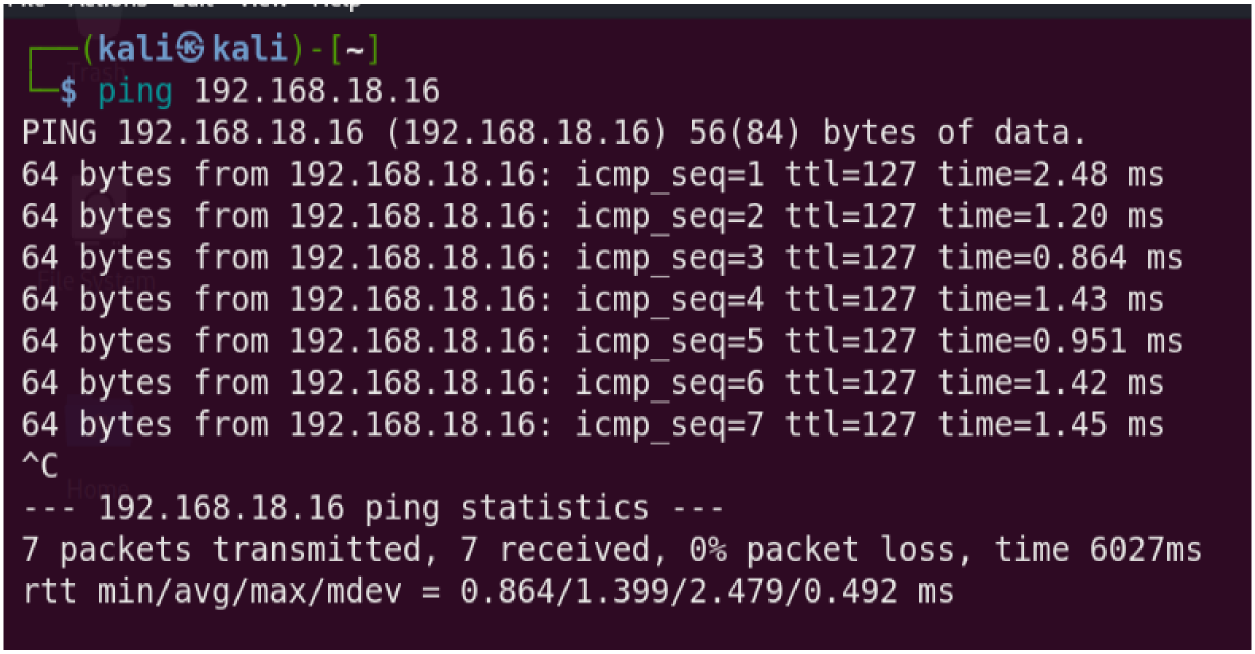
Only discover live hosts, without port scanning.

Like these, there are various switches which one use according to need.

Use-Case:

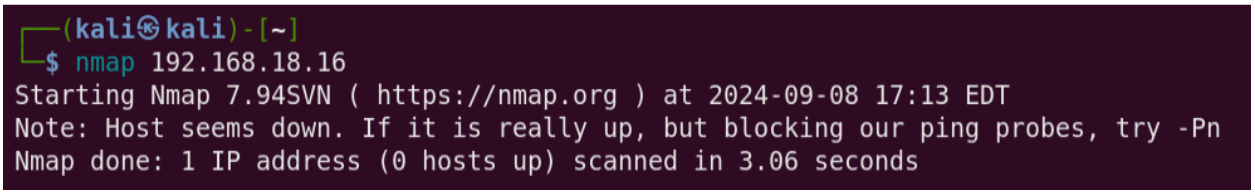
In this section , we will perform a basic scan using nmap. For this we will use a linux VM which I use kali and a host windows . We will scan the host using nmap.

First step of scanning is to see if you can reach the target or not else your packets cannot reach the target.



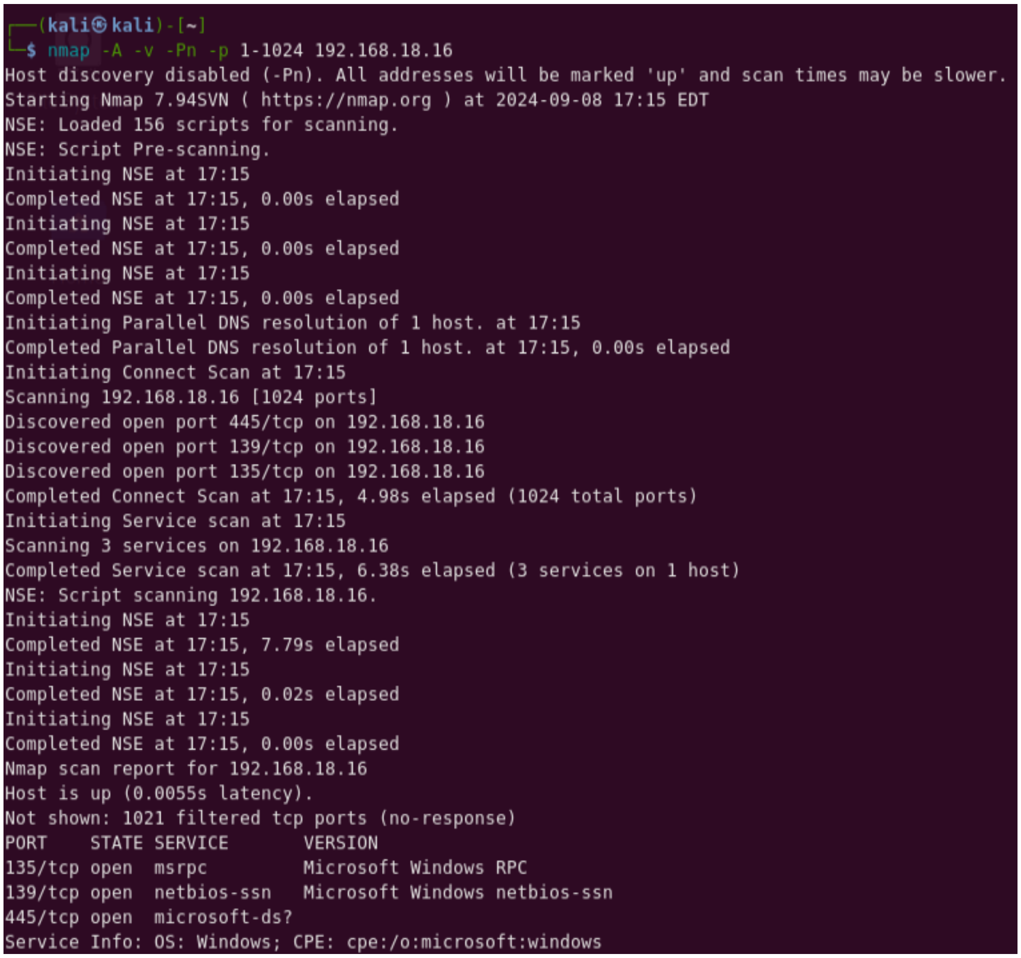
```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.18.16
PING 192.168.18.16 (192.168.18.16) 56(84) bytes of data.
64 bytes from 192.168.18.16: icmp_seq=1 ttl=127 time=2.48 ms
64 bytes from 192.168.18.16: icmp_seq=2 ttl=127 time=1.20 ms
64 bytes from 192.168.18.16: icmp_seq=3 ttl=127 time=0.864 ms
64 bytes from 192.168.18.16: icmp_seq=4 ttl=127 time=1.43 ms
64 bytes from 192.168.18.16: icmp_seq=5 ttl=127 time=0.951 ms
64 bytes from 192.168.18.16: icmp_seq=6 ttl=127 time=1.42 ms
64 bytes from 192.168.18.16: icmp_seq=7 ttl=127 time=1.45 ms
^C
--- 192.168.18.16 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6027ms
rtt min/avg/max/mdev = 0.864/1.399/2.479/0.492 ms
```

So, to check connectivity we ping the host and it responds. Now we will start the scan.

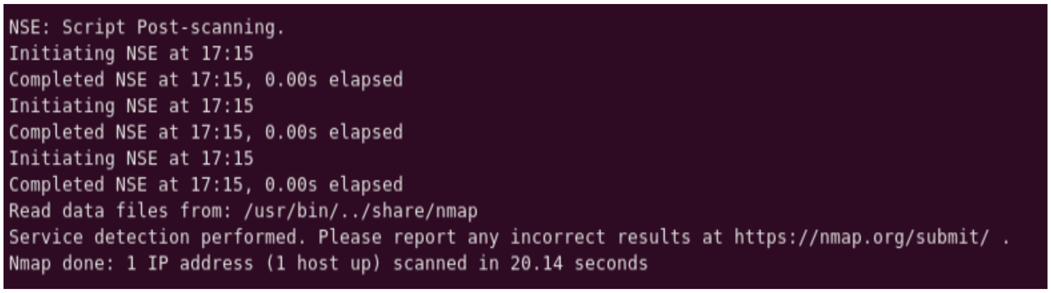


```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.18.16
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-08 17:13 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.06 seconds
```

This is the basic scan and the result shows that we should use **–Pn** .



```
┌──(kali㉿kali)-[~]
└─$ nmap -A -v -Pn -p 1-1024 192.168.18.16
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-08 17:15 EDT
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 17:15
Completed NSE at 17:15, 0.00s elapsed
Initiating NSE at 17:15
Completed NSE at 17:15, 0.00s elapsed
Initiating NSE at 17:15
Completed NSE at 17:15, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 17:15
Completed Parallel DNS resolution of 1 host. at 17:15, 0.00s elapsed
Initiating Connect Scan at 17:15
Scanning 192.168.18.16 [1024 ports]
Discovered open port 445/tcp on 192.168.18.16
Discovered open port 139/tcp on 192.168.18.16
Discovered open port 135/tcp on 192.168.18.16
Completed Connect Scan at 17:15, 4.98s elapsed (1024 total ports)
Initiating Service scan at 17:15
Scanning 3 services on 192.168.18.16
Completed Service scan at 17:15, 6.38s elapsed (3 services on 1 host)
NSE: Script scanning 192.168.18.16.
Initiating NSE at 17:15
Completed NSE at 17:15, 7.79s elapsed
Initiating NSE at 17:15
Completed NSE at 17:15, 0.02s elapsed
Initiating NSE at 17:15
Completed NSE at 17:15, 0.00s elapsed
Nmap scan report for 192.168.18.16
Host is up (0.0055s latency).
Not shown: 1021 filtered tcp ports (no-response)
PORT    STATE SERVICE       VERSION
135/tcp open  msrpc         Microsoft Windows RPC
139/tcp open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```



```
NSE: Script Post-scanning.
Initiating NSE at 17:15
Completed NSE at 17:15, 0.00s elapsed
Initiating NSE at 17:15
Completed NSE at 17:15, 0.00s elapsed
Initiating NSE at 17:15
Completed NSE at 17:15, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.14 seconds
```

So this is a nmap scan . The scan results shows that 3 ports(**135**,**139**,**445**) are open . We use some switches and we got the information accordingly. **–A** switch provide the OS info to be **Windows. –v** provides extra info about scan . By using –Pn switch we were able to scan the host. **–p** switch is used to specify the ports to scan