WEEK-2

Asad Muhammd Channar

DHC-56

Task-2:

Vulnerability Scanning with Nmap

Install & Configure: Ensure Nmap is set up in your VM (from Week 1) or install it if you haven't already.

Required:

- Run an advanced Nmap scan on your local network.
- Identify open ports, running services, and potential vulnerabilities.
- Document: Write a 1page report with your findings, explaining the risks and how they could be mitigated. Mention any new commands or techniques you used compared to Week 1.

Nmap

Nmap (Network Mapper) is a powerful, open-source tool widely used for network discovery, security auditing, and vulnerability scanning. It allows users to identify active devices on a network, discover open ports, detect services running on those ports, and gather information about the operating system and software versions. Nmap supports various scan techniques, including TCP, UDP, and OS detection, making it a valuable tool for network administrators and security professionals. Its flexibility, efficiency, and ability to scan both small and large networks make it a go-to tool for cybersecurity assessments.

Network Scanning:

For this, I will use my kali VM and scan my host system. First, we will run a general scan and then **TCP** and **UDP** scans

General Scan:

For the general scan we use the following command.

nmap -A -v -Pn -p 1-1024 <target-ip>

The result of the scan is as follows

```
┌──(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 2024-09-21 05:25 EDT
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 05:25
Completed NSE at 05:25, 0.00s elapsed
Initiating NSE at 05:25
Completed NSE at 05:25, 0.00s elapsed
Initiating NSE at 05:25
Completed NSE at 05:25, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 05:25
Completed Parallel DNS resolution of 1 host. at 05:25, 0.04s elapsed
Initiating Connect Scan at 05:25
Scanning 192.168.18.16 [1024 ports]
Discovered open port 139/tcp on 192.168.18.16
Discovered open port 445/tcp on 192.168.18.16
Discovered open port 135/tcp on 192.168.18.16
Completed Connect Scan at 05:25, 5.04s elapsed (1024 total ports)
Initiating Service scan at 05:25
Scanning 3 services on 192.168.18.16
Completed Service scan at 05:25, 6.12s elapsed (3 services on 1 host)
NSE: Script scanning 192.168.18.16.
Initiating NSE at 05:25
Completed NSE at 05:25, 7.77s elapsed
Initiating NSE at 05:25
Completed NSE at 05:25, 0.02s elapsed
Initiating NSE at 05:25
Completed NSE at 05:25, 0.00s elapsed
Nmap scan report for 192.168.18.16
Host is up (0.0053s 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
```

```
Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_clock-skew: 1s
| smb2-time:
|   date: 2024-09-21T09:25:37
|_  start_date: N/A

NSE: Script Post-scanning.
Initiating NSE at 05:25
Completed NSE at 05:25, 0.00s elapsed
Initiating NSE at 05:25
Completed NSE at 05:25, 0.00s elapsed
Initiating NSE at 05:25
Completed NSE at 05:25, 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 19.84 seconds
```

As we see three ports **135/tcp** , **139/tcp** and **145/tcp** are open . We also use a **–A** switch which provide us the OS information as in this case I am running windows on my host. **–v** switch is used for verbose mode which provides extra information about the scan .

TCP Scan:

For the TCP scan we use the following command.

nmap –Pn -sS <target-ip>

The result of this scan is as follows.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -Pn  -sS 192.168.18.16
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-21 05:27 EDT
Nmap scan report for 192.168.18.16
Host is up (0.0042s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 4.95 seconds
```

-sS switch is used for TCP scan. One thing to note here is that same ports are shown in both the scan. The reason for this is that by default nmap runs a TCP scan on the target ip. In the general

scan we use extra switches so we get more insight into the scan but in TCP scan we just use 2 switches. So, this is also a very good demonstraton of using switches in scans.

UDP Scan:

For the UDP scan we use the following command.

nmap -Pn -sU <target-ip>

The result of scan is as follows:

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -Pn -sU 192.168.18.16
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-21 05:28 EDT
Stats: 0:00:47 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 22.83% done; ETC: 05:32 (0:02:42 remaining)
Stats: 0:05:31 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 88.03% done; ETC: 05:35 (0:00:45 remaining)
Nmap scan report for 192.168.18.16
Host is up (0.0017s latency).
Not shown: 991 filtered udp ports (port-unreach)
PORT     STATE         SERVICE
67/udp   open|filtered dhcps
123/udp  open|filtered ntp
137/udp  open|filtered netbios-ns
138/udp  open|filtered netbios-dgm
1900/udp open|filtered upnp
4500/udp open|filtered nat-t-ike
5050/udp open|filtered mmcc
5353/udp open|filtered zeroconf
5355/udp open|filtered llmnr

Nmap done: 1 IP address (1 host up) scanned in 388.72 seconds
```

So, These are the open|filtered UDP ports. Thing to Observe is that these ports are neither open nor filterd but b the port's status is ambiguous—Nmap cannot definitively determine if the port is open or if it is being filtered by a firewall or other network security devices.