Assignment-6

Acknowledgment

Name: Sarvesh Anand Mankar
MIS: 142203013
Subject: Cryptography Network and Security Labs
Class: Div-2, T2

Objective

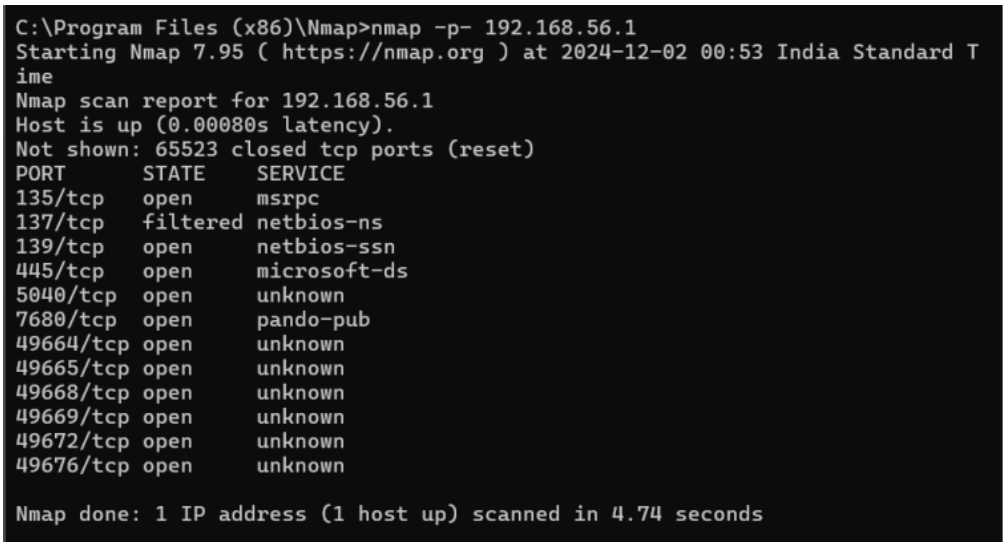
To understand and utilize the capabilities of Nmap for network analysis and security auditing.

Tasks

1. Find Open Ports on a System

- Use Nmap to scan for open ports on a specified target system.
- Example command:

```
nmap -p- <target-ip>
```



2. Find the Machines Which Are Active

- Discover active machines on a network using Nmap's ping sweep functionality.
- Example command:

```
nmap -sn <network-range>
```

```
C:\Program Files (x86)\Nmap>nmap -sn 10.100.99.136/20
Starting Nmap 7.95 ( https://nmap.org ) at 2024-12-01 20:32 India Standard Time
Nmap scan report for 10.100.96.115
Host is up (0.21s latency).
MAC Address: 10:68:38:8C:AD:73 (AzureWave Technology)
Nmap scan report for 10.100.96.130
Host is up (0.61s latency).
MAC Address: 44:16:FA:42:CA:B5 (Samsung Electronics)
Nmap scan report for 10.100.96.131
Host is up (0.59s latency).
MAC Address: 20:2B:20:EF:11:B3 (Cloud Network Technology Singapore PTE.)
Nmap scan report for 10.100.96.133
Host is up (0.35s latency).
MAC Address: 20:0B:74:0D:0B:83 (AzureWave Technology)
Nmap scan report for 10.100.96.136
Host is up (0.16s latency).
MAC Address: D4:1B:81:83:6A:EB (Chongqing Fugui Electronics)
Nmap scan report for 10.100.96.144
Host is up (0.14s latency).
MAC Address: 2C:3B:70:1E:1C:F3 (AzureWave Technology)
Nmap scan report for 10.100.96.149
Host is up (0.14s latency).
MAC Address: EE:D6:D9:A3:1A:E1 (Unknown)
Nmap scan report for 10.100.96.156
Host is up (0.19s latency).
MAC Address: F6:13:6C:0E:83:C6 (Unknown)
Nmap scan report for 10.100.96.157
Host is up (0.064s latency).
MAC Address: A0:02:A5:DC:7C:88 (Intel Corporate)
Nmap scan report for 10.100.96.161
Host is up (0.18s latency).
MAC Address: 14:13:33:14:C4:5D (AzureWave Technology)
Nmap scan report for 10.100.96.178
Host is up (0.054s latency).
MAC Address: 28:16:AD:E8:08:69 (Intel Corporate)
Nmap scan report for 10.100.96.180
Host is up (0.10s latency).
MAC Address: 56:F1:A8:5C:B9:CC (Unknown)
Nmap scan report for 10.100.96.188
Host is up (0.083s latency).
MAC Address: 5A:5E:16:40:9E:B8 (Unknown)
Nmap scan report for 10.100.96.191
Host is up (0.050s latency).
MAC Address: 94:54:CE:37:F0:BF (Guangdong Oppo Mobile Telecommunications)
Nmap scan report for 10.100.96.197
Host is up (0.060s latency).
MAC Address: 94:BB:43:B2:EA:0D (AzureWave Technology)
Nmap scan report for 10.100.96.204
Host is up (0.18s latency).
MAC Address: 3C:13:5A:98:A2:84 (Xiaomi Communications)
Nmap scan report for 10.100.96.217
Host is up (0.16s latency).
MAC Address: 34:B9:8D:69:98:6D (Xiaomi Communications)
```

```
Nmap scan report for 10.100.111.232
Host is up (0.031s latency).
MAC Address: 6A:32:00:69:58:8F (Unknown)
Nmap scan report for 10.100.111.235
Host is up (0.092s latency).
MAC Address: 1C:86:82:27:BA:AC (Apple)
Nmap scan report for 10.100.111.248
Host is up (0.065s latency).
MAC Address: DC:45:46:CB:FA:CA (Intel Corporate)
Nmap scan report for 10.100.99.136
Host is up.
Nmap done: 4096 IP addresses (456 hosts up) scanned in 30.56 seconds
```

3. Find the Version of Remote OS on Other Systems

- Identify the operating system of remote systems using Nmap's OS detection feature.
- Example command:

```
nmap -O <target-ip>
```

```
C:\Program Files (x86)\Nmap>nmap -O -v 192.168.56.1
Starting Nmap 7.95 ( https://nmap.org ) at 2024-12-02 00:37 India Standard T
ime
Initiating Parallel DNS resolution of 1 host. at 00:37
Completed Parallel DNS resolution of 1 host. at 00:37, 0.01s elapsed
Initiating SYN Stealth Scan at 00:37
Scanning 192.168.56.1 [1000 ports]
Discovered open port 139/tcp on 192.168.56.1
Discovered open port 445/tcp on 192.168.56.1
Discovered open port 135/tcp on 192.168.56.1
Completed SYN Stealth Scan at 00:37, 0.18s elapsed (1000 total ports)
Initiating OS detection (try #1) against 192.168.56.1
Nmap scan report for 192.168.56.1
Host is up (0.00050s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
Device type: general purpose
Running: Microsoft Windows 10|11
OS CPE: cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_11
OS details: Microsoft Windows 10 1607 - 11 23H2
Uptime guess: 10.494 days (since Thu Nov 21 12:47:04 2024)
Network Distance: 0 hops
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: Incremental

Read data files from: C:\Program Files (x86)\Nmap
OS detection performed. Please report any incorrect results at https://nmap.
org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.68 seconds
           Raw packets sent: 1016 (45.418KB) | Rcvd: 2043 (87.214KB)
```

4. Find the Version of Software Installed on Other Systems

- Check for versions of software running on remote systems using Nmap's service version detection.
- Example command:

```
nmap -sV <target-ip>
```

```
C:\Program Files (x86)\Nmap>nmap -sV -Pn 192.168.56.1
Starting Nmap 7.95 ( https://nmap.org ) at 2024-12-02 00:31 India Standard T
ime
Nmap scan report for 192.168.56.1
Host is up (0.00021s latency).
Not shown: 997 closed tcp ports (reset)
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

Service detection performed. Please report any incorrect results at https://
nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.00 seconds
```