CompTIA Security+ 601

Assessment Project

Task-1

Obtain a scanning report of the entire network and identify how many terminals are connected with the Windows operating system and the Linux-based systems.

Step 1: ipconfig/all

IP Address : 192.168.0.105

Default Gateway : 192.168.0.1

NetMask : 255.255.255.0

MAC Address : 00-F4-8D-F9-D2-C3

Class C IP Address so CIDR would 24

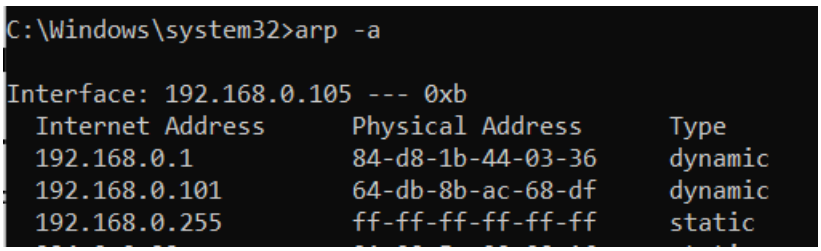
```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Qualcomm Atheros QCA9377 Wireless Network Adapter
   Physical Address. . . . . . . . . : 00-F4-8D-F9-D2-C3
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::a487:5bb9:3823:f4a9%11(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.0.105(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 26 August 2021 20:58:32
   Lease Expires . . . . . . . . . . : 27 August 2021 00:58:32
   Default Gateway . . . . . . . . . : 192.168.0.1
   DHCP Server . . . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 83948685
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-28-83-73-87-00-F4-8D-F9-D2-C3
   DNS Servers . . . . . . . . . . . : 192.168.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Step 2 : arp -a for all the host discovery

Default Gateway : 192.168.0.1

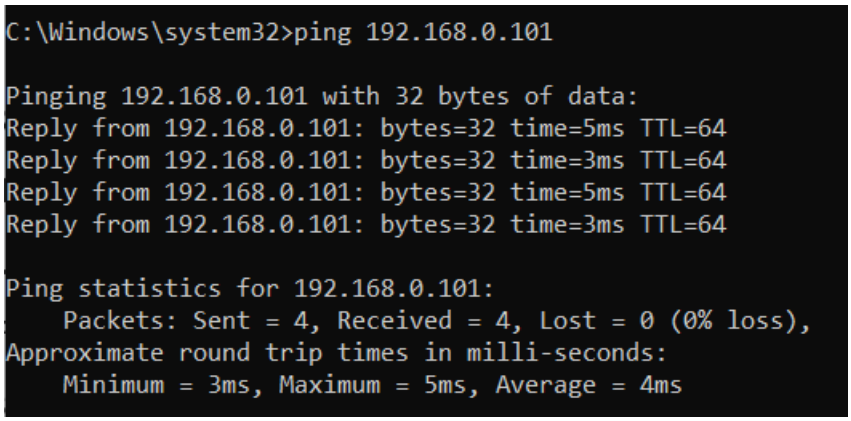
Victim's IP Address : 192.168.0.101

Router IP : 192.168.0.255



Step 3 : ping 192.168.0.101 Connection

is active with victim's IP



Step 4: TTL=64 in ping reply

Victim's OS : Mac Machine

Server's OS : Microsoft Windows 10 1809 – 1909 1

Terminal Connected with Apple MAC

```
C:\Windows\system32>ping 192.168.0.101

Pinging 192.168.0.101 with 32 bytes of data:
Reply from 192.168.0.101: bytes=32 time=5ms TTL=64
Reply from 192.168.0.101: bytes=32 time=3ms TTL=64
Reply from 192.168.0.101: bytes=32 time=5ms TTL=64
Reply from 192.168.0.101: bytes=32 time=3ms TTL=64

Ping statistics for 192.168.0.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 5ms, Average = 4ms
```

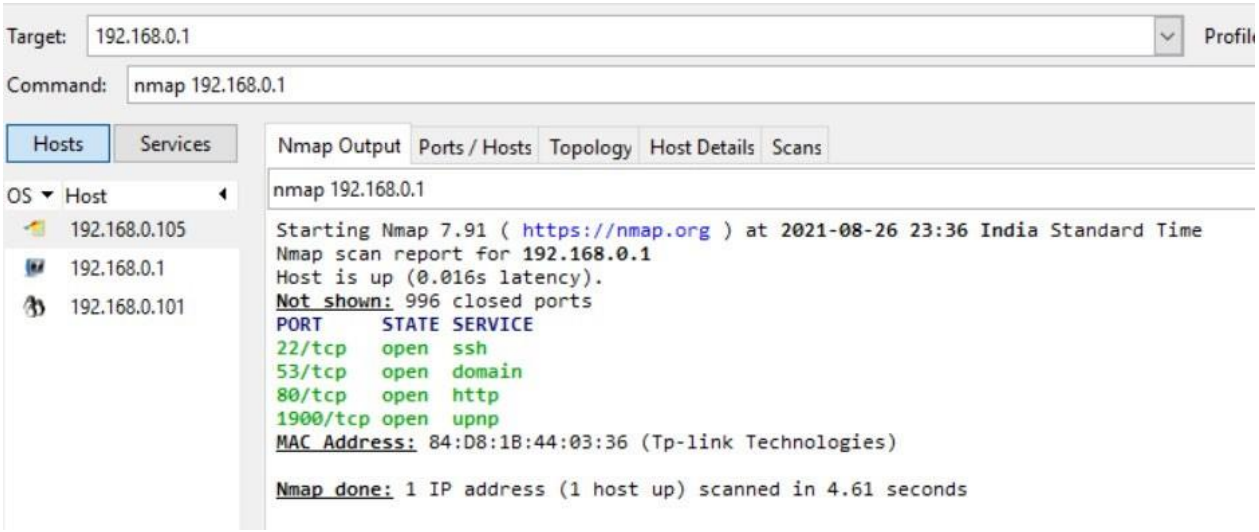
Task-2

Identify CVE score of the victim's vulnerability.

Step 1: nmap 192.168.0.1

Open Ports are:

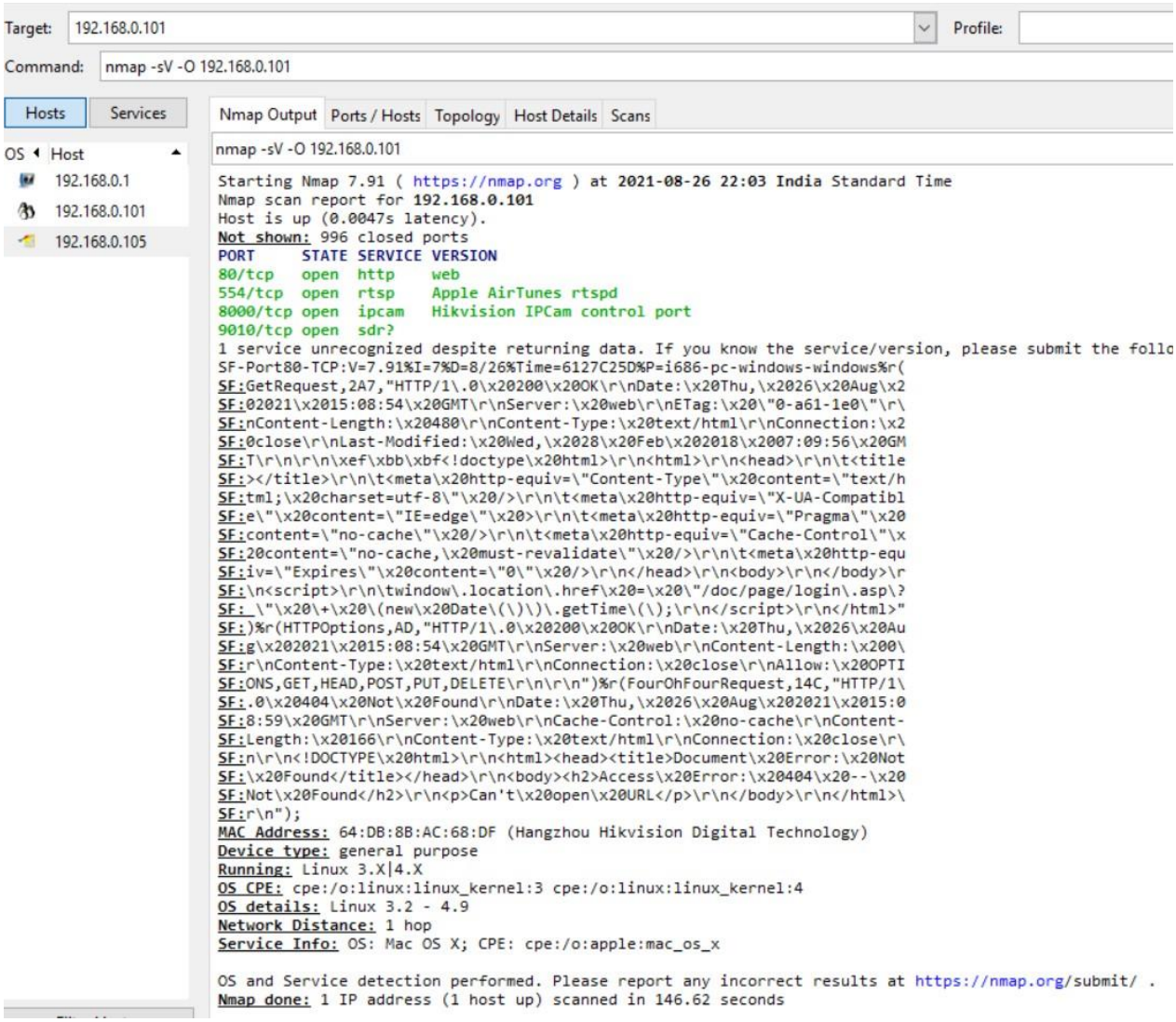
PORT	STATE	SERVICE
80/tcp	open	http
554/tcp	open	rtsp
8000/tcp	open	http-alt
9010/tcp	open	sdr



Step 2: nmap -O -sV 192.168.0.101 (OS and Version)

PORT	STATE	SERVICE	VERSION
80/tcp	open	http	web
554/tcp	open	rtsp	Apple AirTunes rtspd
8000/tcp	open	ipcam	Hikvision IPCam control port
9010/tcp	open	sdr	?

OS : Linux 3.2 - 4.9



CVE SCORE:

80/tcp 9.8 CRITICAL

554/tcp : 5.3 MEDIUM

8000/tcp 7.5 HIGH

9010/tcp 7.5 HIGH

Average : 7.5 HIGH

Task-3

Identify whether the victim's terminal is affected with MiTM attack or not and submit the incident report for the same.

Step 1: arp -a 192.168.0.101

Interface: 192.168.0.105 --- 0xb

Internet Address	Physical Address	Type
192.168.0.1	84-d8-1b-44-03-36	dynamic

```
C:\Windows\system32>arp -a 192.168.0.101

Interface: 192.168.0.105 --- 0xb
  Internet Address      Physical Address      Type
  192.168.0.101         64-db-8b-ac-68-df     dynamic
```

As there are no other PCs or any other internet device is connected so there is no possibility of MiTM attack as no suspicious IP address is found.

Task-4

Use email forensics analysis and identify the sender's IP address

Step 1: Open the email and select other options and from there select SHOW ORIGINAL

Step 2: Copy Email header with option Copy To Clipboard Step 3:

Perform Email Forensics

Sender's IP : 209.85.220.41

ISP : Google

Latitude : 37.751

Longitute : -97.822