

## 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

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

Interface: 192.168.0.105 --- 0xb
    Internet Address      Physical Address      Type
    192.168.0.1           84-d8-1b-44-03-36    dynamic
    192.168.0.101        64-db-8b-ac-68-df    dynamic
    192.168.0.255        ff-ff-ff-ff-ff-ff    static
```

**Step 3 :** ping 192.168.0.101 Connection

is active with victim's IP

```
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
```

**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
```

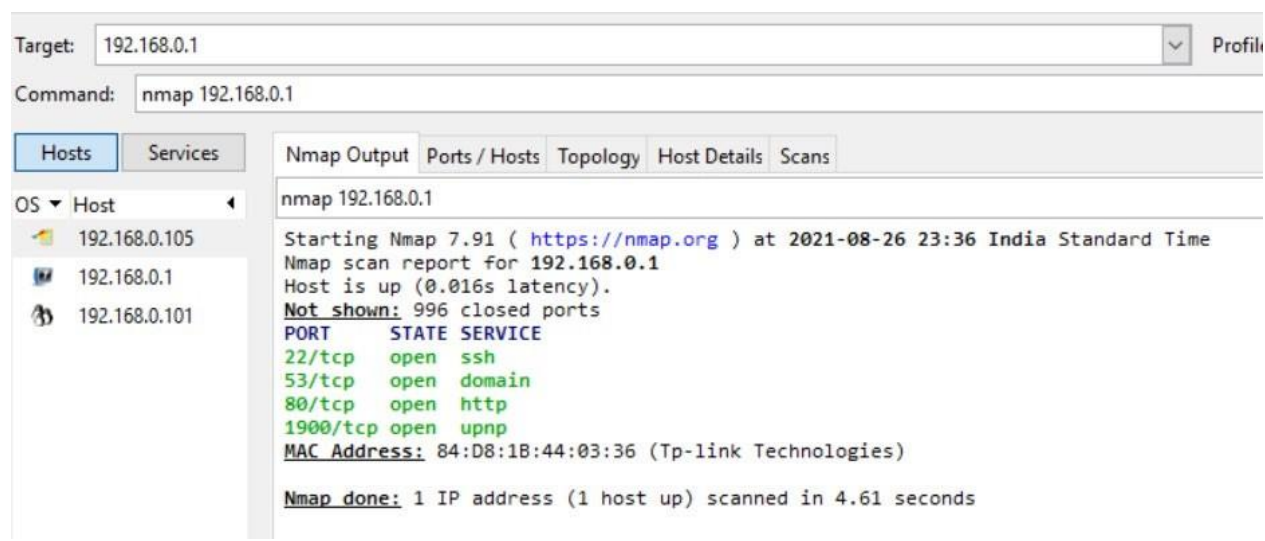
**Task-2**

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

**Target:** 192.168.0.101

**Profile:**

**Command:** nmap -sV -O 192.168.0.101

Hosts

Services

Nmap Output

Ports / Hosts

Topology

Host Details

Scans

OS Host

▲

192.168.0.1

192.168.0.101

192.168.0.105

nmap -sV -O 192.168.0.101

Starting Nmap 7.91 ( <https://nmap.org> ) at 2021-08-26 22:03 India Standard Time

Nmap scan report for 192.168.0.101

Host is up (0.0047s latency).

**Not shown:** 996 closed ports

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

1 service unrecognized despite returning data. If you know the service/version, please submit the following:

```

SF-Port80-TCP:V=7.91I=7%D=8/26%Time=6127C25D%P=i686-pc-windows-windows%R(
SF:GetRequest,2A7,"HTTP/1.0\x20200\x200K\r\nDate:\x20Thu,\x2026\x20Aug\x2
SF:02021\x2015:08:54\x20GMT\r\nServer:\x20web\r\nETag:\x20\"0-a61-1e0\"\\\r
SF:nContent-Length:\x20480\r\nContent-Type:\x20text/html\r\nConnection:\x2
SF:0close\r\nLast-Modified:\x20Wed,\x2028\x20Feb\x202018\x2007:09:56\x20GM
SF:T\r\n\r\n\xef\xbb\xbf<!doctype\x20html>\r\n<html>\r\n<head>\r\n<title
SF:></title>\r\n<meta\x20http-equiv=\x20\"Content-Type\"\\\x20content=\x20\"text/h
SF:tml;\x20charset=utf-8\"\\\x20/>\r\n<meta\x20http-equiv=\x20\"X-UA-Compatib
SF:e\"\\\x20content=\x20\"IE=edge\"\\\x20/>\r\n<meta\x20http-equiv=\x20\"Pragma\"\\\x20
SF:content=\x20\"no-cache\"\\\x20/>\r\n<meta\x20http-equiv=\x20\"Cache-Control\"\\\x
SF:20content=\x20\"no-cache,\x20must-revalidate\"\\\x20/>\r\n<meta\x20http-eq
SF:iv=\x20\"Expires\"\\\x20content=\x20\"0\"\\\x20/>\r\n</head>\r\n<body>\r\n</body>\r
SF:n<script>\r\n\twindow.location.href\x20=\x20\"/doc/page/login.asp?
SF:\x20+\x20(new\x20Date(\x20)\x20)\x20.getTime(\x20)\x20\"\\\r\n</script>\r\n</html>\"
SF:)%r(HTTPOptions,AD,\"HTTP/1.0\x20200\x200K\r\nDate:\x20Thu,\x2026\x20Au
SF:g\x202021\x2015:08:54\x20GMT\r\nServer:\x20web\r\nCache-Control:\x20no-cache\r\nContent-
SF:r\nContent-Type:\x20text/html\r\nConnection:\x20close\r\nAllow:\x20OPTI
SF:ONS,GET,HEAD,POST,PUT,DELETE\r\n\r\n\")%r(FourOhFourRequest,14C,\"HTTP/1
SF:0\x20404\x20Not\x20Found\r\nDate:\x20Thu,\x2026\x20Aug\x202021\x2015:0
SF:8:59\x20GMT\r\nServer:\x20web\r\nCache-Control:\x20no-cache\r\nContent-
SF:Length:\x20166\r\nContent-Type:\x20text/html\r\nConnection:\x20close\r
SF:n\r\n<!DOCTYPE\x20html>\r\n<html><head><title>Document\x20Error:\x20Not
SF:\x20Found</title></head>\r\n<body><h2>Access\x20Error:\x20404\x20- \x20
SF:Not\x20Found</h2>\r\n<p>Can't\x20open\x20URL</p>\r\n</body>\r\n</html>
SF:r\n");
MAC Address: 64:DB:8B:AC:68:DF (Hangzhou Hikvision Digital Technology)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Mac OS X; CPE: cpe:/o:apple:mac_os_x

```

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

**Nmap done:** 1 IP address (1 host up) scanned in 146.62 seconds

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

Longitude : -97.822