



CODING SAMURAI

CODING YOUR ASCENT. LEARN. CODE. UPSKILL.

Internship in
Cyber Security

Home Network Security Audit(Task II)

Submitted by

AVIJIT DAS

Batch E

SEP 24 – OCT 22

Network Inventory:

```
File Actions Edit View Help
Currently scanning: Finished! | Screen View: Unique Hosts

248 Captured ARP Req/Rep packets, from 6 hosts. Total size: 14880

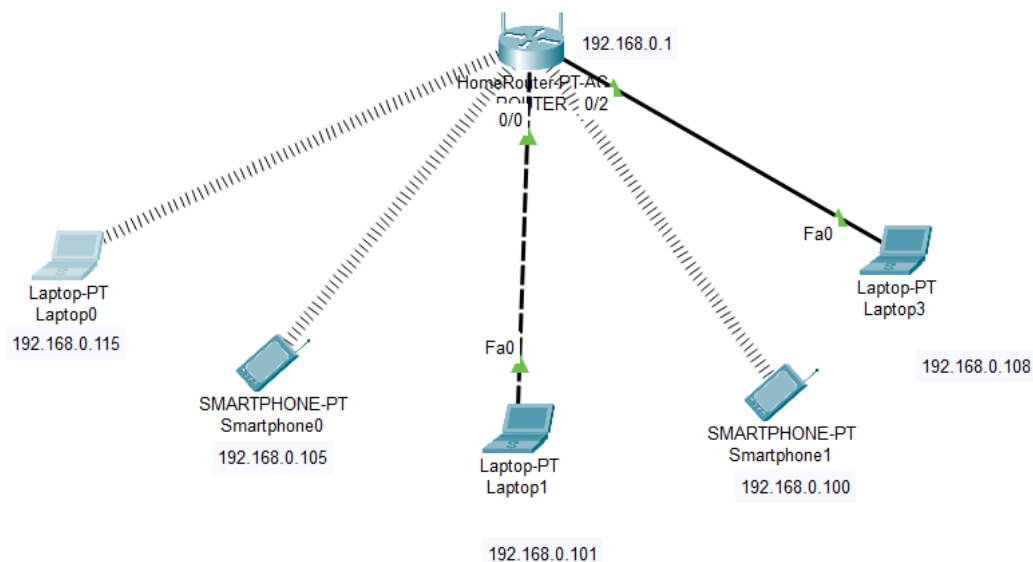
+-----+-----+-----+-----+-----+
| IP           | At MAC Address | Count | Len | MAC Vendor / Hostname |
+-----+-----+-----+-----+-----+
| 192.168.0.1  | 48:22:54:be:2d:e4 | 243   | 14580 | TP-Link Corporation Limited |
| 192.168.0.108 | 5c:ea:1d:c5:95:87 | 1     | 60   | Hon Hai Precision Ind. Co.,Ltd. |
| 192.168.0.101 | 62:c8:fa:e5:fb:c8 | 1     | 60   | Unknown vendor |
| 192.168.0.105 | c2:93:cb:f8:1a:a3 | 1     | 60   | Unknown vendor |
| 192.168.0.115 | 7c:70:db:00:e6:aa | 1     | 60   | Intel Corporate |
| 192.168.0.100 | 20:34:fb:65:84:5b | 1     | 60   | Xiaomi Communications Co Ltd |
+-----+-----+-----+-----+-----+

zsh: suspended netdiscover -r 192.168.0.0/24

root@kali:~#
```

This is my home network, Including my device total 5 devices are connected to the router. In these five devices three are Laptops and two are smart phones.

Network Diagram:



Vulnerability Assessment:

```
(root@kali)-[/home/kali]
# nmap -sV -Pn 192.168.0.1
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-18 00:22 IST
Nmap scan report for 192.168.0.1
Host is up (0.0072s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE      SERVICE VERSION
23/tcp    filtered  telnet
80/tcp    open      http
1900/tcp   open      upnp     Portable SDK for UPnP devices 1.6.19 (Linux 3.10.14; UPnP 1.0)
```

```
# nmap -sV -sC 192.168.0.108
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-17 23:08 IST
Nmap scan report for 192.168.0.108
Host is up (0.00039s latency).
Not shown: 995 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?
2869/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
7070/tcp  open  ssl/realserver?
|_ssl-date: TLS randomness does not represent time
|_ssl-cert: Subject: commonName=AnyDesk Client
| Not valid before: 2022-01-20T10:08:04
|_Not valid after: 2072-01-08T10:08:04
MAC Address: 5C:EA:1D:C5:95:87 (Hon Hai Precision Ind.)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
(root@kali)-[/home/kali]
# nmap -sV -sC -sX 192.168.0.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-17 23:16 IST
Nmap scan report for 192.168.0.101
Host is up (0.0077s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE      SERVICE      VERSION
5060/tcp  open|filtered tcpwrapped
MAC Address: 62:C8:FA:E5:FB:C8 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.70 seconds
```

```
(root@kali)-[/home/kali]
# nmap -sV -sC 192.168.0.100
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-17 23:17 IST
Nmap scan report for 192.168.0.100
Host is up (0.011s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE      SERVICE VERSION
5060/tcp  filtered  sip
MAC Address: 20:34:FB:65:84:5B (Xiaomi Communications)
```

Password Audit:

This is my router's password strength, it might be hacked but it will take 284 million years.

Router Security:

☒ Enable Wireless Radio

Network Name (SSID):

SINCE_@)!^_5G

☐ Hide SSID

Security:

WPA/WPA2 Personal (Recommended)

Version:

☒ Auto☐ WPA-PSK☐ WPA2-PSK

Encryption:

☒ Auto☐ TKIP☐ AES

Password:

Mode:

802.11a/n/ac mixed

Channel:

Auto

Channel Width:

Auto

Transmit Power:

☐ Low☐ Middle☒ High

Save

In my home router not have WPA3, till its use WPA2 and for encryption its use TKIP and AES both, so I'm using Auto. Password is hidden for privacy purpose.

Firewall Configuration:

Advanced

Firewall

IPv4 SPI Firewall:

IPv6 SPI Firewall:

All firewalls are active mode to check the traffic and prevent the malicious attack.

Guest Network:

In our Router guest network option are not available, so I can't set any isolated guest network separated from main network.

Device Patching:

Hardware Version: Archer C20 v5 00000004

New Firmware File:

Upgrade

Network Monitoring:

No.	Time	Source	Destination	Protocol	Length	Info
4	0.853139689	Fe80::2960:68d1:5e5...	Ff02::16	ICMPv6	110	Multicast Listener Report Message v2
5	1.008235527	192.168.0.108	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
6	5.373218078	TP-Link-be:2d:e4	Broadcast	ARP	60	Who has 192.168.0.108? Tell 192.168.0.1
7	5.377189020	TP-Link-be:2d:e4	Broadcast	ARP	60	Who has 192.168.0.117? Tell 192.168.0.1
8	5.377231580	PcsCompu:53:9c:ba	TP-Link-be:2d:e4	ARP	42	192.168.0.117 is at 08:00:27:53:0c:ba
9	5.379126252	192.168.0.1	192.168.0.117	NBNS	92	Name query NBSTAT *<00-c0-00-00-00-00-c0-00-00-00-00-00-00-00-00-00-00>
10	5.379207170	192.168.0.1	192.168.0.117	ICMP	120	Destination unreachable (Port unreachable)
11	6.354535588	TP-Link-be:2d:e4	Broadcast	ARP	60	Who has 192.168.0.108? Tell 192.168.0.1
12	6.356608444	TP-Link-be:2d:e4	Broadcast	ARP	60	Who has 192.168.0.117? Tell 192.168.0.1
13	6.356111991	PcsCompu:53:9c:ba	TP-Link-be:2d:e4	ARP	42	192.168.0.117 is at 08:00:27:53:0c:ba
14	6.357679417	192.168.0.1	192.168.0.117	NBNS	92	Name query NBSTAT *<00-c0-00-00-00-00-c0-00-00-00-00-00-00-00-00-00-00>
15	6.357774569	192.168.0.117	192.168.0.1	ICMP	120	Destination unreachable (Port unreachable)
16	6.895109955	HenHuip-c5:95:87	Broadcast	ARP	60	Who has 192.168.0.108? Tell 192.168.0.108
17	6.954644116	TP-Link-be:2d:e4	Broadcast	ARP	60	Who has 192.168.0.108? Tell 192.168.0.1
18	6.960146978	TP-Link-be:2d:e4	Broadcast	ARP	60	Who has 192.168.0.117? Tell 192.168.0.1
19	6.960169183	PcsCompu:53:9c:ba	TP-Link-be:2d:e4	ARP	42	192.168.0.117 is at 08:00:27:53:0c:ba
20	6.961461392	192.168.0.1	192.168.0.117	NBNS	92	Name query NBSTAT *<00-c0-00-00-00-00-c0-00-00-00-00-00-00-00-00-00-00>
21	6.961468074	192.168.0.1	192.168.0.1	ICMP	90	Destination unreachable (Port unreachable)
22	8.285330342	Fe80::4a22:54ff:feb...	Ff02::16	ICMPv6	110	Router Advertisement from 48:22:54:be:2d:e4
23	8.297127262	Fe80::2960:68d1:5e5...	Ff02::16	ICMPv6	110	Multicast Listener Renor. Messaage v2

Frame 13: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0

Ethernet II, Src: PcsCompu:53:9c:ba (08:00:27:53:0c:ba), Dst: TP-Link-be:2d:e4 (48:22:54:be:2d:e4)

Address Resolution Protocol (reply)

0000	0010	0020	0030	0040	0050	0060	0070	0080	0090	00A0	00B0	00C0	00D0	00E0	00F0
48	22	54	be	2d	e4	08	00	27	53	0c	ba	08	00	60	01
27	53	0c	ba	08	00	00	00	27	53	0c	ba	08	00	a8	75
0020	48	22	54	be	2d	e4	c0	a8	00	00	01				

H'T'-----S-----

H'T'-----

I monitored my home network using Wireshark, but not at all finding any malicious activity in my network, there are only connectivity round router and device and also some request from my device which are not malicious request or any malicious response.