CODING SAMURAI

CODING YOUR ASCENT: LEARN. CODE. UPSKILL

Internship in

Cyber Security

Home Network Security Audit(Task II)

Submitted by

AVIJIT DAS

Batch E

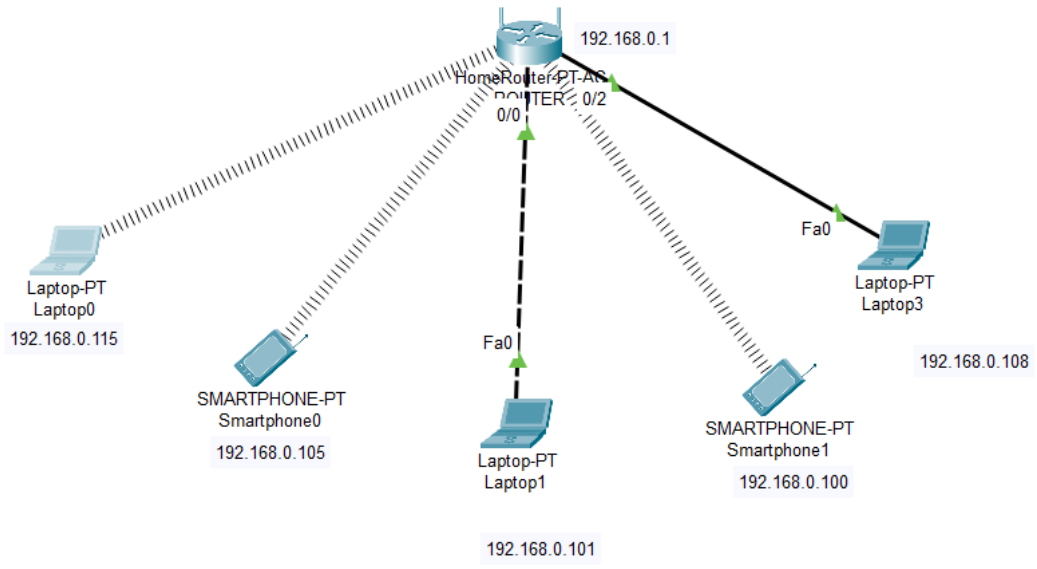
SEP 24 – OCT 22

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)-[/home/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:

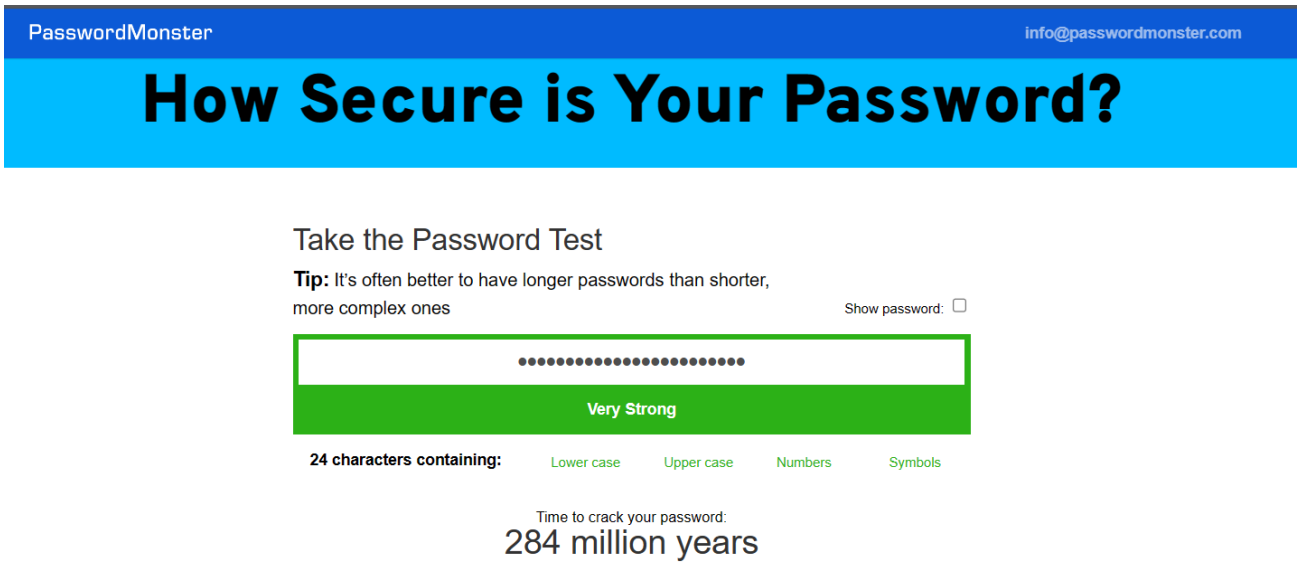
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -Pn 192.168.0.1
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-18 00:22 IST
Nmap scan report for 192.168.0.1
Host is up (0.0072s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE    SERVICE VERSION
23/tcp   filtered telnet
80/tcp   open     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)
```

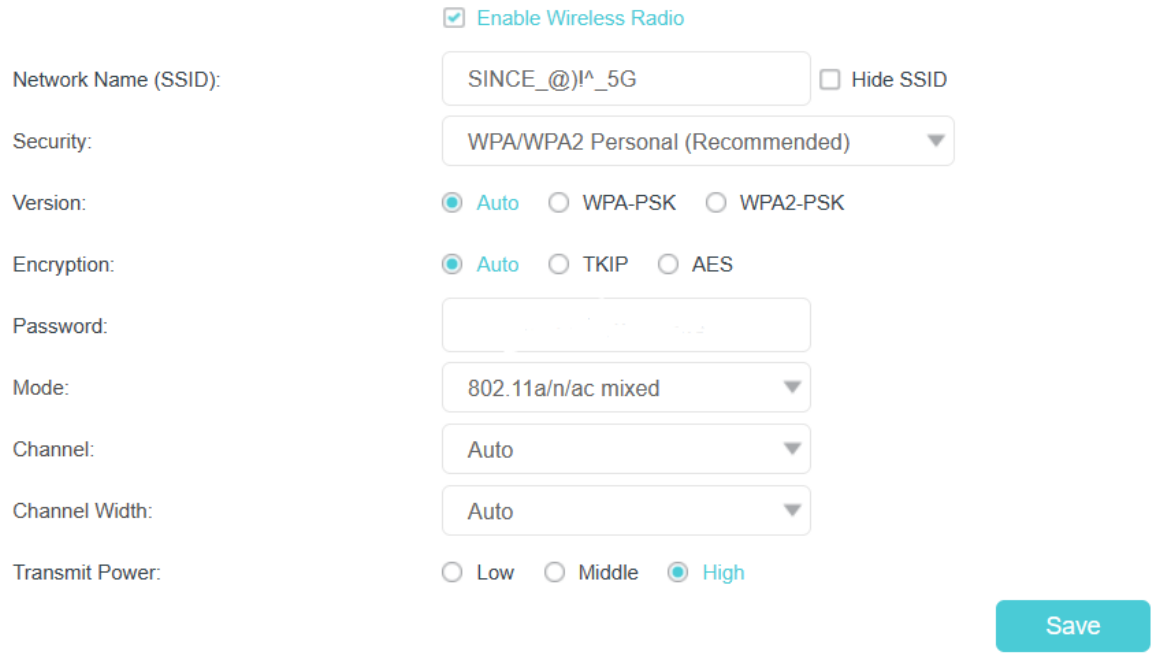
I checked all my device which are connected to my home router. I didn't find any vulnerabilities, all port which are open using updated version of services which cannot be hacked till day.

Password Audit:



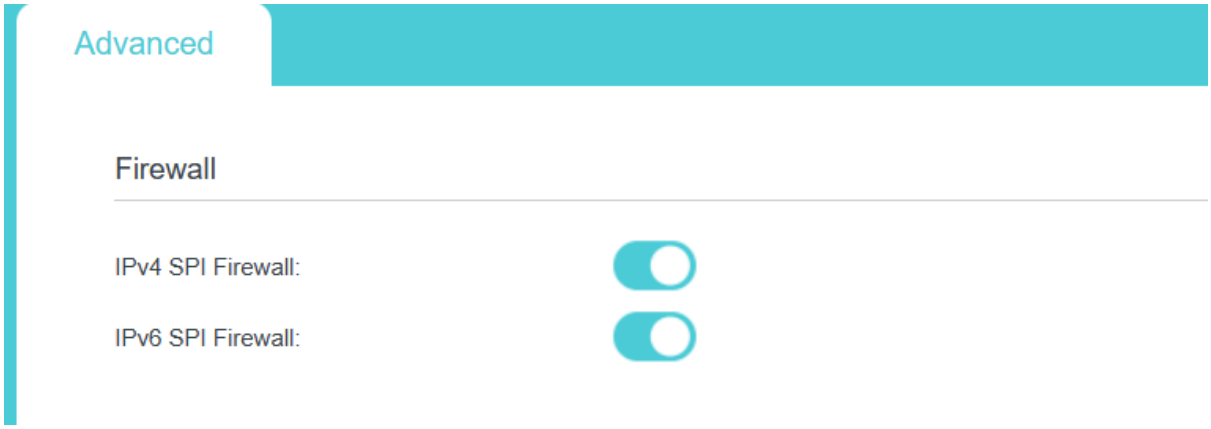
This is my router's password strength, it might be hacked but it will take 284 million years.

Router Security:



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:

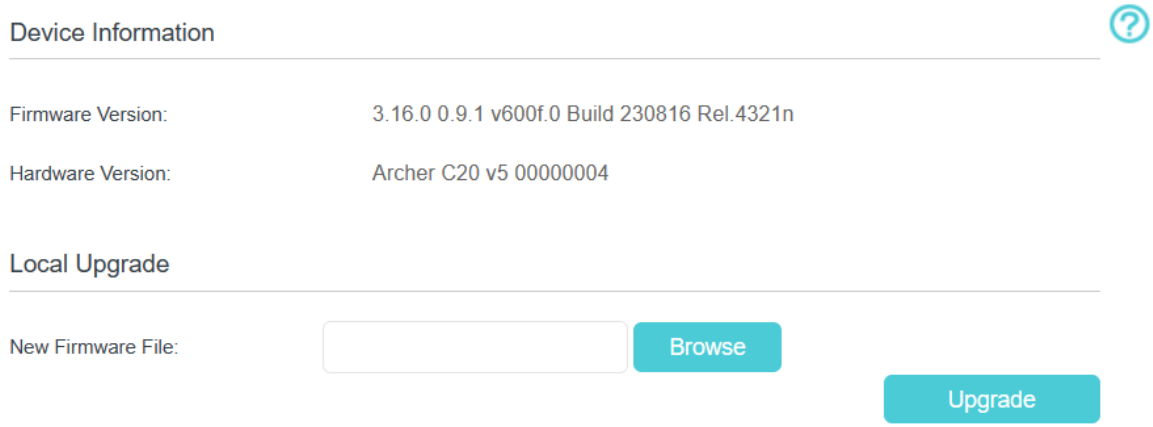


All firewalls are active mode to check the traffic and prevent the malicious attack.

Guest Network:

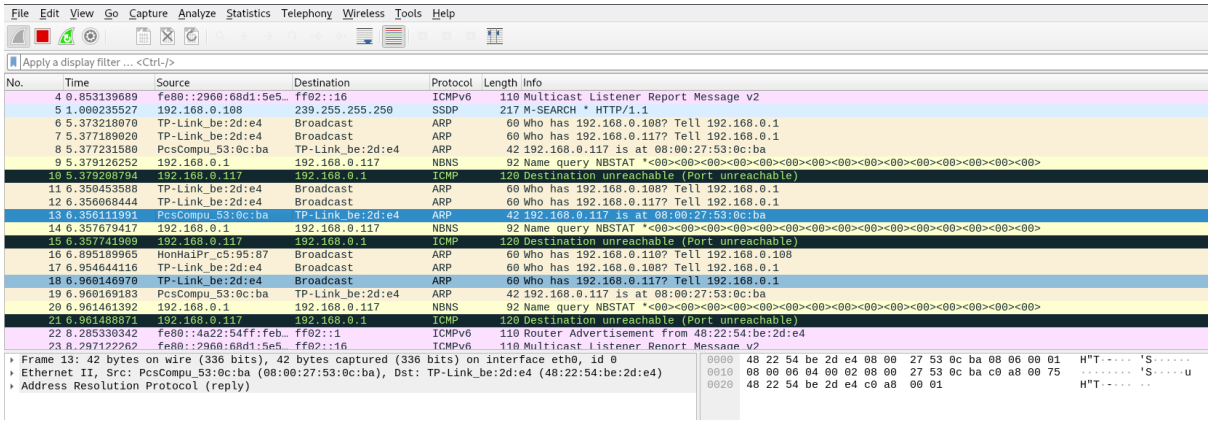
In our Router guest network option are not available, so I can't set any isolated guest network separated from main network.

Device Patching:



This is the latest updated version of firmware, No updates came after this version.

Network Monitoring:



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.