Network Security Audit Report

Security Scope & Intent

The purpose of this network audit is to evaluate the security of my local area network (LAN) and the host laptop. The audit aims to identify potential vulnerabilities, improve network security, assess devices connected to the network, and ensure that the host laptop is configured securely to prevent unauthorized access or data leaks.

Objectives:

1. **Identify potentially unsafe or unauthorized devices** – Catalog all devices connected to the local network, classify them by type, and verify that only trusted devices have access to the gateway. Detect and flag any unauthorized or suspicious connections.

2. **Evaluate and improve overall network security –** includes reviewing and strengthening router administration settings, verifying Wi-Fi encryption standards (e.g. WPA2/WPA3), assessing SSID configuration, evaluating password practices for both the wireless network & router, reviewing WAN port exposure, and conducting a physical assessment of network devices for potential vulnerabilities.

3. **Assess the security of the host laptop** – Review open ports, and system defences of the primary endpoint to identify vulnerabilities to the device. Strength protection to reduce its risk as an entry point into the network.

4. **Prepare for potential security incidents** – Develop procedures for responding to detected threats, ensuring the network can be recovered quickly and securely.

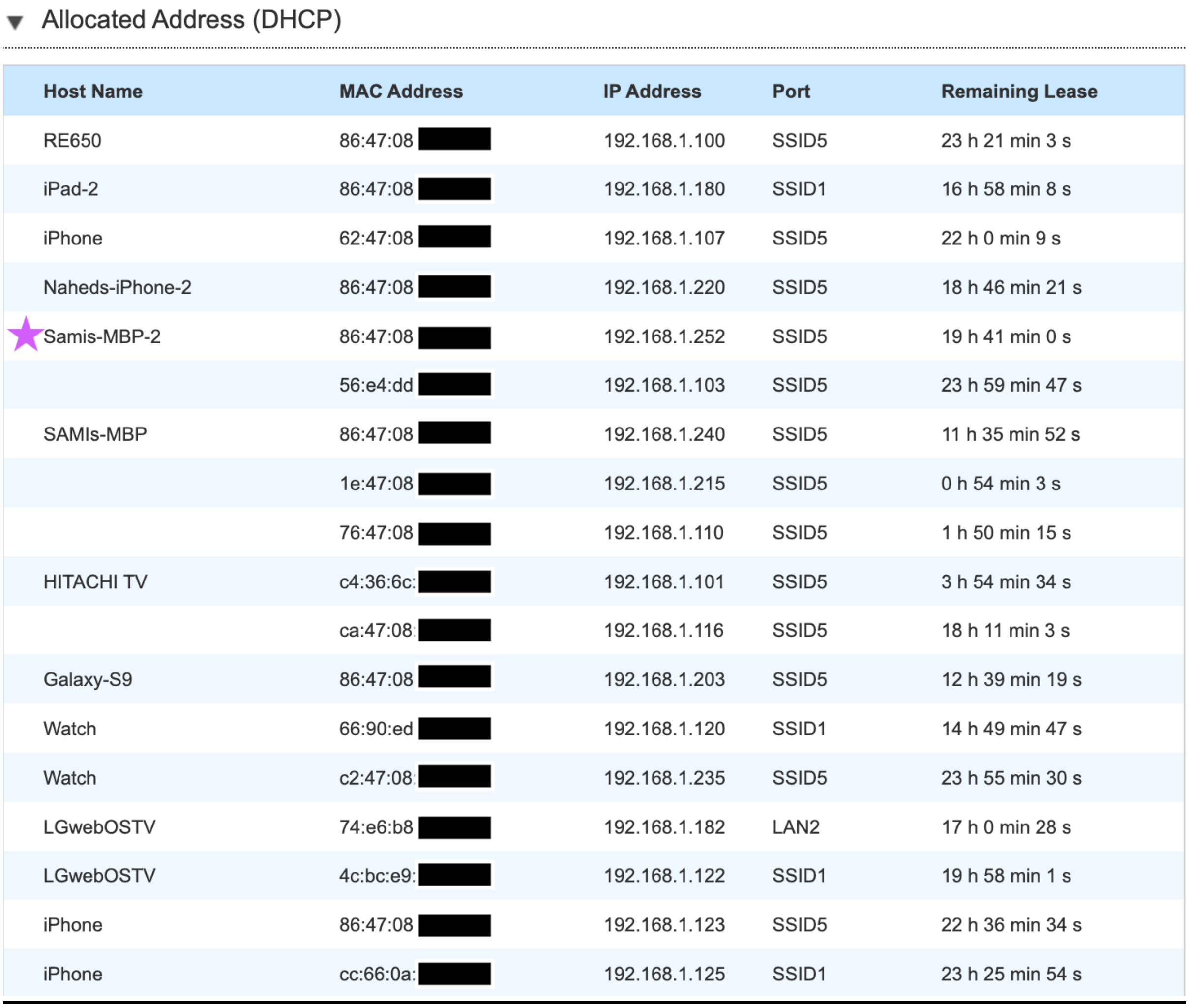
5. **Provide actionable recommendations** to enhance both immediate and long-term security for the network and connected devices.

Approach

This audit is conducted from the host laptop operating MacOS using terminal-based (CLI with Bash) tools to identify connected devices, review open ports and assess administrative configurations. Results are cross-checked against best practices to reduce risk.

DHCP leases in this environment are configured with a 24-hour renewal cycle, which means that the IP addresses change throughout this audit. For accuracy, host admin IP may be updated throughout the audit.

Via DHCP Configuration, there are 18 hosts according to gateway admin information:



▼ Allocated Address (DHCP)

Host Name	MAC Address	IP Address	Port	Remaining Lease
RE650	86:47:08 [redacted]	192.168.1.100	SSID5	23 h 21 min 3 s
iPad-2	86:47:08 [redacted]	192.168.1.180	SSID1	16 h 58 min 8 s
iPhone	62:47:08 [redacted]	192.168.1.107	SSID5	22 h 0 min 9 s
Naheds-iPhone-2	86:47:08 [redacted]	192.168.1.220	SSID5	18 h 46 min 21 s
★ Samis-MBP-2	86:47:08 [redacted]	192.168.1.252	SSID5	19 h 41 min 0 s
	56:e4:dd [redacted]	192.168.1.103	SSID5	23 h 59 min 47 s
SAMIs-MBP	86:47:08 [redacted]	192.168.1.240	SSID5	11 h 35 min 52 s
	1e:47:08 [redacted]	192.168.1.215	SSID5	0 h 54 min 3 s
	76:47:08 [redacted]	192.168.1.110	SSID5	1 h 50 min 15 s
HITACHI TV	c4:36:6c: [redacted]	192.168.1.101	SSID5	3 h 54 min 34 s
	ca:47:08 [redacted]	192.168.1.116	SSID5	18 h 11 min 3 s
Galaxy-S9	86:47:08 [redacted]	192.168.1.203	SSID5	12 h 39 min 19 s
Watch	66:90:ed [redacted]	192.168.1.120	SSID1	14 h 49 min 47 s
Watch	c2:47:08 [redacted]	192.168.1.235	SSID5	23 h 55 min 30 s
LGwebOSTV	74:e6:b8 [redacted]	192.168.1.182	LAN2	17 h 0 min 28 s
LGwebOSTV	4c:bc:e9: [redacted]	192.168.1.122	SSID1	19 h 58 min 1 s
iPhone	86:47:08 [redacted]	192.168.1.123	SSID5	22 h 36 min 34 s
iPhone	cc:66:0a: [redacted]	192.168.1.125	SSID1	23 h 25 min 54 s

1.0 Identify Potentially Unsafe/Unauthorized Devices

1.1 Identify host laptops private IPv4 & MAC address

Command:

```
ipconfig getifaddr en0
```

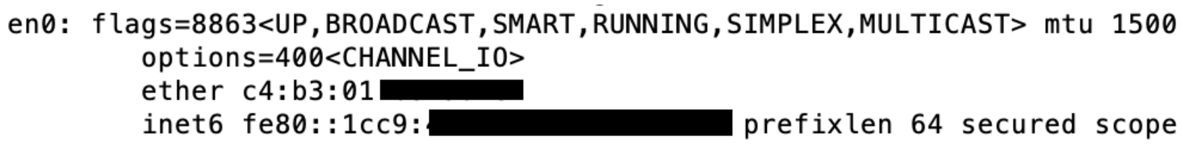
Output:

```
192.168.1.252
```

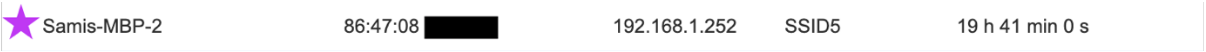
Command:

```
ifconfig
```

Output:



```
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=400<CHANNEL_IO>
        ether c4:b3:01[redacted]
        inet6 fe80::1cc9:[redacted] prefixlen 64 secured scope
```



★ Samis-MBP-2   86:47:08[redacted]   192.168.1.252   SSID5   19 h 41 min 0 s

Results:

Host laptop is cross identified with DHCP table as **IPV4 192.168.1.252** with host name **SAMI's-MBP-2** and **MAC 86:47:08** identified with a purple star.

Modern operating systems (including macOS, iOS, windows, Linux etc) often randomize the MAC address when connecting to the Wi-Fi network. This explains the difference observed between the MAC address listed in the DHCP table and the physical MAC address of the en0 Wi-Fi interface which is shown above.

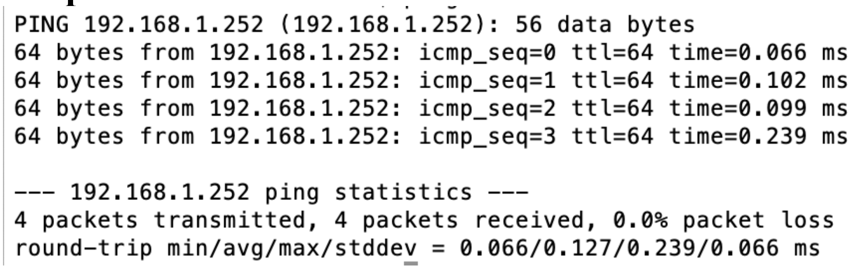
1.2 Connectivity Test on Host Laptop (ICMP Ping)

Pinging the host laptop. Failure could indicate misconfigured IP settings/blocked ICMP traffic or could indicate the host laptop may have issues communicating within the network.

Command:

```
ping -c 4 192.168.1.252
```

Output:



```
PING 192.168.1.252 (192.168.1.252): 56 data bytes
64 bytes from 192.168.1.252: icmp_seq=0 ttl=64 time=0.066 ms
64 bytes from 192.168.1.252: icmp_seq=1 ttl=64 time=0.102 ms
64 bytes from 192.168.1.252: icmp_seq=2 ttl=64 time=0.099 ms
64 bytes from 192.168.1.252: icmp_seq=3 ttl=64 time=0.239 ms

--- 192.168.1.252 ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.066/0.127/0.239/0.066 ms
```

Result: Replies successful 4/4 packets received.

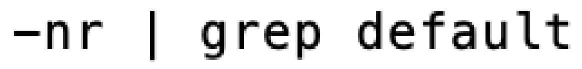
Conclusion:

- Wi-Fi interface (en0) NIC is configured correctly with IP address assigned by DHCP server.
- ICMP stack is functioning correctly.
- OS is able to reply to ICMP.

1.3 Pinging Default Gateway (ICMP Ping)

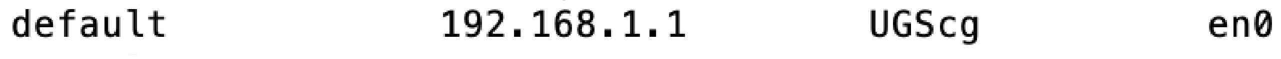
The default gateway (router) was pinged to confirm Gateway IP address & gateway availability and establish LAN connectivity

Command:



```
-nr | grep default
```

Output:



```
default                 192.168.1.1         UGScg           en0
```

We confirmed default gateway's IP address as 192.168.1.1

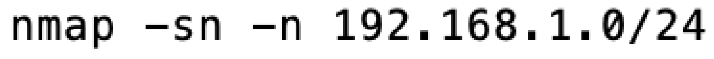
- ☑ Functioning TCP/IP stack functionality

- ☑ Verified connectivity and response form the network router

IMPORTANT
 The ethernet interface (eth1) was not tested with ICMP as the active connection for this audit is Wi-Fi, not wired. The Ethernet interface (eth1) is working and functioning correctly.

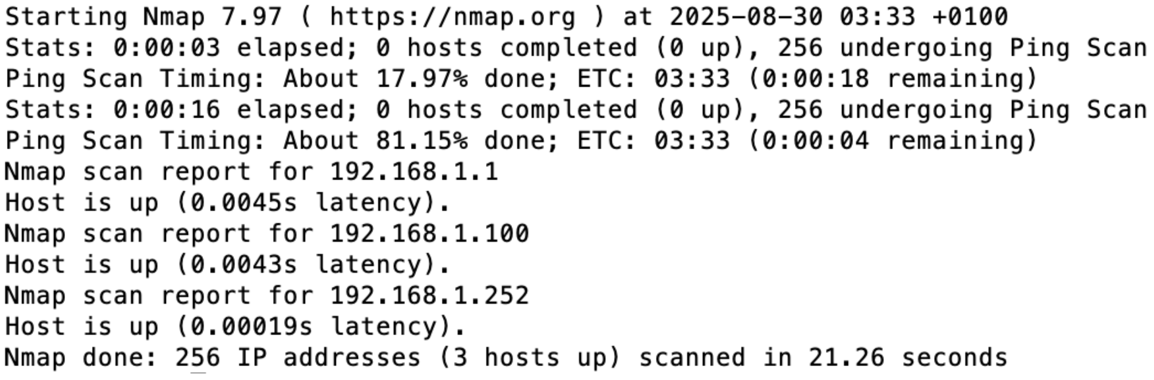
1.4 NMAP Host Discovery Scan (no DHS resolution)

This scan does an ARP ping sweep, which provides a list of all currently active devices that responded in the local network.



```
nmap -sn -n 192.168.1.0/24
```

Output:



```
Starting Nmap 7.97 ( https://nmap.org ) at 2025-08-30 03:33 +0100
Stats: 0:00:03 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Ping Scan Timing: About 17.97% done; ETC: 03:33 (0:00:18 remaining)
Stats: 0:00:16 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Ping Scan Timing: About 81.15% done; ETC: 03:33 (0:00:04 remaining)
Nmap scan report for 192.168.1.1
Host is up (0.0045s latency).
Nmap scan report for 192.168.1.100
Host is up (0.0043s latency).
Nmap scan report for 192.168.1.252
Host is up (0.00019s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 21.26 seconds
```

Result:
Scan suggest there are only 3 currently active devices on the network. Cross identified with DHCP to see the host names of the devices.

Identified devices:

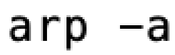
1) 192.168.1.1 ➔ Default Gateway (Router)
2) 192.168.1.100 ➔ RE650 (Host name)
3) 192.252 ➔ Samis-MBP-2 (Host admin Laptop), also identified previously in the audit referenced in Section 1.1

- ☑ Authorised devices are connected to the network
- ☑ 3/18 devices are alive in the network

1.5. ARP Cache Scan on host admin laptop

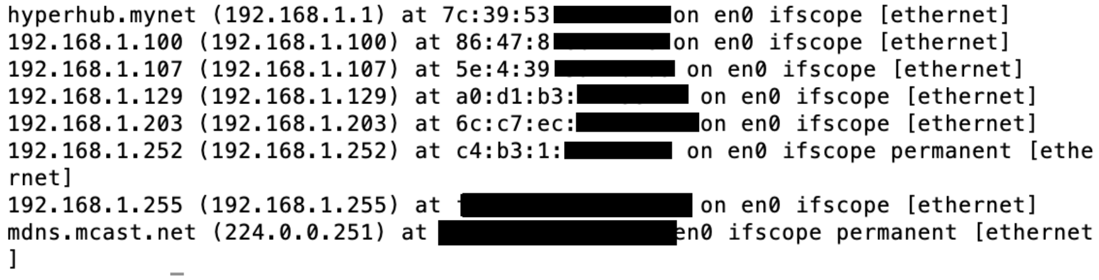
This scan examines the host's laptop ARP cache, which stores recently used IP-to-MAC address mappings for devices the host has communicated with. Performing this scan, can give us insight with what devices the host laptop has been communicating with. Any malicious devices or unauthorized devices communicating with the host may be identified through this scan.

Command:



```
arp -a
```

Output:



```
hyperhub.mynet (192.168.1.1) at 7c:39:53[redacted]on en0 ifscope [ethernet]
192.168.1.100 (192.168.1.100) at 86:47:8[redacted]on en0 ifscope [ethernet]
192.168.1.107 (192.168.1.107) at 5e:4:39[redacted] on en0 ifscope [ethernet]
192.168.1.129 (192.168.1.129) at a0:d1:b3:[redacted] on en0 ifscope [ethernet]
192.168.1.203 (192.168.1.203) at 6c:c7:ec:[redacted]on en0 ifscope [ethernet]
192.168.1.252 (192.168.1.252) at c4:b3:1:[redacted] on en0 ifscope permanent [ethe
rnet]
192.168.1.255 (192.168.1.255) at [redacted] on en0 ifscope [ethernet]
mdns.mcast.net (224.0.0.251) at [redacted]n0 ifscope permanent [ethernet
]
```

Results:

6 devices including the default gateway are saved in the ARP cache. Ip address 192.168.1.255 is broadcasting IP address, so this entry can be excluded as this does not represent an actual device. Similarly, mdns.mcast.net is a multicast MAC and is not a unique device, so it is also excluded from analysis.

DHCP table referenced in the beginning of the audit is used to cross identify the devices with their host names. A tick verifies the device has been crossed checked with DHCP table as safe.

1) 192.168.1.1 MAC: 7c:39:53➔ Default Gateway (router) ☑
2) 192.168.1.100 MAC: 86:47:08➔ RE650 ☑
3) 192.168.1.107 MAC: 5e:4:39➔ Unidentified device ❓
4) 192.168.1.129 MAC: a0:d1:b3➔ Unidentified device❓
5) 192.168.1.203 MAC: 6c:c7:ec➔ Unidentified device ❓
6) 192.168.252 MAC: c4:b3:1 ➔ Samis-MBP-2 (Host Laptop) ☑

3/6 Devices are identified by host names via DHCP. Verifying these devices as **SAFE and low risk.**

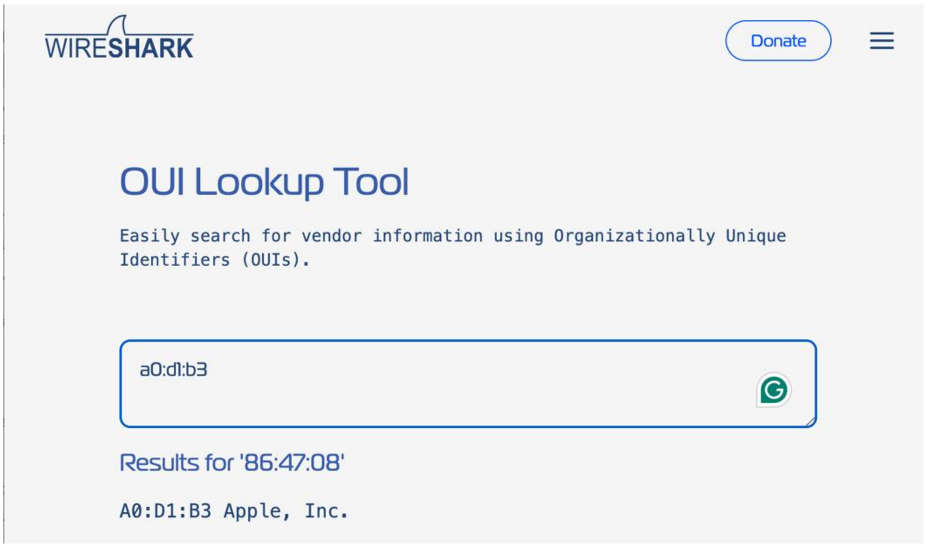
Device 3 (192.168.1.107, MAC: 5e:4:39) and **device 5** (192.168.1.203, MAC 6c:c7:ec) were not visible in the DHCP table at the time of scanning and did not appear in host discovery scan in section 1.4. Initially they appeared as unidentified in the ARP cache.

Device 3 & **device 5** were then physically located within the network and turned on manually for verification. Their MAC addresses were verified, confirming them as **legitimate and safe devices.**

Device 4 was not found among the physically verified devices on the network at the time of inspection. As a result, further investigation was carried out into the device to assess its legitimacy and confirm whether it poses any risk.

1.5.1**⚠ Investigating unidentified device 4 192.168.1.129 with MAC a0:d1:b3:xx:xx:xx**

1. Perform a **MAC OUI lookup** to identify vendor/manufacturer of device. Using first 6 digits of MAC address, an OUI lookup was performed. Results suggests this MAC corresponds to an Apple, Inc device.



OUI Lookup Tool

Easily search for vendor information using Organizationally Unique Identifiers (OUIs).

a0:d1:b3

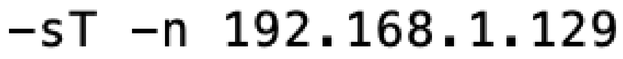
Results for '86:47:08'

A0:D1:B3 Apple, Inc.

Based on the MAC vendor, the device is likely to be an apple product such as an iPhone or a MacBook. This is only a preliminary identification and will be verified in the next steps.

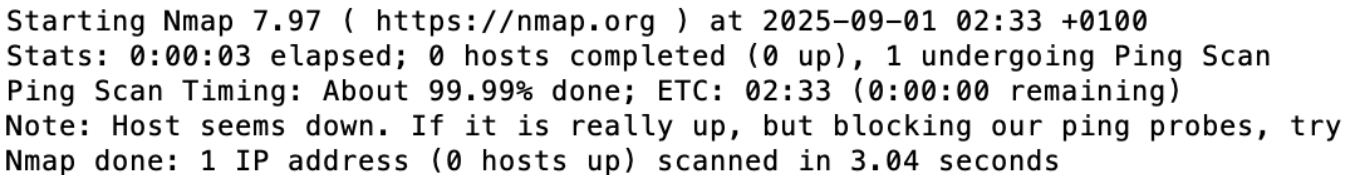
1.5.2 Port Scan of Unidentified device (192.168.1.129), top 1000 ports

Command:



```
-sT -n 192.168.1.129
```

Output:



```
Starting Nmap 7.97 ( https://nmap.org ) at 2025-09-01 02:33 +0100
Stats: 0:00:03 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Ping Scan Timing: About 99.99% done; ETC: 02:33 (0:00:00 remaining)
Note: Host seems down. If it is really up, but blocking our ping probes, try
Nmap done: 1 IP address (0 hosts up) scanned in 3.04 seconds
```

Results:

- Unidentified device with IP 192.168.1.129 (recorded in ARP cache) did not respond to ICMP echo requests or TCP/UDP port scans at the time of testing.

- No ports were identified during this scan.

Conclusion:

- The device was either powered off, or disconnected from the network, or configured not to respond to scans.

- No active network exposure was observed at the time,

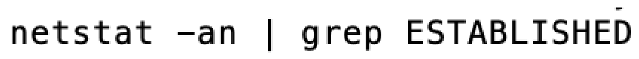
- Device is labelled **LOW RISK** as it’s not a danger to any devices currently.

Vulnerability ⚠
Due to MAC address randomization implemented by modern operating systems, the MAC addresses observed in the ARP ache may not always match the static entries in the DHCP table. Reducing the reliability of cross-identifying devices by IP-MAC bindings. Long term monitoring within the LAN can become more difficult, potentially creating blind spots for asset management.

1.6 Local enumeration of active TCP connections on host admin laptop

A TCP scan was performed on the host to verify no unnecessary or sensitive services were listening on open ports and to ensure no confidential information was being transmitted to devices on the network that could be attempting IP spoofing.

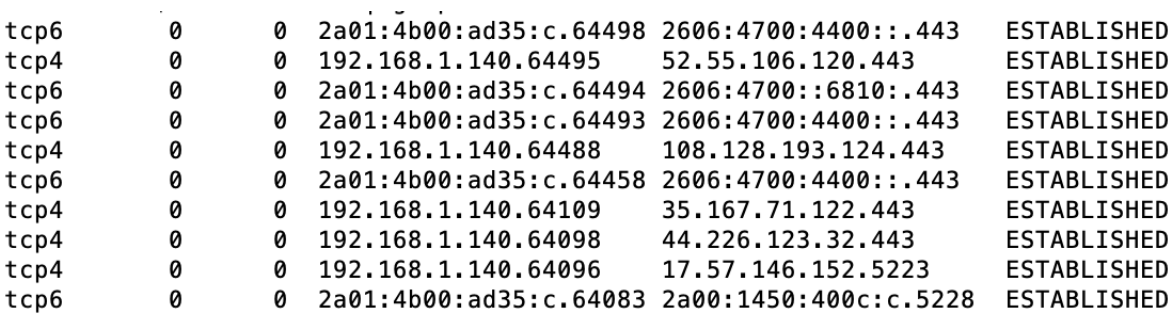
Command:



```
netstat -an | grep ESTABLISHED
```

Output:

Total of 10 connections are made at the time of the scan with the host admin laptop.



```
tcp6       0      0  2a01:4b00:ad35:c.64498 2606:4700:4400::.443   ESTABLISHED
tcp4       0      0  192.168.1.140.64495    52.55.106.120.443      ESTABLISHED
tcp6       0      0  2a01:4b00:ad35:c.64494 2606:4700::6810:.443   ESTABLISHED
tcp6       0      0  2a01:4b00:ad35:c.64493 2606:4700:4400::.443   ESTABLISHED
tcp4       0      0  192.168.1.140.64488    108.128.193.124.443    ESTABLISHED
tcp6       0      0  2a01:4b00:ad35:c.64458 2606:4700:4400::.443   ESTABLISHED
tcp4       0      0  192.168.1.140.64109    35.167.71.122.443      ESTABLISHED
tcp4       0      0  192.168.1.140.64098    44.226.123.32.443      ESTABLISHED
tcp4       0      0  192.168.1.140.64096    17.57.146.152.5223     ESTABLISHED
tcp6       0      0  2a01:4b00:ad35:c.64083 2a00:1450:400c:c.5228  ESTABLISHED
```

- ☑ 8/10 connections are on port 443 (HTTPS) which are safe, standard encrypted web traffic

- ☑ 1 Connection on port 5223 which is used for Apple services (apple.com)

- ☑ 1 Connection on port 5228 which is used for traffic on Google services (google.com)

1.6.1 Further verification of TCP IP addresses Connected to the Host Laptop

1. DNS verification:

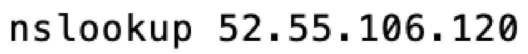
- Use of “nslookup” command on each IP to confirm the associated domain name.
- This ensures the IP is linked to a known entity and that no sensitive data is being share with unverified addresses.

2. **Reputation Check (If no PTR record**)

- If “nslookup” returns no PTR record, the IP is further verified using AbuseIPDB to confirm its not reported for malicious activity.

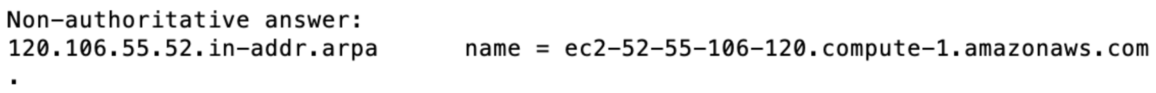
Example below shows a DNS reverse lookup of the 2nd TCP connection & IP check on abuseIPDB; all other IP’s are checked in the same manner.

Command:



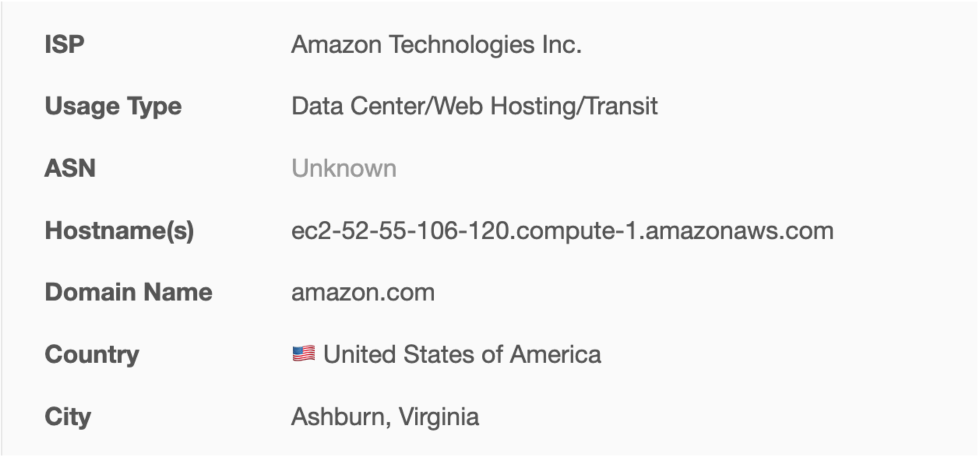
```
nslookup 52.55.106.120
```

Output:



```
Non-authoritative answer:
120.106.55.52.in-addr.arpa      name = ec2-52-55-106-120.compute-1.amazonaws.com
.
```

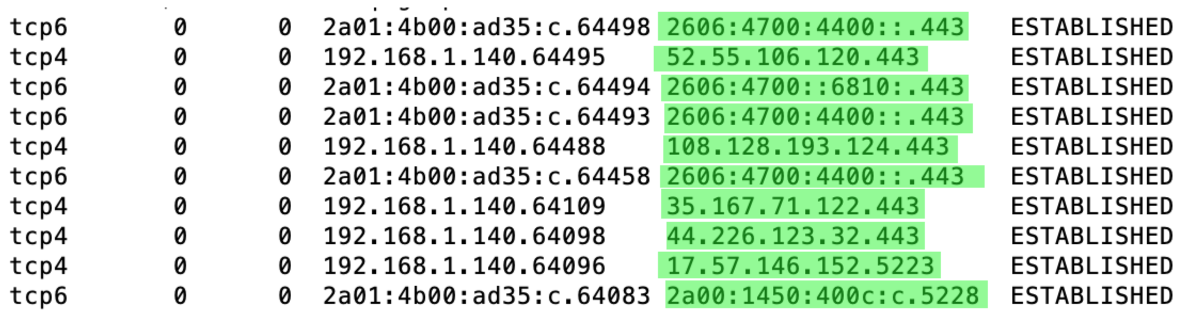
Reputation checks via AbuseIPDB:



ISP	Amazon Technologies Inc.
Usage Type	Data Center/Web Hosting/Transit
ASN	Unknown
Hostname(s)	ec2-52-55-106-120.compute-1.amazonaws.com
Domain Name	amazon.com
Country	🇺🇸 United States of America
City	Ashburn, Virginia

SAFE - 2nd connection with IPv4 52.55.106.120 is confirmed to be Amazonaws.com, with their EC2 instance hostname ec2-52-55-106-120.compute-1.amazonaws.com

The screenshot below shows all IPv4 and IPv6 addresses connected to the host laptop, green indicators mark IP's that have been verified as safe, through DNS reverse lookups and necessary reputation checks via AbuseIPDB.



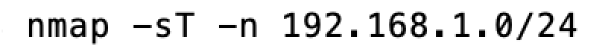
```
tcp6       0      0  2a01:4b00:ad35:c.64498  2606:4700:4400::.443    ESTABLISHED
tcp4       0      0  192.168.1.140.64495     52.55.106.120.443       ESTABLISHED
tcp6       0      0  2a01:4b00:ad35:c.64494  2606:4700::6810:.443    ESTABLISHED
tcp6       0      0  2a01:4b00:ad35:c.64493  2606:4700:4400::.443    ESTABLISHED
tcp4       0      0  192.168.1.140.64488     108.128.193.124.443     ESTABLISHED
tcp6       0      0  2a01:4b00:ad35:c.64458  2606:4700:4400::.443    ESTABLISHED
tcp4       0      0  192.168.1.140.64109     35.167.71.122.443       ESTABLISHED
tcp4       0      0  192.168.1.140.64098     44.226.123.32.443       ESTABLISHED
tcp4       0      0  192.168.1.140.64096     17.57.146.152.5223      ESTABLISHED
tcp6       0      0  2a01:4b00:ad35:c.64083  2a00:1450:400c:c.5228   ESTABLISHED
```

All Established connections are confirmed to be SAFE.

1.7 TCP Port Scan of all LAN network devices

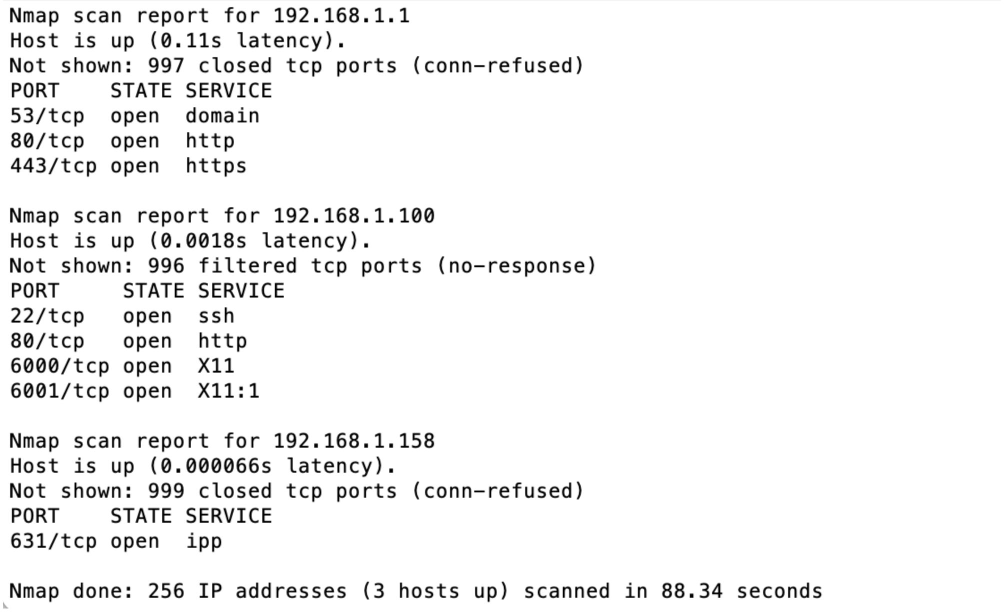
A TCP scan of all active devices on the network was conducted to identify each device and determine the services they are running. This helps us classify device types and verify that only trusted devices with DHCP assigned IP addresses are connected to the LAN.

Command:



```
nmap -sT -n 192.168.1.0/24
```

Output:



```
Nmap scan report for 192.168.1.1
Host is up (0.11s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT    STATE SERVICE
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https

Nmap scan report for 192.168.1.100
Host is up (0.0018s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
6000/tcp open  X11
6001/tcp open  X11:1

Nmap scan report for 192.168.1.158
Host is up (0.000066s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT    STATE SERVICE
631/tcp open  ipp

Nmap done: 256 IP addresses (3 hosts up) scanned in 88.34 seconds
```

Identified devices:

IP 192.168.1.1 ➔ Default Router
IP 192.168.1.100 ➔ RE650
IP 192.168.158 ➔ SAMI's-MBP-2 (NEW DHCP assigned IP address for Host laptop)

Router (192.168.1.1):
Port 53 (DNS) – used for domain name resolution safe ☑
Port 80 (HTTP) – standard web traffic, safe ☑
Port 443 (HTTPS) – secure web traffic, safe ☑

Device RE650 (192.168.1.100):
Port 22 (SSH) – used for secure remote management, safe ☑
Port 80 (HTTP) – standard web traffic, safe ☑
Port 6000 & 6001 – X11 graphical interface ports, safe on a local network☑

Host laptop (192.168.1.158):
Port 631 (IPP – printing) – used for printing services, safe for internal use ☑

All detected ports corresponding ports are considered safe within the secured internal network environment. No unusual or unauthorized ports were identified.

Objective 1 – Identify Potentially unsafe or unauthorized devices

Scans & Methods Conducted:

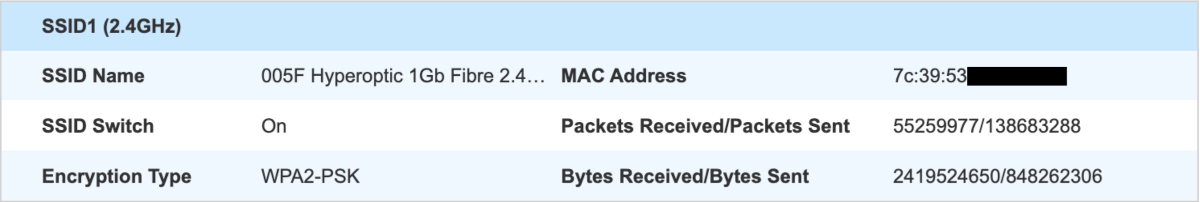
☑ 1.1 Host Laptop IP identification – Identifying Host Laptop
☑ 1.2 Connectivity Tests - on host laptop to confirm functioning in network
☑ 1.3 Pinging Default Gateway Scan
☑ 1.4 Host Discovery Scan – 3 active devices on network confirmed SAFE
☑ 1.5 ARP cache Scan – 5/6 devices in ARP cache confirmed SAFE, 1/6 device was unresponsive to scans, therefore labelled LOW RISK
☑ 1.6 TCP connection scan on Host laptop – returning all SAFE connections.

All DHCP assigned devices were verified as trusted household hardware. 3 devices were active at the time of scanning, 15 devices were offline, posing a low risk. One unidentified device was found in an ARP cache scan (Section1.5), which initially was thought to be a risk but later identified as an iPhone via OUI lookup and determined safe.

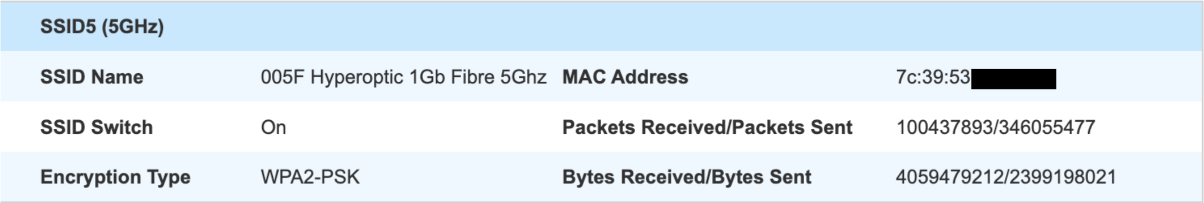
2.0 Evaluate & Improve Network Security

2.1 Network configuration review

2 SSID’s were identified within the local network: SSID 1 & SSID 5.



SSID1 (2.4GHz)			
SSID Name	005F Hyperoptic 1Gb Fibre 2.4…	MAC Address	7c:39:53[redacted]
SSID Switch	On	Packets Received/Packets Sent	55259977/138683288
Encryption Type	WPA2-PSK	Bytes Received/Bytes Sent	2419524650/848262306



SSID5 (5GHz)			
SSID Name	005F Hyperoptic 1Gb Fibre 5Ghz	MAC Address	7c:39:53[redacted]
SSID Switch	On	Packets Received/Packets Sent	100437893/346055477
Encryption Type	WPA2-PSK	Bytes Received/Bytes Sent	4059479212/2399198021

SSID 1 & SSID 5: Both networks are configured with **WPA2 encryption**, which is high level encryption to ensure confidentiality and integrity of data transmitted across the wireless network.

2.2 Main LAN Wi-Fi password & Router/Admin Account Password

The Wi-Fi password has been changed from the ISP-provided default to a unique, strong password. ISP-supplied defaults are often predictable or reused across customers.

- This reduces the risk of unauthorized access since ISP default passwords are often predictable.

- Using a randomly generated 8-12 password is used, reducing the risk of unauthorized access

2.2.1 Router/Admin Account Password

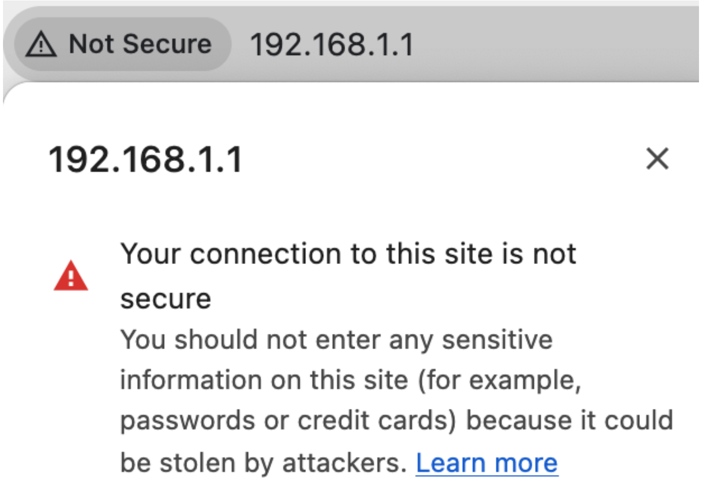
The router/admin account password was also changed from the default to protect router/ONT management interface. Weak password can result in a threat actor taking full control of the network and adjusting router configurations.

- Random generated 8-12 password is used, minimizing the risk of brute-force guessing.

- Strong unique credentials are important to prevent unauthorized access to router settings and network configurations.

Found Security Concern:

The router's administrative interface is only accessible via HTTP. Authentication credentials (username and password) are transmitted in plaintext over the network.



⚠ Not Secure 192.168.1.1

192.168.1.1 ×

Your connection to this site is not secure

You should not enter any sensitive information on this site (for example, passwords or credit cards) because it could be stolen by attackers. Learn more

Severity: High

Risk: HTTP does not use TLS/SSL encryption, any device connected to the network can intercept administrative credentials using packet-sniffing tools (e.g. Wireshark).
While WPA2 provides encryption between a client and the access point, this does not protect against devices already connected to the same network. As a result, the plaintext HTTP traffic can still be captured and read, rendering WPA2 ineffective in mitigating this risk. An attacker who gains access to the network could log into the router and gain full control of the network configuration.

Impact:

- Unauthorized access to router configurations
- Ability to modify DNS settings, potentially redirecting user traffic to malicious sites.
- Potential for network disruption or interception of traffic
- Risk increases if guest devices or untrusted users are present on the LAN

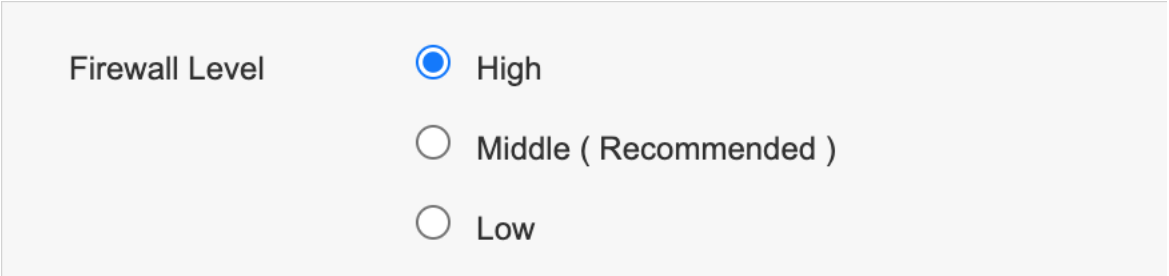
Recommendation:

- Enforce HTTPS for the router administrative interface
- Restrict access to router administrative interface (wired only access, IP allow list)
- Disable remote/WAN access to the admin interface unless strictly required (already configured in the extra's configuration section)

Adjusted configuration:
Remote administration from the WAN has been disabled. This reduces the chances of threat actors from the internet from adjusting the configurations within the LAN.

2.3 Network Firewall Configuration

The network provides three optional firewall levels. High being the most secure. At this level, the firewall offers strong protection against internet-based attacks, including attempts to access the router via its public IP.



Firewall Level

● High

○ Middle (Recommended)

○ Low

Firewall configured to the highest level suggesting:

- ☑ WAN ➔ LAN inbound traffic is blocked, preventing the internet from reaching the local networks' devices

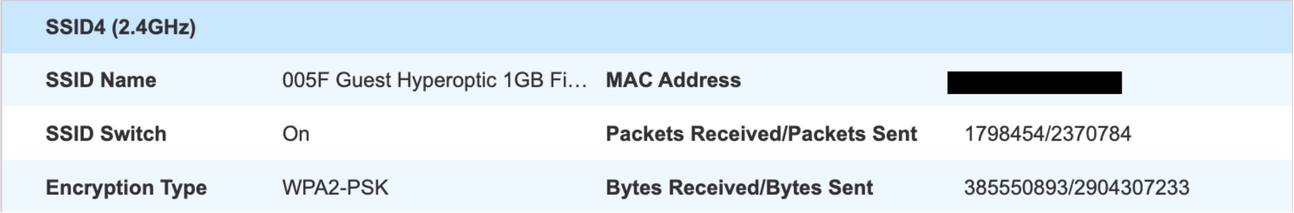
- ☑ WAN ➔ Router/device = No remote access from the internet unless explicitly allowed

- ☑ ICMP pings request from the internet are blocked, making the network less discoverable. Stopping threats from seeing if the router is functioning or not.

2.4 Guest Segmentation Network (SSID 5/ Guest Network)

A separate wireless network (Guest Segmentation Network) has been created for guests to prevent devices from accessing the main LAN. Guests

will be advised to join the Guest network to maintain security. In order to improve security and reduce the chances of threats gaining access to the main network.



SSID4 (2.4GHz)			
SSID Name	005F Guest Hyperoptic 1GB Fi...	**MAC Address**	[redacted]
SSID Switch	On	**Packets Received/Packets Sent**	1798454/2370784
Encryption Type	WPA2-PSK	**Bytes Received/Bytes Sent**	385550893/2904307233

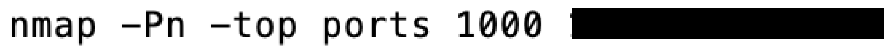
- ☑ Network Segmentation helps reduce the risk of unauthorized access and ensures the critical main LAN stays protected
- ☑ WPA2 level encryption
- ☑ 8+ character password for the Guest network (high security)
- ☑ SSID isolation, meaning device to device communication is blocked within the network. Devices won’t be able to ping each other over this network.
- ☑ Traffic is redirected into the guest network, reducing traffic in the main LAN

2.5 WAN Port Hardening/ Blocking Unnecessary Listening Ports

Routers often expose certain ports to the internet (WAN) for services such as HTTP (port 80), HTTPS (port 443), Telnet (port 23) or SSH (port 22). Any open administrative port accessible from the WAN represents a potential attack vector that could be exploited by attackers attempting to gain control of the router.

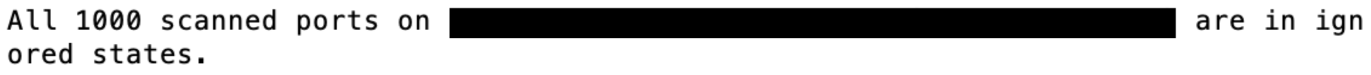
Public IP Port Scan: Perform a port scan of the routers Public IP address to identify any open/listening ports on the router which could be used as a potential attack surface.

Command:



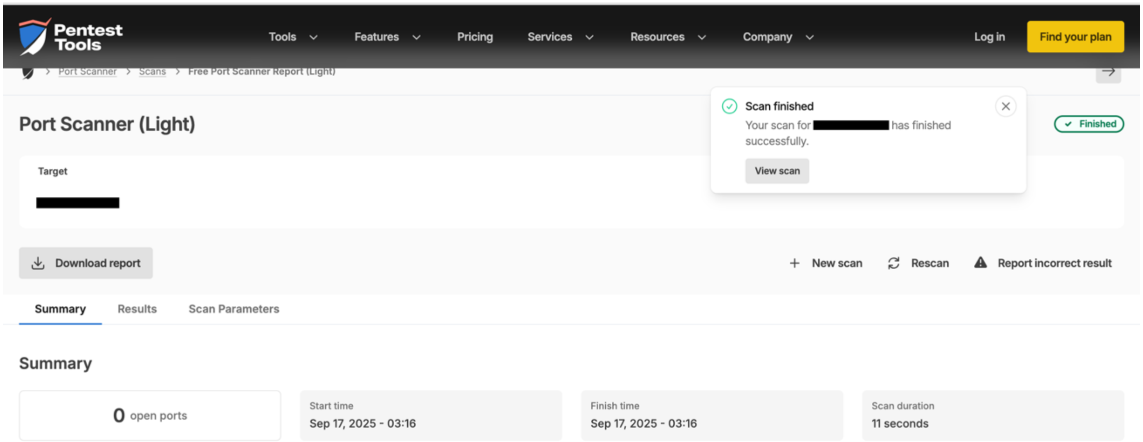
```
nmap -Pn -top ports 1000 [redacted]
```

Output:



```
All 1000 scanned ports on [redacted] are in ign
ored states.
```

The results of the router’s WAN port scan was also confirmed using a web-based port scanner, which likewise reported no open or exposed ports on the public IP.



Port Scanner > Scans > Free Port Scanner Report (Light)

Port Scanner (Light)

Target

[redacted]

Scan finished

Your scan for [redacted] has finished successfully.

Summary

0 open ports

Start time
Sep 17, 2025 - 03:16

Finish time
Sep 17, 2025 - 03:16

Scan duration
11 seconds

Interpretation:

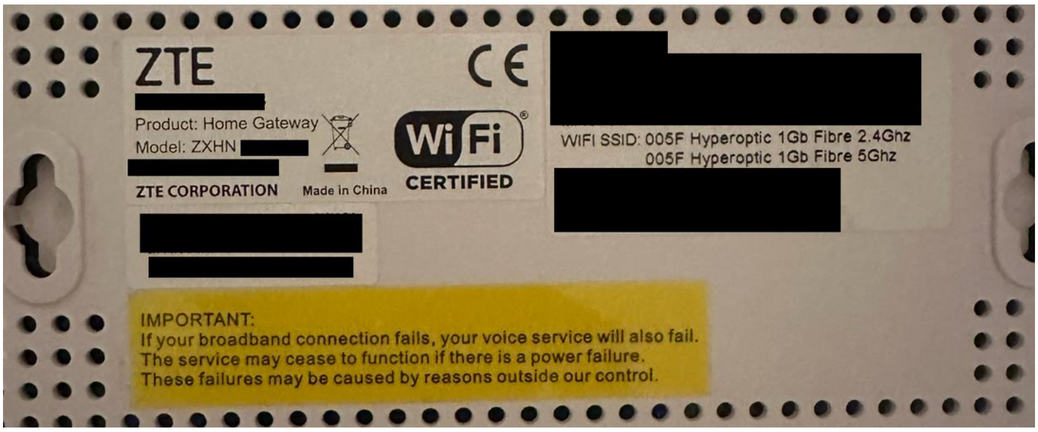
The scan results indicate that the ports are in ignored/filtered states. This implies the router’s firewall are configurated to effectively blocks external access to administrative ports, reducing potential attack services.

Physical Network Security Risks

2.6 Router Model Vulnerabilities

Vulnerability 1 – Outdated Firmware / Lack of Security Updates

The current ISP provided ZTE ZXHN-series router, while functional, this is an older model type and no longer receive frequent firmware or security updates.



ZTE

[redacted]

Product: Home Gateway

Model: ZXHN [redacted]

[redacted]

ZTE CORPORATION Made in China

[redacted]

WIFI SSID: 005F Hyperoptic 1Gb Fibre 2.4Ghz
005F Hyperoptic 1Gb Fibre 5Ghz

[redacted]

[redacted]

IMPORTANT:
If your broadband connection fails, your voice service will also fail.
The service may cease to function if there is a power failure.
These failures may be caused by reasons outside our control.

Risks:

- Attackers could exploit firmware vulnerabilities to gain administrative access.
- Increases risk of zero day or unpatched vulnerabilities and other unpatched security flaws

Vulnerability 2 – HTTP management interface & WPS feature

Risks:

- The router's management interface uses HTTP, meaning data (including credentials) is transmitted unencrypted and could be intercepted via packet sniffing.
- The router also supports WPS, which allows devices to connect using an 8-digit pin. Although hidden in the interface, the PIN exists internally and is vulnerable to brute-force attacks due to its shortened.
  ~ **11,000 maximum possible combinations** as the PIN consists of 7 digits plus a checksum, allowing potential unauthorized access to the Wi-Fi network.

Improvements:

- Request a new router model from the ISP that supports modern security protocols such as WPA3/HTTPS-secured management interfaces & no WPS option. The current device is several years old, and replacement should be treated as a high-priority action to reduce exposure to unpatched vulnerabilities.

2.7 ONT (Optical Network Terminal) Security

The ONT is the entry point for internet services into the premises and must be physically secured. If left exposed, an attacker could tamper with the connection, attempt to intercept traffic, or cause service disruption via a denial-of-service (DOS) attack.

[redacted]

ONT box must be secured in a secure area, or the network can be vulnerable to a full-service disruption if accessible to everyone.

Ensuring the CAT5 cable located in a secure area, mitigates the risk of entire network connectivity loss or tampering.

Ensuring the CAT5/CAT6 cable and ONT are located in a secure area, which mitigates the risk of entire network connectivity loss.

Objective 2 – Identify Potentially unsafe or unauthorized devices

Scans & Methods Conducted:

☑ 2.1 Network SSID's are identified with WPA2 encryption
☑ 2.2 Wi-Fi & Router admin interface password changed
☑ 2.3 Network Firewall configuration reviewed
☑ 2.4 Guest segmentation network created
☑ 2.5 WAN port hardening/blocking unnecessary ports
☑ 2.6 Router model vulnerabilities
☑ 2.7 ONT (Optical Network Terminal) security verified

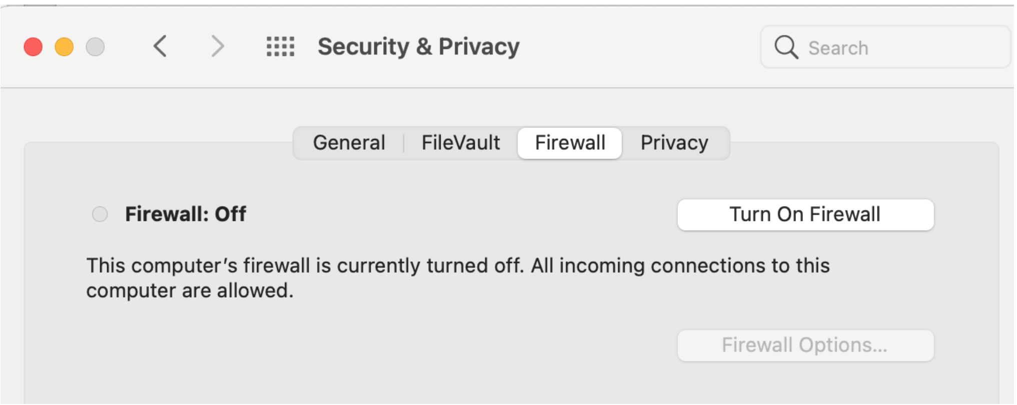
3.0 Access the Security of the Host Laptop

Objective: Evaluate the host laptop to identify potential vulnerabilities and strengthen defences to reduce its risk as an entry point into the network

3.1 Host Laptop Firewall assessment

The purpose of this assessment is to verify the status and effectiveness of the host laptop's built-in firewall. A properly configured host firewall helps protect the device from unsolicited inbound connections, including potential threats originating from other devices on the same network or compromised internal services.

Observations/Findings:



○ Firewall: Off

This computer's firewall is currently turned off. All incoming connections to this computer are allowed.

The host laptops’ firewall was initially turned off. This is a safety risk. As the firewall is necessary for filtering/blocking outbound and inbound connections.

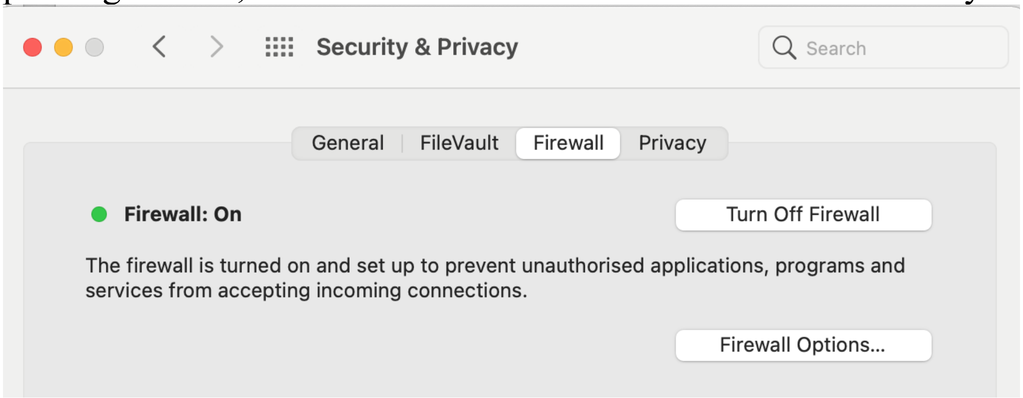
Impact/risk:

Without an active host firewall, unauthorized applications or devices on the LAN could attempt to connections to open ports. Increasing the risk of lateral attacks or malware infection.

Remediation:

The host firewall has now been enabled, providing protection by blocking unauthorized inbound connections.

Inbound connections are automatically blocked for all applications except the printing service, while outbound connections are not restricted by the firewall.



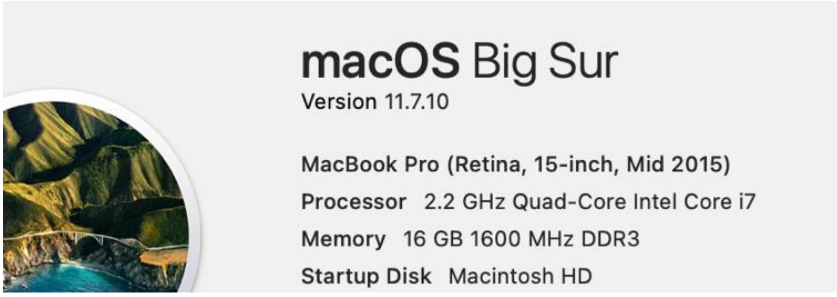
● Firewall: On

The firewall is turned on and set up to prevent unauthorised applications, programs and services from accepting incoming connections.

3.2 Review System & OS updates

Ensuring the host laptop’s operating system and applications are up to date with the latest security patches to reduce potential vulnerabilities and protect against malicious actors

Observations/Findings:



macOS Big Sur
Version 11.7.10

MacBook Pro (Retina, 15-inch, Mid 2015)
Processor 2.2 GHz Quad-Core Intel Core i7
Memory 16 GB 1600 MHz DDR3
Startup Disk Macintosh HD

- Host laptop is currently running macOS 11.7.10 (Big Sur)

- This version is outdated and lacks security patches, leaving the system vulnerable to exploits
- Keeping the OS up to date is essential to maintain security

Impact / Risk:

An outdated operating system are common targets for attackers, as they may contain known vulnerabilities. Unpatched systems can act as entry points into the network, potentially compromising sensitive data.

Recommendation:

- **Immediate macOS update on host laptop,** to the latest stable macOS version (macOS 15.6.1 Sequoia) to ensure all security patches and fixes are applied.
- Enabling automatic updates where possible to maintain ongoing protection.

3.3 Host Anti-virus Assessment

Purpose:

To evaluate whether the host laptop has effective antivirus protection in place to defend malware and other malicious software. As part of this assessment, an antivirus scan will be conducted to check if any malware or viruses are present on the host laptop.

Observations / Finding:

- The host laptop initially did not have any third-party antivirus installed.
- MacOS provides built in security features (XProtect, Gatekeeper, System Integrity Protection) that offer baseline protection, but these are not comprehensive against all forms of malware.

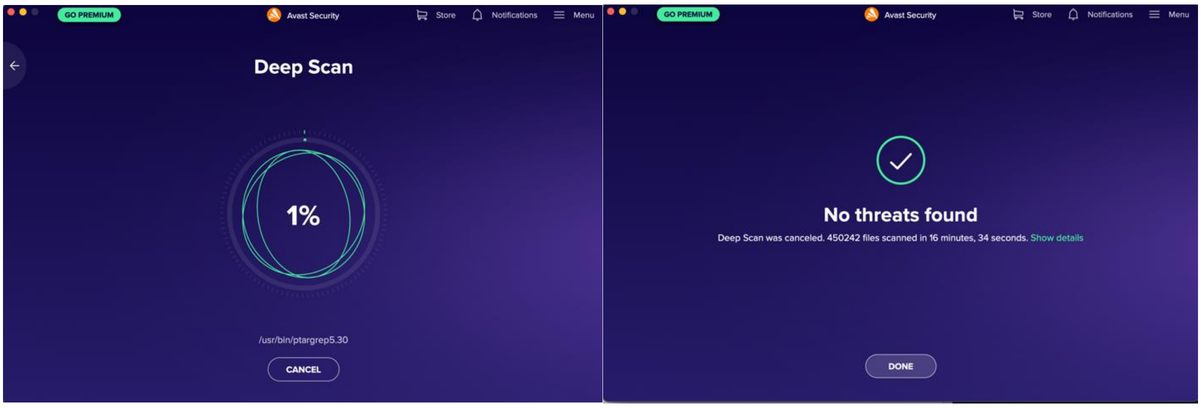
Impact / Risk:

Without dedicated antivirus software, the laptop would rely only on macOS's built in protections, leaving it more vulnerable to advanced or newly emerging threats. This increases the risk of malware infections, ransomware, or unauthorized applications running on the device.

Remediation:

Avast Security antivirus software was installed and is being used for real-time protection. In addition, a full/deep virus scan using Avast Security was conducted. Regular scans and automatic updates have been enabled to maintain ongoing protections.

Deep scan: Comprehensive scan which checks all files/folders, directories, hidden files, background processes, external drives. Any areas of the disk where malware may try to hide.



No threats found

Deep Scan was canceled. 450242 files scanned in 16 minutes, 34 seconds. Show details

Results:

The results of the Avast Security antivirus scan show that no viruses, malware, or other malicious threats were detected on the host laptop, confirming that the system is currently free of active infections.

3.4 TCP Port Scan of Host Admin Laptop

Purpose:

To evaluate which TCP ports are open on the host laptop and ensure they do not expose the device to unnecessary risks.

Command:

```
nmap -sT -n 192.168.158
```

Findings:

```
Nmap scan report for 192.168.1.158
Host is up (0.000066s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT    STATE SERVICE
631/tcp open  ipp
```

- The scan results for the host laptop showed only the following ports open/listening: 631 (IPP – printing service)

- These ports are considered safe and necessary for normal laptop operations.

Impact / risk:

No unnecessary or vulnerable ports were detected, minimizing exposure to unauthorized inbound connections or network attacks.

Remediation:

No further action required. The open ports are required for standard operations and the firewall is active in blocking all other unsolicited connections.

3.5 Browser Extensions Risk:

Browser extensions are potential areas where sensitive information can be exposed. Malicious or compromised extensions can:

- Collect personal or browsing data without the user's knowledge

- Inject unwanted code or ads, or even download malware onto the device

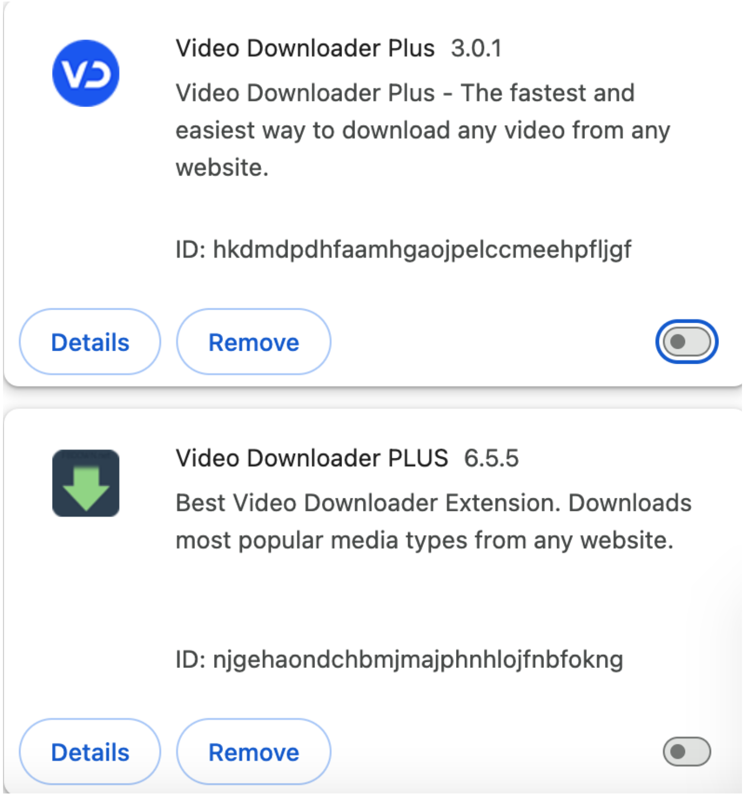
- Spread malware if the extension provider is hacked or if the extension itself is compromised

Such vulnerabilities could affect a large number of users and devices. Making extension review and removal of untrusted extensions an important part of the host laptop security.

Remediation:

A review of installed browser extensions was conducted. Unnecessary or high risk extensions were uninstalled to reduce potential security and privacy risks. Web browser extensions can serve as a potential entry point for attackers.

Two examples extensions are shown below for reference.



Video Downloader Plus 3.0.1

Video Downloader Plus - The fastest and easiest way to download any video from any website.

ID: hkdmdpdhfaamhgaojpelccmeehpfljgf

Video Downloader PLUS 6.5.5

Best Video Downloader Extension. Downloads most popular media types from any website.

ID: njgehaondchbmjmajphnhlojfnbfokng

Extensions that are occasionally required for legitimate tasks can be temporarily reinstalled and removed after use, maintaining ongoing host laptop security.

By limiting extensions to only trusted and necessary ones, the host laptop is better protected against these future threats.

Objective 3 – Identify Potentially unsafe or unauthorized devices

Scans & Methods Conducted:

☑ 3.1 Host laptop firewall assessment
☑ 3.2 Review system and OS updates
☑ 3.3 Host anti-virus assessment
☑ 3.4 TCP port scan of host admin laptop
☑ 3.5 Browser extension risk

4.0 Preparation for Potential Security Incidents

4.1 Software Hash Verification

Purpose:

This measure provides preparation and protection against potential security incidents by ensuring that downloaded software is authentic and has not been tampered with. By verifying the files hash against the value provided by the vendor, the risk of installing malware or modified software is reduced.

Observation/Findings:

Software downloads from third-party sources can be intercepted, altered, or replaced with malicious versions. Without hash verification, users may unknowingly install compromised applications, leading to data breaches or malware infections.

Impact/risk:

Failure to verify software integrity increases the likelihood of supply chain attacks, where compromised files masquerade as legitimate software. Which could result in unauthorized access, data theft, or complete system compromise.

Example: The Linux Mint ISO Hack (2016) where attackers hacked the Linux Mint website and replaced the official ISO download link with a trojanized version of Linux Mint that contained a backdoor. Thousands of users downloaded a compromised operating system. Users who verified the ISO against the published hash would have seen it did not match, immediately detecting the tampered download.

Remediation / Good Practice:

To strengthen preparations for potential incidents, software hash verifications will be adopted as part of the host laptop's security practices. For example, a downloaded Wireshark installer was checked by generating its SHA-256 hash using macOS's 'shasum' command. The calculated has matched the vendors published hash, confirming authenticity.

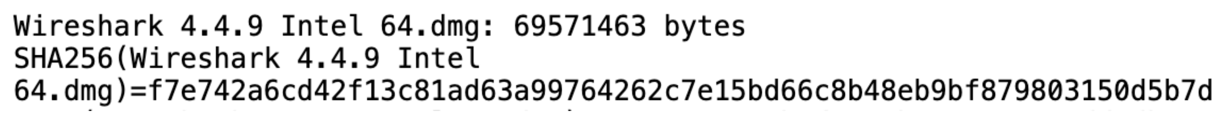
This method can be repeated for any future software installation:

- Download the software only from the official vendor site.
- Run a hash calculation
- Compare it against the vendor's published hash or signed key file.

Hash verification of Wireshark installer:

To ensure the downloaded Wireshark installer was authentic and has not been tampered with, the file's SHA-256 hash was calculated locally and compared with the official hash provided on the Wireshark website.

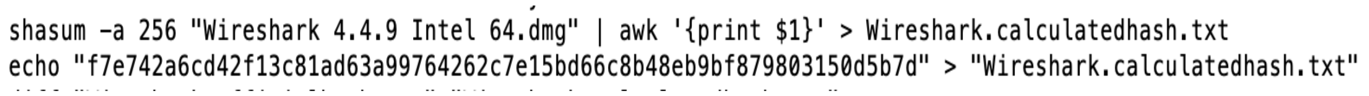
Hash of Wireshark installer from the official website:



```
Wireshark 4.4.9 Intel 64.dmg: 69571463 bytes
SHA256(Wireshark 4.4.9 Intel
64.dmg)=f7e742a6cd42f13c81ad63a99764262c7e15bd66c8b48eb9bf879803150d5b7d
```

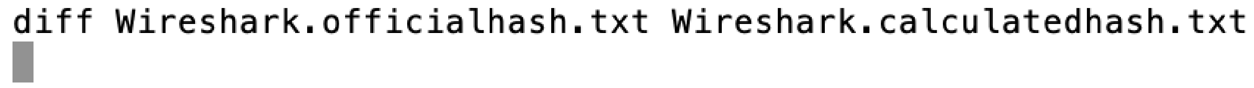
Checking the hash of the Wireshark installer:

- The calculated hash was saved in a file named “Wireshark.calculatedhash.txt”
- The official hash was saved in a file named “Wireshark.officialhash.txt”



```
shasum -a 256 "Wireshark 4.4.9 Intel 64.dmg" | awk '{print $1}' > Wireshark.calculatedhash.txt
echo "f7e742a6cd42f13c81ad63a99764262c7e15bd66c8b48eb9bf879803150d5b7d" > "Wireshark.calculatedhash.txt"
```

Compares both the files:



```
diff Wireshark.officialhash.txt Wireshark.calculatedhash.txt
```

- A file comparison (diff) was performed between the two.

If any differences were found, this would indicate the installer had been altered, potentially with malware. However, the comparison confirmed that both hashes were identical, verifying the installer’s integrity and authenticity.

This verification process demonstrates a repeatable and effective method to ensure the integrity of any software installed on the host laptop in the future.

4.2 Data backup & recovery planning

Purpose:

To ensure critical files remain available in the event of malware infection, ransomware, hardware failure, or other incidents that render the host laptop unusable.

Observation/Findings:

Personal and sensitive files such as passport photos, scanned identification, financial documents, education records represent critical data that must be protected. If the host laptop were compromised, these files could be lost permanently or exposed.

Impact/Risk:

Without a secure backup, incidents such as ransomware or physical device failure could results in irreversible data loss. This would not only cause personal disruption but could also pose risks if sensitive documents (e.g. ID scans) were leaked.

Remediation/ Good practice:

To mitigate these risks, critical files will be periodically backed up to an encrypted portable external hard drive. This ensures:

- Files remain accessible if the host laptop becomes unavailable.
- Sensitive data is not solely dependent on a single device.
- Backups can be stored securely offline, reducing the risk of ransomware encrypting them.

This practice can be scaled by implementing cloud-based encrypted backup solutions. These allow for continuous or schedule backups to secure servers, ensuring data remains recoverable at any time while providing redundancy and accessibility across locations. Combining offline and cloud-based approaches offers the strongest protection against both cyber and physical threats.

Objective 4 – Prepare for potential security incidents

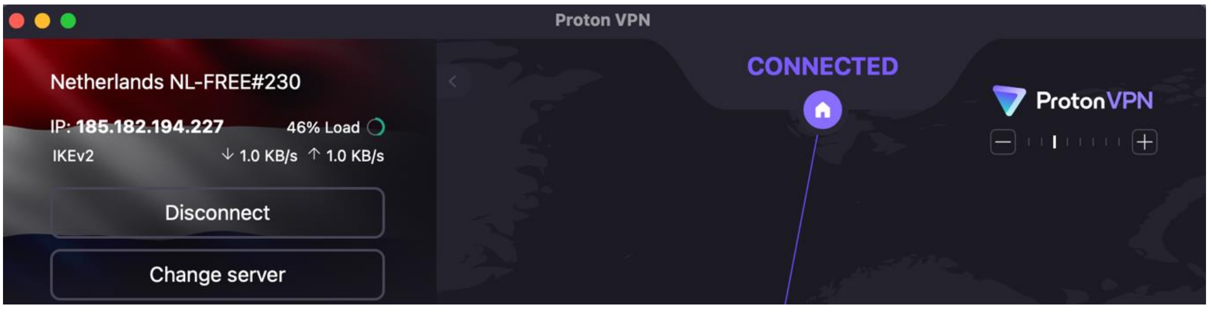
Scans & Methods Conducted:

☑ 4.1 Software hash verification
☑ 4.2 Data backup & recovery planning

5.0 Possible long-term improvements:

1. Installing and configuring ProtonVPN for external communications on host admin laptop

Within the audit, it was identified that, while port hardening ProtonVPN was installed on the administrator's laptop to protect data transmitted over the internet. The VPN encrypts outbound traffic that leaves the network, ensuring that sensitive information is not exposed to interception when using public or untrusted networks. VPNs also mask the laptop's public IP address, adding an extra layer of privacy and security for all internet communications.



Proton VPN

Netherlands NL-FREE#230

IP: 185.182.194.227 46% Load

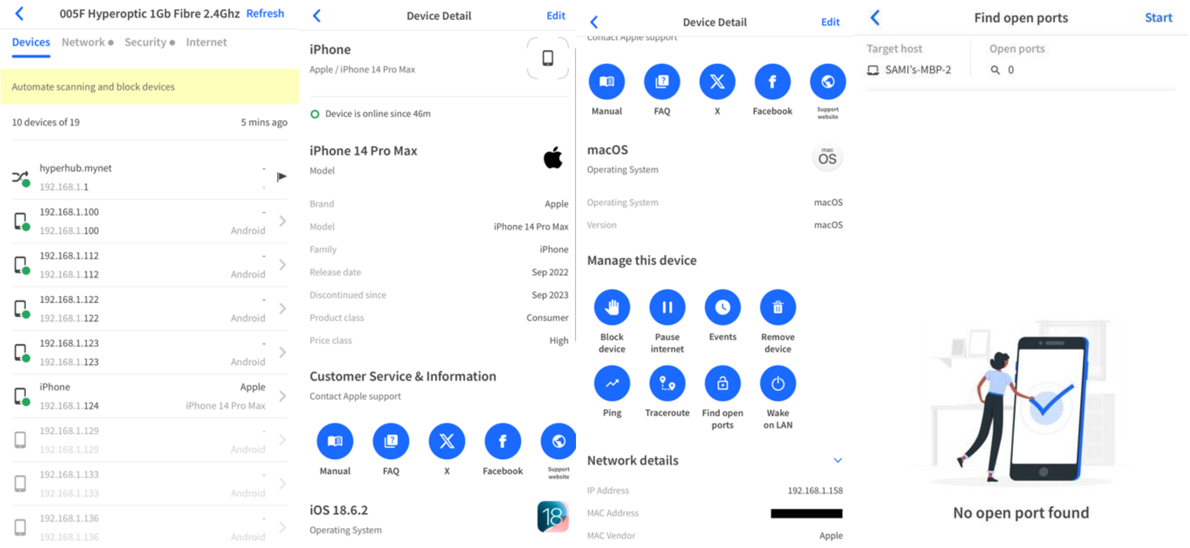
IKEv2 ↓ 1.0 KB/s ↑ 1.0 KB/s

CONNECTED

2. **Device Fingerprinting for network identification**

Currently, device identification within the LAN primarily relies on DHCP leases, which link IP addresses to MAC addresses. However, MAC addresses can be spoofed, and modern devices use MAC randomization, making this method even harder for long term device identification. The audit highlighted that accurately identifying devices can be difficult without manually verifying their burned-in MAC address.

Fing was trialed on a mobile device to evaluate its effectiveness for LAN device fingerprinting. The screenshots below demonstrate its ability to profile devices (MAC address, hostname, operating system), identify open ports, and provides simple management actions such as pinging or disconnecting devices.



005F Hyperoptic 1Gb Fibre 2.4Ghz

Automate scanning and block devices

10 devices of 19 5 mins ago

hyperhub.mynet - 192.168.1.1 -
192.168.1.100 - 192.168.1.100 Android
192.168.1.112 - 192.168.1.112 Android
192.168.1.122 - 192.168.1.122 Android
192.168.1.123 - 192.168.1.123 Android
iPhone Apple 192.168.1.124 iPhone 14 Pro Max
192.168.1.129 - 192.168.1.129 Android
192.168.1.133 - 192.168.1.133 Android
192.168.1.136 - 192.168.1.136 Android

Device Detail

iPhone
Apple / iPhone 14 Pro Max

Device is online since 46m

iPhone 14 Pro Max
Model

Brand Apple
Model iPhone 14 Pro Max
Family iPhone
Release date Sep 2022
Discontinued since Sep 2023
Product class Consumer
Price class High

Customer Service & Information
Contact Apple support

iOS 18.6.2
Operating System

Device Detail

Contact Apple support

macOS
Operating System

Operating System macOS
Version macOS

Manage this device

Network details

IP Address 192.168.1.158
MAC Address [redacted]
MAC Vendor Apple

Find open ports

Target host SAMI's-MBP-2
Open ports 0

No open port found

Following the trial, Fing has been implemented as an additional method of device identification, used alongside ARP cache and DHCP lease monitoring providing an improved and more reliable way of identifying devices on the LAN.

3. **Updating Routers' current model type**

The Hyperoptic Zyxel EX3301 model has now been ordered from the ISP to replace the current ZTE ZXHN-series router. This is the newest ISP router that provides stronger security features, including **WPA3** encryption (an update over WPA2) and enforced **HTTPS** access for the admin interface. While **WPS** remains enabled by default the EX3301, it can be adjusted through the admin interface settings.

4. **Multi-Factoring Authentication (MFA)**

MFA has been enabled on critical accounts (e.g. email, banking, cloud storage) to significantly reduce the risk of unauthorized access, if passwords were compromised. MFA adds an extra layer of security by requiring a second factor such as a mobile authenticator app, SMS code, or hardware token. Ensuring that access cannot be granted with stolen credentials alone, making it one of the most effective measures against phishing and credential theft.

Conclusion:

This audit identified several critical vulnerabilities, including an outdated router model, WPS exposure, and an unencrypted HTTP-based management interface. These weaknesses represented significant risks but were remediated through router replacement, disabling insecure features, and applying stronger configurations.

Additional improvements were introduced, including VPN usage, device fingerprinting with Fing, multi-factor authentication for critical accounts, WAN port restrictions, guest network segmentation, and a structured backup plan. The host laptop is also protected with updated antivirus software, a properly configured firewall, and regular operating system updates.

This audit reinforced the importance of addressing router-level vulnerabilities early, layering multiple defences (device, network, and cloud), and validating configurations through hands-on testing. Security is not static, and continuous monitoring, updating, and reviewing remain essential to maintaining a strong defence.