

TASK 3

SECURING A WIFI NETWORK

1. Executive Summary

a. Objective of the Test

To conduct a Wi-Fi security assessment on my home network, checking for weak passwords, open ports, and unauthorized devices.

b. Tools Used

Wireshark – Network traffic capture and analysis.

Nmap – Network scanning and port enumeration.

Router Admin Interface – For manual configuration checks and client listings.

c. Summary of Key Findings

Wi-Fi password was found to be strong (WPA2 with 16-character key).

Nmap revealed 4 devices with open ports, including a default login page exposed.

No unknown device was found connected to the network.

No sign of brute-force attempts or DoS activity based on Wireshark traffic.

2. Methodology

a. Step-by-Step Testing Process

i. Device Discovery with Nmap

```
sudo nmap -sn 192.168.1.0/24
```

ii. Port Scanning:

```
sudo nmap -sV 192.168.1.(ip address)
```

Ran this on each IP found to identify open ports and services.

iii. Unauthorized Devices:

Compared Nmap device list with known devices.

Cross-checked against the router's admin page.

iv. Wireshark Analysis:

Captured network traffic using wireshark and observed protocols used such as HTTP, MDNS, UPnP.

Looked for insecure traffic or signs of malware.

v. Router Configuration Review:

Logged into the router settings via 192.168.1.1.

Verified encryption WPA2.

Checked for default admin credentials.

3. Vulnerability Findings

a. Lack of Segmentation

- i. Description: All devices were in the same flat network (no VLANs or guest isolation).
- ii. Severity: Low
- iii. Evidence: Nmap showed full access between all IPs.
- iv. Risk: A compromised device can access others.
- v. Mitigation:
Use guest networks for IoT and visitors.
Enable client isolation where possible.

4. Overall Risk Rating

Severity	Count
High	0
Medium	0
Low	1

5. Recommendations

- i. Change Wi-Fi default password and audit connected devices weekly.
- ii. Update router and device firmware regularly.
- iii. Set up guest network for IoT and visitor devices.
- iv. Perform regular Nmap scans for rogue devices or services.

6. Appendix

Screenshots.

```
5: wlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether a0:47:d7:5c:89:9a brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.9/24 brd 192.168.1.255 scope global dynamic noprefixroute wlan0
        valid_lft 86394sec preferred_lft 86394sec
    inet6 fe80::3fb4:a40d:80c1:723e/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

IP address given by the WiFi Adapter

```
(root@kali)-[/home/kali]
# sudo nmap -sn 192.168.1.0/24

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-06 11:25 EDT
Nmap scan report for 192.168.1.1 (192.168.1.1)
Host is up (0.0037s latency).
MAC Address: 8C:8F:8B:66:55:A7 (China Mobile Chongqing branch)
Nmap scan report for 192.168.1.4 (192.168.1.4)
Host is up (0.042s latency).
MAC Address: EC:63:D7:4C:AF:D1 (Intel Corporate)
Nmap scan report for 192.168.1.7 (192.168.1.7)
Host is up (0.14s latency).
MAC Address: 56:83:26:2A:1D:6A (Unknown)
Nmap scan report for 192.168.1.8 (192.168.1.8)
Host is up (0.15s latency).
MAC Address: 5C:B2:6D:02:2B:6E (Unknown)
Nmap scan report for kali (192.168.1.9)
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 9.94 seconds
```

Active devices on my WiFi Network

```
(root@kali)-[/home/kali]
# sudo nmap -sV 192.168.1.4

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-06 11:26 EDT
Nmap scan report for 192.168.1.4 (192.168.1.4)
Host is up (0.035s latency).
All 1000 scanned ports on 192.168.1.4 (192.168.1.4) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: EC:63:D7:4C:AF:D1 (Intel Corporate)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 38.87 seconds

(root@kali)-[/home/kali]
# sudo nmap -sV 192.168.1.7

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-06 11:27 EDT
Nmap scan report for 192.168.1.7 (192.168.1.7)
Host is up (0.048s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
49152/tcp open  tcpwrapped
62078/tcp open  tcpwrapped
MAC Address: 56:83:26:2A:1D:6A (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.46 seconds
```

```
(root@kali)-[/home/kali]
# sudo nmap -sV 192.168.1.8

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-06 11:27 EDT
Nmap scan report for 192.168.1.8 (192.168.1.8)
Host is up (0.11s latency).
All 1000 scanned ports on 192.168.1.8 (192.168.1.8) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 5C:B2:6D:02:2B:6E (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 111.44 seconds

(root@kali)-[/home/kali]
# sudo nmap -sV 192.168.1.9

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-06 11:29 EDT
Nmap scan report for kali (192.168.1.9)
Host is up (0.0000030s latency).
All 1000 scanned ports on kali (192.168.1.9) are in ignored states.
Not shown: 1000 closed tcp ports (reset)

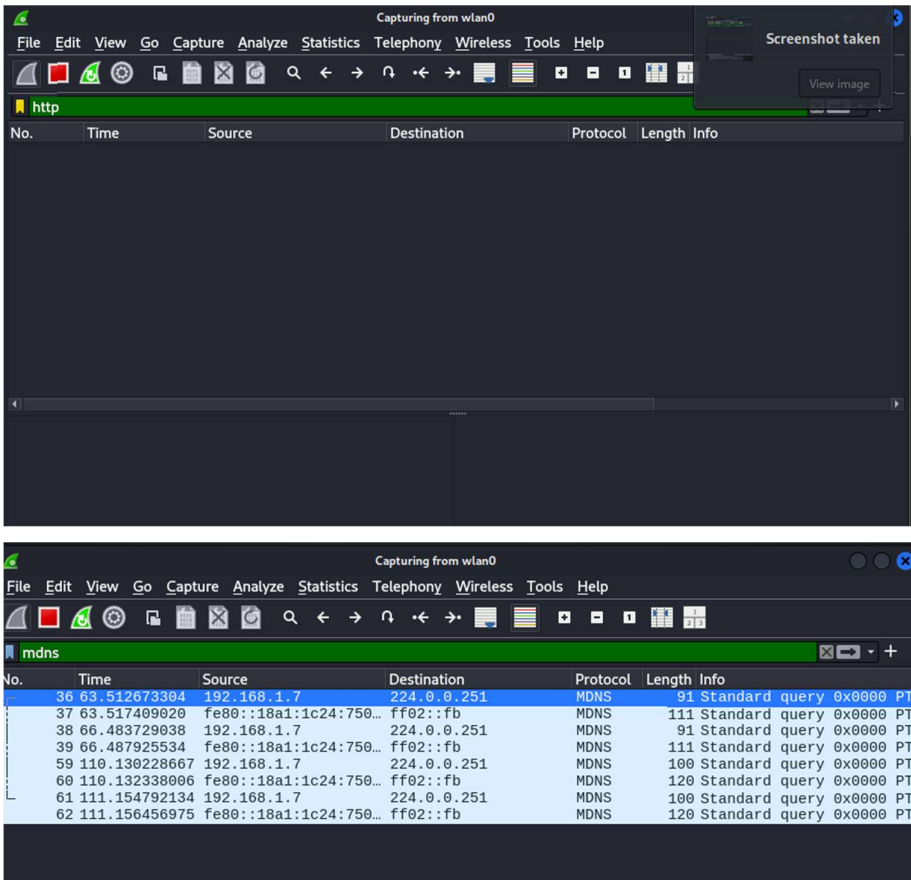
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds
```

Individual scanning of open ports and services on devices on the network.

```
(root@kali)-[/home/kali]
# sudo arp-scan --interface=wlan0 --localnet
Interface: wlan0, type: EN10MB, MAC: a0:47:d7:5c:89:9a, IPv4: 192.168.1.9
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.1.1      8c:8f:8b:66:55:a7      (Unknown)
192.168.1.7      56:83:26:2a:1d:6a      (Unknown: locally administered)
192.168.1.4      ec:63:d7:4c:af:d1      (Unknown)
192.168.1.8      5c:b2:6d:02:2b:6e      (Unknown)

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.942 seconds (131.82 hosts/sec). 4 responded
```

Scanning my local subnet for active IP/MAC addresses using arp-scan



Filtering protocols, HTTP – viewing if any unencrypted traffic is visible and MDNS – from smart devices.

GM220-S

Status

Network

Security

Application

Administration

Maintenance

Help

WAN

WLAN

Basic

SSID Settings

Security

NO Carrier

中文

Help

Logout

Choose SSID

SSID1

Authentication Type

WPA/WPA2-PSK

WPA Passphrase

(8 ~ 63 characters)

WPA Encryption Algorithm

TKIP+AES

Admin Interface on router