Wi-Fi Security Assessment Report

# 1. Introduction

This report provides a summary of the Wi-Fi security assessment carried out on my personal home network as part of an internship task. The goal was to identify potential vulnerabilities and suggest recommendations for strengthening the network's security posture. Tools such as Nmap and Wireshark were utilized for scanning and traffic analysis.

# 2. Objectives

- Assess the strength of the Wi-Fi password and encryption method.  
- Scan for open ports and identify potential vulnerabilities.  
- Detect unauthorized devices connected to the network.  
- Analyze network traffic for security issues.

# 3. Tools Used

- Nmap: For scanning devices and ports on the network.  
- Wireshark: For capturing and analyzing packet data.  
- VirtualBox with Kali Linux: Used as the assessment environment.

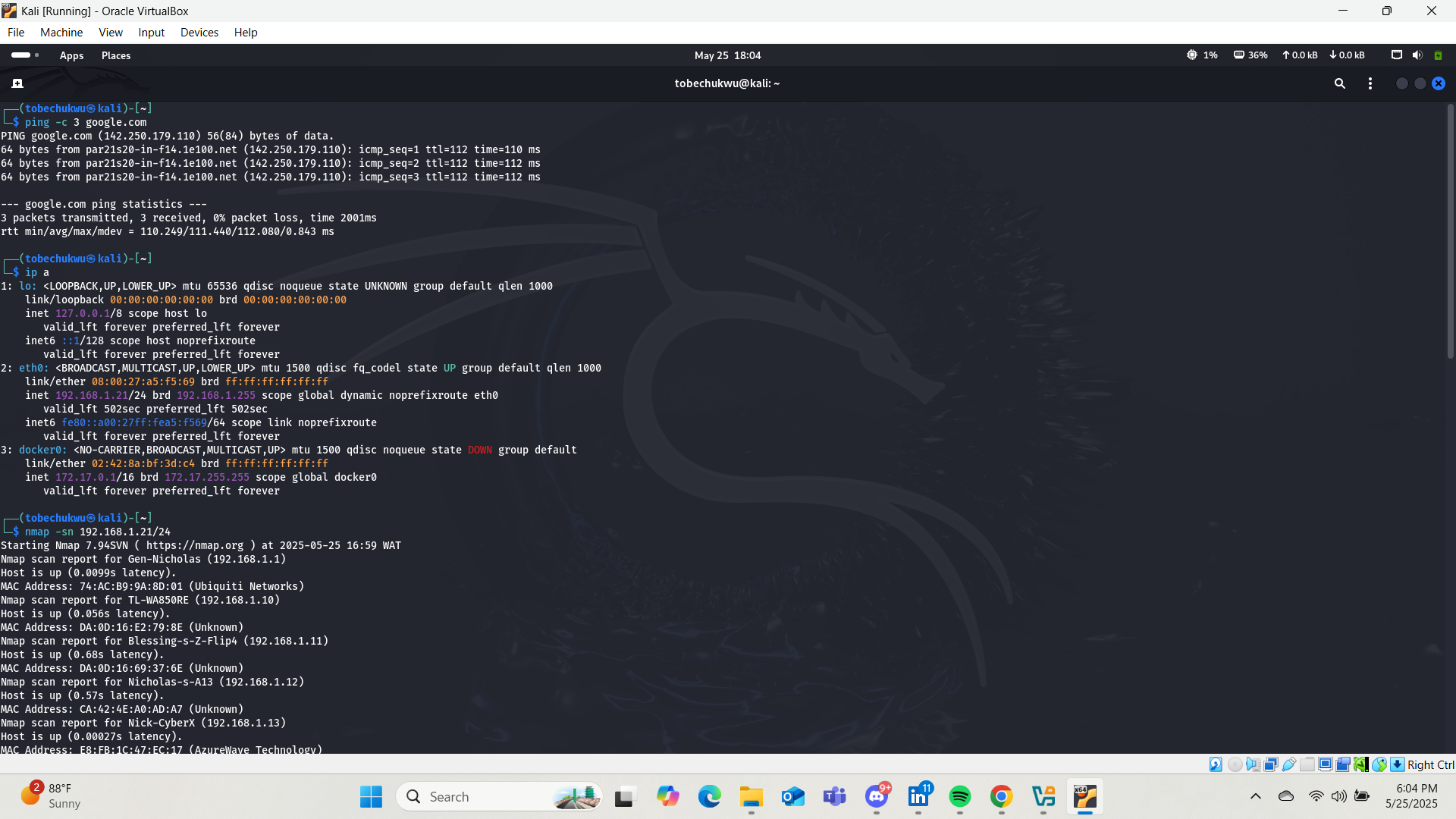
# 4. Methodology

## 4.1 Network Discovery

Using Nmap, a ping scan was performed to identify active devices on the network:

nmap -sn 192.168.1.0/24

This command revealed all live hosts on the local subnet.



## 4.2 Port Scanning

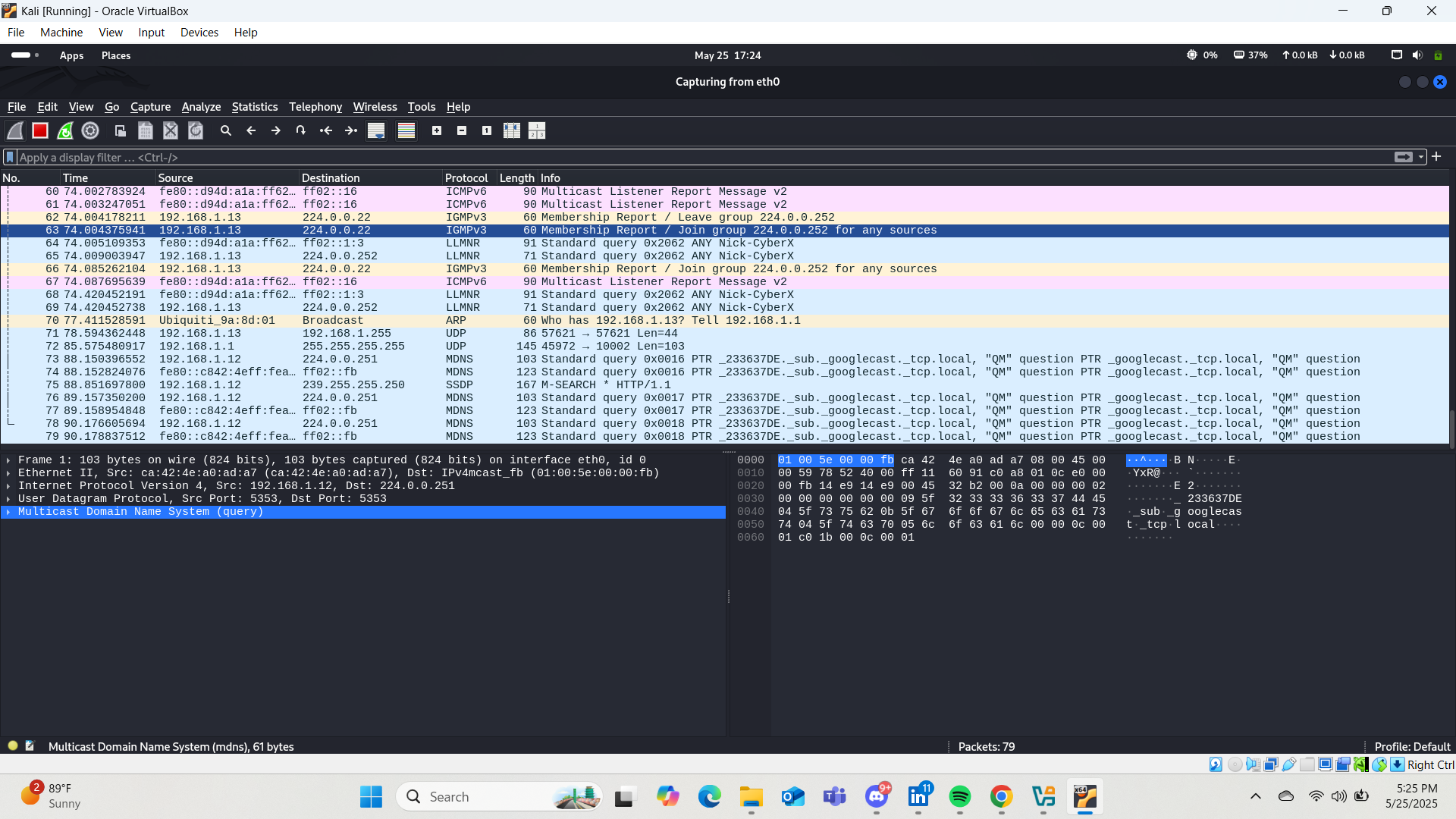
A service version scan was conducted on selected devices using:

nmap -sV 192.168.1.X

This identified open ports and services running on the devices, such as HTTP (port 80), HTTPS (port 443), and other services depending on the device.

## 4.3 Packet Capture

Wireshark was launched in the Kali Linux VM, and the correct network interface was selected for live capture. Network traffic was generated by browsing websites and pinging domains. Filters such as http and dns were applied to isolate specific traffic types. Observed traffic included DHCP, mDNS, ICMPv6, ARP and general UDP packets, indicating healthy baseline network activity.



## 4.4 Router Configuration Review

A manual inspection of the router configuration was done via the web interface:  
- Encryption Type: WPA2-PSK confirmed as active.  
- Wi-Fi Password: Verified to be strong and not a default password.  
- WPS: Confirmed disabled.  
- Admin Credentials: Changed from defaults to a secure password.

# 5. Findings

- No unauthorized devices were detected on the network.  
- No critical ports (like Telnet or FTP) were found open.  
- The router uses WPA2 encryption and has WPS disabled.  
- Most traffic observed was local broadcast traffic typical for a secure home network.

# 6. Recommendations

- Periodically review connected devices for unfamiliar entries.  
- Keep router firmware up to date.  
- Upgrade to WPA3 encryption if supported by devices.  
- Consider disabling services (like UPnP) that are not actively used.

# 7. Challenges Experienced

- Lack of a USB Wi-Fi Adapter: Limited the ability to capture Wi-Fi packets from surrounding devices or perform monitor mode analysis.  
- Virtual Machine Limitations: The VM setup restricted full visibility of all traffic on the network, especially from wireless clients.

# 8. Conclusion

The assessment demonstrated a generally secure home network environment with no major vulnerabilities discovered. Despite hardware limitations, the tools used were sufficient to evaluate key aspects of the network. Future assessments with a dedicated Wi-Fi adapter could provide deeper insights into wireless-layer security.