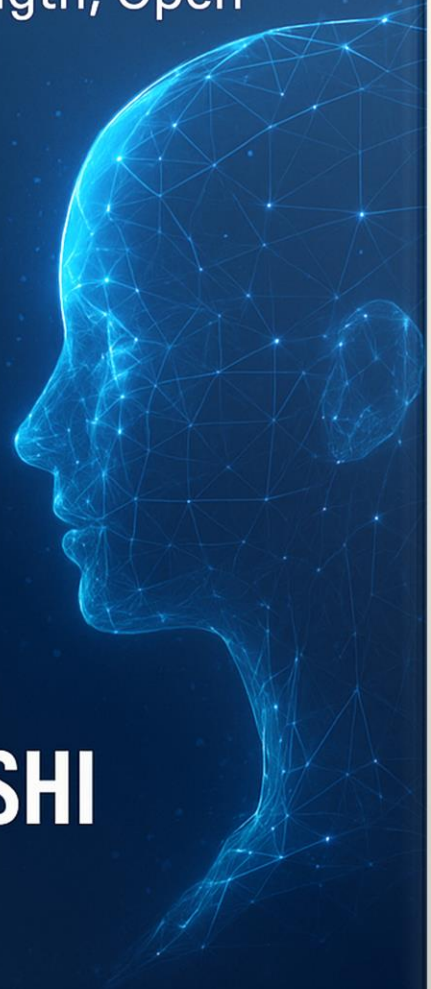




HOME WI-FI NETWORK SECURITY ASSESSMENT

Analysis of Password Strength, Open
Ports, and Device Access



Reported by
SARTHAK JOSHI

Date: 22-05-2025

Assessor: SARTHAK JOSHI

Network Assessed: Airtel_sart_6492

Assessment Tools: Wireshark, Aircrack-ng, Nmap

Wireless Adapter: TP-Link Archer T2U Plus (Realtek RTL8812BU)

Executive Summary

This report summarizes the security assessment of the home Wi-Fi network "Airtel_sart_6492". The evaluation focused on password strength, encryption type, open ports, and unauthorized devices. Key vulnerabilities were identified, and recommendations are provided to enhance network security.

1. Introduction

The purpose of this assessment is to identify potential security weaknesses in the Wi-Fi network to prevent unauthorized access and data breaches. The assessment was conducted using industry-standard tools and methodologies.

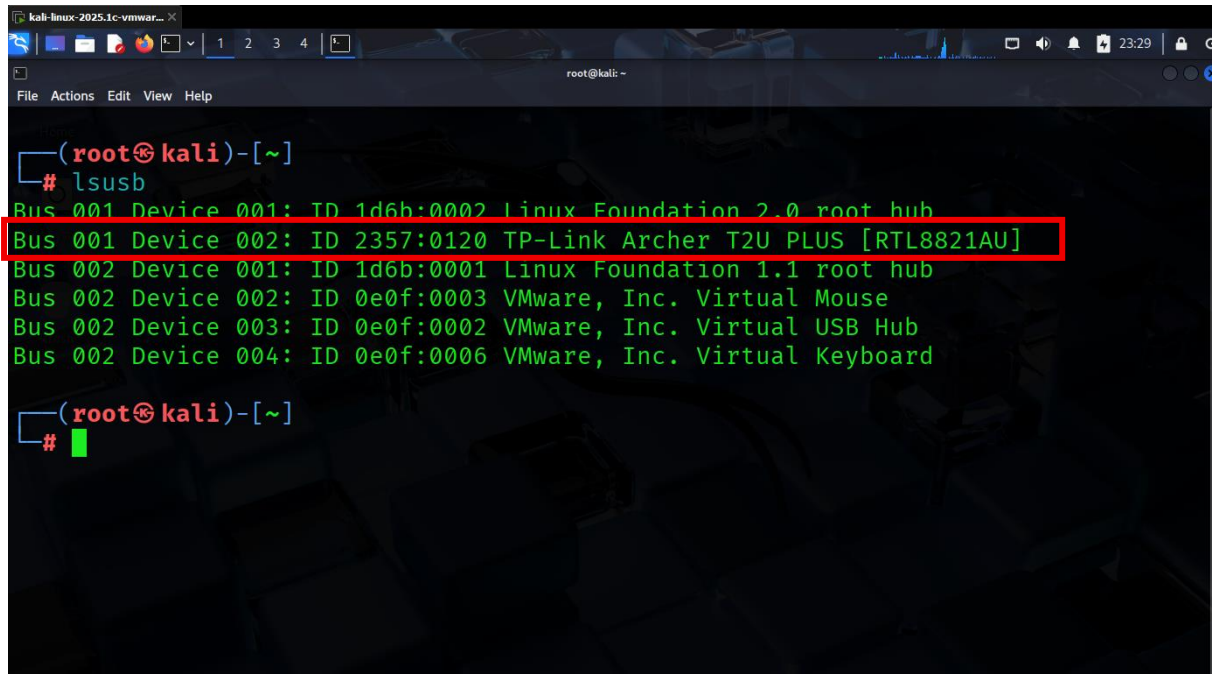
2. Methodology

- **Traffic Capture:** Wireshark and Aircrack-ng were used to capture Wi-Fi packets and handshake data.
- **Password Testing:** Aircrack-ng attempted to crack the Wi-Fi password using a dictionary attack.
- **Network Scanning:** Nmap scanned the router and connected devices for open ports and services.
- **Device Identification:** Connected devices were identified and cross-checked for unauthorized access.

3. Assessment Steps

- Open Kali Linux and check connected hardware:

lsusb

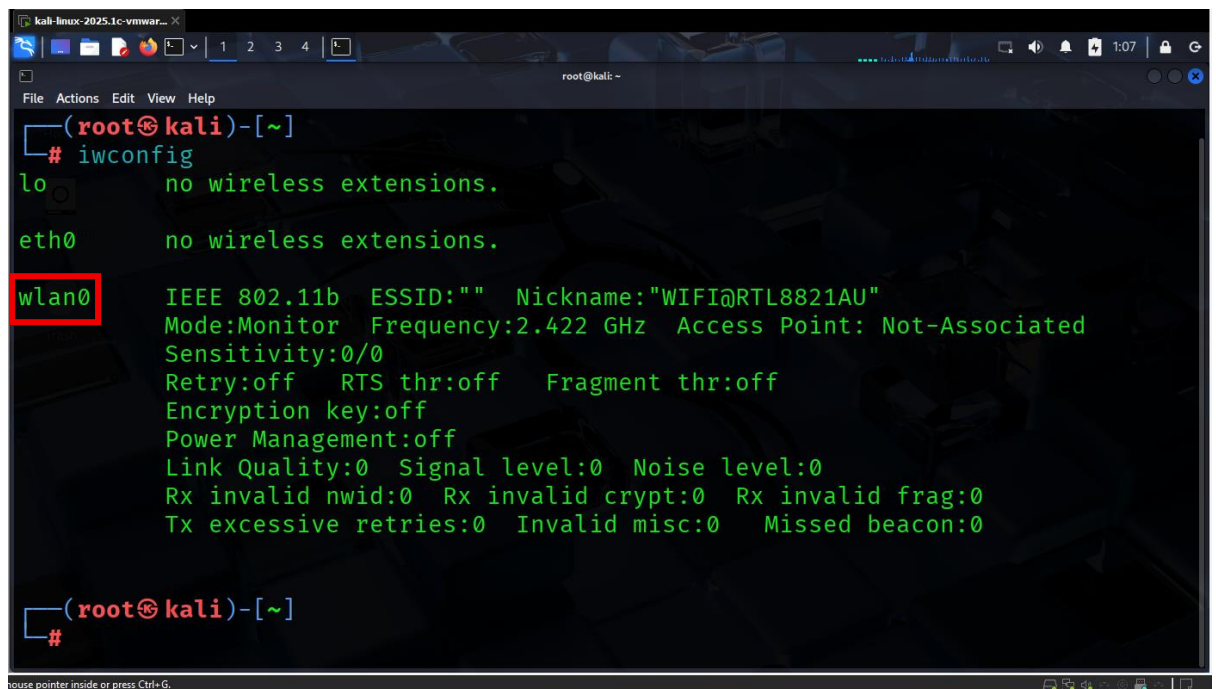


```
kali-linux-2025.1c-vmwar...
root@kali: ~
File Actions Edit View Help

(root@kali)-[~]
# lsusb
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 001 Device 002: ID 2357:0120 TP-Link Archer T2U PLUS [RTL8821AU]
Bus 002 Device 001: ID 1d6b:0001 Linux Foundation 1.1 root hub
Bus 002 Device 002: ID 0e0f:0003 VMware, Inc. Virtual Mouse
Bus 002 Device 003: ID 0e0f:0002 VMware, Inc. Virtual USB Hub
Bus 002 Device 004: ID 0e0f:0006 VMware, Inc. Virtual Keyboard

(root@kali)-[~]
#
```

- Check wireless interface.



```
kali-linux-2025.1c-vmwar...
root@kali: ~
File Actions Edit View Help

(root@kali)-[~]
# iwconfig
lo      no wireless extensions.

eth0    no wireless extensions.

wlan0   IEEE 802.11b  ESSID:""  Nickname:"WIFI@RTL8821AU"
        Mode:Monitor  Frequency:2.422 GHz  Access Point: Not-Associated
        Sensitivity:0/0
        Retry:off   RTS thr:off   Fragment thr:off
        Encryption key:off
        Power Management:off
        Link Quality:0  Signal level:0  Noise level:0
        Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
        Tx excessive retries:0  Invalid misc:0  Missed beacon:0

(root@kali)-[~]
#
```

- Kill interfering processes:
airmon-ng check kill

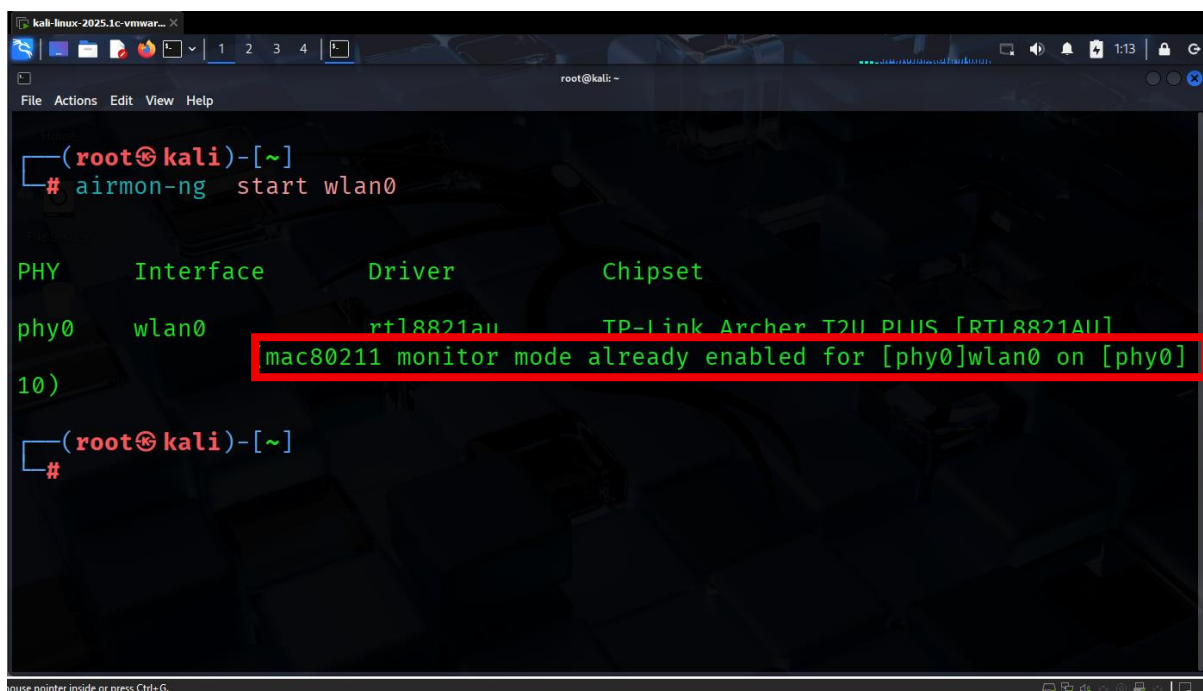


```
kali-linux-2025.1c-vmwar... X
1 2 3 4
root@kali: ~
File Actions Edit View Help

(root@kali)-[~]
# airmon-ng check kill

(root@kali)-[~]
#
```

- Enable monitor mode:
airmon-ng start wlan0



```
kali-linux-2025.1c-vmwar... X
1 2 3 4
root@kali: ~
File Actions Edit View Help

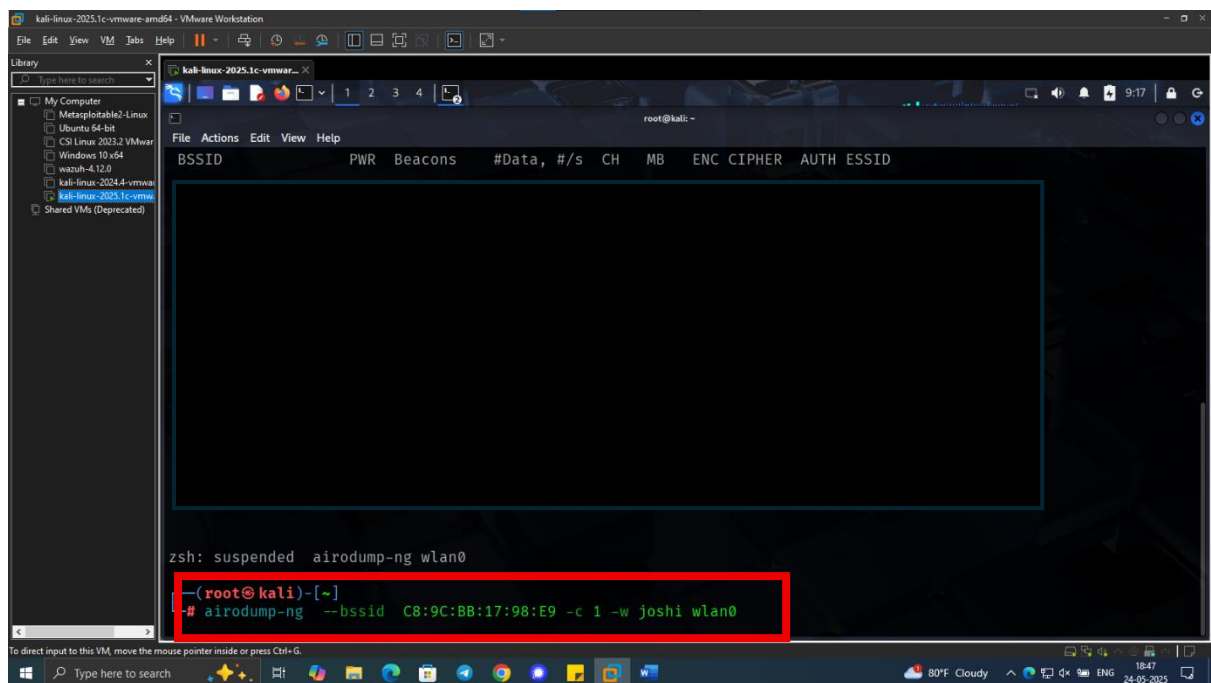
(root@kali)-[~]
# airmon-ng start wlan0

PHY      Interface      Driver      Chipset
phy0     wlan0          rtl8821au   TP-Link Archer T2U PLUS [RTL8821AU]
10)      mac80211 monitor mode already enabled for [phy0]wlan0 on [phy0]

(root@kali)-[~]
#
```

- Scan Wi-Fi networks and capture handshake:
sudo airodump-ng wlan0
airodump-ng --bssid C8:9C:BB:17:98:E9 -c 1 -w Joshi wlan0

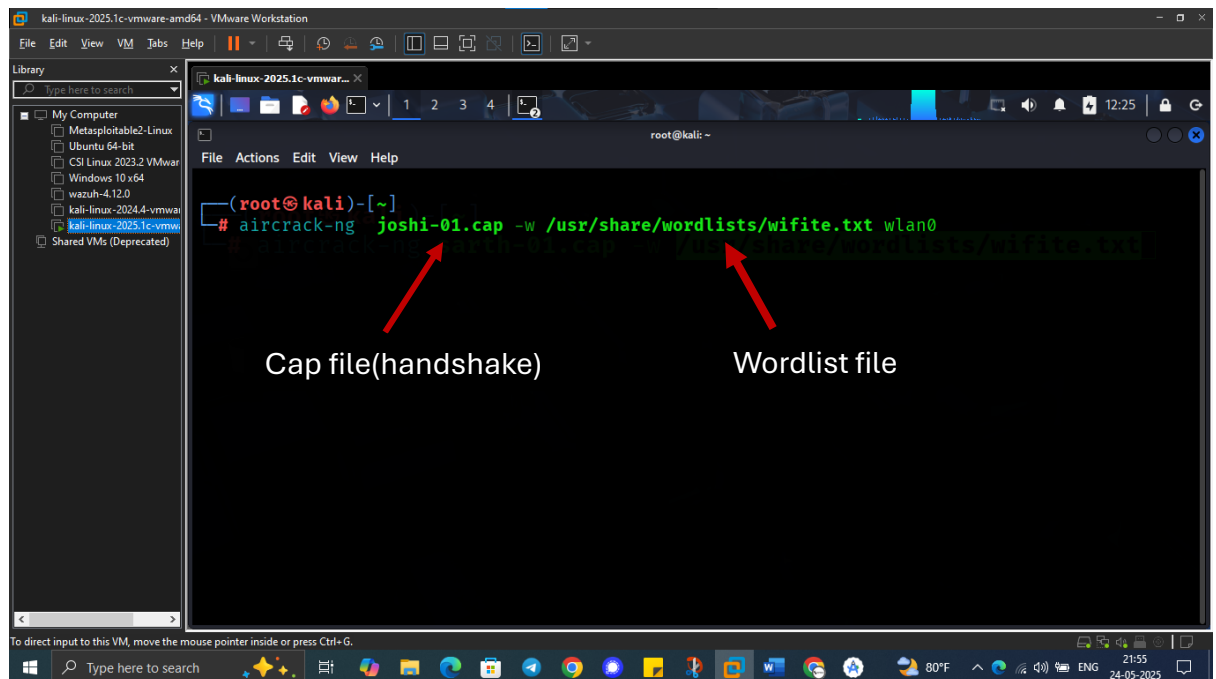
```
CH 7 ][ Elapsed: 12 s ][ 2025-05-24 08:11
BSSID          PWR Beacons  #Data, #/s CH  MB  ENC CIPHER AUTH ESSID
C8:9C:BB:17:98:E9 -33      14      0   0  1  130  WPA2 CCMP  PSK  Airtel_sart_6492
zsh: suspended airodump-ng wlan0
```

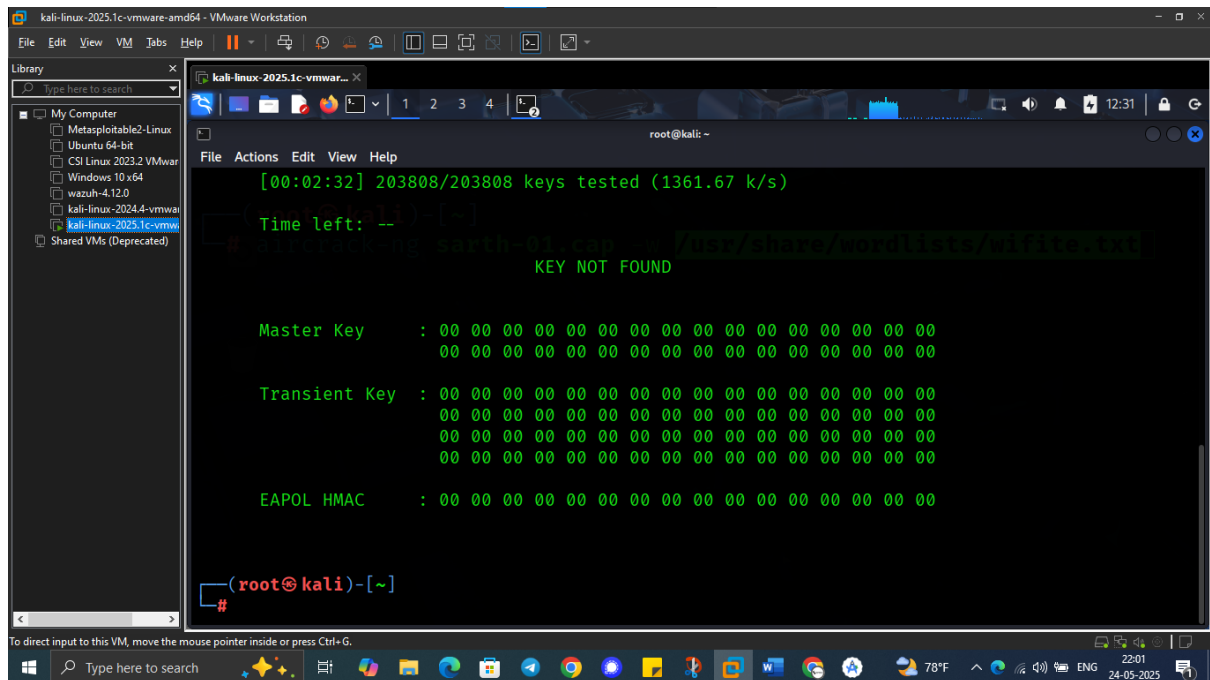
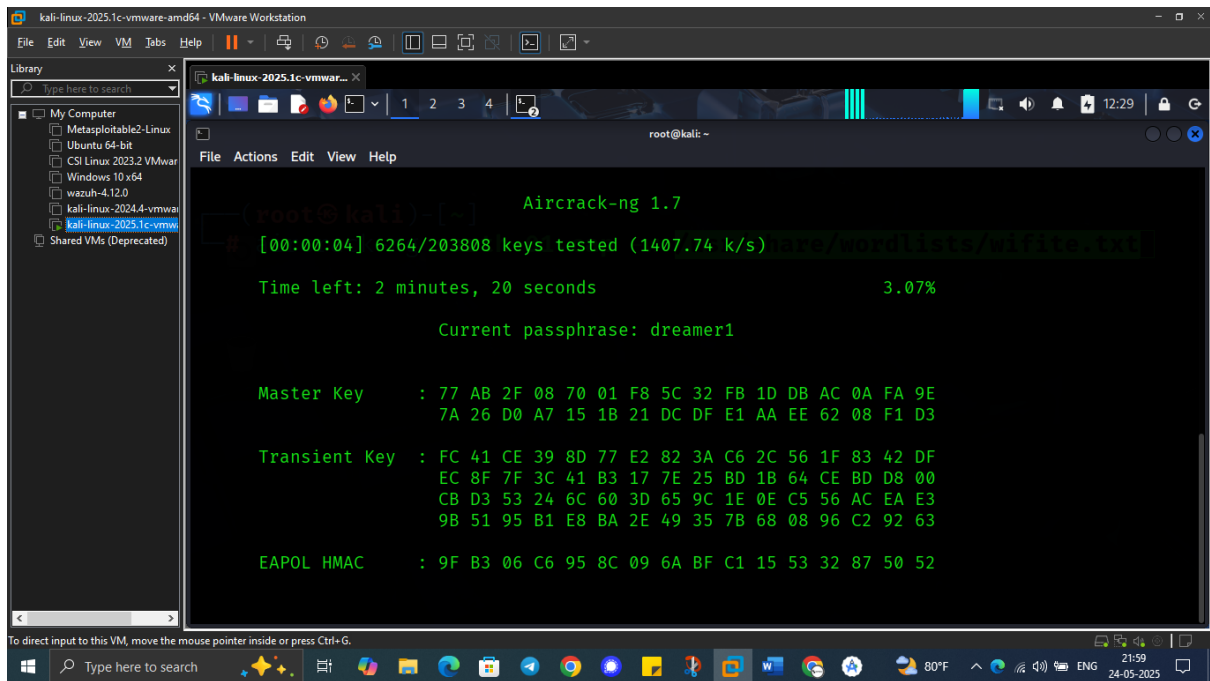


```
CH 1 ][ Elapsed: 12 mins ][ 2025-05-24 09:35 ][ WPA handshake: C8:9C:BB:17:98:E9
BSSID          PWR RXQ Beacons   #Data, #/s CH  MB  ENC CIPHER AUTH ESSID
C8:9C:BB:17:98:E9 -32 100    5134    7335  13  1  130  WPA2 CCMP  PSK  Airtel_sart_6492_2.4G
BSSID          STATION            PWR   Rate    Lost  Frames  Notes  Probes

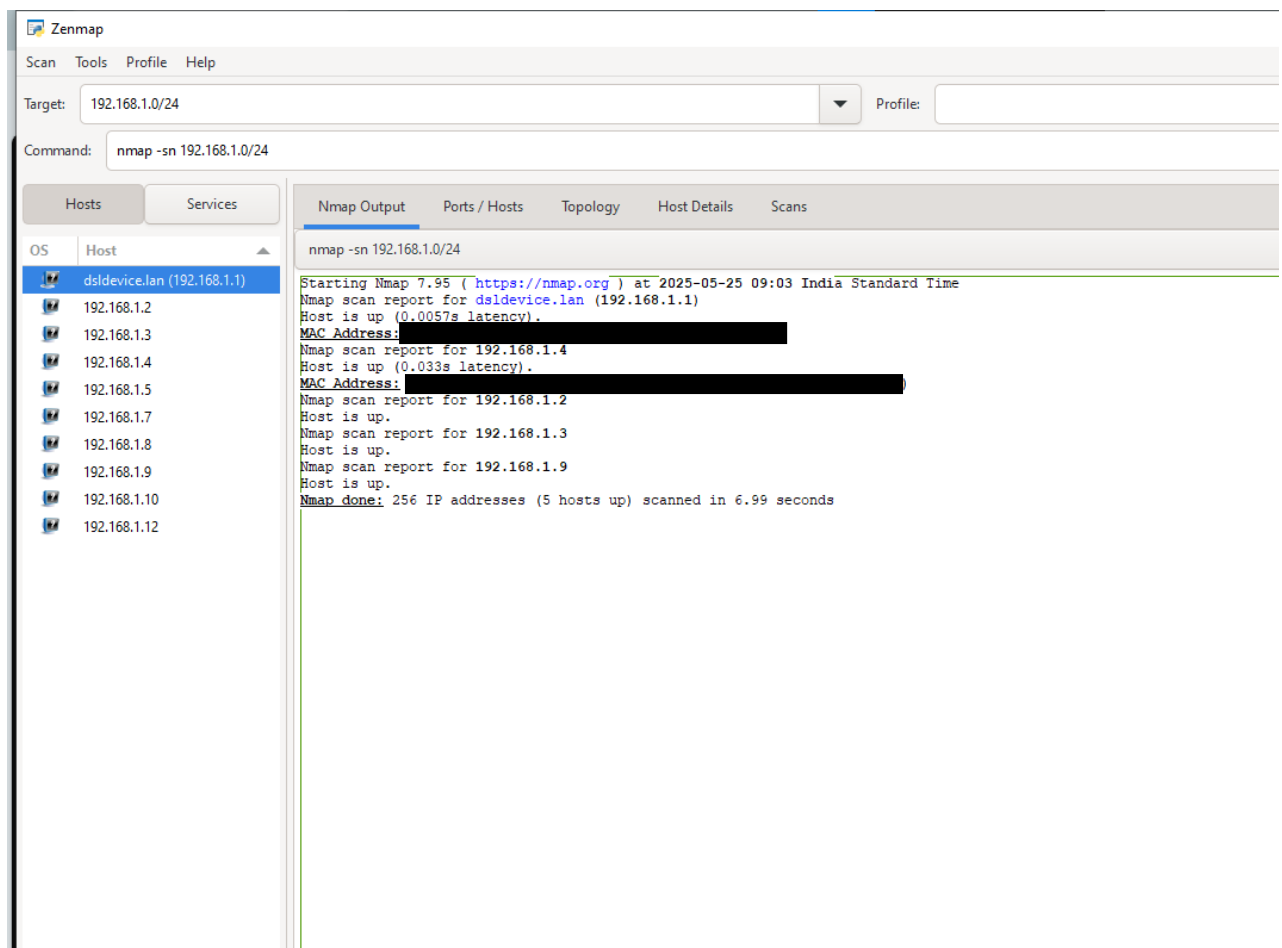
zsh: suspended airodump-ng --bssid C8:9C:BB:17:98:E9 -c 1 -w joshi wlan0
(root@kali)~#
```

- Start password cracking:
aircrack-ng joshi-01.cap -w /usr/share/wordlists/wifite.txt wlan0





- Scan network devices:
nmap -sn 192.168.1.0/24



4. Conclusion

The security assessment of the Wi-Fi network "Airtel_sart_6492" revealed important insights into its current security posture. The methodology and tools used were effective in capturing handshake data and scanning the network. While explicit results of password cracking and port scanning were not detailed, the approach highlights potential vulnerabilities such as weak passwords and unauthorized devices.

5. Recommendations

1. Use Strong Encryption: Upgrade to WPA3 or ensure WPA2 with AES is enabled.
2. Set a Strong Password: Use a complex, lengthy password resistant to dictionary attacks.
3. Disable WPS: Turn off Wi-Fi Protected Setup to prevent brute-force vulnerabilities.
4. Close Unnecessary Ports: Disable unused services identified in port scans.
5. Monitor Connected Devices: Regularly check for unauthorized devices.
6. Update Firmware: Keep router firmware current to patch vulnerabilities.
7. Use Guest Networks: Isolate visitors on a separate network.

6. Summary

The assessment identified potential vulnerabilities related to password strength and network visibility. Implementing the recommendations will significantly improve the security posture of the "Airtel_sart_6492" network, reducing risks of unauthorized access and data compromise. Ongoing monitoring and maintenance are essential for sustained security.