# 🔐 Wi-Fi Security Assessment Report

**Task 3 – Secure Your Own Wi-Fi Network**
**Candidate:** Joshwa
**Date:** 31-05-2005

---

## 🔸 Objective

To assess the security of a personal mobile hotspot by identifying weak passwords, open ports, and unauthorized connected devices using tools like Aircrack-ng, Nmap, and Wireshark.

---

## 🔸 Network Details

| Parameter | Value |
|---|---|
| Hotspot IP | 192.168.0.1 |
| Local Device IP | 192.168.0.5 |
| Subnet Range | 192.168.0.0/24 |
| Wireless Interface | wlan0 (monitor: wlan0mon) |

---

## 🔸 Tools Used

- **Aircrack-ng** – Capturing and cracking Wi-Fi password.
- **Airodump-ng & Aireplay-ng** – Handshake capture and deauthentication.
- **Nmap** – Network and port scanning.
- **Wireshark** – Packet sniffing and traffic analysis.
- **Wifite** – Automation tool for wifi security pentest.

---

## 🔸 Methodology

**1. Monitoring Mode Activation**

Enabled monitor mode on interface using:

```
sudo airmon-ng check kill
sudo airmon-ng start wlan0
```

**2. Network Discovery**

Identified hotspot details using:

```
 sudo airodump-ng wlan0mon
```

**3. Handshake Capture**

Captured handshake using:

```
 sudo airodump-ng --bssid <BSSID> -c <Channel> -w capture wlan0mon
```

Forced reconnection (if needed) using:

```
 sudo aireplay-ng --deauth 5 -a <BSSID> wlan0mon
```

**4. Password Cracking**

Attempted WPA2 password cracking with:

```
 aircrack-ng -w /usr/share/wordlists/rockyou.txt -b <BSSID> capture-01.cap
```

**5. Port and Host Scan (Nmap)**

Scanned the hotspot for open ports:

```
 nmap -sV 192.168.0.1
```

Identified all devices in the subnet:

```
 nmap -sn 192.168.0.0/24
```

**6. Traffic Analysis (Wireshark)**

- Captured packets to detect any unencrypted/suspicious traffic.

---

## 🔸 Findings

| Category | Result/Observation |
|---|---|
| Password Strength | Weak |
| WPA2 Handshake | Not Captured] |
| Open Ports | 53,80,8888 |
| Unauthorized Devices | No |
| Encryption Type | Unknown |
| Suspicious Traffic | No |

---

## 🔸 Recommendations

- ✅ Use **strong WPA2/WPA3 password** (avoid dictionary-based ones).
- ✅ Regularly check connected devices on the hotspot.
- ✅ Disable hotspot when not in use.
- ✅ Update hotspot firmware if possible.
- ✅ Limit the number of devices allowed to connect.
- ✅ Use MAC filtering (if available on device).

---

## 🔸 Conclusion

This assessment demonstrated the potential risks even on temporary personal networks like mobile hotspots. Through active scanning, password testing, and traffic analysis, several areas of improvement were identified. Implementing the above recommendations will significantly enhance the overall security of the network.