Practical No. 5

Aim: Practical on Wireless and Bluetooth attacks.

Lab Environment:

1. Kali Linux as the attacker machine

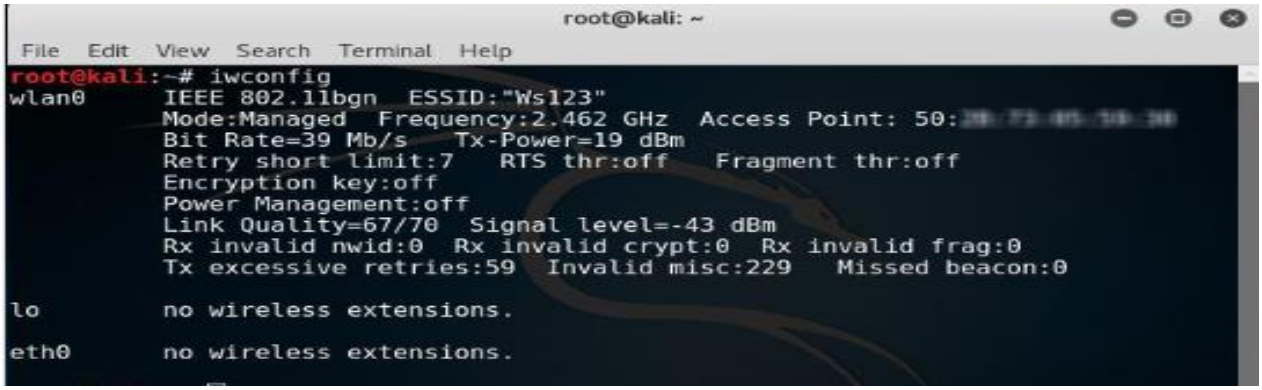
2. Web browser with internet connection

3. Administrative privileges

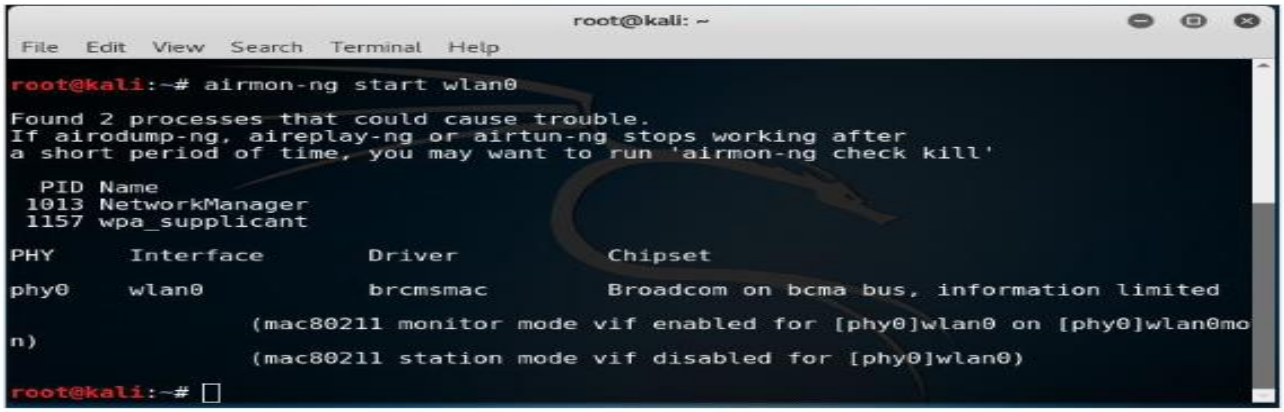
Implementation:

1. Log in to kali Linux and launch the command terminal

2. First, check if the wireless card is connected or not by using the "iwconfig" command, as shown in figure

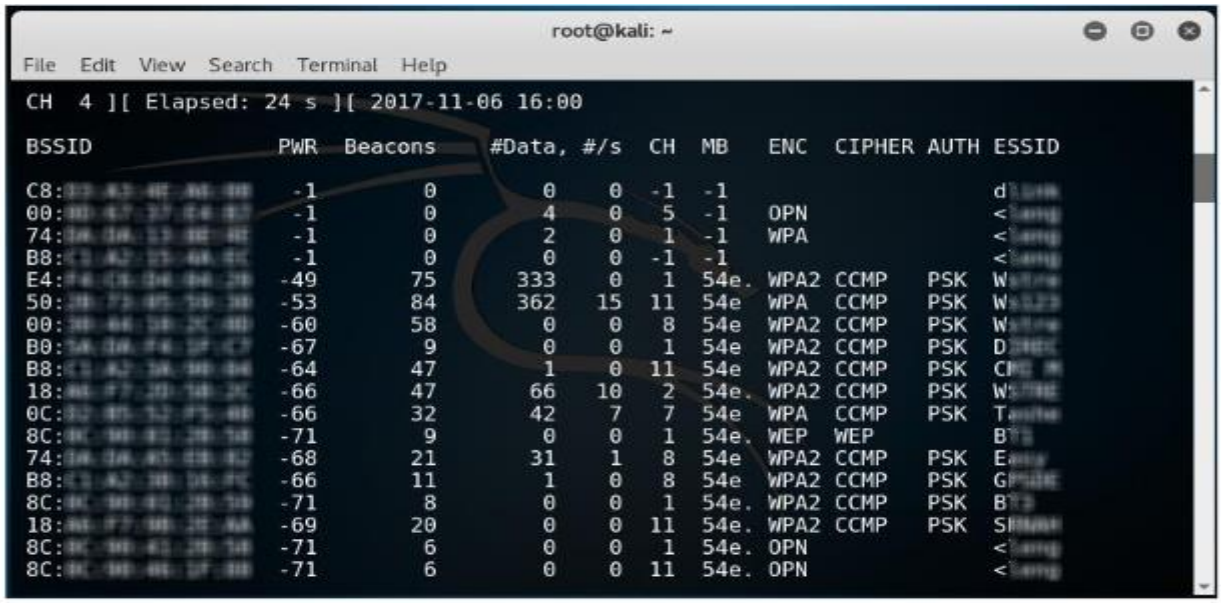


3. Change the wireless interface inti monitor mode using "airmon-ng start wlan0" command with wlan0 as your wireless interface name, as shown in figure



4. use "airodump" to find out the SSID on the interface using the command:

"airodump-ng -write capture wlan0"



The screen will display a list of WI-FI networks as shown in figure

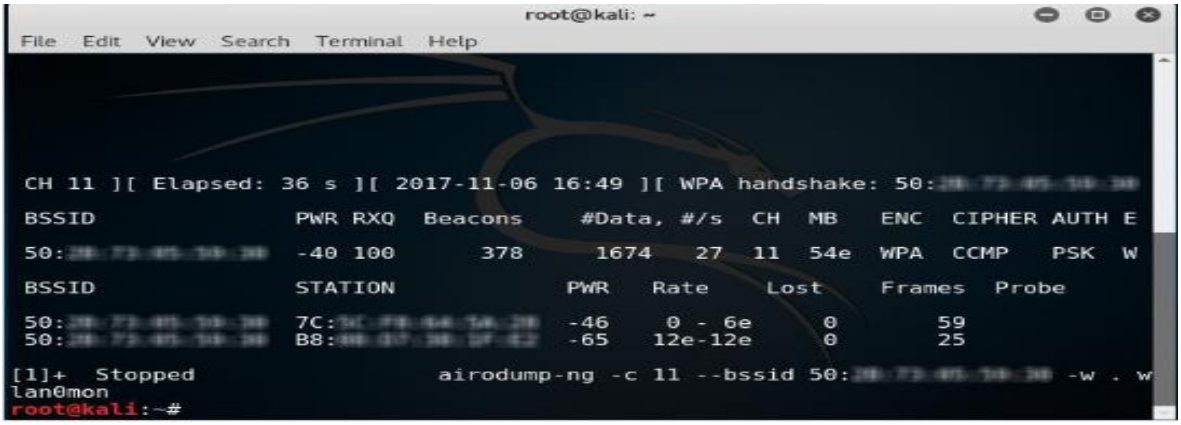
5. Use the following command to capture a 4-way handshake by using airmon-ng to monitor traffic on the target network using the channel and BSSID values

"airodump-ng -c 3--bssid 9C:5C:XX:XX:XX:XX -w.wlan0"

where

"-c 3" is used to specify the channel number 3

6. Now, wait to capture the handshake packet. Once you have capture a packet, you will see the output similar to figure



7. You will see a capture .cap file in your /root location which is a default location

8. Now, run this capture file against a wordlist to crack the WPA key