**EXPERIMENT 5**

**WIFI HACKING**

**INTRODUCTION:**

* Wifi hacking is essentially cracking the security protocols in a wireless network, granting full access for the hacker to view, store, download, or abuse the wireless network. Usually, when someone hacks into a Wifi, they are able to observe all the data that is being sent via the network.

**TOOLS**:

1. Kali Linux
2. Wifi adapter

**Step1:**

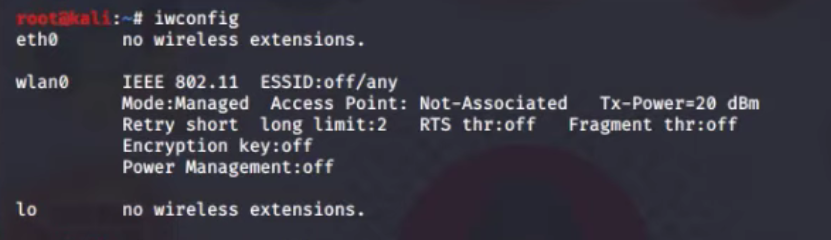
****

Figure 5.1

* Goto the kali Linux and open the terminal and type “**iwconfig**” if it show wlan0 then we go for next step.
* If it not show wlan0 disconnect the wifi adapter and again connect it.

**Step2:**

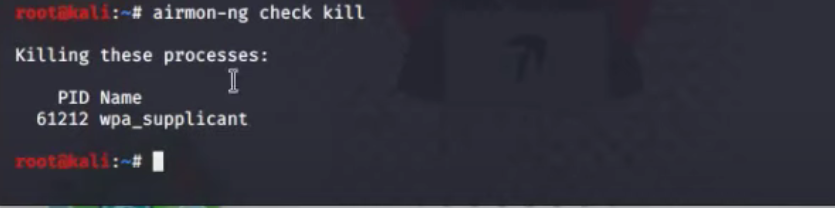


Figure 5.2

* Then we type **check kill** for kill all airmon**-ng** process.

**Step3:**

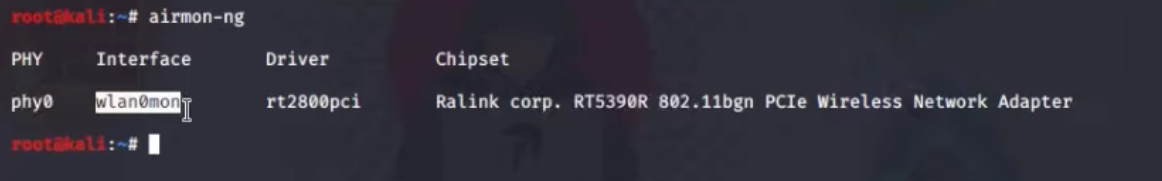


Figure 5.3

* In airmon-ng we find the **interface wlan0** and **chipset name of the wifi adapter we use.**

**Step4:**

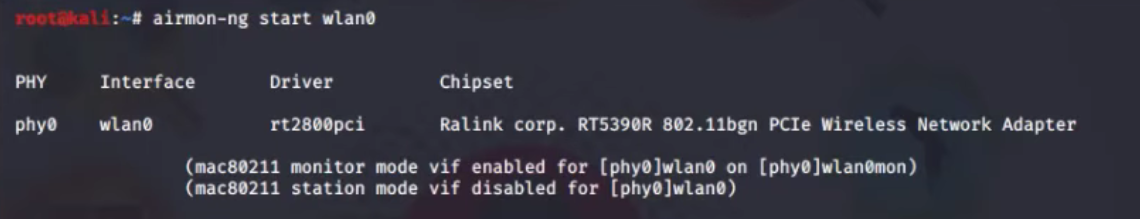


Figure 5.4

* In here we show that we are in **monitor** mode.
* It allows a computer with a wireless network interface controller (WNIC) to monitor all traffic received on a wireless channel.

**Step5:**

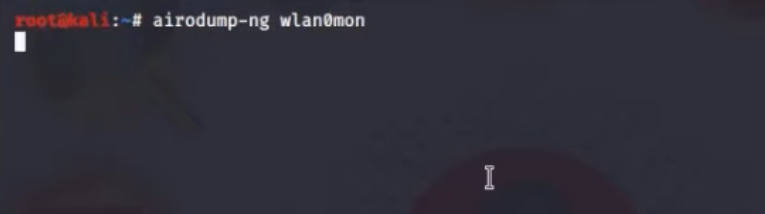


Figure 5.5

* In this step we try to catch wifi BBSID.

**Step6:**

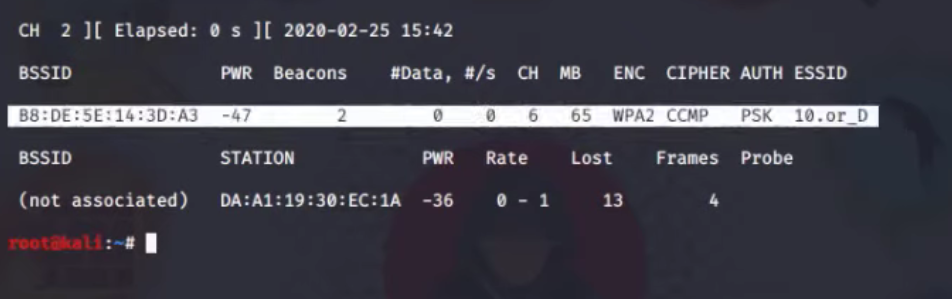


Figure 5.6

* Now we find one **wifi BSSID** and **CH** no 6.

**Step7:**



Figure 5.7

* Now we try to catch the WIFI handshake File name is **target handshake.**
* And it store**.cap** file format.

**Step8:**

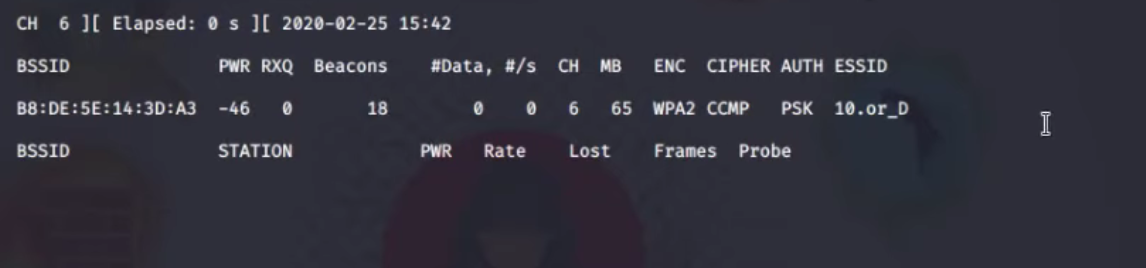


Figure 5.8

* Now our handshake capture process is start.

**Step9:**

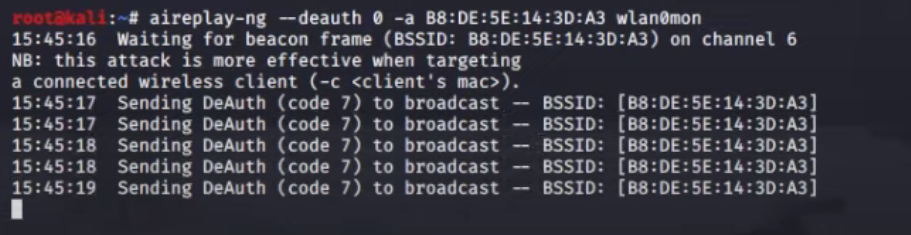


Figure 5.9

* In this step we send the multiple requests to router to disconnect the router to one any device which is connect to the router.

**Step10:**

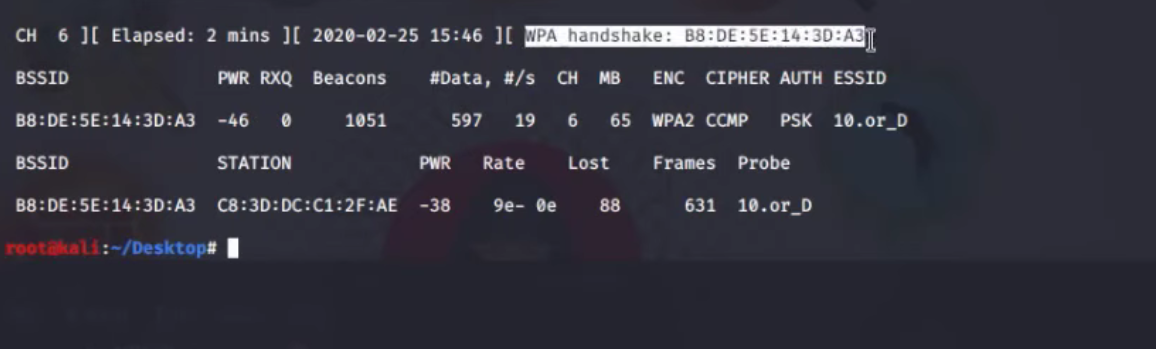


Figure 5.10

* In this step we disconnect one device which is connect to the router.
* And when the devices again connect to the router, we catch the **handshake**.

**Step11:**

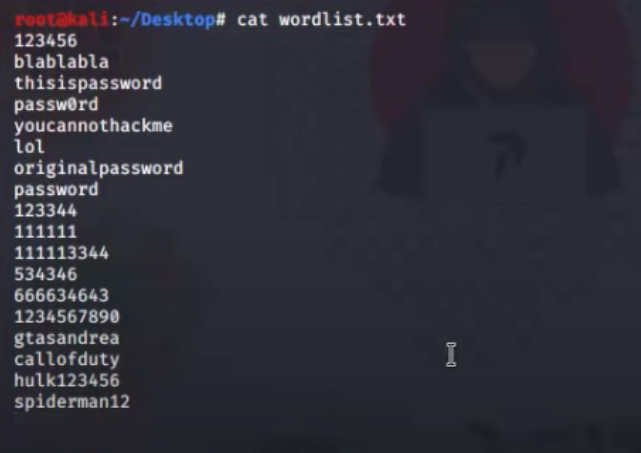


Figure 5.11

* We make a **wordlist** file to Which is using to catch the Wi-Fi password.

**Step12:**

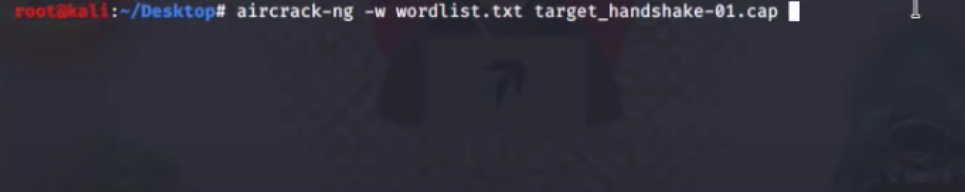


Figure 5.12

* We set our **wordlist** file path and our **handshake** file path.
* Then we start the **Brute force** attack to find the password of WIFI. Then press enter

**Step13:**

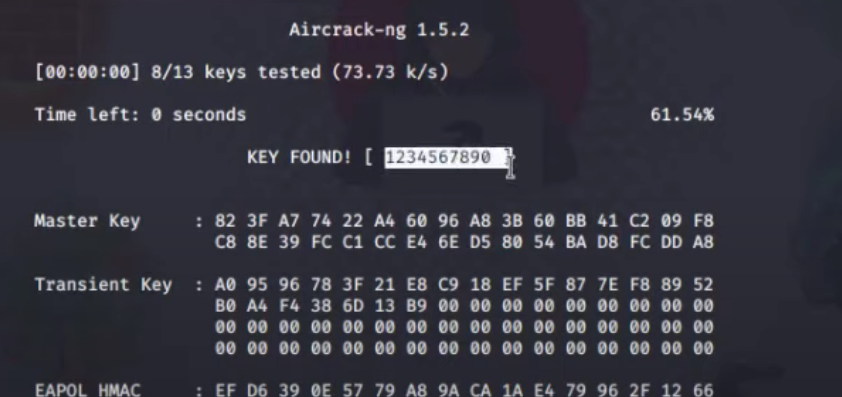


Figure 5.13

* Then our attack is start. And we got the Wi-Fi password in plane test.

**Result**: The Wi-Fi password was obtained which was found to be 123456790