# **WPA2 PSK Attack on Router**

**By**

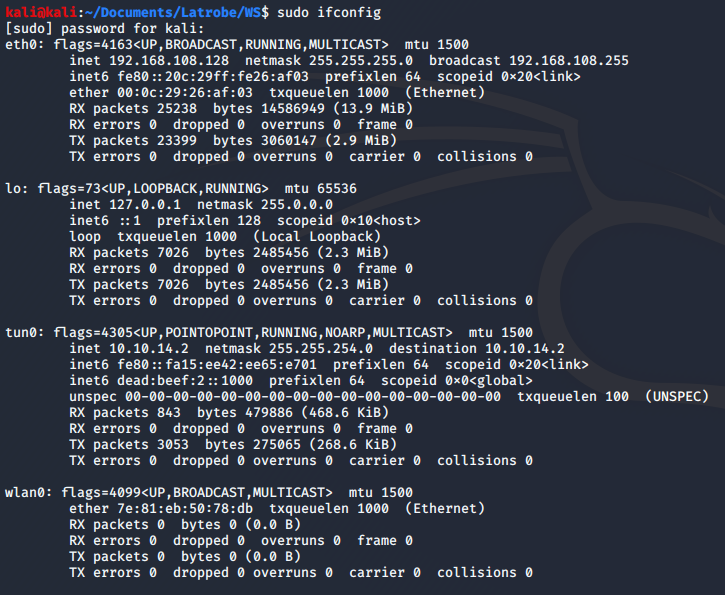
**Rehoodie09**

# Test Environment:

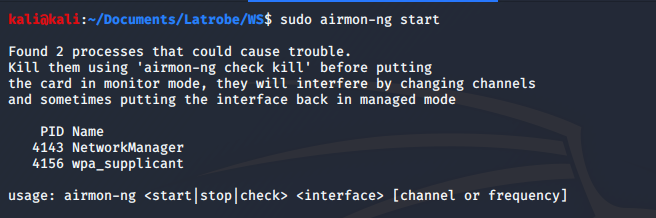
* Host Machine: Windows 10 Pro
* Virtual Machine: Vmware workstation pro 15.5
* Attack OS: Kali Linux – vmware -2020.1- amd64
* Wireless Adapter: ALFA Atheros AR9271

## Step 1 (Setup kali on monitor mode):

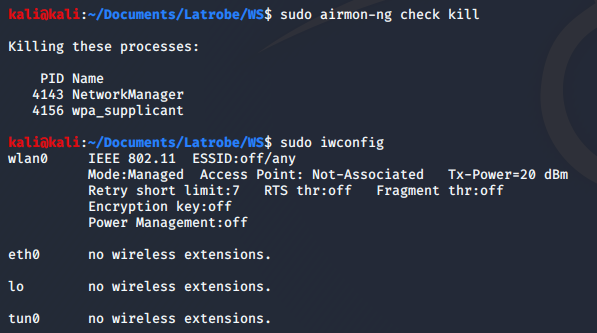
Connect the ALFA wifi card to the Kali Linux machine running on vmware. Ifconfig command will show wlan0 on the terminal.



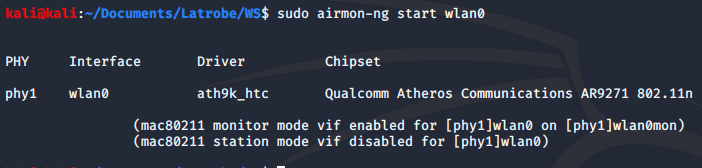
Start airmon-ng to go the monitor mode. Here we can see there are 2 processes are running. We will have to kill these network processes to start the monitor mode.



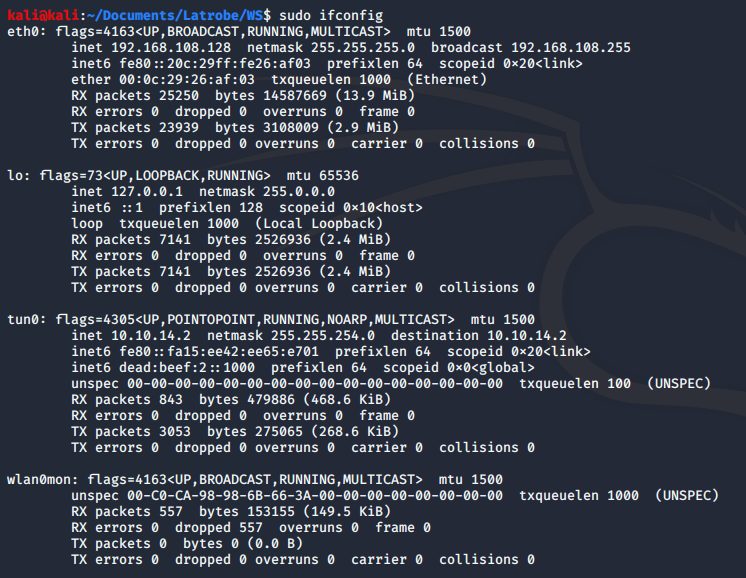
**sudo airmon-ng check kill**



**sudo airmon-ng start wlan0** (here wlan0 is the interface)



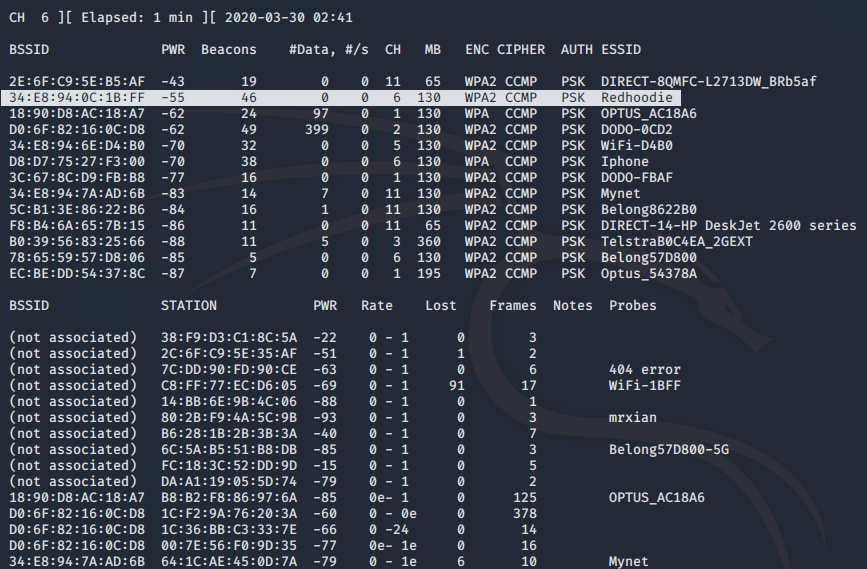
Here we can see wlan0mon which is the monitor mode.



## Step 2 (Search for the target AP):

To search the network area around the attack machine and determine the specific AP we are going to target.

**sudo airodump-ng wlan0mon**

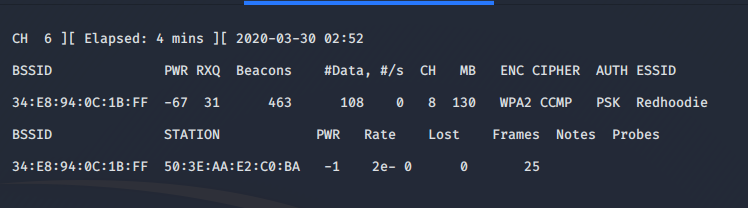


Above we can see, ESSID Redhoodie which is our target AP. BSSID is showing the mac address, PWR is the power (ideally the closer you are to the AP (-n\*) value will decrease. It means attack machine is closer to -55 AP than -86 Ap Mynet).

\*\*Although here the channel is showing 6 for our target but more isolated enumeration is telling us it is actually running on channel 8.

## Step 3 (Capture the handshake):

**sudo airodump-ng -c 8 --bssid 34:E8:94:0C:1B:FF -w redhoodie wlan0mon**



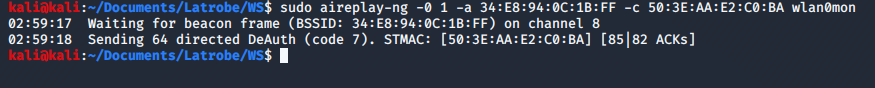
Here, the terminal is showing the AP is running on channel 8. We are looking for the handshake to show up on the top next to date & time. This process might take some time. Let’s keep the airodump running…

\*\*\*We can fast track this process through a deauth attack. (Sometimes we might have to run this attack few times to capture the handshake. Here we are trying to kickout a client for a fraction of a second out of the network, then the client will try to connect again, and we will capture the handshake. But do not run it too many times, it might cause other disruption on the network.

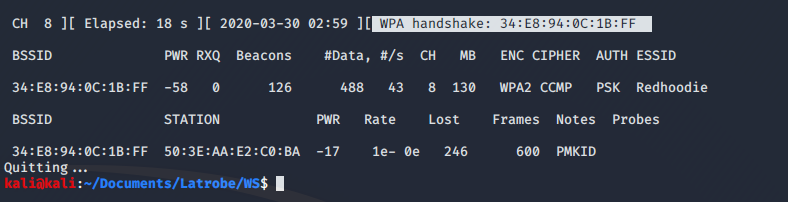
Open a new window and run…

**sudo aireplay-ng -0 1 -a 34:E8:94:0C:1B:FF -c 50:3E:AA:E2:C0:BA wlan0mon**

* -0 = to deauth
* 1 = it will run once
* -a = mac address
* -c = station address
* Wlan0mon = interface



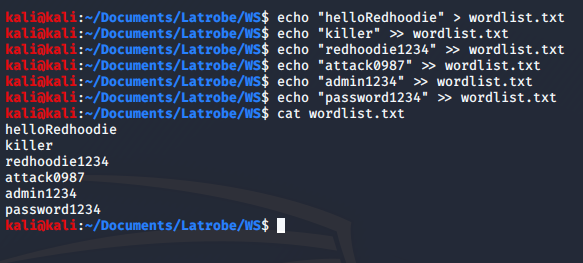
Go back to the airdump window



4-way handshake captured

## Step 4 (Lets crack the password of the router):

Here I have created a .txt file with some common passwords just a Proof of concept. The other password files we can try which is already in the kali machine are located **usr/share/wordlists** or we can download **seclists** from github.

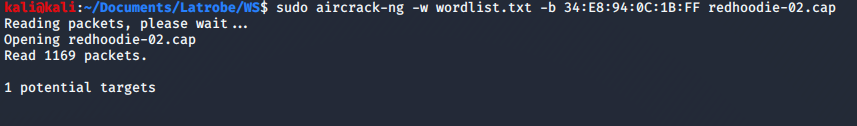


**sudo aircrack-ng -w wordlist.txt -b 34:E8:94:0C:1B:FF redhoodie-02.cap**

-w = wordlist.txt file containing the password we want to try

-b = mac address of the AP

Then specify the captured file





Air crack-ng cracked the password in less than a second. Although, I only run it with 6 passwords given on the wordlist I have created. Most of the time, people leave their router password as default, which is admin/admin (worth a try), companies use password in relation to their company name, department name or street name. These information’s can be obtained through OSINT tools to narrow down the password list. Therefore, it is recommended to use WPA2 Enterprise solution even for the small business environment.

#### (This walkthrough is only for educational purposes. Please do not use it for any unethical activities.)