Brute-force attacks : WPA and WPA2 .

Kali Linux can be used for many things, but it probably is best known for its ability to do penetration test, or "hack," WPA and WPA2 networks. There is one way that hackers get into your network, and that is with a Linux-based OS, a wireless card capable of monitor mode, and aircrack-ng or similar.

1. Step :

Start Kali Linux and login as root.

2. Step:

Plugin your injection-capable wireless adapter.

3. Step :

Disconnect from all wireless networks, open a Terminal, and type airmon-ng

Fig. 7 result of airmon-ng command

This will list all of the wireless cards that support monitor (not injection) mode, my card supports monitor mode and that it's listed as wlan0.

4. Stepr:

Type **airmon-ng start** followed by the interface name of the wireless card. mine is **wlan0**, so my command would be: **airmon-ng start wlan0**

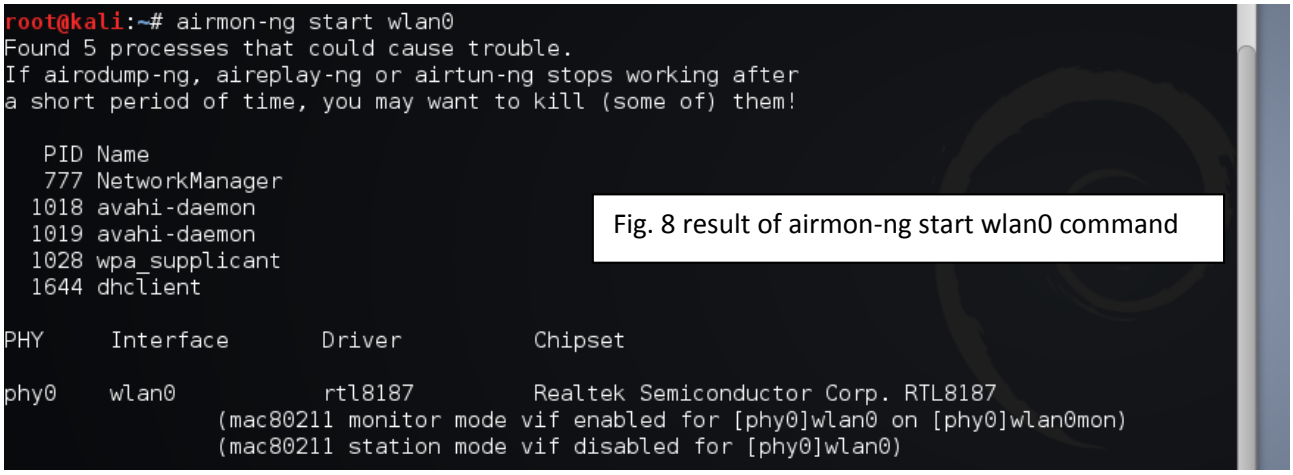

Fig. 8 result of airmon-ng start wlan0 command

The "(monitor mode enabled)" message means that the card has successfully been put into monitor mode. Note the name of the new monitor interface, **wlan0mon**.

5. Step:

Type **airodump-ng** followed by the name of the new monitor interface, **wlan0mon.**

6. Step:

Airodump will now list all of the wireless networks in your area, and a lot of useful information about them. Locate your network or the network that you have permission to penetration test. Once you've spotted your network hit **Ctrl + C**on your keyboard to stop the process. Note the channel of your target network.

In this case I have created a Wi-Fi with my phone called AndroidAP.

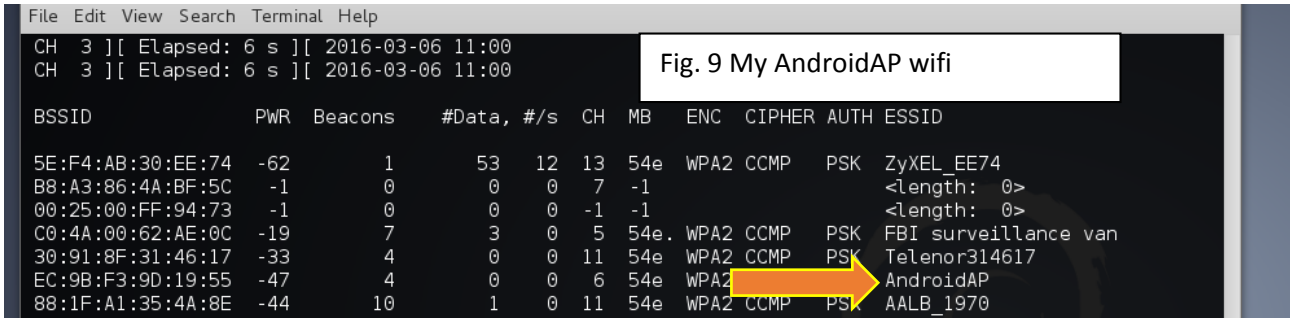

Fig. 9 My AndroidAP wifi

7. **Step :**

Copy the BSSID of the target network

Now type this command:

airodump-ng -c [channel] --bssid [bssid] -w /root/Desktop/ [monitor interface]

Replace [channel] with the channel of your target network. Paste the network BSSID where [bssid] is, and replace [monitor interface] with the name of your monitor-enabled interface, (**wlan0mon**). The "–w" and file path command specifies a place where airodump will save any intercepted 4-way handshakes (necessary to crack the password). Here I saved it to the Desktop.

A complete command should look similar this:

airodump-ng -c 6 --bssid EC:9B:F3:9D:19:55 -w /root/Desktop/ wlan0mon

Now press enter.

8. **Step:**

Airodump with now monitor only the target network, allowing us to capture more specific information about it. What we're really doing now is waiting for a device to connect or reconnect to the network, forcing the router to send out the four-way handshake that we need to capture in order to crack the password.
Also, four files should show up on your desktop, this is where the handshake will be saved when captured.

But we're not really going to wait for a device to connect, that's not what impatient hackers do. We're actually going to use another tool that belongs to the aircrack suite called aireplay-ng, to speed up the process. Instead of waiting for a device to connect, hackers can use this tool to force a device to reconnect by sending deauthentication (deauth) packets to one of the networks devices, making it think that it has to reconnect with the network.

Of course, in order for this tool to work, there has to be someone else connected to the network first, so watch the airodump-ng and wait for a client to show up.
You can see in this picture, that a client has appeared on my network, allowing me to start the next step.

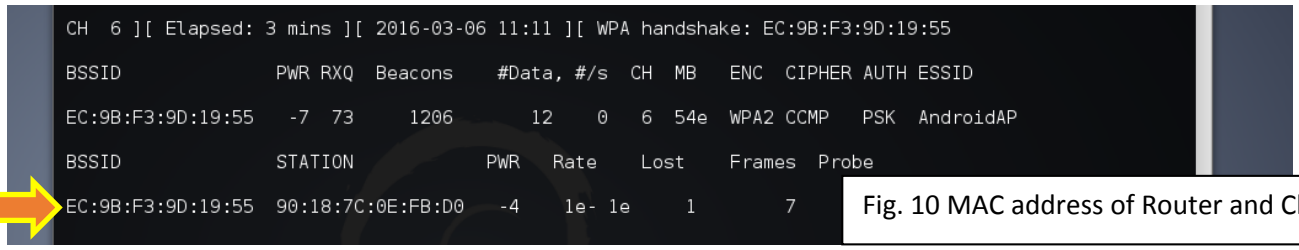

Fig. 10 MAC address of Router and Client

9. Step:

Leave **airodump-ng** running and open a second terminal. In this terminal, type this command:

aireplay-ng –0 2 –a [router bssid] –c [client bssid] mon0

The **–0** is a short cut for the deauth mode and the **2** is the number of deauth packets to send.

-a indicates the access point/router's BSSID, replace [router bssid] with the BSSID of the target network, which in my case, is EC:9B:F3:9D:19:55.

-c indicates the client's BSSID, the device we're trying to deauth, noted in the previous picture. Replace the [client bssid] with the BSSID of the connected client, this will be listed under "STATION."

My complete command looks like this:

aireplay-ng –0 2 –a EC:9B:F3:9D:19:55 –c 90:18:7C:0E:FB:D0 wlan0mon

10. Step:

Upon hitting Enter, you'll see aireplay-ng send the packets and the deauthentication process works, this message will appear on the airodump screen (which you left open):

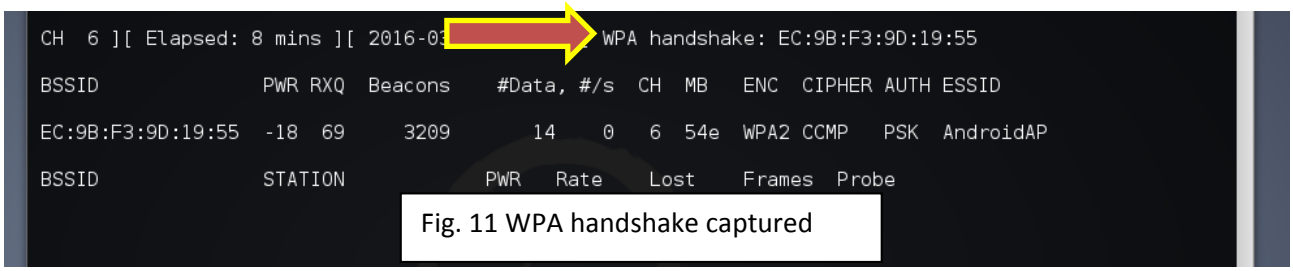

Fig. 11 WPA handshake captured

This means that the handshake has been captured, the password is in the hacker's hands, in some form or another.

11. Step:

From now on, the process is entirely between your computer, and those four files on your Desktop. Actually, it's the .cap one, that is important. Open a new Terminal, and type in this command:

aircrack-ng -a2 -b [router bssid] -w [path to wordlist] /root/Desktop/*.cap

-a is the method aircrack will use to crack the handshake, 2=WPA method.

-b stands for bssid, replace [router bssid] with the BSSID of the target router, mine is EC:9B:F3:9D:19:55.

-w stands for wordlist, replace [path to wordlist] with the path to a wordlist that you have downloaded. I have a wordlist called "password.txt" in the root folder.

/root/Desktop/*.cap is the path to the .cap file containing the password. The * means wild card in Linux, and since I'm assuming that there are no other .cap files on your Desktop, this should work fine the way it is.

My complete command looks like this:

aircrack-ng –a2 –b EC:9B:F3:9D:19:55 –w /root/password.txt /root/Desktop/*.cap

Now press Enter.

12. Step:

Aircrack-ng will now launch into the process of cracking the password. However, it will only crack it if the password happens to be in the wordlist that you've selected. Sometimes, it's not. If this is the case, you can try other wordlists. If you simply cannot find the password no matter how many wordlists you try, then it appears your penetration test has failed, and the network is at least safe from basic brute-force attacks.

Cracking the password might take a long time depending on the size of the wordlist.