

Forum:[Hack Forums](#)

Thread: [Hacking using a wifi pineapple \(or laptop\) - Part Two - Sniffing](#)

FractumSeraph - December 24, 2015, 11:12 pm

Hello again, this time will be covering How to Sniff Packets Over a WiFi Network.

Requirements:SSH (Included in Pineapple/Kali)[/*]
Aircrack Suite (Included in Pineapple/Kali)[/*]
WiFi Card that supports monitor mode (Included in Pineapple)[/*]

The first thing we need to do is [connect to the pineapple using ssh](#).

Code ssh root@172.168.42.1Once we are there, we can go ahead and run ifconfig to make sure our wifi interface is up.

Spoiler ([Click to View](#))

As you can see here, both of my wireless interfaces are running. If yours are not, don't forget to bring them up as covered in the previous tutorial. (ipconfig wlanX up)

The next thing we need to do is put them into '[monitor mode](#)'. A brief explanation of monitor mode is that it allows your wireless card to pick up traffic from ALL the wireless networks in range, instead of just the one you are connected to. (More to it than that, but that will suffice until we get to promiscuous mode in a later tutorial.)

Not all wireless cards can do this. Both of the ones on the pineapple can, and so can the one sold at the shop ([AWUS036NEH](#)). If you are lucky, you already have a device that has one. My laptops wifi is able to do this, however the one I had before it cannot. In order to check we will be using a new set of applications called the Aircrack Suite.

The tool used to put your card in monitor mode is Airmo-ng. So lets go ahead and run that.

Spoiler ([Click to View](#))

In order to attempt to put one of them into monitor mode, we will run this command:

Code airmon-ng start wlanXairmon-ng is the name of the program

start is what we are telling the program to do

wlanX is telling it which wifi card to start (Replace X with whichever number your card is, in my case I can use either 0 or 1)

Spoiler ([Click to View](#))

Now lets check ifconfig to see if anything has changed.

Spoiler ([Click to View](#))

You should notice that the name of wlan1 has changed to wlan1mon

At this point either it's working, or it's not.

Sometimes, other programs you have open will interfere with it, so you may need to close them. To do this run this command:

Code airmon-ng check killairmon-ng is the program
check tell it to check if anything is interfering with it
kill tells it to close the programs if they are

Spoiler ([Click to View](#))

If you have any problems, I recommend running this command and trying again.

wpa_supplicant which is the main program Kali Linux 2.0 (Sana) uses for wifi will cause problems, so it will have to be killed. Unfortunately this means you will not be able to use the network manager while you are in monitor mode. (Meaning you will lose wireless connectivity)

Thankfully, this is not a problem on the Pineapple.

So if your lucky and have a device that will go into monitor mode, we can continue. If not then I'm afraid there is nothing you can do until you get one.

Now that we have a device in monitor mode, we will use a tool called Airodump to take a look at what this wifi card can see. For now, simply run:

Code airodump-ng wlanXmonAirodump-ng is the program
wlanXmon is the interface we are selecting

After this, the window will change a bit

Spoiler ([Click to View](#))

I'll explain a the parts you need to worry about at the moment. The top is all the access points the card has detected (WiFi Routers in this case). The bottom is all of the devices connected.

For the Access Points, or APs, you will see the BSSID (MAC addresses, like serial numbers) of the device, the PoWeR (Signal Strength), the CHannels, and the ENCryption type. (Open, WEP, or WPA)

For the devices, you will see the MAC addresses of the AP it is connected to, the MAC address of the device, and any probes it has made.

What's a probe? Here is a non-technical explanation.

Spoiler ([Click to View](#))

A probe is when a device checks if there are any known networks around. Whenever you have a network saved in your phone or laptop, it will constantly scan to see if it's in range of the networks. If it is, it will connect to it. If it's not, it will wait a few moments and try again. For example, one of the devices shown above is my cell phone. The probe is Mullins-WiFi, meaning that my cell phone

asked the the network named Mullins-WiFi was in range. Since my router was close enough to hear it, it responded by saying "Yes! I'm right here!" and then my phone connected to it.

These probes are useful because it will show the names of networks a device has previously connected to, and you can also fool devices into connecting to a network of your own if you give it the same name.

Now let's go ahead and exit that. We do this by pressing Control + C at the same time. As a sidenote, this is a nearly universal linux command, this is how to exit, or cancel on most linux terminal programs.

This time we are going to run the airodump command again, except now we are going to add another argument.

Code `airodump-ng -w MyFirstDump wlanXmon` So the newest addition is `-w MyFirstDump`

`-w` tells it to save everything it captures

`MyFirstDump` is the name of the saved file.

The reason we want to save this is so we can use it for the next tutorial, which will be showing how to get the password of nearby WiFi networks.

Of course this isn't the only thing it's useful for, but it is the first thing I'll be going over.