

Forum:[Hack Forums](#)

Thread: [Hacking using a wifi pineapple \(or laptop\) - Part Three - Cracking WiFi](#)

FractumSeraph - December 25, 2015, 1:04 am

Welcome to part three of my tutorial series. I will be showing you How to Capture a 4-way Handshake. The first of two steps in cracking a WiFi password.

Requirements:SSH[/*]
WiFi Card with Monitor Mode[/*]
Aircrack Suite[/*]
Dictionary[/*]
mdk3 (Optional)[/*]

So if you've been following along you should now be able to sniff packets from a wireless card in monitor mode.

I'll briefly explain what we need to do.

We need to start recording just like we did before with airodump.
While that is running, we need to also do a deauthentication attack at the same time.
Optionally, we may may strip the file down to save space.
Then we can run a bruteforce attack using the data we just collected.

First we need to start monitor mode and start capturing as shown on part two.

```
ifconfig wlan1 up  
airmon-ng check kill  
airmon-ng start wlanX  
airodump-ng -w MySecondDump wlanXmon
```

Now that we have that running in the background, capturing all the network traffic, we need to work on capturing a 4-way handshake.

So what's a 4-way handshake anyways?

Spoiler ([Click to View](#))

Whenever you connect to a WiFi access point, a couple of things happen. First the AP has to announce that it is there and ready to give wifi.(Called a beacon) Then your phone has to let the router know that it wants to connect. The router will have a set way of authenticating a user, usually WPA PSK, so it will ask for a password. You type the password into your device and send it. Then the AP either accepts it or denies it.

If we can record this entire process using airodump, we will have all the information we need to perform an attack to get the actual password. The easiest way of doing this is simply to let airodump capture and record packets. Eventually someone will come along and connect to the network, then we will have the handshake.

So at this point in time you should have airodump running and collecting packets. In order to check if it has captured a 4-way handshake or not, simply run this command:

Code `aircrack-ng MySecondDump-01.cap`(It automatically adds an 01 to the end of the name, to prevent to files from having the same name.)

Either you didn't wait long enough (Nobody connected to the network while it was capturing)

Spoiler [\(Click to View\)](#)

Or somebody connected to the network and it was successfully recorded.

Spoiler [\(Click to View\)](#)

Now I realize that sitting there and waiting on someone to connect to the network might not be the funnest thing to do, or the fastest. So you can GREATLY speed this up, as long as there is already a wireless device on the network. The way we do this is by a deauthentication attack. Basically we force their devices to reconnect to the network, so we can capture the handshake when they do. I find the best way to do this is with a tool called mdk3. This is a part of Kali, but it's not built in on the pineapple. To install it on the pineapple, simply run:

Code `opkg install mdk3`Now that we have mdk3, we can use it to run this attack. There are two ways to run this attack. One way is by running the attack against anything, basically creating a WiFi jammer. The second (And nicer) way, it to target a device and attack it.

To do it the first way, you will simply use:

Code `mdk3 wlanXmon d -c`

Spoiler [\(Click to View\)](#)

mdk3 is the tools
wlanXmon is the wifi card to use
d tells it to do a deauthitication attack
-c tells it to run the attack on all channels

If you would like to do it the second way, you need to know the targets MAC address. Once you have this address, save it in a text file named Targets.txt Then the command would be:

Code `mdk3 wlanXmon d -b Targets.txt -c`

By either waiting long enough, or by using this trick (Or both) you will eventually capture the handshake.

Now we can use it to bruteforce the wifi password. This is where the dictionary comes in. You're going to need a password list. The ways this works is that it tests every single password in

the list, and if one of them is right, it will tell you.

A good place to find them is [here](#).

Now that we have both a .cap file containing the 4-Way handshake and a dictionary, we can start the attack.:

Code `aircrack-ng MySecondDump.cap -w Dictionary.txt`It will then ask you which network you would like to attack. Simply type the number to the left, then press enter.

Now it will go through every password in the list until either it finds the password, or it goes through every password and it's not on the list.

Spoiler ([Click to View](#))

[img]<http://s17.postimg.org/5wc7dthdr/e1dbf7425724bcdd519241617a844592.png>[/img]

A few notes. The first one is that the speed of the crack depends on the capabilities of your computer. Using Both my CPU and GPU, my computer takes about 3 hours to test my massive 13Gb list, which contains just under one billion passwords. (i7 6700 3.4gh, Nvidia GTX960, 16gb RAM)

If you have a computer less powerful, you'll want to look for smaller, more optimized lists. Things like the most commonly used passwords.

Another note is that using the mdk3 tool without a target is extremely disruptive, please don't do it this way. It will kick everyone in range off of whatever wifi they are on, the only reason I even include it here is so you don't go around doing it unknowingly.

Also, aircrack only uses your computer's CPU, so having a good video card will not make it run faster. I will create another tutorial later showing how to use a few alternatives. Just as deauthentication without mdk3, and using tshark, cowpatty, and pyrit to verify handshakes instead of aircrack. And also how to capture and strip your .cap files at the same time.

It's 3AM on December 25th, so I will be out with family most of the day tomorrow, odds are I won't have a chance to right part four until Saturday.

teddy69 - January 2, 2022, 7:35 pm

is the dictionary in this attack one you created or downloaded, can you share the link if it is download for kali