

Forum:[Hack Forums](#)

Thread: [How to Hack Wi-Fi | Detailed!](#)

Threat - October 4, 2019, 9:34 am

In this post I will teach you a way of Wi-Fi hacking WITHOUT using brute force techniques!

There is a lot of required pre-requisites with the terminology, and please, remember, this won't work as not all people are dumb enough to fall for this. However, it will most likely work so please don't get yourself in trouble, and I am not responsible for anything you do! Take this post as Knowledge

Firstly, you will need a Virtual Machine or computer running any type of Linux, preferably Kali Linux: [Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution](#)

Once you have that, continue to download the tool:

Spoiler

So before we start, I will explain how this tool works:

- â€¢ Scan the networks.
- â€¢ Capture a handshake (can't be used without a valid handshake, it's necessary to verify the password)
- â€¢ Use WEB Interface
- â€¢ Launch a FakeAP instance to imitate the original access point
- â€¢ Spawns a MDK3 process, which deauthenticates all users connected to the target network, so they can be lured to connect to the Fake-AP and enter the WPA password.
- â€¢ A fake DNS server is launched in order to capture all DNS requests and redirect them to the host running the script
- â€¢ A captive portal is launched in order to serve a page, which prompts the user to enter their WPA password
- â€¢ Each submitted password is verified by the handshake captured earlier
- â€¢ The attack will automatically terminate, as soon as a correct password is submitted

TLDR:

Scans for Wi-Fi, captures a packet that is used to authenticate password, then creates a "Fake" Wi-Fi access point that acts like the original one and simultaneously kicks everyone off the original network. This causes people to join your fake access point instead of the real access point. Then when they access your fake wireless point, they will be greeted with a "login" that requires them to put in their Wi-Fi credentials, that then are sent to you by validating that capture packet that you took at the beginning. Now you have access to the Wi-Fi network!

Now, this technique is not always guaranteed to work, it is a Social Engineering method! (Tricks

people)

I recommend you target your own network first to play with it and test it first before trying it out on your target.

----- Steps

STEP 1: <https://i.imgur.com/C4xoWI3.png>

Select all channels to scan for Wi-Fi

STEP 2: <https://i.imgur.com/dZ18Wf4.png>

Find your target Wi-Fi network

STEP 3: <https://i.imgur.com/B4lldBc.png>

Choose the first option for medium connection and second for slower connection

STEP 4: <https://i.imgur.com/7n5KDw4.png>

STEP 5: <https://i.imgur.com/Ha5r0U1.png>

STEP 6: <https://i.imgur.com/ufJrNvs.png>

Choose both, see which one works better, try the first one then try mkdr3. (Both should work fine)

STEP 7: <https://i.imgur.com/U4uT8yR.png>

STEP 8: after waiting 1-2 minutes; <https://i.imgur.com/Krk0Q2M.png>

STEP 9: <https://i.imgur.com/gpLXeHh.png>

This is the point in the guide where after this you must choose your web interface. Say you are in Australia, a big internet provider is Telstra. There are some premade web interfaces available for selection.

STEP 10: <https://i.imgur.com/Ege9NDL.png>

STEP 11: <https://i.imgur.com/3BG17cb.png>

STEP 12: <https://i.imgur.com/QZZdghc.png>

Here are the two networks, one of which are inaccessible (the real one), and yours (the fake one)

STEP 13: <https://i.imgur.com/KVE7CJO.png>

If successful, the target will input their WPA password into the fake website, which then will be redirected to you.

STEP 14: <https://i.imgur.com/GUVFgyt.png>

If successful, this window will show. You are then able to retrieve the password from the saved folder in your /root/ directory..

japakoni - October 7, 2019, 3:45 am

I dont know how but it works for me, THANKS

Threat - October 12, 2019, 1:28 pm

(Oct 12, 2019 01:27 PM)jeeje009 Wrote: [\[CITE\]](#) it's one of the basics but very important I believe. Great job my man.

lol why are you spamming all my threads with the same message