

Forum:[Hack Forums](#)

Thread: [\(TUT\)Hack Wifi Hotspots in Hotels, Coffee shops, and more](#)

Mr. Corleone - September 14, 2016, 1:55 pm

How to hack Wifi hotspots in Hotels, coffee shops, and more

[img]http://cdn.osxdaily.com/wp-content/uploads/2012/03/change-mac-address.jpg[/img]

How does it work?

You all know that moment: the happy moment that you find a public hotspot followed with the disappointment because of a pop-up that asks for a login-code.

Everyone's #1 frustration, at least it is mine. Now you can either be a nice guy and buy one of those cards, or you can be stubborn and try to hack stuff.

We're going for the second one.

The security on these hotspots are usually based on MAC-addresses.

The router has already been set-up to decide which computers can and cannot use the internet. During the login process, access is given to the internet with a code: your MAC-address is being saved in a sort of database.

This will stay there for a couple of hours, depending on how much you paid for. After these hours are over,

the MAC-address will be automatically removed from the database that's from the router, and your access to the internet will be removed.

If you don't have one of these cards, you won't be able to use the internet either.

But you are however connected to the network (At least the connection to the network that connects you to the login page.)

You might feel it coming already, you can pry/spy into the network! What we will do isn't really difficult and I will sum it up in three steps:

1. Look which devices are connected to the network (Which MAC-addresses have internet.)
2. Change your MAC-address to a MAC-address with access to the internet.
3. Re-connect to the Access Point, the Hotspot.

Once you connect to the network again, the router will recognize you as a user that paid to use the internet and it will grant you access to the internet.

Execution

It's best if you have Linux to execute this. I myself use Kali Linux, but any distro should work.

Open your terminal, we will turn off our wlan interface. Type:

Code `ifconfig wlan0 down`

Now we will put our network interface in a monitor mode:

Code `iwconfig wlan0 mode monitor`

And now we will check if that actually happened:

Code `iwconfig`

Now we will look for all networks nearby you. These networks will then be shown with a BSSID MAC-address.

Code `airodump-ng wlan0`

Wait a while until your 'target network' appears and then copy the BSSID that belongs to it. Then press CTRL+C to stop airodump-ng. Otherwise it will endlessly continue to search for networks.

Now we will look for every device on the network.

The devices are the computers that are connected to the network and are shown in the form of a MAC-address.

It can take a while before these computers are found. It's important to wait a while to see which MAC-address has a lot of traffic.

This is the one that we will use, copy the MAC-address.

Code airodump-ng -bssid [MAC ADDRESS OF THE NETWORK HERE] wlan0

Then:

Code ifconfig wlan0 down

And then we can change our MAC-address to the one which you choose:

Code macchanger -m [MAC ADDRESS OF THE COMPUTER WHICH YOU CHOSE] wlan0

Now you will get a verification that your MAC-address has changed.

If you successfully did this, we will change our interface again in 'manage mode':

Code iwconfig wlan0 mode manage

Then turn on our WiFi-adapter again:

Code ifconfig wlan0 up

Check to see if it's on:

Code ifconfig

Now you will go to the network interface GUI. Connect again with your Hotspot and you can enjoy your free internet.

Conclusion

As you can see you can have access to the internet in a few easy steps.

The way around the security in this way is much faster and the chance to succeed is much faster than the standard way of WEP/WPA2 hacking.

Please take a second to say thanks so everyone can see this, thanks :)

rm -rf I - September 14, 2016, 2:43 pm

Good HQ post, will definitely help out beginners getting their feet wet. Thanks for the share!

iiGalaxy - September 14, 2016, 4:59 pm

Aye mate thanks, i'll save this thread on my bookmark

THC - September 14, 2016, 11:14 pm

Defiantly a okish tutorial.

OP just as a suggestion, include a section on how to test wifi cards for monitor mode compatibility. This can be done via the aircrack suite with relative ease.

Mr. Corleone - September 15, 2016, 12:16 am

(Sep 14, 2016 02:43 PM)rm -rf / Wrote: [\[CITE\]](#) Good HQ post, will definitely help out beginners getting their feet wet. Thanks for the share!

Thanks alot, appreciate it :)

(Sep 14, 2016 11:14 PM)M.D. Wrote: [\[CITE\]](#) Defiantly a okish tutorial.

OP just as a suggestion, include a section on how to test wifi cards for monitor mode compatibility. This can be done via the aircrack suite with relative ease.

Thanks for the feedback.

I don't really feel like expanding anything on this topic as of right now, simply because I think it's not really that 'special' or important. That's the reason why I placed it in the beginner hacking section. This also gives a little view of how this works, etc.

Omicron. - September 15, 2016, 12:55 am

nice one :) can you name necessary tools or maybe even the way on windoze?

Mr. Corleone - September 15, 2016, 2:25 am

(Sep 15, 2016 12:55 AM)Omicron. Wrote: [\[CITE\]](#) nice one :) can you name necessary tools or maybe even the way on windoze?

<https://www.aircrack-ng.org/>

Honestly it's way easier with Linux, since you can do everything in a terminal.
In Windows you'll have to work with several GUIs, which can be pretty annoying.

weary_learner - September 15, 2016, 2:30 am

Thank you for this!

I'm going to try this out tonight! :D

CyberError - September 15, 2016, 2:36 am

Thanka gonna try this out too

dollar95 - September 15, 2016, 4:45 am

Thanks for this great tut!

derekalex - September 15, 2016, 6:01 am

Great tutorial. Can't wait to try it!

Cute - September 15, 2016, 6:08 am

Thanks man, gonna try out today.

kpown - September 15, 2016, 7:18 am

Good tutorial OP! This should work on airlines too correct? If so then this is extremely useful. Don't have to pay ridiculous sums for shitty wifi on long flights

Anxious.exe - September 15, 2016, 8:04 am

HQ post, really great tut. User is definitely HQ !

Mr. Corleone - September 15, 2016, 9:10 am

(Sep 15, 2016 07:18 AM)kpown Wrote: [\[CITE\]](#) Good tutorial OP! This should work on airlines too correct? If so then this is extremely useful. Don't have to pay ridiculous sums for shitty wifi on long flights

Yeah. With some places you get like 1 hour free, and after 1 hour you can try this out.

ikp_error404 - September 15, 2016, 10:05 am

Thank you :) It's really useful, will try this later

Kali_GFX - September 16, 2016, 3:54 am

Thanks alot, appreciate it

onlyhackzz - September 18, 2016, 6:33 am

Nice HQ tutorial, very well explained. This tutorial will definitely will help the beginners out.

Mr. Corleone - September 18, 2016, 7:10 am

(Sep 18, 2016 06:33 AM)onlyhackzz Wrote: [\[CITE\]](#) Nice HQ tutorial, very well explained. This tutorial will definitely will help the beginners out.

Thanks alot, appreciate the feedback.

sp??k? - September 18, 2016, 10:21 am

Very detailed tutorial. I will save this thanks alot!

EM1EL - September 18, 2016, 10:22 am

Thanks man going to try this out

Exkodera - September 18, 2016, 11:32 am

Nice tutorial keep it up!

Kess78 - June 4, 2017, 8:07 am

Does anyone know if this will disconnect the user that actually paid for the thing or we can both be connected ?

pbrnby11 - June 4, 2017, 10:21 am

Thanks, seen this explained in many places before but this is one of the most straight forward and concise guides out there.

Mr. Corleone - June 4, 2017, 7:06 pm

(Jun 4, 2017 08:07 AM)Kess78 Wrote: [\[CITE\]](#) Does anyone know if this will disconnect the user that actually paid for the thing or we can both be connected ?

It won't disconnect the other user.

Because if the router had a rule to only let 1 MAC address on the internet, then it would not let you connect with the spoofed mac in the first place.

Horus God - June 4, 2017, 7:17 pm

login without pass wifi ? ?

sprite77 - June 5, 2017, 11:26 pm

i heard that, they use pos pc to MIMF

chechulmao - June 7, 2017, 3:00 pm

thanks a lot man, gonna try as soon as I can. Will comment how it did