

Forum:[Hack Forums](#)

Thread: [PLEASE HELP How to bypass WiFi time limit?](#)

TheDailyGrind - October 23, 2016, 11:27 am

Hey guys,

So I recently pissed off my Dad, and he disabled my WiFi, also he has MAC filtering, and yes, he did change the router password. I can still access it when I used it wired, but I want to use it wireless. I do have some a plan though spoof my MAC Address to match someone elses MAC Address in the house. If someone else has an idea, please post it.

Blue7ornado - October 23, 2016, 3:41 pm

You can use macchanger if you're on linux :)

macchanger needs your interface not working while it's changing your mac address.. so you would use:

```
ifconfig wlan0 down
```

then the macchanger command:

```
macchanger -m (stands for mac address) XX:XX:XX:XX:XX:XX (the mac address you want to choose) wlan0
```

so.. for instance:

```
macchanger -m XX:XX:XX:XX:XX:XX wlan0
```

and then turn your interface up

```
ifconfig wlan0 up
```

That's it!

TheDailyGrind - October 23, 2016, 6:34 pm

Thank you so much, for now I am gonna grab all the other MAC Addresses, write them down, and just use them when my time limit kicks in. Thanks!

Asdethprime - October 23, 2016, 8:23 pm

Hi TheDailyGrind,

Lemme tech you an evil way.

The first thing you want to do is connect to the router at the same time you dad's connect to it. Then go to your terminal and type "ifconfig" which will allow you to see your IP address. Note the ip address down.

Let's pretend your IP address happens to be 192.166.7.112

What you want to do next is run a nmap scan on the whole domain as a root user,

```
sudo nmap -A 192.166.7.2-255
```

This will allow you to see your dad's MAC address. Remember for all this you will have to be manually connected to the router since you do not have the password (which is what I am guessing)

The next thing you want to do is reset the router [there is a small button behind the router that you can press normally with a pen's tip for few seconds) this will flush out the previous

username/password and change it to the default setting. This will now let you access the router. Your dad is going to eventually figured out that you've change the password hence now we need to a way to make sure you can find the wifi password whenever you want even if your dad decided to change it.

Under the WPS tab inside the router setting you will see a WPS pin, copy that somewhere and make sure you force the WPS pin to be enable.

Now you have 2 things with you:

1) Your dad's MAC address [which is always going to be among the allowed IP address to connect to WiFi]

Run macchange to change the MAC address to your dad's MAC address, when he isn't logged in on the WiFi

2) The WPS pin from which you can use reaver to extract wifi password whenever you want.

To get the password from reaver use the following step:

DO EVERYTHING HERE EXCEPT THE LAST STAGE

<http://lifelifehacker.com/5873407/how-to-crack-a-wi-fi-networks-wpa-password-with-reaver>

before you actually run reaver, add an additional flag --pin

From the example in the link you would do this:

```
reaver -i mon0 -b 8D:AE:9D:65:1F:B2 --pin <pin you got on the second step>
```

This will give you the wifi password right away because reaver here no longer has to guess the pin.

Unless your dad is smart enough to go in and manually disable the WPS option you can keep getting the password and masquerading as your dad's mac and log in anytime you want.

Hope this is helpful, the only real downside is your dad is going to know you reset the router once.

22gotya - October 23, 2016, 8:32 pm

You could always just manually reset the router to factory settings by holding the reset button down for 15 seconds and then connect to it with the default password or WPS option. This will reset everything and kick everybody off though, so you would have to re login everybody to avoid being caught. After you do that just go to 192.168.0.1 and set up your own admin account..