

Forum:[Hack Forums](#)

Thread: [\[TUT\] Easy DOS attack on a wireless router](#)

SIM-2015410 - March 23, 2014, 11:31 pm

Hello Again HF!,

Welcome to another Hacking Tutorial by MeshCollider.

If you are interested, here are links to my other hacking tutorials: Spoiler ([Click to View](#))

Metasploit 1: <https://hackforums.net/showthread.php?tid=4124763>

Metasploit 2: <https://hackforums.net/showthread.php?tid=4124800>

Metasploit 3: <https://hackforums.net/showthread.php?tid=4124838>

Cracking WiFi - WEP: <https://hackforums.net/showthread.php?tid=4126315>

Remote view a webcam/microphone: <https://hackforums.net/showthread.php?tid=4126349>

Cracking WiFi - WPA/WPA2: <https://hackforums.net/showthread.php?tid=4127410>

Hacking/Crashing windows 7 with a shortcut file:

<https://hackforums.net/showthread.php?tid=4127314>

PDF backdoor: <https://hackforums.net/showthread.php?tid=4127426>

DNS Spoof password stealing: <https://hackforums.net/showthread.php?tid=4131834>

Scan for vulnerabilities in a webserver: <https://hackforums.net/showthread.php?tid=4131870>

This tutorial will be very brief ?

Aircrack-NG is the "New Generation" of the original aircrack tools. One of these tools, aireplay-ng, allows us to easily DOS a wireless access point (AP).

I have installed the Aircrack-NG suite on my linux computer, and by using this simple command, I can deny any users from connecting or remaining connected to the access point.

First, put your wireless adapter into monitor mode:

Code `airmon-ng start wlan0`

Then, if you know the bssid for the target AP and the MAC address of your computer, use this command:

Code `aireplay-ng --deauth 1000 -a 00:11:22:33:44:55 -h 99:88:77:66:55:44 mon0`(Replace 00:11:22:33:44:55 with the bssid for the target AP and 99:88:77:66:55:44 with the MAC address of your computer)

This command will send 1000 deauthentication frames to the target AP - kicking users off the router repeatedly. Feel free to increase the number. Keep running the command for as long as you want to stop all access to the AP wirelessly ?

Bonus tutorial to steal wireless connections:

Run airbase to set up a fake AP

Code `airbase-ng -a 00:11:22:33:44:55 --essid "ExampleNetwork" -c 1 mon0`Kick the users off the original network using the aireplay commands in the tutorial.

Boost power to your network so the signal strength is stronger, and he will automatically connect to your network! You can then feed him fake webpages, etc, to capture credentials or monitor his activity

Code iwconfig wlan0 txpower 27

Thanks for reading, please reply with your thanks if you enjoyed this and/or found it useful.

Watch out for future hacking tutorials from me - further wireless cracking, metasploit and other common hacking topics!

Written by MeshCollider ?

Kebabs - March 23, 2014, 11:43 pm

dont know if this work, but sounds cool haha

SIM-2015410 - March 23, 2014, 11:48 pm

(Mar 23, 2014 11:43 PM)hambain Wrote: [\[CITE\]](#) dont know if this work, but sounds cool haha
It definitely works! it uses the same command to kick users off the WiFi that we use when hacking wireless network passwords: to force the user to reauthenticate. And this is really fun if you have an annoying neighbor ?

Kebabs - March 24, 2014, 12:23 am

thanks just what i need, and read your thread on cracking wep, that will come in handy. great work keep it up.

SIM-2015410 - March 24, 2014, 12:39 am

(Mar 24, 2014 12:23 AM)hambain Wrote: [\[CITE\]](#) thanks just what i need, and read your thread on cracking wep, that will come in handy. great work keep it up.

Thanks man, nice to hear some good feedback. It seems that most of my threads are being ignored. I need to get upgraded. Then people will pay attention. But I am only 16 with no income...I can't afford l33t :(

BobDarling - March 24, 2014, 2:04 am

Hello m3shc0llid3r :

Defiitely this is a working method. You can even push further by faking the targeted AP and force user to relog on your fake AP and listening to all their traffic/redirecting them to some virus one.

SIM-2015410 - March 24, 2014, 10:21 pm

(Mar 24, 2014 02:04 AM)BobDarling Wrote: [\[CITE\]](#) Hello m3shc0llid3r :

Defiitely this is a working method. You can even push further by faking the targeted AP and force user to relog on your fake AP and listening to all their traffic/redirecting them to some virus one.

Yeah! I might make a seporate tutorial for this, but here is the basic method:

Run airbase to set up a fake AP

Code airbase-ng -a 00:11:22:33:44:55 --essid "ExampleNetwork" -c 1 mon0Kick the users off the original network using the aireplay commands in the tutorial.

Boost power to your network so the signal strength is stronger, and he will automatically connect to your network! You can then feed him fake webpages, etc, to capture credentials or monitor his activity

Code iwconfig wlan0 txpower 27

Thanks for the feedback BobDarling ?

Shinigami-san - March 25, 2014, 1:28 am

nice tutorial.

for those who dont know, you can find the BSSID by typing:
airodump-ng mon0

and find your MAC address by:

```
ifconfig -a  
on the eth0
```

SIM-2015410 - March 25, 2014, 11:48 am

(Mar 25, 2014 01:28 AM)Shinigami-san Wrote: [\[CITE\]](#) nice tutorial.
for those who dont know, you can find the BSSID by typing:
airodump-ng mon0

and find your MAC address by:

```
ifconfig -a  
on the eth0
```

Thanks for the reply. The tutorial assumes a bit of basic knowledge learnt in the first 2 tutorials but thanks for adding that anyway ?

SIM-2015410 - March 27, 2014, 4:53 pm

Why do none of my threads get any attention!

Nova1 - March 28, 2014, 2:39 am

Thank you for this my man :) I like it

Austad - March 28, 2014, 4:58 am

thanks for the tutorial. looks great and informative.

SIM-2015410 - March 28, 2014, 5:15 pm

Thanks for the replies guys! appreciate the feedback and the thanks!

Replies give me an indication of how useful my tutorials have been. if i don't get any replies, i am inclined to think that i am being ignored ?

vagabund132 - August 5, 2014, 3:10 pm

dear meshcollider.. will this work when they are connected with lan ? because there is such application called Wifkill for androids which is obviously based on linux and it can disconnect users from network regardless of them being lan/wlan

Elixirz - August 5, 2014, 8:39 pm

Seems pretty legit. Does this also work with Windows operating systems?

SIM-2015410 - August 5, 2014, 10:17 pm

(Aug 5, 2014 08:39 PM)Elixirz Wrote: [\[CITE\]](#) Seems pretty legit. Does this also work with Windows operating systems?

I believe you can get the aircrack software for Windows, so i assume the same commands would apply.