

Forum:[Hack Forums](#)

Thread: [\[TUTORIAL\] WiFi Cracking Tutorial - PART 2](#)

SIM-2015410 - March 21, 2014, 3:59 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>

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

Hacking/Crashing windows 7 with a shortcut file:

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

In this tutorial, I will demonstrate how to crack WEP's big brothers: WPA and WPA2

In the last tutorial we saw how weak and easy to crack WEP encryption is. I will now show you how to crack the most popular replacement for WEP. WPA2 uses a stronger encryption algorithm, AES, that's very difficult to crack—but not impossible.

When a user connects to a WPA2 Access point, the client and AP use a "4 way handshake" to authenticate the client. This is how we can crack the encryption: if we can capture the 4 way handshake, we can crack the password. We will again use aircrack-ng, and this time we will use a dictionary attack to crack the password.

1) Put your WiFi Adapter into Monitor mode, to monitor and capture traffic on the network:
Code `airmon-ng start wlan0` Replace wlan0 with the identifier of your adapter, as in tutorial 1.
Note that aircrack-ng has renamed your wlan0 adapter to mon0.

IF YOU WANT TO REMAIN ANONYMOUS FROM A SYSTEM ADMINISTRATOR, run these commands:

Spoiler ([Click to View](#)) Code `ifconfig wlan0 down`
`macchanger -m 99:88:77:66:55:44 wlan0`
`ifconfig wlan0 up` This will change your MAC address of your wireless adapter, you can run it again for mon0.

2) Begin capturing traffic:

We will again use airodump-ng to capture packets sent over the wireless network. First we need to get the information about the network we are trying to crack:

Code `airodump-ng mon0`

3) Capture traffic on the target AP:

Now we will focus on a single network, make sure its encryption is WPA2. Run this command:
Code `airodump-ng --bssid 00:11:22:33:44:55 -c 11 --write example mon0` replace 00:11:22:33:44:55 with the bssid of the target network, and 11 with the channel. "example" is the file the captured packets will be written to.

4) Force a 4 way handshake:

To capture the password, we need to capture the authentication process. We can quickly do this by forcing them off the network, whereby their system will automatically reauthenticate them. Open a new terminal window and run this command:

Code `aireplay-ng --deauth 1 -a 00:11:22:33:44:55 mon0`The 1 is the number of de-authenticate frames you want to send, and 00:11:22:33:44:55 is the bssid of the access point.

If the command was successful, we should see "WPA handshake." in the top corner of our airodump terminal. We now have the encrypted password!

5) Cracking the password

We can now use aircrack-ng to crack the encrypted password in our "example" file. This is a dictionary attack, so the attack is only as good as the dictionary file you use. Use Ctrl + C to stop the airodump process running, and then run this command in a new terminal:

Code `aircrack-ng example-01.cap -w /root/desktop/examplewordlist`We don't need to be in range of the network to crack the password. You can also use multiple wordlists to crack the password, but double ups in the 2 lists will increase the cracking time as the program will have to check the same password twice. You can download wordlists from the internet: [CrackStation's Password Cracking Dictionary](#)

[SkullSecurity's Password Dictionaries](#)

The default directory for wordlists on kali is "/pentest/passwords/wordlists/" so if you have a default dictionary there, feel free to use that.

6) Wait. This process of cracking could take a long time - hours to days. The stronger the password, the longer it will take to crack it - if ever. A strong password can sometimes only be cracked with a bruteforce attack (testing every possible combination of numbers, letters and symbols), and that takes much much longer. If you can't crack this password, find another network to attack. When the password is found, it will be displayed on your screen. You now have access!

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 ?

CustomSync - March 27, 2014, 6:16 pm

If you are considering a bruteforce attack against WPA, one thing to try first may be the functions of a tool called "Reaver". Most newer routers are vulnerable and it can crack WPA in no time (depending on signal strength).

Good tutorial!

Nova1 - March 28, 2014, 2:26 am

Thank you for this. I appreciate it dude.

SIM-2015410 - March 28, 2014, 5:09 pm

(Mar 27, 2014 06:16 PM)CustomSync Wrote: [\[CITE\]](#) If you are considering a bruteforce attack against WPA, one thing to try first may be the functions of a tool called "Reaver". Most newer routers are vulnerable and it can crack WPA in no time (depending on signal strength).

Good tutorial!

Thanks for the feedback and the addition to the thread!

(Mar 28, 2014 02:26 AM)Nova1 Wrote: [\[CITE\]](#) Thank you for this. I appreciate it dude.
Thanks for the reply, hope you find it helpful ?

opsafrica - March 29, 2014, 1:48 am

Brilliant tutorial very helpful! Thanks a million!

Beznadzieja - March 29, 2014, 5:15 am

A lot of cracking Wi-Fi tutorials with backtrack but it's best I seen. Thanks for sharing dude.

emvc05 - April 19, 2014, 6:18 pm

can someone help me please. i been trying to hack my home router but when i use reaver the router just timed out like if is protecting from the attack. can someone help me bypass this? do i have to use some port forwarding ?

LanceGrass - April 20, 2014, 12:43 pm

For anyone on the fence, I can attest to it's efficacy. Thanks for making it easy to understand M3sh.

WheredYouGo - April 22, 2014, 8:02 am

This is very helpful. Thank you Mesh :D

SIM-2015410 - April 24, 2014, 8:25 pm

No problem guys, appreciate the feedback!

Im currently writing another tutorial, watch out for it!

linxx - May 8, 2014, 6:19 pm

Thank you so much for this awesome tutorial. Just cracked my first wpa network, and it sure feels good to have something work for a change.

One question...

Now that I have the password and can log onto the network, is there a way to access the router settings?

linxx - May 10, 2014, 4:00 pm

I tried that, and it looks like I will have to get the pass (brute force?) after all. No biggie as I can at least access the WiFi network, and that is, to me, amazing. Your tutorials are so complete and easy to follow that even an "old fart" like me can follow them and make them work.

Just another silly question...

When I am working with aircrack on a Wsp-2 network, I sometimes get this message after doing the aireplay-ng --deauth 1 -a (bssid) mon0.

Everything is working, except I don't get the handshake and I get this message...

NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>)

Now, I am wondering - how would I acquire the client's mac, and if I get it, where would I place it in the code line?

iDuL - May 11, 2014, 12:49 am

This is an absolutely incredible tutorial OP, thanks for the share.

SIM-2015410 - May 11, 2014, 12:23 pm

(May 11, 2014 12:49 AM)iDuL Wrote: [\[CITE\]](#) This is an absolutely incredible tutorial OP, thanks for the share.

I appreciate the feedback man, it has had hundreds of views but only 15 posts. So thanks for bothering to reply ?

lhax1225 - June 20, 2014, 3:38 pm

I vouch for this method. It works for WPA2. Nice job.

SIM-2015410 - June 20, 2014, 5:44 pm

(Jun 20, 2014 03:38 PM)lhax1225 Wrote: [CITE](#) I vouch for this method. It works for WPA2. Nice job.

Glad it worked, thanks for replying!

myusername2 - September 3, 2014, 12:05 pm

I never managed to break wpa passwords.

Tiggggger - September 4, 2014, 2:47 pm

thanks for the tutorial did so one has long sought

Discounted - September 4, 2014, 3:29 pm

I must try this later xD thanks in advance

graks - September 5, 2014, 10:32 am

nice tut , but i wonder if you have tried WIFITE, its on backtrack and Kali and its amazing, see my guide here : <http://hackyourgadget.net/2012/06/09/wifite-v2-automated-wepwpa-attack-tool/>