

Forum:[Hack Forums](#)

Thread: [WiFi Password Crack - How to get a neighbors WiFi password??](#)

TonyPD - March 6, 2016, 5:12 pm

I need solution how to get password from my neighbor's WiFi??

Lexluthor708 - March 6, 2016, 8:21 pm

try brute forcing the pass using kali usually works

x\$pl0it - March 6, 2016, 8:34 pm

What type of encryption is the network using? WEP, WPA, or WPA2?

hackforumspro - March 6, 2016, 10:03 pm

^ Correct you need to know what type of password encryption the network is using for wifi

WEP or WPA or WPA2

They get more secure in each order...

WEP is 100% decryptable to plain text.. All you need to do is set your wifi nic "network interface card" into monitor mode.

Then you set it to the target wifi channel the network is on most are 11-8

And you capture auth packets through that network host by targeting its MAC & Packet channel.. Once you have enough of these auth packets captured you can then decrypt the WEP password to plain text.

If the password is WPA encryption or WPA2 then it requires much much more captured auth packets as this encryption algorithm is not decryptable but crackable, So you need to brute it with a rainbowtable or custom list table.

The aircrack-ng suite on linux is a perfect example of this. So I would suggest you go about looking into how to use aircrack-ng to crack these encryptions.

?Fazzer - March 6, 2016, 10:08 pm

I used aircrack-ng twice, I was able to sneak in a wifi but the other wifi failed. The latest routers have brute force protection. So you won't be able to do anything. They will just block your Mac address if you repeatedly try.

Well try aircrack-ng and see if you able to get the password.

brutaliner - March 7, 2016, 12:37 am

I used Kali linux for cracking neighbors wifi. If WPS available u should use Reaver, very nice tool, helped me a lot.

x\$pl0it - March 7, 2016, 1:31 am

(Mar 7, 2016 01:37 AM)brutaliner Wrote: [\[CITE\]](#) I used Kali linux for cracking neighbors wifi. If WPS

available u should use Reaver, very nice tool, helped me a lot.

That's only if it's one of the WPA/WPA2 encryption standards. If it's WEP don't bother, it's easier to get the WEP key than the WPS key.

N3H4L - November 1, 2016, 11:24 am

You can try fluxion tool its batter one

Freshnuts - November 1, 2016, 1:58 pm

And I was going to say the easiest way, which is to walk to that neighbor's house and tell him that your internet is down.

It's like asking for sugar nowadays lol

lusr - November 1, 2016, 2:02 pm

(Mar 6, 2016 06:12 PM)TonyPD Wrote: [\[CITE\]](#) I need solution how to get password from my neighbor's WiFi??

If you have Kali, run airodump-ng in order to scan for possible target. Then (or instead of airodump-ng) run wash in order to know if the AP is wps locked. If not, then run reaver and you can obtain the pwd.

Hope this help.

Sniper - November 1, 2016, 2:08 pm

Best method is to use the airo tools to deauth and capture the handshake, then use hashcat to crack the capture file. Be warned, it needs hefty hardware or a few excellent wordlists to crack in a decent timeframe.

THC - November 1, 2016, 2:09 pm

Try phishing, that usually works for me, plus it disregards wpa2.

Day Vide - November 1, 2016, 2:11 pm

If it was my case I would make a fake access point.

Malicious Intent - November 1, 2016, 2:14 pm

Step1. Get Linux

Step2. Install Aircrack-ng Package

Step3. Use Aircrack Package as per manual to capture wpa handshake (its 21st century so i assume its wpa, hard to find wep encrypted network in wild nowadays).

Step4. Create a password database with Crunch for linux (check man page for help)

Step5. Run the aircrack with your password list against the wpa hashed key. (this is slow option as aircrack doesnt support GPU use for cracking so you will probably get 1500 passwords per second).

Step6. Bare in mind that you might wait for years depending on the complexity of password you are trying to crack.

to give you an example - 8 characters password with only capital letters(26 in english alphabet) would take ~40 days to crack if you use decent GPU.

8 character password with full ascii table takes 6.68 quadrillion of combinations now keep in mind that most people or ISPs will only use small and capital letters and numbers those limiting the number of combinations to ~ 64^8 (its still a huge number).

If your neighbours SSID (network name) is custom name it means that most likely someone changed router settings and also updated generic password so it could be something really easy and small letters only so always worth to give it a bash. If generic router name present password is

most likely default provided by the vendor so its most likely a mix of capitol and small letters and possibly numbers too. Good luck. If you need help with tools let me know or search through wifi hacking section of this forum.

P.s there are other types of attack but it depends on the router if they can be used. Also to the person above that mentioned bruteforce against router... lol thats stupid idea.. its not about bruteforcing a router.. its the hashed key that needs cracked..

My recommendation is - read up on everything i have mentioned and then look into parallel computing. Or some computer clusters for rent(there are options online where you can hire supercomputer for a short time and blast some hashes with it, even amazon offers their vps with tesla gpus)

PSEUCHO - November 1, 2016, 3:52 pm

Try sophrons wifiphisher, get it with git clone

You will need two wifi adapters tho

TATER-DaN69 - November 26, 2016, 8:38 pm

(Nov 1, 2016 01:58 PM)Freshnuts Wrote: [\[CITE\]](#) And I was going to say the easiest way, which is to walk to that neighbor's house and tell him that your internet is down.

It's like asking for sugar nowadays lol

lol i was trying to get my neighbor's wifi for like 3 days and i just got sick of it and walked to his house and was like give you 10\$ for your wifi password XD