

Forum:[Hack Forums](#)

Thread: [Mass hacking your local town / WPA2 wardrive hacking.](#)

Mr. Robot - July 13, 2019, 2:13 am

Quick guide on mass hacking your local town.

This attack will provide you with WPA2 keys for a lot of networks in your city/town extremely easily. It doesn't rely on getting a 4way handshake and uses PMKIDs

-- Important note. Because we are mass hacking with a dictionary. It's 'almost' guaranteed you'll hack 1 or 2 in less than an hour. If you're lucky you might get 100 in an hour or more which means overall it's the 'fastest' way of hacking WiFi (except if you are specifically targeting a network)

To make this easier for you I have color coded it:
This color signifies setup and collection of packets
This color signifies cracking the passwords

>>This is a client-less attack, that doesn't need a 4-way handshake or special output format.

Alright, i'd highly recommend using a raspberry pi for this due to its portability with a battery pack however you can just live boot a laptop and drive around/change power settings to still run while closed and walk around. I'll write this up in laptop terms mainly but it's the same for a pi more or less.

>>Alright.

Step 1. Download and put Kali Linux onto a USB to live boot your laptop.

Spoiler ([Click to View](#)) Creating a Bootable Kali USB Drive on Windows

Download the 32 or 64 bit from here of Kali linux:

<https://www.kali.org/downloads/>

Download win32 disk imager from here:

<https://sourceforge.net/projects/win32diskimager/>

Plug your USB drive into an available USB port on your Windows PC, note which drive designator (e.g. "F:") it uses once it mounts, and launch the Win32 Disk Imager software you downloaded.

Choose the Kali Linux ISO file to be imaged and verify that the USB drive to be overwritten is the correct one. Click the "Write" button.

Some times it wont show up, so in the file browser when selecting the image, follow this gif to select all file types:

Once the imaging is complete, safely eject the USB drive from the Windows machine. You can now use the USB device to boot into Kali Linux.

To boot your laptop off the USB - you will need to press f8/f12/del or other to enter the boot device selection and choose the USB from there. If you have issues with this, you may need to check your BIOS settings and disable UEFI boot and check you are on legacy boot.

Awesome so now you are all booted up into Kali Linux. The desktop has loaded or has prompted you for a username and password (root/toor).

Step 2. Connect to your WiFi network using the internal wireless adapter on the laptop. Once connected, open up a terminal and follow the commands below.

In this spoiler - I will describe each line and what it does.

Spoiler ([Click to View](#))

`sudo su` // this command makes sure your entire session inside this terminal is run as Super User. It's not needed as we are running everything as sudo anyway for installation it just helps avoid any problems you might have with specific hardware.

`apt install` // this command runs "Advanced Package Tool" to install the packages listed after it. Each one is needed and if you have an issue where one isn't found, you will need to edit the file containing your 'known packages' which is where it looks online (urls) for the files to install.

`git clone` // this command clones the repository from github which is where the creator of this tool keeps their code and files.

`cd hcxdumptool` // after cloning from github in the previous command, a folder is made with the name of the tool (hcxdumptool.git into hcxdumptool folder) by using the cd command it enters that folder so we can now access it directly in terminal.

`make` // the make command looks at your systems layout and then decides if anything needs to be altered/changed and if everything it needs is installed to places it can find.

`make install` // now that make has made sure and configured file locations depending on your setup (in this case Kali Linux) the make install command will install and create binaries if necessary to put everything in its place. This is so you can run a tools name usually without being in that folder (cd) from anywhere inside the terminal.

`cd ..` // this command moves you up one directory. At this stage you will be inside the hcxdumptool folder and have already configured it, so now you need to go back to the root directory and this command will shift you one folder previous.

>> This this is repeated again for the other tools.

Code `sudo su`

`sudo apt install libssl-dev libcurl4-openssl-dev libpcap0.8-dev zlib1g-dev`

`sudo git clone https://github.com/ZerBea/hcxdumptool.git`

`sudo git clone https://github.com/ZerBea/hcxttools.git`

`sudo git clone https://github.com/hashcat/hashcat.git`

`cd hcxdumptool`

`sudo make`

```
sudo make install
cd ..
cd hcxtools/
sudo make
sudo make install
cd ..
cd hashcat
sudo make
sudo make install
```

After it's all installed and ready to go, I plug in a powerbank to my raspberry pi, throw it in my backpack and it's almost time to walk around.

If you are doing this on a laptop, instructions are basically the same. Plug in your WiFi adapter and let's get to work.

I still need to run this here to disconnect the raspberry pi from my home network that I used to download the github files so while I still have a monitor connected:

```
Code ifconfig wlan0 down
iwconfig wlan0 mode monitor
ifconfig wlan0 up
airmon-ng check kill
hcxdumpool -o yourcityname.pcapng -i wlan0 --enable_status 1
```

Because you are using a laptop, your internal wireless card might not work with monitor mode or have the right drivers available for this. I'm using a version 2.0 of the TL-WN722N - check your card to see if it works with monitor mode.

For laptop users - in a terminal enter

Code iwconfig

Check what device name your USB adapter is in there (usually wlan1 if you have an internal card connected to internet otherwise disconnect from WiFi and use your internal card)

Run the following - changing out wlan0 for whatever position your adapter is in.

```
Code ifconfig wlan0 down
iwconfig wlan0 mode monitor
ifconfig wlan0 up
airmon-ng check kill
hcxdumpool -o yourcityname.pcapng -i wlan0 --enable_status 1
```

>> Last step for laptop users is to click on your power settings (settings/power or battery) and disable sleep and disable sleep on closed lid. This is so you can close the lid and make sure the script is still running while you are able to put it in a backpack.

Awesome! Go for a walk/drive - No need to hover outside a particular place, it's extremely fast and effective.

Now you are back home - make sure your device didn't die, i'm untested/unsure on whether or not the file will save if your battery dies so play it safe or record it to a USB drive/internal harddrive on the "-o yourcityname.pcapng" you would change that to "-o /mnt/c/yourcityname.pcapng" as an example. Then before your battery dies while you are out, simply ctrl+c to save the session. The reason we do this is we are live booting on the USB which means once the laptop turns off or the USB is unplugged running Kali Linux, it won't save anything you have done.

Time to start cracking!!!!

In your terminal run this changing out yourcitynameoutputs.16800 with what you want to call your output file and yourcityname.pcapng with the file we created from the wardrive.

```
Code hcxpcaptool -E ssidlist -I identitylist -U usernamelist -z yourcitynameoutputs.16800  
yourcityname.pcapng
```

This will convert it to a few files so you can easily see what's going on. The main file we need however is the .16800 file. I'd recommend copying it to a machine with a bit more processing power than the or your laptop if you have one available.

One way I like to do this is to connect my device back to WiFi when I am home, move all the files to /var/www/html/ such as this:

```
/var/www/html/yourcitynameoutputs.16800  
/var/www/html/ssidlist  
/var/www/html/identitylist  
/var/www/html/usernamelist
```

You can use the mv command which is extremely handy for this

```
Code mv yourcitynameoutputs.16800 /var/www/html/yourcitynameoutputs.16800  
mv ssidlist /var/www/html/ssidlist  
mv identitylist /var/www/html/identitylist  
mv usernamelist /var/www/html/usernamelist
```

Then running the command

Code ifconfig

To find my ipv4 address (mine was 192.168.1.30 in this instance)
Then running

Code service apache2 start

This means I can hop on any computer in my network and in my browser go to:

Code 192.168.1.30/yourcitynameoutputs.16800

And it will download it straight to my Desktop environment.

>> Now it's time to start cracking. If you seriously don't have a good computer you can post on HF to have some try crack it for you here:

[Hash Bounties](#)

Otherwise you can pay money if they are successful here:

<https://gpuhash.me>

Time to download hashcat! Right at the top download the binaries.

<https://hashcat.net/hashcat/>

Put it all in a nice folder > Also move your yourcitynameoutputs.16800 to that folder too - mine is in C:\Users\MrRobot\Documents\hashcat-5.1.0\hashcat-5.1.0

>> Once it's in there download rockyou.txt from here and put it in the same folder as the hashcat64.exe:

<https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt>

Now open up a command prompt and CD into that directory - for me it was:

Code cd C:\Users\MrRobot\Documents\hashcat-5.1.0\hashcat-5.1.0

The first one we will simply run the rockyou.txt file.

Code hashcat64.exe -m 16800 yourcitynameoutputs.16800 -w 3 rockyou.txt

This will just run the dictionary with no rules/modifiers. I'd recommend beforehand however throwing your town name into the top of Rockyou.txt such as

NewYork
Newyork
newyork
new york
New York

A lot of places will use your town name in their passwords.

Personally I walked down my main street and collected 144 PMKIDs and running simply the rockyou dictionary alone, cracked 67 of them.

I then ran it using a rule set best64.rule

Code hashcat64.exe -m 16800 yourcitynameoutputs.16800 -w 3 rockyou.txt -r rules/best64.rule

This will now alter each word in the rockyou.txt file to try and try crack it - the reason why we do this second is it takes more time and if you do the standard rockyou dictionary first it will give you some WPA2 keys to play with in the meantime.

If there are still somehow some left after all of that a rule set oneruletorulethemall.rule - download it from google.

Code hashcat64.exe -m 16800 yourcitynameoutputs.16800 -w 3 rockyou.txt -r
OneRuleToRuleThemAll.rule

This will take substantially longer however will most likely get you A LOT of what you want/need.

After running all of these 3 which took around 3 days total for the latter two, I was left with only 6 uncracked of 144.

Example of running hashcat and the output of passwords

Extra: If you know that the password is 8 to 10 numbers long you can download crunch_win (crunch for windows) and pipe it directly into hashcat like so

(Reasons for piping: Cracking times are roughly the same however to create a massive file takes storage space you might not have)

Code crunch_win.exe 8 10 1234567890 | hashcat64.exe -m 16800 yourcitynameoutputs.16800 -w
3

If for example you know it's only 8 characters long and it's all capitals with numbers.

```
Code crunch_win.exe 8 8 1234567890ABCDEFGHIJKLMNOPQRSTUVWXYZ | hashcat64.exe -m 16800 yourcitynameoutputs.16800 -w 3
```

If for example you know it's only 8 numbers long I would recommend trying something like this which is faster, what the -d toggle does is stops characters repeating themselves right next to each other.

```
Code crunch_win.exe 8 8 1234567890 -d 1 | hashcat64.exe -m 16800 yourcitynameoutputs.16800 -w 3
```

So this last one above with the -d 1 switch will never repeat a number next to itself. So if it wouldn't try something like 11123456 as there are 1's next to themselves. This can be handy because it cuts down the cracking time and the chances of a letter or number repeating itself is pretty slim. The first one it would try would be something like

12121212 >> This last command is one I highly recommend for a quick gather of a lot of passwords. Minimum length is usually 8 characters and it's really common.

You can also make toggles so a number never repeats at all in the string if you know no numbers repeat.

Last_viking - July 13, 2019, 12:15 pm

This went above my head lol.

Mr. Robot - July 13, 2019, 5:36 pm

(Jul 13, 2019 12:15 PM)Last_viking Wrote: [\[CITE\]](#) This went above my head lol.
Hey man not a problem, i'll try and simplify it a bit over the next few days.

mrknol - July 14, 2019, 3:19 am

That's a very well made thread with a lot details. That's what I call real hacking tutorial.

Mr. Robot - July 14, 2019, 3:28 am

(Jul 13, 2019 12:15 PM)Last_viking Wrote: [\[CITE\]](#) This went above my head lol.
I've made some changes to help clarify. Anyone should be able to follow it now.

SIM-3205632 - July 14, 2019, 3:33 am

Another HQ tutorial by Mr robot thank you.

Mr. Robot - July 14, 2019, 3:36 am

(Jul 14, 2019 03:33 AM)P I M P Wrote: [\[CITE\]](#) Another HQ tutorial by Mr robot thank you.
No, thank you for taking the time to post acknowledging the thread. Nothing worse than something dying and other people can't see it.

Last_viking - July 14, 2019, 3:40 am

This is a effective way to crack wifi passwords now I understand each step taken. Thank you @mr. Robot for adding gif :-)

Mr. Robot - July 14, 2019, 3:42 am

(Jul 14, 2019 03:40 AM)Last_viking Wrote: [\[CITE\]](#) This is a effective way to crack wifi passwords now I understand each step taken. Thank you @mr. Robot for adding gif :-)

Not a problem, if you have any issues / questions if you choose to follow it along - feel free to post so if I need to, I can add it to the main thread to avoid others having the same issues

duplex - July 14, 2019, 3:51 am

Your tutorials are nothing but the highest quality.

Dotexe - July 14, 2019, 3:54 am

The only person that actually puts effort on these tutorials. Keep up the hacking section alive Mr. Robot ?

Lux Interior - July 14, 2019, 4:20 am

Great tutorial Mr. Robot and I've just ordered a new USB stick so I can test it out.

Bit of a lame question, but what do I do once/if I find a password for one of my neighbor's WiFis?

Lux

Mr. Robot - July 14, 2019, 4:20 am

(Jul 14, 2019 03:51 AM)duplex Wrote: [\[CITE\]](#) Your tutorials are nothing but the highest quality.

(Jul 14, 2019 03:54 AM)Dotexe Wrote: [\[CITE\]](#) The only person that actually puts effort on these tutorials. Keep up the hacking section alive Mr. Robot ?

Thank you both <3 As said previously any questions feel free to ask. Happy to help.

(Jul 14, 2019 04:20 AM)Lux Interior Wrote: [\[CITE\]](#) Great tutorial Mr. Robot and I've just ordered a new USB stick so I can test it out.

Bit of a lame question, but what do I do once/if I find a password for one of my neighbor's WiFis?

Lux

Doesn't have to be just your neighbor - but you can do a lot of fun stuff.

Log images/websites/passwords they use.

Troll them with playing sounds on every page they visit.

Flip all their images upside down.

Infect their computer/other devices.

Use their network as a proxy.

Report it to help them out.

Just a few - but not all.

A raspberry pi setup like this will take you no time to setup at all - I use a long cable for my wireless adapter so I can run it up my sleeve if I want to. You can also make the internet wireless card host a network that you can connect to and control using your phone via vnc or ssh.

The battery life on a 4400mah for the PI should be around 20 hours.

HackersI - July 14, 2019, 9:49 am

Please keep guid kids like me,we are learning from you much.waiting for another tutorials.thax

Mr. Robot - July 14, 2019, 11:21 am

(Jul 14, 2019 09:49 AM)HackersI Wrote: [\[CITE\]](#) Please keep guid kids like me,we are learning from you much.waiting for another tutorials.thax

Hey man - will do - thanks for the support

Sigma - July 14, 2019, 1:19 pm

Lol, I should have viewed this first, I just created the same tutorial. Hashcat is one of my favorite tools. Yours is a lot better than mine though, no joke. ?

Stoner - July 14, 2019, 1:26 pm

Although I'm not that interested in this one it's a very good tutorial and I would love to see more from you!

Mr. Robot - July 14, 2019, 9:35 pm

(Jul 14, 2019 01:26 PM)Stoner Wrote: [\[CITE\]](#) Although I'm not that interested in this one it's a very good tutorial and I would love to see more from you!

Well definitely more to come!

itzgame - July 15, 2019, 5:44 am

Is dictionary useful? I think it is not. Can you explain me new methods if you know?

Mr. Robot - July 15, 2019, 6:08 am

(Jul 15, 2019 05:44 AM)itzgame Wrote: [\[CITE\]](#) Is dictionary useful? I think it is not. Can you explain me new methods if you know?

What.. Of course dictionary is useful. How do you think the majority of shit online is hacked lmao

itzgame - July 15, 2019, 6:16 am

(Jul 15, 2019 06:08 AM)Mr. Robot Wrote: [\[CITE\]](#) What.. Of course dictionary is useful. How do you think the majority of shit online is hacked lmao

I mean wifi's passwords use random letters, numbers or symbols. Isn't it hard to find the correct password?

Mr. Robot - July 15, 2019, 6:21 am

(Jul 15, 2019 06:16 AM)itzgame Wrote: [\[CITE\]](#) I mean wifi's passwords use random letters, numbers or symbols. Isn't it hard to find the correct password?

Not at all. On such a large scale of simply running this then driving/walking around for an hour or so - you'll collect thousands of pmkids without an issue. You'll surely crack 60% of those using dictionaries alone then you might have to bruteforce a lot of the rest.

You could still easily hack 600+ networks in less than a week if not more.

Most businesses believe it or not use the minimum 8 character length in lowercase with numbers if it's custom.

itzgame - July 15, 2019, 6:25 am

(Jul 15, 2019 06:21 AM)Mr. Robot Wrote: [\[CITE\]](#) Not at all. On such a large scale of simply running this then driving/walking around for an hour or so - you'll collect thousands of pmkids without an issue. You'll surely crack 60% of those using dictionaries alone then you might have to bruteforce a lot of the rest.

You could still easily hack 600+ networks in less than a week if not more.
Most businesses believe it or not use the minimum 8 character length in lowercase with numbers if it's custom.
What's the best and most effective WPA2's dictionary in internet?

Mr. Robot - July 15, 2019, 6:30 am

(Jul 15, 2019 06:25 AM)itzgame Wrote: [\[CITE\]](#) What's the best and most effective WPA2's dictionary in internet?

My recommendations are rockyou.txt with bestrule / oneruletorulethemall

As well as weakpass_1_wifi / weakpass_2_wifi / weakpass _3_wifi.

If you collect the packets and want me to try crack a bunch of them, let me know.

itzgame - July 15, 2019, 6:31 am

(Jul 15, 2019 06:30 AM)Mr. Robot Wrote: [\[CITE\]](#) My recommendations are rockyou.txt with bestrule / oneruletorulethemall

As well as weakpass_1_wifi / weakpass_2_wifi / weakpass _3_wifi.

If you collect the packets and want me to try crack a bunch of them, let me know.
Do you need .hccap or .cap file?

Mr. Robot - July 15, 2019, 6:34 am

(Jul 15, 2019 06:31 AM)itzgame Wrote: [\[CITE\]](#) Do you need .hccap or .cap file?
Neither, follow my tutorial. You'll end up with a .16800 file.

itzgame - July 15, 2019, 6:55 am

In my main pc it doesn't have wireless card, can I crack WiFi without it?

Mr. Robot - July 15, 2019, 7:28 am

(Jul 15, 2019 06:55 AM)itzgame Wrote: [\[CITE\]](#) In my main pc it doesn't have wireless card, can I crack WiFi without it?
You can crack the hashes, you wont be able to collect them though.

Sophoclito - July 15, 2019, 10:40 am

So what does hcxdumptool do exactly ?

I have been conducting attacks against wireless networks before using deauthentication and 4 way handshake capture (airodump-ng / aireplay-ng / aircrack-ng) but I'm curious to know how it can be done otherwise.

(Jul 15, 2019 10:40 AM)Sophoclito Wrote: [\[CITE\]](#) So what does hcxdumptool do exactly ?

I have been conducting attacks against wireless networks before using deauthentication and 4 way handshake capture (airodump-ng / aireplay-ng / aircrack-ng) but I'm curious to know how it can be done otherwise.

It's literally in the title, PKMIDs, I checked it out so I have the answers to my questions haha, sorry for the spam, cool stuff though ! I might give it a run :)

Mr. Robot - July 15, 2019, 11:00 am

(Jul 15, 2019 10:40 AM)Sophoclito Wrote: [\[CITE\]](#) So what does hcxdumptool do exactly ?

I have been conducting attacks against wireless networks before using deauthentication and 4 way handshake capture (airodump-ng / aireplay-ng / aircrack-ng) but I'm curious to know how it can be done otherwise.

It's literally in the title, PKMIDs, I checked it out so I have the answers to my questions haha, sorry for the spam, cool stuff though ! I might give it a run :)

Not a problem, glad you got the answer you were after. Once you gather up the stuff, let me know!

itzgame - July 15, 2019, 1:24 pm

Can I crack handshake with Windows?

Mr. Robot - July 15, 2019, 1:34 pm

(Jul 15, 2019 01:24 PM)itzgame Wrote: [\[CITE\]](#) Can I crack handshake with Windows?

You can indeed, my tutorial covers that.

steiger - July 16, 2019, 11:33 am

Awesome tutorial and explanation.

Thank you OP.

Mr. Robot - July 16, 2019, 3:01 pm

(Jul 16, 2019 11:33 AM)steiger Wrote: [\[CITE\]](#) Awesome tutorial and explanation.

Thank you OP.

If you need any help just ask.

Darth Gexe - July 20, 2019, 8:10 am

Lol I have to try this with a canaima laptop and my wn7200nd.

The cracking part will be the one that will be difficult for me a little, but we'll see what comes out.

Legal Coding - July 20, 2019, 9:47 am

wow good and very useful tutorial

de_g3ntl3m4n - July 20, 2019, 6:45 pm

Im dead about to try it out, hahah, but wow, much respect homie! gotta learn from the best to be the best

Unk0wn - July 21, 2019, 1:39 am

Hah def gonna try this around my school area lots of apartments so probs a lot of easy passwords

Thanks for the guide OP hats off to you ?

Bastille - July 21, 2019, 1:42 am

I really like your contents, it's always a pleasure to see good threads/posts about hacking here ?

Thanks for sharing, +rep for you !

Mr. Robot - July 21, 2019, 5:38 pm

I'll be offering some hashcracking for people following this.

boy rteis - July 21, 2019, 6:50 pm

I need your help, PM me, because I am a new member, can not reply to you, please leave your contact information

VIXV - July 23, 2019, 1:13 pm

Giving this a bump.

Outstanding thread here Mr.Robot. HQ Post + Repped.

?

Sigma - July 23, 2019, 4:13 pm

One of the better tutorials I have seen on this site. Well done, again.

FullCourseMeal - July 24, 2019, 9:41 am

Probably one of the best and easiest to follow tutorials I've seen in a very long time.

de_g3ntl3m4n - July 24, 2019, 5:50 pm

Makes me wanna get a raspberry pi now, bout to try this out shortly, keep it up man

z1ph3r - July 24, 2019, 9:01 pm

Great tutorial! ?

May I also add if it hasn't already that most NETGEARXX (e.g. NETGEAR76) routers are extremely easy to crack and took less than 10 minutes on my GTX970 using the right dictionary file.

The default WPA pass they use is a combination of an adjective + noun + 3 random digits. Most of these can be cracked on gpuhash.me in less than 15 minutes but if you're broke like me and have a gaming computer laying around you can almost definitely crack them pretty quick.

I ran a command in hashcat like:

```
hashcat -m 16800 netgearpkmids.16800 -w 4 -a 6 netgearlist.dict ?d?d?d [correct if I am wrong]
```

I am confident that 50-80% of NETGEARXX are susceptible to this.

You can find the dictionary list of most (if not all) of the adjectives and nouns Netgear used to make their default WPA passwords online pretty easily but I'm happy to share it with anyone via PM if you are having any trouble finding it.

Only problem I ran into was not being able to get the PKMID from a couple NETGEARXX I tested but hey, you can't win em all.

Have fun!

Mr. Robot - July 25, 2019, 12:11 pm

(Jul 24, 2019 09:01 PM)z1ph3r Wrote: [\[CITE\]](#) Great tutorial! ?

May I also add if it hasn't already that most NETGEARXX (e.g. NETGEAR76) routers are extremely easy to crack and took less than 10 minutes on my GTX970 using the right dictionary file.

The default WPA pass they use is a combination of an adjective + noun + 3 random digits. Most of these can be cracked on gpuhash.me in less than 15 minutes but if you're broke like me and have a gaming computer laying around you can almost definitely crack them pretty quick.

I ran a command in hashcat like:

```
hashcat -m 16800 netgearpkmids.16800 -w 4 -a 6 netgearlist.dict ?d?d?d [correct if I am wrong]
```

I am confident that 50-80% of NETGEARXX are susceptible to this.

You can find the dictionary list of most (if not all) of the adjectives and nouns Netgear used to make their default WPA passwords online pretty easily but I'm happy to share it with anyone via PM if you are having any trouble finding it.

Only problem I ran into was not being able to get the PKMID from a couple NETGEARXX I tested but hey, you can't win em all.

Have fun!

A lot of routers have known default keyspaces so it's always good to double check those.

superboy803 - July 29, 2019, 4:55 pm

This is a awesome tutorial for anyone looking for a new way to hack WPA2 networks. The fact you included GIFs made it more innovative. Keep up the great work.

AceBadEggs - July 29, 2019, 5:46 pm

Glad this has been a good way to see about getting my feet wet. Learning like this gives me a high.

Mr. Robot - July 29, 2019, 6:14 pm

(Jul 29, 2019 05:46 PM)AceBadEggs Wrote: [\[CITE\]](#) Glad this has been a good way to see about getting my feet wet. Learning like this gives me a high.

Hey i'm glad, that's how I like to lay out my tutorials - so people get interested in the field and are encouraged to dig deeper.

SUI-3183372 - July 30, 2019, 2:37 pm

Looks like a good guide. For my final project in school I'm working on some surveillance devices that utilize wifi monitoring, so I have a lotttt of Pi's with a lotttt of various wifi adapters that support monitor mode, may have to give this a try. What sort of battery do you use as a power source when doing this?

Mr. Robot - July 30, 2019, 2:46 pm

(Jul 30, 2019 02:37 PM)BV1 Wrote: [\[CITE\]](#) Looks like a good guide. For my final project in school I'm working on some surveillance devices that utilize wifi monitoring, so I have a lotttt of Pi's with a lotttt of various wifi adapters that support monitor mode, may have to give this a try. What sort of battery do you use as a power source when doing this?

Any battery pack works fine, this is my usual setup - a 10,000mah battery which gives me around 40 hours of battery life. So you can easily use a smaller one.

superboy803 - August 1, 2019, 12:31 pm

Using this great tutorial, I was able to capture many PMKIDs from my local neighborhood. With the help of Mr. Robot, we were able to easily crack the majority of the PMKIDs. This is truly the holy grail for capturing and cracking PMKIDs. I highly recommend this tutorial for anyone looking into trying a better and efficient way of hacking WiFi networks.

Mr. Robot - August 1, 2019, 3:07 pm

(Aug 1, 2019 12:31 PM)superboy803 Wrote: [\[CITE\]](#) Using this great tutorial, I was able to capture many PMKIDs from my local neighborhood. With the help of Mr. Robot, we were able to easily crack the majority of the PMKIDs. This is truly the holy grail for capturing and cracking PMKIDs. I highly recommend this tutorial for anyone looking into trying a better and efficient way of hacking WiFi networks.

Always happy to help my dude.

DrDoof - August 2, 2019, 11:02 am

I drove around my small town for 20 mins last night and got 60 PMKIDs. Had my desktop GPU try to crack it for 4 hours so far without success, using yourock.txt and best64.rule. Estimates 3 days to run through all guesses just for this command but I'll be away for the weekend so might as have it sit and crunch. Do you think yourock.txt is more likely to be successful in the US than Sweden?

Thanks for the tutorial btw, it's real cool even if I fail the crack.

ModernJS - August 2, 2019, 11:39 am

Thanks for this tutorial, you seem to really know your thing.

Doesn't necessarily require kali linux tough.

Mr. Robot - August 2, 2019, 12:36 pm

(Aug 2, 2019 11:02 AM)DrDoof Wrote: [\[CITE\]](#) I drove around my small town for 20 mins last night and got 60 PMKIDs. Had my desktop GPU try to crack it for 4 hours so far without success, using yourock.txt and best64.rule. Estimates 3 days to run through all guesses just for this command but I'll be away for the weekend so might as have it sit and crunch. Do you think yourock.txt is more likely to be successful in the US than Sweden?

Thanks for the tutorial btw, it's real cool even if I fail the crack.

Send it through - also always start with 8 length 0-9 as it's the fastest

DrDoof - August 2, 2019, 12:54 pm

(Aug 2, 2019 12:36 PM)Mr. Robot Wrote: [\[CITE\]](#) Send it through - also always start with 8 length 0-9 as it's the fastest

Yeah I did try the 0-9 first, but no luck, am gonna try 10 length and 12 length as that's the social security number lengths in Sweden and I have multiple friends who use that lol

You mean send you the pmkids?

Mr. Robot - August 2, 2019, 12:56 pm

(Aug 2, 2019 12:54 PM)DrDoof Wrote: [\[CITE\]](#) Yeah I did try the 0-9 first, but no luck, am gonna try 10 length and 12 length as that's the social security number lengths in Sweden and I have multiple friends who use that lol

You mean send you the pmkids?

Yeah i'll try crack some

funtela - August 2, 2019, 3:17 pm

Nice thread man. Definitely caught my interest. I've never really gotten into hacking. I'd love to learn though. Care to point me to some basics?

Durham - August 2, 2019, 4:08 pm

Wow, what a beautiful guide Mr.Robot! Good job!

Mr. Robot - August 2, 2019, 4:19 pm

(Aug 2, 2019 03:17 PM)funtela Wrote: [\[CITE\]](#) Nice thread man. Definitely caught my interest. I've never really gotten into hacking. I'd love to learn though. Care to point me to some basics?

Guess it really depends on what you want to focus on - such as an end goal, I can run you through some scenarios with multiple options to reach the same goal.

SIM-4086413 - August 3, 2019, 2:31 pm

Posting to come back to here... damn nice job..

Mr. Robot - August 3, 2019, 7:26 pm

(Aug 3, 2019 02:31 PM)Delphine Wrote: [\[CITE\]](#) Posting to come back to here... damn nice job.. If you need help while doing it, just let me know.

Mr. Robot - August 7, 2019, 6:10 pm

If anyone needs a hand with this, just let me know.

1337inc - August 11, 2019, 10:20 am

Nice guide, thanks for the info. I prefer ParrotSec OS to Kali, it comes bundled with more tools.

BlackRose83 - August 11, 2019, 2:22 pm

woow so hot sir Mr. Robot thx

Mr. Robot - August 11, 2019, 10:02 pm

(Aug 11, 2019 10:20 AM)1337inc Wrote: [\[CITE\]](#) Nice guide, thanks for the info. I prefer ParrotSec OS to Kali, it comes bundled with more tools.

I personally prefer Kali over Parrot but each to their own

SUI-3183372 - August 23, 2019, 12:51 am

Finally had an opportunity to go out and try this and a couple other experiments with wifi monitoring (my final project for uni is based on monitoring wifi). I have an abundance of Pi's and wifi adapters capable of monitoring, so I decided to put 3 of them up against eachother and see who the best is.

3 adapters used:

<https://www.amazon.com/gp/product/B073J3HXZH/>

<https://www.amazon.com/gp/product/B00JDVRCI0/>

<https://www.amazon.com/gp/product/B01LY35HGO/>

With one of these powering all 3 Pi's:

<https://www.amazon.com/gp/product/B0759TDR3H/>

Anyways, as you probably expect, the \$35 Panda adapter captured the most during my quick test, it seemingly simply had superior range and was able to capture quite a bit more than both its competitors. It also supports 5GHz if that matters at all for any other projects you may be working on.

The big free standing wifi adapter in the pic below is the \$35 Panda adapter. You can also remove it from it's stand and plug it directly into the Pi, but it is a bit bulky and the price of a Pi its self. I bought out US Amazon's supply of the \$7 adapter, but if they're ever back in stock they're awesome for the job.

Spoiler [\(Click to View\)](#)

Mr. Robot - August 23, 2019, 1:49 am

(Aug 23, 2019 12:51 AM)BV1 Wrote: [\[CITE\]](#) Finally had an opportunity to go out and try this and a couple other experiments with wifi monitoring (my final project for uni is based on monitoring wifi). I have an abundance of Pi's and wifi adapters capable of monitoring, so I decided to put 3 of them up against eachother and see who the best is.

3 adapters used:

<https://www.amazon.com/gp/product/B073J3HXZH/>

<https://www.amazon.com/gp/product/B00JDVRCI0/>

<https://www.amazon.com/gp/product/B01LY35HGO/>

With one of these powering all 3 Pi's:

<https://www.amazon.com/gp/product/B0759TDR3H/>

Anyways, as you probably expect, the \$35 Panda adapter captured the most during my quick test, it seemingly simply had superior range and was able to capture quite a bit more than both its competitors. It also supports 5GHz if that matters at all for any other projects you may be working on.

The big free standing wifi adapter in the pic below is the \$35 Panda adapter. You can also remove it from it's stand and plug it directly into the Pi, but it is a bit bulky and the price of a Pi its self. I bought out US Amazon's supply of the \$7 adapter, but if they're ever back in stock they're awesome for the job.

Spoiler ([Click to View](#))

Awesome man, what was your crack ratio?

SUI-3183372 - August 23, 2019, 2:09 am

(Aug 23, 2019 01:49 AM)Mr. Robot Wrote: [\[CITE\]](#) Awesome man, what was your crack ratio? I'm not attempting to crack into any networks, just wanted to try my hand at mass collection.

SIM-3343347 - August 23, 2019, 3:46 am

So i need to have a laptop or just rasp or both

Mr. Robot - August 23, 2019, 10:15 am

(Aug 23, 2019 03:46 AM)Auzsalsa Wrote: [\[CITE\]](#) So i need to have a laptop or just rasp or both As long as your wireless adapter works, either.

(Aug 23, 2019 02:09 AM)BV1 Wrote: [\[CITE\]](#) I'm not attempting to crack into any networks, just wanted to try my hand at mass collection.

Well if you want, you can send them through to me and i'll run some basic word lists against them. Always good to collect real used lists.

InvictusLatinus - August 23, 2019, 6:31 pm

Mr. Robot,

Thank you for this wonderful tutorial. Even just for the sake of learning, this is a great resource, and a reference/starting point for anyone interested in auditing wireless networks. I read through your tutorial and understood most of it, but I was wondering why you posted this two times;

```
Quote:ifconfig wlan0 down
iwconfig wlan0 mode monitor
ifconfig wlan0 up
airmon-ng check kill
hcxdumpool -o yourcityname.pcapng -i wlan0 --enable_status 1
```

Thanks again for your effort. I look forward to reading more of the content that you share.

Lumpo442 - August 25, 2019, 12:43 am

Mega Tutorial Mr. Robot <3 Im gonna test it

docka - August 28, 2019, 11:25 am

The way this man talks will never bore me

Fish - August 29, 2019, 3:41 pm

Looks legit, I'll look into this in a bit. Maybe I'll give it a shot. Thanks

Prizford - August 31, 2019, 12:29 pm

Your tutorials are nothing but the highest quality. Unreal mate

Thomas Anderson - August 31, 2019, 12:42 pm

Thank you for the tutorial. Really HQ and I understand steps.

Mr. Robot - August 31, 2019, 2:44 pm

(Aug 31, 2019 12:29 PM)Prizford Wrote: [\[CITE\]](#) Your tutorials are nothing but the highest quality. Unreal mate

Hey thanks dude. Appreciate it.

Takehito Morokuzu - September 2, 2019, 11:21 am

I'll have to try this sometime. Does it really have such a high success rate? Like only 6 of 144 weren't hacked? I don't know it just seems a bit unrealistic to me.

And would this Raspberry PI work?

https://www.amazon.co.uk/RASPBERRY-Plate-Model-Cortex-11811853/dp/B07KKBCXLY/ref=sr_1_71?keywords=raspberry+pi&qid=1567448629&s=gateway&sr=8-71

Mr. Robot - September 2, 2019, 4:52 pm

(Sep 2, 2019 04:25 PM)BV1 Wrote: [\[CITE\]](#) No, you need an ethernet port so you can use a wifi adapter that has monitor mode enabled. Look at the Raspberry Pi model 3 B+

If you want to pull your hair out, technically you can use what you linked, but you'd need to do something like this in order to get the onboard wifi to enter monitor mode:

<https://github.com/seemoo-lab/nexmon>

Also yes, you will generally experience rather high success rates with this, as long as you have a decent rig for hash cracking (or if your neighbors use poor passwords).

You don't need an ethernet port but it helps.

Takehito Morokuzu - September 2, 2019, 5:08 pm

(Sep 2, 2019 04:25 PM)BV1 Wrote: [\[CITE\]](#) No, you need an ethernet port so you can use a wifi adapter that has monitor mode enabled. Look at the Raspberry Pi model 3 B+

If you want to pull your hair out, technically you can use what you linked, but you'd need to do something like this in order to get the onboard wifi to enter monitor mode:

<https://github.com/seemoo-lab/nexmon>

Also yes, you will generally experience rather high success rates with this, as long as you have a decent rig for hash cracking (or if your neighbors use poor passwords).

So I can't use a USB adapter with it? I was never planning to use the onboard one, this is just the cheapest raspberry pi on amazon which is why I linked it

SUI-3183372 - September 2, 2019, 5:33 pm

(Sep 2, 2019 04:52 PM)Mr. Robot Wrote: [\[CITE\]](#) You don't need an ethernet port but it helps. (Sep 2, 2019 05:08 PM)Takehito Morokuzu Wrote: [\[CITE\]](#) So I can't use a USB adapter with it? I was never planning to use the onboard one, this is just the cheapest raspberry pi on amazon which is why I linked it

Sorry, idk what I was on about earlier. Totally mislead you by stating you need an ethernet port. Don't know why I said that, it's not even remotely correct. For whatever reason when I made my reply earlier, my mindset was 'Wifi adapter goes into ethernet port!' like some sort of mong. My bad.

You can use a USB based WiFi adapter, you just need to ensure it runs in monitor mode. Any of these will work for under \$20 USD:

<https://www.amazon.com/gp/product/B00NAXX40C/>

<https://www.amazon.com/gp/product/B003EVO9U4/>

<https://www.amazon.com/gp/product/B00EQT0YK2/>

<https://www.amazon.com/gp/product/B00JDVRCI0/>

<https://www.amazon.com/gp/product/B073J3HXZH/> (What I use)

or if you also want to spend a little extra to monitor 5ghz

<https://www.amazon.com/gp/product/B01LY35HGO/>

Takehito Morokuzu - September 3, 2019, 1:13 am

(Sep 2, 2019 05:33 PM)BV1 Wrote: [\[CITE\]](#) Sorry, idk what I was on about earlier. Totally mislead you by stating you need an ethernet port. Don't know why I said that, it's not even remotely correct. For whatever reason when I made my reply earlier, my mindset was 'Wifi adapter goes into ethernet port!' like some sort of mong. My bad.

You can use a USB based WiFi adapter, you just need to ensure it runs in monitor mode. Any of these will work for under \$20 USD:

<https://www.amazon.com/gp/product/B00NAXX40C/>

<https://www.amazon.com/gp/product/B003EVO9U4/>

<https://www.amazon.com/gp/product/B00EQT0YK2/>

<https://www.amazon.com/gp/product/B00JDVRCI0/>

<https://www.amazon.com/gp/product/B073J3HXZH/> (What I use)

or if you also want to spend a little extra to monitor 5ghz

<https://www.amazon.com/gp/product/B01LY35HGO/>

No problem, thanks for the help.

callmejoehacker - September 3, 2019, 10:26 am

what an absolute lad. sick guide

Ajat123 - September 6, 2019, 9:05 am

Very high quality tutorial, thanks for posting these!

Mr. Robot - September 6, 2019, 6:49 pm

(Sep 6, 2019 09:05 AM)Ajat123 Wrote: [\[CITE\]](#) Very high quality tutorial, thanks for posting these!

No problem man. Hope it helps.

BTC - September 13, 2019, 8:40 am

Solid tutorial, nicely written.

Never seen this method before and was extremely intrigued. Thanks again for your help Mr. Robot

Mr. Robot - September 18, 2019, 9:49 pm

Hopefully this could help some more people !

kane2026 - September 19, 2019, 5:53 am

This is a nice tutorial. I already tried Hashcat before but I will give it another try. I have a few days off from work so I might just try this out.

I did have one question. Why do you use Hashcat in Windows? Is it a personal preference? I mean in the tutorial you showed the steps of installing it on Linux (Kali) so it felt a bit random to switch.

Mr. Robot - September 19, 2019, 6:13 am

(Sep 19, 2019 05:53 AM)kane2026 Wrote: [\[CITE\]](#) This is a nice tutorial. I already tried Hashcat

before but I will give it another try. I have a few days off from work so I might just try this out.

I did have one question. Why do you use Hashcat in Windows? Is it a personal preference? I mean in the tutorial you showed the steps of installing it on Linux (Kali) so it felt a bit random to switch.

Personally prefer to game while cracking hashes.

kane2026 - September 19, 2019, 6:15 am

Aah a person after my own heart

Mr. Robot - October 13, 2019, 12:37 pm

Anyone need tips on doing this?

Mr. Robot - November 25, 2019, 1:32 am

Anyone still need this old tutorial - works wonders.

barbiegirl100 - November 26, 2019, 6:14 pm

very good but i rather have a huge satellite wireless card to use everybody internet around my house

Mr. Robot - December 1, 2019, 2:06 pm

(Nov 26, 2019 07:14 PM)barbiegirl100 Wrote: [\[CITE\]](#) very good but i rather have a huge satellite wireless card to use everybody internet around my house

Ok well your comment makes 0 sense.

Forte - December 6, 2019, 8:39 am

Incredibly well written and comprehensible guide. I'll be using this in the future.

Enjoy the greens.

vRWN - December 6, 2019, 8:49 am

This method looks really sick, nice work OP, this is HQ!

SchwererGustav - December 7, 2019, 6:24 am

woooow you really worked hard for this , you really deserve to earn your name and the fame ..

w1l5t3r - December 7, 2019, 12:07 pm

Great tutorial!!! I done this back in 2018 with the WiFi Pineapple nano (with battery pack) and the tetra (in car) works awesome. This is one of the best tutorials I have read on this!

If anyone has an old WiFi pineapple collecting dust then dig it out, This is the guide for the pineapple (not my work)

[WiFi Pineapple tutorial](#)

Drowzy - December 9, 2019, 10:02 am

I don't think I am the right level to do this. I understood the start but then got lost. I will give it ago once I have leveled up

Mr. Robot - December 9, 2019, 10:04 am

(Dec 9, 2019 11:02 AM)Drowzy Wrote: [\[CITE\]](#) I don't think I am the right level to do this. I understood the start but then got lost. I will give it ago once I have leveled up

If you have any questions or get stuck please let me knowq.

Mr. Robot - August 16, 2020, 4:08 pm

I gave a bit more info in this one so thought it could have some updates.

