

Forum:[Hack Forums](#)

Thread: [Hack 1000+ WiFi networks per day. So you want to be a hacker? - Start here.](#)

Mr. Robot - January 2, 2020, 11:41 am

So let's just get into it. What will you achieve through this thread? You will be able to gain access to WiFi almost anywhere in the world in the same day.

You're traveling the world but you don't have WiFi? You have your laptop and a wireless adapter that is compatible? In just a few hours if not sooner you will have access to AT LEAST 1 network and if you need more, well just let it run a bit longer.

How easy is it? Well you could automate the entire process like I have or just run it manually when you need too.

>> I'll be adding changes with frequently asked questions if anyone has issues.

I've been able to get access to 1,000+ networks in the same day.

Process color coded and split into 3 categories.

1. Installation and setup
2. Running the tool and stopping the tool.
3. Upload text file online and wait.

What equipment do I need?

1. A wireless adapter that supports monitor mode.
2. A laptop OR Desktop OR Raspberry PI
3. A USB with Kali Linux (or install it if using laptop) (Copy of Kali Linux download if using Desktop) (Kali Linux on Raspberry PI if using PI)

Wireless adapters that work:

<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/>

I'd highly recommend a laptop for this due to the fact you can carry it in a backpack while walking in range of WiFi networks.

If using a desktop computer please follow this for installing Kali Linux:

<https://hackforums.net/showthread.php?tid=6032234>

If using a laptop please follow this for installing or booting Kali Linux:

<https://www.kali.org/docs/usb/kali-linux-live-usb-install/>

Otherwise follow this:

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/>

This set here, you can type in line by line exactly how they are written and it will all install perfectly for you. No stress. Make sure you have an internet connection when first installing. Remember if you are live booting, the entire distro will be wiped when you reboot so you will need to copy the final file off the device before rebooting it.

Code sudo apt-get update

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 hcxttools/

sudo make

sudo make install

cd ..

cd hashcat

sudo make

sudo make install

Commands we used if you want an explanation

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.

As soon as we run the following, the wireless adapter will go down, be put into monitor mode, be

brought back online, check for any interfering processes - then start the attack. Any WiFi networks vulnerable in range will drop like flies and you will have a pmkid. This will be the command list you will run every time once it is already installed to your device. If you type in "iwconfig" and don't see wlan0 but another wireless device name, replace wlan0 with that - it could be wlan1, or something else entirely.

While this is running, feel free to walk around or go for a drive - collect as many as you can then get home and ctrl+c to stop

Code ifconfig wlan0 down

iwconfig wlan0 mode monitor

ifconfig wlan0 up

airmon-ng check kill

hcxdumpool -o yourcityname.pcapng -i wlan0 --enable_status 1

Remember to hit ctrl+c on your keyboard when it is done.

Now what we need to do is convert that file we made "yourcityname.pcapng" to a file type we can read and crack. We can do that by typing in the following. It will output a few files but we only want the one ending in 16800. The other files will contain other information you can look at like WiFi names but we can obtain those directly from the 16800 file too.

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

Voila - now we are all done! Last thing to do is head to hashes.com and crack them all! You can manually run a smaller word list but i'd recommend just uploading the entire file like so:

Go to Hashes.com and register for an account. Once logged in - head to "profile" and "add bitcoin"

Send like \$10 or more to the bitcoin address depending on how bad you want it cracked.

>Then click Escrow - Upload new list.

This is my list - you can watch it get cracked in real time:

<https://pastebin.com/7xsXGDjW>

<https://hashes.com/escrow/item/?id=471>

>Now select your file (.16800) and choose the Algorithm "PMKID"

>Input a price in USD Per hash. The more you put in, the more the users out there will try and crack. I'd recommend judging it by total price rather than individual hash. The minimum you can offer is "0.00000050" which currently as of writing this is \$0.003 USD. So at that price it would cost \$3 to crack them all. I'd increase that to at least \$0.009 per for your first run (\$9 total for 1,000 hashes) otherwise if it's a specific network you want cracked offer as much as you would like for both speed and likelihood of getting it cracked!

If it isn't cracked, you can always cancel it and increase the price you are offering for it which in turn will speed up the rate it's cracked due to more people trying to get it done.

Any money left on your account you can withdraw later.

Here is my job, I posted a really low price on it for this just to show for this thread.

<https://hashes.com/escrow/item/?id=471>

Bastille - January 2, 2020, 11:46 am

Fav fav fav !!!

Looks like you started one of your resolution for 2020 ?

Nice thread

Mr. Robot - January 2, 2020, 11:47 am

(Jan 2, 2020 12:46 PM)Yseurk Wrote: [\[CITE\]](#) Fav fav fav !!!

Looks like you started one of your resolution for 2020 ?

Nice thread

Getting there, making a few changes to make it as easy to follow as possible. Give it a shot at some point and let me know any issues you encounter (hardware or software specific) so I can make sure everyone can follow it.

Dhoroty - January 2, 2020, 12:10 pm

Great tut, nicely explain everything, liked the hashes.com part.

Also nice explanation of for the "Got my 2020 Mass WiFi hacking setup ready" topics :)

Mr. Robot - January 2, 2020, 12:11 pm

(Jan 2, 2020 01:10 PM)Dhoroty Wrote: [\[CITE\]](#) Great tut, nicely explain everything, liked the hashes.com part.

Also nice explanation of for the "Got my 2020 Mass WiFi hacking setup ready" topics :)

Why 'sank yuu ;)

Work in progress as literally every tut I do is, but it's just about waiting for people to try it - find issues and then I can resolve them and add up to make it as flawless as possible.

Dhoroty - January 2, 2020, 12:18 pm

(Jan 2, 2020 01:11 PM)Mr. Robot Wrote: [\[CITE\]](#) Work in progress as literally every tut I do is, but it's just about waiting for people to try it - find issues and then I can resolve them and add up to make it as flawless as possible.

Maybe when using the virtual box method, the vid not shows how to attach the USB wifi adapter from the host to the virtual environment. That should help for some, who blindly trying to type the "ifconfig wlan0 down" command, and only gets errors.

Mr. Robot - January 2, 2020, 12:20 pm

(Jan 2, 2020 01:18 PM)Dhoroty Wrote: [\[CITE\]](#) Maybe when using the virtual box method, the vid not shows how to attach the USB wifi adapter from the host to the virtual environment. That should help for some, who blindly trying to type the "ifconfig wlan0 down" command, and only gets errors.

Will do for sure. Appreciate it.

Takehito Morokuzu - January 2, 2020, 7:18 pm

How long would it take to crack it myself?

My desktop is i5 8400 + GTX 1080

Laptop is i7 8750h and GTX 1060 (i7 undervolted to reduce throttling, runs at 3.5ghz all cores)

Mr. Robot - January 2, 2020, 7:24 pm

(Jan 2, 2020 08:18 PM)Takehito Morokuzu Wrote: [\[CITE\]](#) How long would it take to crack it myself?

My desktop is i5 8400 + GTX 1080

Laptop is i7 8750h and GTX 1060 (i7 undervolted to reduce throttling, runs at 3.5ghz all cores)

That depends on 2 main factors - if we are only wanting 1 WiFi out of hundreds you collect.

1. Your wordlist and/or number list/mask (I'd start with 8 digits long, 0-9)
2. How many networks you have collected and are attacking.

So if you were just doing a space of 8 digits in length which in most cases would get you at least one out of a hundred, it shouldn't take more than 10 minutes in most cases.

Gizmo - January 3, 2020, 1:48 am

Awesome and very nice explanation of hacking WIFI!

Thanks for the high quality share. It's unique seeing such a detailed and well explained tutorial.

Roytoy - January 3, 2020, 2:49 am

Seems like a really informative tutorial!

Mr. Robot - January 3, 2020, 4:16 am

(Jan 3, 2020 03:49 AM)Roytoy Wrote: [\[CITE\]](#) Seems like a really informative tutorial!

Thanks dude appreciate it.

Gizmo - January 3, 2020, 6:26 am

I just tested it out and it works perfectly!

I have one question though regarding this command:

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

Specific about the "-U usernamelist" . When looking into the manual of hcxpcaptool it has to output some sort of username list, why do you include that part in this command? Is it because some wifi networks require a username? Thanks!

Heads up:

When browsing to your link (<https://hashes.com/escrow/item/?id=471>) I get: Invalid List

Mr. Robot - January 3, 2020, 11:21 am

(Jan 3, 2020 07:26 AM)Gizmo Wrote: [\[CITE\]](#) I just tested it out and it works perfectly!

I have one question though regarding this command:

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

Specific about the "-U usernamelist" . When looking into the manual of hcxpcaptool it has to output some sort of username list, why do you include that part in this command? Is it because some wifi networks require a username? Thanks!

Heads up:

When browsing to your link (<https://hashes.com/escrow/item/?id=471>) I get: Invalid List
You can actually convert with out any toggles except -z but for ease of use I used an extended command to help me fix issues people might have.

The list I put up I deactivated to increase my offer price which gave it a new ID but just reposted it now

Gizmo - January 3, 2020, 1:56 pm

(Jan 3, 2020 12:21 PM)Mr. Robot Wrote: [\[CITE\]](#) You can actually convert with out any toggles except -z but for ease of use I used an extended command to help me fix issues people might have.

The list I put up I deactivated to increase my offer price which gave it a new ID but just reposted it now

All clear, thank you for the reply.

Mr. Robot - January 3, 2020, 3:09 pm

(Jan 3, 2020 02:56 PM)Gizmo Wrote: [\[CITE\]](#) All clear, thank you for the reply.
Not a problem, any issues just hit me up.

SchwererGustav - January 4, 2020, 9:57 am

veryyyyyy nice i like it .. but can we do a rainbow crack instead of sending the specimen to that website ?, how can we really effective when using rainbow tables ?

Mr. Robot - January 4, 2020, 12:14 pm

(Jan 4, 2020 10:57 AM)SchwererGustav Wrote: [\[CITE\]](#) veryyyyyy nice i like it .. but can we do a rainbow crack instead of sending the specimen to that website ?, how can we really effective when using rainbow tables ?

You can however it's much easier to pay a few dollars and get a lot cracked than run it on a single GPU.

ETH - January 5, 2020, 12:31 am

What is your recommendation ?

Dual booting Kali with other OS or Virtualisation

Mr. Robot - January 5, 2020, 1:14 am

(Jan 5, 2020 01:31 AM)ETH Wrote: [\[CITE\]](#) What is your recommendation ?
Dual booting Kali with other OS or Virtualisation

Either works just fine, even live boot is fine. Depends on your main system specs and how it can handle virtualization.

dhragon11 - January 6, 2020, 5:56 am

(Jan 2, 2020 12:41 PM)Mr. Robot Wrote: [\[CITE\]](#) Here is my job, I posted a really low price on it for this just to show for this thread.

<https://hashes.com/escrow/item/?id=471>

[/color][[/align]

You can also use <https://www.onlinehashcrack.com/> it is basically the same with the site you suggested, not sure which one is cheaper to use.

Mr. Robot - January 6, 2020, 11:16 am

(Jan 6, 2020 06:56 AM)dhragon11 Wrote: [\[CITE\]](#) You can also use <https://www..com/> it is basically the same with the site you suggested, not sure which one is cheaper to use.

DO NOT USE THAT SITE. Getting your hash cracked by others vs a site charging money ? fuck that.

Mr. Robot - January 9, 2020, 9:50 pm

Got some updates for the people DMing me.

erotic - January 11, 2020, 4:42 am

(Jan 2, 2020 12:41 PM)Mr. Robot Wrote: [\[CITE\]](#)

So let's just get into it. What will you achieve through this thread? You will be able to gain access to WiFi almost anywhere in the world in the same day.

You're traveling the world but you don't have WiFi? You have your laptop and a wireless adapter that is compatible? In just a few hours if not sooner you will have access to AT LEAST 1 network and if you need more, well just let it run a bit longer.

How easy is it? Well you could automate the entire process like I have or just run it manually when you need too.

>> I'll be adding changes with frequently asked questions if anyone has issues.

I've been able to get access to 1,000+ networks in the same day.

Process color coded and split into 3 categories.

1. Installation and setup
2. Running the tool and stopping the tool.
3. Upload text file online and wait.

What equipment do I need?

1. A wireless adapter that supports monitor mode.
2. A laptop OR Desktop OR Raspberry PI
3. A USB with Kali Linux (or install it if using laptop) (Copy of Kali Linux download if using Desktop) (Kali Linux on Raspberry PI if using PI)

Wireless adapters that work:

<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/>

I'd highly recommend a laptop for this due to the fact you can carry it in a backpack while walking in range of WiFi networks.

If using a desktop computer please follow this for installing Kali Linux:

<https://hackforums.net/showthread.php?tid=6032234>

If using a laptop please follow this for installing or booting Kali Linux:

<https://www.kali.org/docs/usb/kali-linux-live-usb-install/>

Otherwise follow this:

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/>

This set here, you can type in line by line exactly how they are written and it will all install perfectly

for you. No stress. Make sure you have an internet connection when first installing. Remember if you are live booting, the entire distro will be wiped when you reboot so you will need to copy the final file off the device before rebooting it.

```
Code sudo apt-get update
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/hcxtools.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
```

Commands we used if you want an explanation

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.

As soon as we run the following, the wireless adapter will go down, be put into monitor mode, be brought back online, check for any interfering processes - then start the attack. Any WiFi networks

vulnerable in range will drop like flies and you will have a pmkid. This will be the command list you will run every time once it is already installed to your device. If you type in "iwconfig" and don't see wlan0 but another wireless device name, replace wlan0 with that - it could be wlan1, or something else entirely.

While this is running, feel free to walk around or go for a drive - collect as many as you can then get home and ctrl+c to stop

Code ifconfig wlan0 down

iwconfig wlan0 mode monitor

ifconfig wlan0 up

airmon-ng check kill

hcxdumpool -o yourcityname.pcapng -i wlan0 --enable_status 1

Remember to hit ctrl+c on your keyboard when it is done.

Now what we need to do is convert that file we made "yourcityname.pcapng" to a file type we can read and crack. We can do that by typing in the following. It will output a few files but we only want the one ending in 16800. The other files will contain other information you can look at like WiFi names but we can obtain those directly from the 16800 file too.

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

Voila - now we are all done! Last thing to do is head to hashes.com and crack them all! You can manually run a smaller word list but i'd recommend just uploading the entire file like so:

Go to Hashes.com and register for an account. Once logged in - head to "profile" and "add bitcoin"

Send like \$10 or more to the bitcoin address depending on how bad you want it cracked.

>Then click Escrow - Upload new list.

This is my list - you can watch it get cracked in real time:

<https://pastebin.com/7xsXGDjW>

<https://hashes.com/escrow/item/?id=471>

>Now select your file (.16800) and choose the Algorithm "PMKID"

>Input a price in USD Per hash. The more you put in, the more the users out there will try and crack. I'd recommend judging it by total price rather than individual hash. The minimum you can offer is "0.00000050" which currently as of writing this is \$0.003 USD. So at that price it would cost \$3 to crack them all. I'd increase that to at least \$0.009 per for your first run (\$9 total for 1,000 hashes) otherwise if it's a specific network you want cracked offer as much as you would like for both speed and likelihood of getting it cracked!

If it isn't cracked, you can always cancel it and increase the price you are offering for it which in turn will speed up the rate it's cracked due to more people trying to get it done.

Any money left on your account you can withdraw later.

Here is my job, I posted a really low price on it for this just to show for this thread.

<https://hashes.com/escrow/item/?id=471>

Don't mind me just commenting to save this for later.

I love the Raspberry Pi idea, then you can literally just put it in a hoodie pocket.

Mr. Robot - January 11, 2020, 4:46 am

(Jan 11, 2020 05:42 AM)RuneArt Wrote: [\[CITE\]](#) Don't mind me just commenting to save this for later.

I love the Raspberry Pi idea, then you can literally just put it in a hoodie pocket.
Sure can, makes it easy as fuck.

JamalNazamAli - January 11, 2020, 10:42 am

Nice, dude! Thank you so much for this tutorial.

Mr. Robot - January 11, 2020, 9:56 pm

(Jan 11, 2020 11:42 AM)JamalNazamAli Wrote: [\[CITE\]](#) Nice, dude! Thank you so much for this tutorial.

No problem, hope it helps. If you get stuck at any point hit me up or post here

JamalNazamAli - January 12, 2020, 10:55 am

(Jan 11, 2020 10:56 PM)Mr. Robot Wrote: [\[CITE\]](#) No problem, hope it helps. If you get stuck at any point hit me up or post here

Okey, thanks. I'll keep that in mind =))

Mr. Robot - January 14, 2020, 7:18 pm

(Jan 12, 2020 11:55 AM)JamalNazamAli Wrote: [\[CITE\]](#) Okey, thanks. I'll keep that in mind =))
Going to be adding some other information based on any issues people have.

JamalNazamAli - January 16, 2020, 3:45 am

(Jan 14, 2020 08:18 PM)Mr. Robot Wrote: [\[CITE\]](#) Going to be adding some other information based on any issues people have.

Do it, sounds good. Good luck!

Mr. Robot - January 16, 2020, 7:13 pm

(Jan 16, 2020 04:45 AM)JamalNazamAli Wrote: [\[CITE\]](#) Do it, sounds good. Good luck!
Have you had a go at it yet?

JamalNazamAli - January 16, 2020, 8:18 pm

(Jan 16, 2020 08:13 PM)Mr. Robot Wrote: [\[CITE\]](#) Have you had a go at it yet?
I haven't been yet. Will go soon

jacob286 - January 18, 2020, 9:21 am

There is an APP available in China
wifi????

de_g3ntl3m4n - January 19, 2020, 5:05 am

Can you also set this up where you are the one that is cracking the hashes? or is the escrow like a services known for cracking hashes?

Mr. Robot - January 19, 2020, 5:07 am

(Jan 19, 2020 06:05 AM)de_g3ntl3m4n Wrote: [\[CITE\]](#) Can you also set this up where you are the

one that is cracking the hashes? or is the escrow like a services known for cracking hashes?
You definitely can if you have the time and hardware

de_g3ntl3m4n - January 19, 2020, 5:09 am

(Jan 19, 2020 06:07 AM)Mr. Robot Wrote: [\[CITE\]](#) You definitely can if you have the time and hardware

Ahhh, interesting, sounds like fun, looks like its something im going to try to look into then. Very nice Tutoirals man keep it up :)

VIXV - January 19, 2020, 11:32 am

Absolutely brilliant thread. Purchased this:

https://www.amazon.co.uk/dp/B07FCNP2VL/ref=cm_sw_r_tw_dp_U_x_36kJEb3ZTKXR3

Really nice thread man, thanks :)

Mr. Robot - January 19, 2020, 11:31 pm

(Jan 19, 2020 12:32 PM)InfoSec Wrote: [\[CITE\]](#) Absolutely brilliant thread. Purchased this:

https://www.amazon.co.uk/dp/B07FCNP2VL/ref=cm_sw_r_tw_dp_U_x_36kJEb3ZTKXR3

Really nice thread man, thanks :)

Not entirely sure if it supports monitor mode.

VIXV - January 20, 2020, 12:58 am

(Jan 20, 2020 12:31 AM)Mr. Robot Wrote: [\[CITE\]](#) Not entirely sure if it supports monitor mode. It does as far as I've seen.

3x3c0 - January 20, 2020, 3:53 am

How would the website crack hashes? Doesn't it act only as a signature to extract the data? What would be cracked from the hash values?

I apologize if I sound like a complete idiot, I'm fairly new to the technology space in general, not to mention hacking.

Mr. Robot - January 20, 2020, 4:06 am

(Jan 20, 2020 04:53 AM)3x3c0 Wrote: [\[CITE\]](#) How would the website crack hashes? Doesn't it act only as a signature to extract the data? What would be cracked from the hash values?

I apologize if I sound like a complete idiot, I'm fairly new to the technology space in general, not to mention hacking.

You would be obtaining the WPA2 passphrase to connect.

The website just offers a space to get people from around the world to crack the hashes for you in an extremely fast manner - as it could take you a year or longer for extremely complex ones.

3x3c0 - January 20, 2020, 4:13 am

Ok thank you for confirming my hypothesis on this matter. But I would like to ask one more question, why would you need to crack thousands of wifi? Cracking a few wifi near the region you reside in would be enough for sufficient wifi connection and it could be done with a few simple software in Kali, why would go to such length for such an absurd amount of wifi password that you won't use?

Sorry for wasting your time, I'm new to this and want some more experience on the matter.

Mr. Robot - January 20, 2020, 4:19 am

(Jan 20, 2020 05:13 AM)3x3c0 Wrote: [\[CITE\]](#) Ok thank you for confirming my hypothesis on this matter. But I would like to ask one more question, why would you need to crack thousands of wifi?

Cracking a few wifi near the region you reside in would be enough for sufficient wifi connection and it could be done with a few simple software in Kali, why would go to such length for such an absurd amount of wifi password that you won't use?

Sorry for wasting your time, I'm new to this and want some more experience on the matter. So i'll point out some main reasons.

1. In your house currently, even if you can see let's say 20 networks right? You might not be able to crack a single one through WEP or WPS - in which case WPA/2 is your only option. In such a scenario, they could all have extremely secure long winded passwords (let's say again, 20 characters long) and your likelihood of cracking one is EXTREMELY low.

In this scenario, using and broadcasting a lot of networks - collecting PMKIDs, it drastically increases the chances of cracking a network. I can GUARANTEE in a town of say 10,000 houses, you can crack AT LEAST 10% of those with a simple attack such as 8 digits. Then move up from there (default keyspaces and custom wordlists)

2. Say you live in a campervan or are traveling the country. Simply upload a hash from WHEREVER you are in the world and get WiFi.

3. Anonymity reasons, using other networks you can easily use as proxies for yourself.

4. MiTM attacks, credential harvesting, RATs/Gaining slaves

There are more reasons than just these, but they generally start to fall under fraud which isn't exactly something to discuss.

Hope you have understood some of this at least.

3x3c0 - January 20, 2020, 4:23 am

I understand, anonymity-wise I'm not sure but thank you for your explanation, I hope I could learn more from you in the future.

Mr. Robot - January 22, 2020, 7:34 pm

(Jan 20, 2020 05:23 AM)3x3c0 Wrote: [\[CITE\]](#) I understand, anonymity-wise I'm not sure but thank you for your explanation, I hope I could learn more from you in the future.

No problem, happy to help whenever.

creatine - January 28, 2020, 5:02 am

Thanks Mr. Robot This is really a good skill, to become a good hacker.

With the kali linux system on persistent usb stationary, not moving, how long to scan before hit Control+c?

For best test result.

Mr. Robot - January 30, 2020, 7:28 pm

(Jan 28, 2020 06:02 AM)creatine Wrote: [\[CITE\]](#) Thanks Mr. Robot This is really a good skill, to become a good hacker.

With the kali linux system on persistent usb stationary, not moving, how long to scan before hit Control+c?

For best test result.

You generally want to run it for a few minutes if you aren't going anywhere, just to make sure it picks them up. If you're traveling about, just let it run the entire time and don't stress about standing around in one place

FalconExploit - January 31, 2020, 10:10 pm

it looks fun. i will try.

Mr. Robot - February 1, 2020, 7:22 pm

(Jan 31, 2020 11:10 PM)FalconExploit Wrote: [\[CITE\]](#) it looks fun. i will try.

Let me know how it goes, post back here.

ubernewb - February 4, 2020, 10:30 am

Interesting. I'm curious how much hashing power is there? For instance, AT&T fiber routers use WPA2 keys with, I think, 15 characters including lower, upper, numbers, and special characters. I did the math on cracking that using my 1080 and I think it was many many years.

Curious what it would cost to crack that and how long it would take...any idea?

billhenrybh - February 9, 2020, 8:14 am

I kne wome of these methods, some gonna test it, thanks-.

This is nice and i want to know more about it thanks

This is nice and i want to know more about it thanks

vrs005 - February 10, 2020, 3:55 pm

It sure looks fun. i will try.

ModernJS - February 12, 2020, 4:34 pm

why would you use "sudo" when you've already called sudo su -

--

Mr. Robot - February 12, 2020, 4:39 pm

(Feb 12, 2020 05:34 PM)ModernJS Wrote: [\[CITE\]](#) why would you use "sudo" when you've already called sudo su -

--

Because new users have issues from basic shit and i'd rather not reply 200 times with the same answer on how they are fucking it up.

ModernJS - February 12, 2020, 5:32 pm

(Feb 12, 2020 05:39 PM)Mr. Robot Wrote: [\[CITE\]](#) Because new users have issues from basic Clay Davis and i'd rather not reply 200 times with the same answer on how they are fugging it up.

Lol. Ego's not your friend

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>

Are these packages even yours? lol

Mr. Robot - February 12, 2020, 5:34 pm

(Feb 12, 2020 06:32 PM)ModernJS Wrote: [\[CITE\]](#) Lol. Ego's not your friend

Neither is helping those who wont help themselves.

ModernJS - February 12, 2020, 5:39 pm

Code git clone <https://github.com/ZerBea/hcxdumptool.git>

Cloning into 'hcxdumptool'..

```
~/wlan
$ cd hcxdumptool
```

```
~/wlan/hcxdumptool on master
$ make
cc -O3 -Wall -Wextra -std=gnu99 -o hcxploff hcxploff.c
cc -O3 -Wall -Wextra -std=gnu99 -o hcxdumptool hcxdumptool.c -lcrypto
```

```
~/wlan/hcxdumptool on master
$ sudo make install
cc -O3 -Wall -Wextra -std=gnu99 -o hcxploff hcxploff.c
cc -O3 -Wall -Wextra -std=gnu99 -o hcxdumptool hcxdumptool.c -lcrypto
install -m 0755 -D hcxploff /usr/local/bin/hcxploff
install -m 0755 -D hcxdumptool /usr/local/bin/hcxdumptool
rm -f hcxploff
rm -f hcxdumptool
rm -f *.o *~??????
```

(Feb 12, 2020 06:34 PM)Mr. Robot Wrote: [\[CITE\]](#) Neither is helping those who wont help themselves.

Stop it dude

You know why you used "sudo make" ??

Mr. Robot - February 12, 2020, 5:42 pm

(Feb 12, 2020 06:39 PM)ModernJS Wrote: [\[CITE\]](#) Code git clone
<https://github.com/ZerBea/hcxdumptool.git>
Cloning into 'hcxdumptool'..

```
~/wlan
$ cd hcxdumptool
```

```
~/wlan/hcxdumptool on master
$ make
cc -O3 -Wall -Wextra -std=gnu99 -o hcxploff hcxploff.c
cc -O3 -Wall -Wextra -std=gnu99 -o hcxdumptool hcxdumptool.c -lcrypto
```

```
~/wlan/hcxdumptool on master
$ sudo make install
cc -O3 -Wall -Wextra -std=gnu99 -o hcxploff hcxploff.c
cc -O3 -Wall -Wextra -std=gnu99 -o hcxdumptool hcxdumptool.c -lcrypto
install -m 0755 -D hcxploff /usr/local/bin/hcxploff
install -m 0755 -D hcxdumptool /usr/local/bin/hcxdumptool
rm -f hcxploff
rm -f hcxdumptool
rm -f *.o *~??????
```

Stop it dude

You know why you used "sudo make" ??

Yes. Because what happens a lot, especially while teaching users via voice and IM - they make a mistake and run different commands in different terminals. This happens far too often and when they do it, at least if they are running with sudo - it will still do as required.

This stops complications and makes the process easier.

I also try tell people to use the exact version of the OS I use in the tutorials - as believe it or not, even when I tell people this - they don't.

Why?

Because they already have a newer version or older version ready to go and they are lazy.

What are the results?

Hundreds of PMs and posts asking about issues they wouldn't have had otherwise.

Anyone with a bit of experience can get around said issues but when you are that new and looking for one solution or one way into learning - following something correctly is often not done.

ModernJS - February 12, 2020, 5:44 pm

(Feb 12, 2020 06:42 PM)Mr. Robot Wrote: [\[CITE\]](#) Yes. Because what happens a lot, especially while teaching users via voice and IM - they make a mistake and run different commands in different terminals. This happens far too often and when they do it, at least if they are running with sudo - it will still do as required.

This stops complications and makes the process easier.

Alright, thanks for that.

Why kali?

(Feb 12, 2020 06:42 PM)Mr. Robot Wrote: [\[CITE\]](#) Yes. Because what happens a lot, especially while teaching users via voice and IM - they make a mistake and run different commands in different terminals. This happens far too often and when they do it, at least if they are running with sudo - it will still do as required.

This stops complications and makes the process easier.

I also try tell people to use the exact version of the OS I use in the tutorials - as believe it or not, even when I tell people this - they don't.

Why?

Because they already have a newer version or older version ready to go and they are lazy.

What are the results?

Hundreds of PMs and posts asking about issues they wouldn't have had otherwise.

Anyone with a bit of experience can get around said issues but when you are that new and looking for one solution or one way into learning - following something correctly is often not done.

I was misunderstanding it.. Nice collection of threads you have.

Mr. Robot - February 12, 2020, 5:46 pm

(Feb 12, 2020 06:44 PM)ModernJS Wrote: [\[CITE\]](#) Alright, thanks for that.

Why kali?

No problem.

Because out of the box it's a good place for new users to start. Once they have successfully done an attack and seen how it works + how to install, they can then use other OS to run it. Albeit they will face different issues but that's when they can start to learn to identify an issue and bypass it to make it work.

To me overall - what's better?

Adding a few extra commands in to make sure they don't sit around for a day or two waiting for a reply - giving up and then never learning or joining the community...

Or making it work as it should and helping them become one day - a future valued member of the community.

I've chosen my bed to lie in. But I do completely understand where you are coming from.

ModernJS - February 12, 2020, 6:06 pm

(Feb 12, 2020 06:46 PM)Mr. Robot Wrote: [\[CITE\]](#) No problem.

Because out of the box it's a good place for new users to start. Once they have successfully done an attack and seen how it works + how to install, they can then use other OS to run it. Albeit they will face different issues but that's when they can start to learn to identify an issue and bypass it to make it work.

To me overall - what's better?

Adding a few extra commands in to make sure they don't sit around for a day or two waiting for a reply - giving up and then never learning or joining the community...

Or making it work as it should and helping them become one day - a future valued member of the community.

I've chosen my bed to lie in. But I do completely understand where you are coming from.

You're a good soldier it seems! Wishing I could buy your services in the near future

Silkroad - February 21, 2020, 9:16 am

I've cracked wifi's numerous times but this method is simply fantastic, thanks a lot for the share [Mr. Robot](#)

Fortunate - February 21, 2020, 12:27 pm

Didn't know it was this easy. I have some WI-FI tools myself but never cracked them. What could you use a 1000 hacked wifi's for? I'm curious.

NoError - February 22, 2020, 7:04 am

Very interested! Could you PM me?

C2B41T - March 3, 2020, 7:56 am

hases.com is down, any other recommendations?

Mr. Robot - March 3, 2020, 8:12 am

(Mar 3, 2020 08:56 AM)C2B41T Wrote: [\[CITE\]](#) hases.com is down, any other recommendations? Hashes.com is still live.

el_ninio - March 3, 2020, 8:20 am

Nice tutorial will come back later when i get my usb stick

C2B41T - March 3, 2020, 8:33 am

(Mar 3, 2020 09:12 AM)Mr. Robot Wrote: [\[CITE\]](#) Hashes.com is still live.

wow, it really is, sorry my bad!

otap1443 - March 8, 2020, 2:14 pm

great tutorial, easy to understand and exciting topic :)

W1NK1LL3RX - March 9, 2020, 9:01 am

Hey are you still cracking hashes?

Mutassas - March 10, 2020, 8:43 am

Wow, it seems nice, but i'll try it soon

You may call me V - March 11, 2020, 4:33 pm

Excellent tutorial thank you so much for this, i now know how to hack into Wifis :)

NoisyBoyTracker - March 19, 2020, 8:28 am

Great tutorial, was looking for something like this to try out some stuff with my raspberry.

WinklerConnect - April 13, 2020, 6:51 pm

(Mar 3, 2020 09:12 AM)Mr. Robot Wrote: [\[CITE\]](#) Hashes.com is still live.

Thank you for the amazing tutorial Mr. Robot.

To extend my range I plan to use a 2.4 GHz WiFi Outdoor Omnidirectional 12 dBi Antenna. This one here:

<https://www.air802.com/antenna-wifi-omni-directional-2.4-ghz-12-dbi-outdoor-mast-mount.html>

I want to be able to connect to a hacked wireless access point from at least 1km away from my physical location in order to mitigate trilateration attempts from state actor adversaries. If I combine said antenna with a Ubiquiti bullet here: <https://www.gowifi.co.nz/wireless/bullet-m2-hp.html> do you think I can achieve a 1km connection in a suburban environment that has no hills but lots of houses and some trees?

Or do you have any recommendations you don't mind sharing?

Mr. Robot - April 13, 2020, 6:56 pm

(Apr 13, 2020 06:51 PM)WinklerConnect Wrote: [\[CITE\]](#) Thank you for the amazing tutorial Mr. Robot.

I plan to use a 2.4 GHz WiFi Outdoor Omnidirectional 12 dBi Antenna. This one here:

<https://www.air802.com/antenna-wifi-omni-directional-2.4-ghz-12-dbi-outdoor-mast-mount.html>

I want to be able to connect to a hacked wireless access point from at least 1km away from my physical location in order to mitigate trilateration attempts from state actor adversaries. If I combine said antenna with a Ubiquiti bullet here: <https://www.gowifi.co.nz/wireless/bullet-m2-hp.html> do you think I can achieve a 1km connection in a suburban environment that has no hills but lots of houses and some trees?

Or do you have any recommendations you don't mind sharing?

I'm far too busy right now to do a proper look at support on packet injection - just make sure you have a long pole to get the best line of sight available.

WinklerConnect - April 13, 2020, 8:53 pm

(Apr 13, 2020 06:56 PM)Mr. Robot Wrote: [\[CITE\]](#) I'm far too busy right now to do a proper look at support on packet injection - just make sure you have a long pole to get the best line of sight available.

Of course you are.

Thanks for the tip?

??¢??? - April 14, 2020, 2:33 pm

Nice effort, but, you failed to mention different use cases that a person might face such as 2.4G / 5G Signals. WPA/WPA2 hashes. A lot of modern routers now come with WPS so we have things like cafe-latte attack and pixie dust.

Nevertheless, good effort.

Mr. Robot - April 14, 2020, 3:26 pm

(Apr 14, 2020 02:33 PM)??¢??? Wrote: [\[CITE\]](#) Nice effort, but, you failed to mention different use cases that a person might face such as 2.5G / 5G Signals. WPA/WPA2 hashes. A lot of modern routers now come with WPS so we have things like cafe-latte attack and pixie dust.

Nevertheless, good effort.

Nice effort but you said 2.5g.

Also no, this thread covers WPA and WPA2 hashes under the PMKID method - and WPS is completely pointless against this type of attack when it can cover a LOT more networks a LOT faster.

Good try in trying to look interesting or somewhat knowledgeable but kids like you really grind my gears.

This tutorial isn't a coverage of every type of WiFi hacking method out there, it's for cracking 1,000 networks a day which you can't do with WPS nor capturing handshakes.

??¢??? - April 14, 2020, 4:08 pm

(Apr 14, 2020 03:26 PM)Mr. Robot Wrote: [\[CITE\]](#) Nice effort but you said 2.5g.

Also no, this thread covers WPA and WPA2 hashes under the PMKID method - and WPS is completely pointless against this type of attack when it can cover a LOT more networks a LOT faster.

Good try in trying to look interesting or somewhat knowledgeable but kids like you really grind my gears.

This tutorial isn't coverage of every type of WiFi hacking method out there, it's for cracking 1,000 networks a day which you can't do with WPS nor capturing handshakes.

First, It was an honest mistake for the typo. There are two types of Band 2.4 and 5-Ghz Wi-Fi. All the links to the products you have given only support 2.4 which means the modern 5-GHz Wi-Fi SSIDs will not be listed by them and as like 80% of the people have already switched to 5Ghz. I am sure a lot of users will face a problem that their target network is not visible.

I merely meant to say was you should mention these key points as well in the thread.

Now coming to your PMKID Method. This is so 2018. When it came out, the biggest advantage was that no more 4-way handshake was required i.e the attack could be performed clientless (your damn thread fails to mention it too).

While you did mention spending money to crack the hash online, you failed to mention the part that this can be cracked locally as well using tools like hashcat which is a bigger advantage if you have a local wordlist with customized keywords country-wise, for example, a user in my country is more likely to have a phone number as a password. So I will create a wordlist with the phone number pattern matching to my country's codes Or common Names of people. This is much more efficient and effective.

Reaver also came around during those days (approx 2011) which worked really as it performed one of the first practical attacks against WPA- and WPA2-encrypted networks, it totally ignored the type of encryption a network used, exploiting poor design choices in the WPS protocol. well but has now become obsolete.

WPS is currently being used in major home networks as its secure and as simple as pressing a button on your device to enable WPS.

Then came the better tools "Airedroid" used to find vulnerable networks, and then Bully used to crack them. While a lot of routers prevent the brute-force attack but it still has the majority of the success rate.

You may have more post count than I do and a shit ton of nonsense awards, but I have been around on these forums and the security domain longer than you have been, you need to understand to never judge a book by its cover. I was appreciating the hard work you did to cover a basic tutorial and mentioned some additional points which could have been added to help beginners understand Wi-Fi hacking in a better way.

I am an OSCP, OSWP Certified BTW and have written 3 bestseller books on the security topics you would probably shit your pants reading about. I gave a talk last year on stage with Kevin Mitnick showing demos of Wi-Fi hacking live in front of hundreds of people lol.

Mr. Robot - April 14, 2020, 4:17 pm

(Apr 14, 2020 04:08 PM)??? Wrote: [\[CITE\]](#) First, It was an honest mistake for the typo. There are two types of Band 2.4 and 5-GHz Wi-Fi. All the links to the products you have given only support 2.4 which means the modern 5-GHz Wi-Fi SSIDs will not be listed by them and as like 80% of the people have already switched to 5GHz. I am sure a lot of users will face a problem that their target network is not visible.

I merely meant to say was you should mention these key points as well in the thread.

Now coming to your PMKID Method. This is so 2018. When it came out, the biggest advantage was that no more 4-way handshake was required i.e the attack could be performed clientless (your damn thread fails to mention it too).

While you did mention spending money to crack the hash online, you failed to mention the part that this can be cracked locally as well using tools like hashcat which is a bigger advantage if you have a local wordlist with customized keywords country-wise, for example, a user in my country is more likely to have a phone number as a password. So I will create a wordlist with the phone number pattern matching to my country's codes Or common Names of people. This is much more efficient and effective.

Reaver also came around during those days (approx 2011) which worked really as it performed one of the first practical attacks against WPA- and WPA2-encrypted networks, it totally ignored the type of encryption a network used, exploiting poor design choices in the WPS protocol. well but has now become obsolete.

WPS is currently being used in major home networks as its secure and as simple as pressing a button on your device to enable WPS.

Then came the better tools "Aircrack-ng" used to find vulnerable networks, and then Bully used to crack them. While a lot of routers prevent the brute-force attack but it still has the majority of the success rate.

You may have more post count than I do and a Clay Davis ton of nonsense awards, but I have been around on these forums and the security domain longer than you have been, you need to understand to never judge a book by its cover. I was appreciating the hard work you did to cover a basic tutorial and mentioned some additional points which could have been added to help beginners understand Wi-Fi hacking in a better way.

I am an OSCP, OSWP Certified BTW and have written 3 bestseller books on the security topics you would probably Clay Davis your pants reading about. I gave a talk last year on stage with Kevin Mitnick showing demos of Wi-Fi hacking live in front of hundreds of people lol.

Alright let's start off with your dumb bullshit response.

Yes the WiFi adapters shown support 2.4ghz networks, as to expected when the majority (85+%) of networks use it world wide over 5ghz.

PMKID attacks are far superior due to the amount of networks you can crack in the shortest available time. As is the purpose of this thread - to cut out the bullshit and start people off with having network access to begin with.

WPS is far inferior and is used in 20% of networks - with an average run time of 11 hours and 5 hours on networks with no lockouts, you can crack the same network via PMKID or even client handshake in far less time.

You also claim to have been around in 'forums' a lot longer than I have been but it takes 2 seconds to find out you haven't been.

OSCP and OSWP are absolutely nothing - I am certified in both as well, yet don't feel the need to bring it up as anyone can pick it up for next to nothing.

Not only that but let's clarify putting Mitnick's name in your reply shows how idiotic you are - For some reason people drop his name like it means something, if you really knew him... You'd be embarrassed at your own reply.

Let's end it with an actual quote from you in 2012.

Quote:It was long back when i was in 9th grade. One of my friends told me that i am a zero in computers and can never learn anything. He bragged about his cousin who was a hacker and can control anyone's PC from his house. My school life was not good as I had just a few friends. Rest just used to make fun of me, curse me, etc . To divert my mind I used to sit on computer browsing the internet, that's when I came across the term hacker, I read about their history did a lot of google search and Kevin Mitnick was the name which inspired me. After reading about him and his history, all I wanted was to be someone like him.

Mr. Robot - June 23, 2020, 1:03 am

Still valid for anyone looking, been a bit dead for a bit but happy to help.

Kieboard - June 25, 2020, 10:21 am

Amazing detailed thread, good way to start hacking, it always starts somewhere :p

menato - June 26, 2020, 7:41 am

Great detailed explanation.

Thanks for the effort.

hdmi - July 3, 2020, 4:04 pm

thanks for the tutorial :)

Mr. Robot - July 3, 2020, 4:33 pm

(Jul 3, 2020 04:04 PM)hdmi Wrote: [\[CITE\]](#) thanks for the tutorial :)

You're welcome, it's all about learning.

Mr. Robot - July 19, 2020, 8:31 pm

If you want a more complex hashcat tutorial let me know.

7 - July 20, 2020, 3:47 am

(Jul 19, 2020 08:31 PM)Mr. Robot Wrote: [\[CITE\]](#) If you want a more complex hashcat tutorial let me know.

Absolutely. Would be interesting to read thanks

murt - July 23, 2020, 2:50 am

Mr robot you're the only reason I check this part of the forum . Much love and many thanks for sharing the wonderful tutorials ! I've used all your tutorials more or less and I feel proud ?

Mr. Robot - July 23, 2020, 5:02 am

(Jul 23, 2020 02:50 AM)murt Wrote: [\[CITE\]](#) Mr robot you're the only reason I check this part of the forum . Much love and many thanks for sharing the wonderful tutorials ! I've used all your tutorials more or less and I feel proud ?

<3 I'm glad dude! I appreciate the support and feedback greatly.

Gindis2007 - August 16, 2020, 1:12 am

Nice , Thanks For Share ...

maybe it will be my 1st WPA2 crack this weekend :D

Mr. Robot - August 16, 2020, 4:36 am

(Aug 16, 2020 01:12 AM)Gindis2007 Wrote: [\[CITE\]](#) Nice , Thanks For Share ...

maybe it will be my 1st WPA2 crack this weekend :D

Well, I wish you the best of luck!

MightyOne - August 16, 2020, 4:48 am

Mr. Robot once again for the win. so fucking awesome.

I wish you would have posted some more tutorials and stuff that's more dated to today!

I know you are occupied with your game, but your threads are always so HQ.

Thanks again! always fun to learn more.

Raikou - August 19, 2020, 9:26 pm

Hi I read through the whole tutorial 3 questions:

1. can I pull it off as a complete noob to kali (I installed kali once and messed around with it for a

day)

2. when do you use the wireless adapter exactly just plug it in before the red (text) section?

3. Can I boot kali from a usb (without wiping my laptop) because thats what I assume you mean.

thank you for teaching us!

Mr. Robot - August 21, 2020, 7:26 am

(Aug 21, 2020 07:21 AM)Mk-2866 Wrote: [\[CITE\]](#) So this might be a wierd issue but it seems like it crashes my adapter after a short while and then it resets the TX-power down to 0. Is this something you've experienced?

Not something I have experienced, what are your specific setups?

Live boot?

Fresh installation?

Adapater?

Following each step, step by step or skipping one because you think you have already done it or don't need it.

Mr. Robot - August 21, 2020, 7:36 am

(Aug 21, 2020 07:29 AM)Mk-2866 Wrote: [\[CITE\]](#) Not a live boot it's kali installed in my virtualbox. It's a fresh install and I'm using an ALFA AWUS036NHA network adapter. I first didn't do every step but now I am doing each step. It's wierd because I just need to reset the power up to 30 and then it runs great again.

Yeah I don't really add a lot of support advice for Virtualbox when it comes to this due to errors with adapters and power.

RegularJoe - August 22, 2020, 12:22 am

Is there a way to crack these hashes for free? Otherwise, getting a SIM card seems like a lot more bang for buck

kane2026 - August 22, 2020, 6:19 am

Another great Wi-Fi tutorial by Mr. Robot. You should write the book on WAP cracking!

EliteManagement - August 22, 2020, 12:07 pm

Great share mate!

Always a pleasure

The Amazing Sinner - August 24, 2020, 11:13 pm

Amazing tutorial, very informative. Thanks for the high quality share.

Raikou - August 26, 2020, 3:04 pm

So what do you use on kali to be more anonymous like proxy chains or something?
would be nice if you added that since it's a beginner tutorial

Mr. Robot - August 26, 2020, 3:05 pm

(Aug 26, 2020 03:04 PM)Raikou Wrote: [\[CITE\]](#) So what do you use on kali to be more anonymous like proxy chains or something?

would be nice if you added that since it's a beginner tutorial

What? So you can connect after? That's not what this tutorial is about.

Raikou - August 26, 2020, 3:10 pm

(Aug 26, 2020 03:05 PM)Mr. Robot Wrote: [\[CITE\]](#) What? So you can connect after? That's not what

this tutorial is about.

I mean while you are collecting the WiFi networks.

Mr. Robot - August 26, 2020, 3:11 pm

(Aug 26, 2020 03:10 PM)Raikou Wrote: [\[CITE\]](#) I mean while you are collecting the WiFi networks. You don't have an internet connection and as such do not need a proxy or VPN.

Raikou - August 26, 2020, 3:13 pm

(Aug 26, 2020 03:11 PM)Mr. Robot Wrote: [\[CITE\]](#) You don't have an internet connection and as such do not need a proxy or VPN.
alright that makes sense thanks

Stanley - September 1, 2020, 5:17 am

I'm Stanley HF's helper bot. This OP (original poster) of this thread wants everyone to see this page and has elected to bump it to the top of the showthread listing. Since HF doesn't want a ton of LQP (Low Quality Posts) this is the best method of bumping your content. There is a small ?yte fee for each bump. Any OP can bump any of their threads on HF from the linked icon on the top of their first post.

If you haven't already read the first post of this thread we encourage you to do so.

Thanks,
Stanley

alurmein - September 2, 2020, 9:00 am

Great thread! Your tutorial is very well written and detailed as well. Thanks for sharing this method with us.

TheCrazyONE - September 12, 2020, 7:06 am

Im new to this thing therefor I have couple questions

This tool will just grab all available wifis when im driving?

What is hashes website used for?

Do I need to brute the wifis with a wordlist I do not understand

Thank you very much for this

Mr. Robot - September 12, 2020, 7:15 am

(Sep 12, 2020 07:06 AM)thecrazy1337 Wrote: [\[CITE\]](#) Im new to this thing therefor I have couple questions

This tool will just grab all available wifis when im driving?

What is hashes website used for?

Do I need to brute the wifis with a wordlist I do not understand

Thank you very much for this
Yes the 'tool' will grab WiFis while driving.

Hashes website is used for cracking for cheap you can pay 0.006 cents per hash you want cracked

or offer more if it's hard/important.

You can run your own wordlist against the hashes if you want.

TheCrazyONE - September 12, 2020, 7:22 am

(Sep 12, 2020 07:15 AM)Mr. Robot Wrote: [\[CITE\]](#) Yes the 'tool' will grab WiFis while driving.

Hashes website is used for cracking for cheap you can pay 0.006 cents per hash you want cracked or offer more if it's hard/important.

You can run your own wordlist against the hashes if you want.

So basically while driving the tool will get me the hashes then I can just put them in that website and it will give me wifi password?

Thank you!

Mr. Robot - September 12, 2020, 7:23 am

(Sep 12, 2020 07:22 AM)thecrazy1337 Wrote: [\[CITE\]](#) So basically while driving the tool will get me the hashes then I can just put them in that website and it will give me wifi password?

Thank you!

Yes absolutely!

You just have to credit your account there with a few dollars and upload the hashes as PMKID - then set a price per hash found.

:)

TheCrazyONE - September 12, 2020, 7:24 am

(Sep 12, 2020 07:23 AM)Mr. Robot Wrote: [\[CITE\]](#) Yes absolutely!

You just have to credit your account there with a few dollars and upload the hashes as PMKID - then set a price per hash found.

:)

This looks quite easy, thank you very much for this tutorial :)

One more question

Will this tool save wifi name too?

Mr. Robot - September 12, 2020, 7:35 am

(Sep 12, 2020 07:24 AM)thecrazy1337 Wrote: [\[CITE\]](#) This looks quite easy, thank you very much for this tutorial :)

One more question

Will this tool save wifi name too?

Part of one of the command will output the "ESSID" which is the name of the network however it wont be connected to the password itself.

After the password is cracked - the format will be:

PMKID:PASSWORD

That PMKID can be turned into the original SSID (network name/wifi name) in a number of ways but the easiest and quickest with no complications would be to go here:

<https://gpuhash.me>

Tak - September 13, 2020, 4:33 pm

Would the Pi Zero W still be the best model for this, out of all the latest models? Assuming the sole purpose was for ONLY this.

Mr. Robot - September 13, 2020, 4:39 pm

(Sep 13, 2020 04:33 PM)Tak Wrote: [\[CITE\]](#) Would the Pi Zero W still be the best model for this, out of all the latest models? Assuming the sole purpose was for ONLY this.

For this in particular, I would say not the pi zero w for this. Use the zero for a pwnagotchi instead.

Tak - September 13, 2020, 4:42 pm

(Sep 13, 2020 04:39 PM)Mr. Robot Wrote: [\[CITE\]](#) For this in particular, I would say not the pi zero w for this. Use the zero for a pwnagotchi instead.

Any reason in particular? [THIS ARTICLE](#) talks about how he used the Zero W, so I am just curious as to the differences.

Mr. Robot - September 13, 2020, 4:47 pm

(Sep 13, 2020 04:42 PM)Tak Wrote: [\[CITE\]](#) Any reason in particular? [THIS ARTICLE](#) talks about how he used the Zero W, so I am just curious as to the differences.

I don't get what you mean? That's exactly what I said - use the Zero for a pwnagotchi - but don't use this tutorial for the Zero. Use this tutorial for a laptop or a standard Raspberry pi.

The pwnagotchi will actively deauth networks to get handshakes and still passively get pmkids - this method is PMKID only and allows for high speed movement to collect pmkids.

Bri4n0ps - September 14, 2020, 11:14 am

Thanks for the post, I've been trying to get aircrack, etc working on my raspi, but no luck so far - I'll have to reference this thread when I'm ready to try again

Mr. Robot - September 15, 2020, 12:04 pm

(Sep 14, 2020 11:14 AM)Bri4n0ps Wrote: [\[CITE\]](#) Thanks for the post, I've been trying to get aircrack, etc working on my raspi, but no luck so far - I'll have to reference this thread when I'm ready to try again

Absolutely, let me know how you go!

pipito - September 17, 2020, 5:35 pm

Wow, great tutorial, buddy. I may try, lately with this contingency I have been very bored at home and I am interested in acquiring hacker skills. xD Thanks for sharing.

LilPeepGBC - September 22, 2020, 6:50 pm

Nice bro! Love it. Gonna start with your tutorial

Chiffon - September 25, 2020, 1:49 pm

First time I see such a clear and precise tutorial!

Raikou - September 26, 2020, 3:34 pm

Hey I really want to try this out I have basically 0 experience (I can load up kali on a usb thats about it)

but what Wireless adapter do you recommend from amazon.de. thanks for your time.

pidgepodge - October 23, 2020, 2:55 pm

How would the hash cracking method work with the increasingly complex passwords that are default on many modern routers. For example, upper and lower case and numbers - 10 characters would be 62^{10} options. I can't see how - even with distributed hashing power - this will ever be attainable.

Mr. Robot - October 23, 2020, 11:41 pm

(Oct 23, 2020 02:55 PM)pidgepodge Wrote: [\[CITE\]](#) How would the hash cracking method work with the increasingly complex passwords that are default on many modern routers. For example, upper and lower case and numbers - 10 characters would be 62^{10} options. I can't see how - even with distributed hashing power - this will ever be attainable.

Most routers use a keyset or methodology and you can start cutting down on potentials based on it.

Under the assumption, that the router is 10 long with upper/lower/number - We can put in parameters such as max reoccurring and max consecutive. Again, analyzing other routers of the same model - being sold on the marketplace, we can start to analyze and speed up attempts. Sure it's wont take it down to 100% as it 'could' fit one of the patterns we take out.

Take a look at "10hex" for example.

<https://github.com/wpatoolkit/10-Hex-Generator>

100% with distributed hashing power it's possible, I don't know where you get that from.

permutate - October 26, 2020, 1:36 pm

Great write up!

Looking forward to trying this out in the future.

Tyler Durden. - November 22, 2020, 3:30 pm

Hi man,

I love your tutorial and have been following it closely step by step, and even tried finding the solution to my problem on my own, however with no luck!

It seems that HCXTOOLS from ZerBea / <https://github.com/ZerBea/hcxtools.git> - does not include the "hcxpcaptool" command anymore.

It does include a similar one, called, "hxcpcapngtool" - however, it cannot (by my knowledge) be used in the same matter as the previous one.

Is there any guidance you can give me to this, as I really am a beginner in Linux systems.

Your help would be extremely appreciated!

Thanks

EDIT:

I kept trying, and did my best with the "hxcpcapNGtool", with the following command:
hxcpcapngtool -E essidlist -I identitylist -U usernamelist -o yourcitynameoutputs.16800
yourcityname.pcapng

Which was basically perfectly similar to your command, but with the "-o" instead of "-z" before the "yourcitynameoutputs...".

I think it worked, and it left me with a: "yourcitynameoutputs.16800" file.

However the "raw" text/data in the file looks like this:

Spoiler ([Click to View](#))

So I am still not completely sure that it is, as it should be.

Once again, can I ask you - does it look to be correct, or no?

Thank you :)

CrystalFlare - November 23, 2020, 4:42 am

Thanks for sharing, very powerful stuff

Mr. Robot - November 23, 2020, 4:43 am

(Nov 22, 2020 04:30 PM)Tyler Durden. Wrote: [\[CITE\]](#) Hi man,

I love your tutorial and have been following it closely step by step, and even tried finding the solution to my problem on my own, however with no luck!

It seems that HCXTOOLS from ZerBea / <https://github.com/ZerBea/hcxtools.git> - does not include the "hcxpcaptool" command anymore.

It does include a similar one, called, "hcxpcapngtool" - however, it cannot (by my knowledge) be used in the same matter as the previous one.

Is there any guidance you can give me to this, as I really am a beginner in Linux systems.

Your help would be extremely appreciated!

Thanks

EDIT:

I kept trying, and did my best with the "hcxpcapNGtool", with the following command:
hcxpcapngtool -E ssidlist -I identitylist -U usernamelist -o yourcitynameoutputs.16800
yourcityname.pcapng

Which was basically perfectly similar to your command, but with the "-o" instead of "-z" before the "yourcitynameoutputs...".

I think it worked, and it left me with a "yourcitynameoutputs.16800" file.

However the "raw" text/data in the file looks like this:

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

So I am still not completely sure that it is, as it should be.

Once again, can I ask you - does it look to be correct, or no?

Thank you :)

It certainly looks right and it seems yes they have updated the code - I did write up somewhere an easier way of doing my tutorial I'll try find it.

From a fresh boot of Kali Linux

Code 1. sudo apt-get update

1a. sudo apt-get install libpcap-dev libcurl4-openssl-dev libssl-dev

2. sudo apt install hcxtools

3. cd Desktop/

4. airmon-ng check kill

5. hcxdumpool -o yourcityname.pcapng -i wlan0 --enable_status 1

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

Tyler Durden. - November 23, 2020, 12:19 pm

(Nov 23, 2020 05:43 AM)Mr. Robot Wrote: [\[CITE\]](#) It certainly looks right and it seems yes they have updated the code - I did write up somewhere an easier way of doing my tutorial I'll try find it.

From a fresh boot of Kali Linux

Code 1. sudo apt-get update

1a. sudo apt-get install libpcap-dev libcurl4-openssl-dev libssl-dev

2. sudo apt install hcxtools

3. cd Desktop/

4. airmon-ng check kill

5. hcxdumptool -o yourcityname.pcapng -i wlan0 --enable_status 1

6. hcxpcaptool -E essidlist -I identitylist -U usernamelist -z yourcitynameoutputs.16800
yourcityname.pcapng

Damn.

I spent around 5 hours last night trying to figure it out, cloning, re-installing, and god knows how many tutorials.

I did a new USB live boot, followed those instructions and hcxpcaptool was there and worked flawlessly!

Thank you a lot - you really saved a lot of my time.

However, while we are talking. I have a question, regarding the 5th command, where it 'finds' the wireless networks.

I have been doing this for educational purposes in my apartment, and the person living under me, has got a very strong (87%) wireless network from my place.

Although, his network does not show up on the 'list' - is there any particular reason for this, different type of encryption or?

I am just asking because I am very curious as to why I can find every other network, but the one that is closest to me seems hidden.

Thank you!

Hustleblvrdr - December 6, 2020, 11:10 pm

so cool ? love hq posts like this that don't require a PM

Mr. Robot - December 6, 2020, 11:12 pm

(Dec 7, 2020 12:10 AM)Hustleblvrdr Wrote: [\[CITE\]](#) so cool ? love hq posts like this that don't require a PM

I can pop it on a new thread with the updated easier method of achieving it in just a few.

7 - December 6, 2020, 11:14 pm

(Dec 7, 2020 12:12 AM)Mr. Robot Wrote: [\[CITE\]](#) I can pop it on a new thread with the updated easier method of achieving it in just a few.

Oh what a good kiwi ;) <3 much luv

Look forward to the updated method.

Mr. Robot - December 6, 2020, 11:23 pm

(Dec 7, 2020 12:14 AM)NulldB Wrote: [\[CITE\]](#) Oh what a good kiwi ;) <3 much luv

Look forward to the updated method.

It's more or less the same, just more streamlined:

<https://hackforums.net/showthread.php?tid=6125936>