

Forum:[Hack Forums](#)

Thread: [Hack your town\(city\) - Tutorial \(in progress\)](#)

Mr. Robot - December 11, 2016, 11:22 am

This is a tutorial in progress which will use tools such as

WiFi wardriving - map your town and who owns what network using google maps and a simple walk/drive.

<https://play.google.com/store/apps/details?id=net.wigle.wigleandroid>

Attacking WPS enabled networks - we will discuss pixie-wps too and how it can obtain the wireless password in under 10 seconds in certain circumstances.

<http://tools.kali.org/wireless-attacks/reaver>

Automated Cracking Wpa2 networks
tools.kali.org/wireless-attacks/wifite

Instant hacking thomson routers and a few others.

<https://play.google.com/store/apps/details?id=io.github.routerkeygen&hl=en>

Using long range antenna (directional and parabolic) to crack those networks from home.

www.wirelesshack.org/long-range-wifi-antenna.html

Using hashcat to crack the wpa2 handshakes(files containing the keyphrase)

<https://hashcat.net/>

[https://forums.kali.org/showthread.php?18261-Cracking-WPA-key-with-crunch-aircrack-\(almost-fullproof-but-how-speed-things-up\)](https://forums.kali.org/showthread.php?18261-Cracking-WPA-key-with-crunch-aircrack-(almost-fullproof-but-how-speed-things-up))

Becoming Man in The Middle (MiTM) on their network to intercept packets such as images, passwords and browsing sessions.

<https://github.com/Subterfuge-Framework/Subterfuge>

<https://ettercap.github.io/ettercap/>

www.ex-parrot.com/~chris/driftnet/

<https://www.zimperium.com/zanti-mobile-penetration-testing>

Exploiting browsers using BeEF (browser exploitation framework) and Setoolkit for fake pages the clients will access.

beefproject.com/

<https://www.trustedsec.com/social-engineer-toolkit/>

Infecting the network with a RAT and spreading that RAT via the LAN(local area network) to other machines

<https://github.com/gentilkiwi/mimikatz>

<https://technet.microsoft.com/en-us/sysinternals/pxexec.aspx>

Using the above mimikatz, we will also grab other saved passwords from their machines including other WiFi network passwords they have saved.

We will also cover some equipment such as using a device using Nethunter (nexus or one plus phone required). Raspberry pis, WiFi pineapples and more

<https://www.kali.org/kali-linux-nethunter/>

<https://www.raspberrypi.org/>

<https://hakshop.com/products/wifi-pineapple>

Last but not least, we will also cover creating infected document files to drop on USB sticks for town infection, and creating USB sticks that are HID keyboard emulators such as the rubber ducky.

<https://hakshop.com/products/usb-rubber-ducky-deluxe>

Hacking the locals who own businesses can be great money at times if they approve of the security check - You can try use things such as leakedsource to find passwords by entering @theirbusiness or @yourtown or @theirwebsite and clicking the wildcard button. This will show all the emails that have those keywords in which means you are on target.

<http://leakedsource.com/>

If you would like to stay subscribed to this thread for when it is complete, please click the subscribe button at the bottom.

If you would like to help me with making this tutorial as complete as possible and feel you can contribute to the discussion, please post below or PM me and we can work on it as a community.

SirNoobHack - December 11, 2016, 11:25 am

Good practical skills to know, will stay tuned.

Mr. Robot - December 11, 2016, 11:30 am

(Dec 11, 2016 12:25 PM)SirNoobHack Wrote: [\[CITE\]](#) Good practical skills to know, will stay tuned.

Hopefully I can find the time and energy to put all of it up, but might take a while. For now I will just work on it locally and put it through when it's done but at least these links should aid those who are interested in doing their own research.

the wolf of blockchain - December 11, 2016, 11:35 am

posting here to come back to

Drug Problems - December 11, 2016, 11:36 am

This thread is going to be massive. Good luck putting it all together Mr. Robot. Looks really interesting and I can't wait to see the completed thread.

ze-slade - December 11, 2016, 11:37 am

Interesting tutorial so far, good luck Mr. Robot!

Toby Flenderson - December 11, 2016, 11:40 am

Can't wait to see the end result, thank you Mr. Robot!

Mr. Robot - December 11, 2016, 11:40 am

(Dec 11, 2016 12:36 PM)Drug Problems Wrote: [\[CITE\]](#) This thread is going to be massive. Good luck putting it all together Mr. Robot. Looks really interesting and I can't wait to see the completed thread.

Yeah it's going to take a while but it's been a while since I put out any tutorials of my own - I usually just PM people or post on their threads.

(Dec 11, 2016 12:37 PM)ze-slade Wrote: [\[CITE\]](#) Interesting tutorial so far, good luck Mr. Robot! Hopefully it will save a lot of troubles with users asking the questions we ask - that's why I would like to get a little team going on discord to help with it, as one thing we might take for granted, another might not understand.

JavaDriveBy - December 11, 2016, 11:41 am

Posting to comeback later.

warbarz - December 11, 2016, 11:41 am

subscribed :) I would recommend also

<http://hackaday.com/2016/11/16/poinsontap-makes-raspberry-pi-zero-exploit-locked-computers/>

lusr - December 11, 2016, 11:42 am

This is great! Of course I subscribe and if you need help, I will be glad to help you!

I also thought that this can be helpful. I found this some time ago (maybe here on HF?) and show all the password of airports:

https://www.google.com/maps/d/viewer?mid=1Z1dl8hoBZSJNWFx2xr_MMxSxSxY&ll=-3.81666561775622e-14%2C39.739915100000076&z=1

Mr. Robot - December 11, 2016, 11:42 am

(Dec 11, 2016 12:41 PM)warbarz Wrote: [\[CITE\]](#) subscribed :) I would recommend also

<http://hackaday.com/2016/11/16/poinsontap-makes-raspberry-pi-zero-exploit-locked-computers/>

While handy and a great tool, it might be included. If we include that, we might as well include the lan turtle mimikatz method of grabbing passwords from a locked computer.

fannas1 - December 11, 2016, 11:43 am

Posting here to come back. Thank you Mr. Robot

Mr. Robot - December 11, 2016, 11:43 am

(Dec 11, 2016 12:42 PM)gabr Wrote: [\[CITE\]](#) This is great! Of course I subscribe and if you need help, I will be glad to help you!

I also thought that this can be helpful. I found this some time ago (maybe here on HF?) and show all the password of airports:

https://www.google.com/maps/d/viewer?mid=1Z1dl8hoBZSJNWFx2xr_MMxSxSxY&ll=-3.81666561775622e-14%2C39.739915100000076&z=1

Completely forgot about that and I appreciate you for putting it forward. This is why I would like to get a group together and have posted this now while I work on it as it allows the community to add their knowledge.

Hopefully this will be a thread to remember and refer back to once complete with a lot of resources.

ze-slade - December 11, 2016, 11:48 am

(Dec 11, 2016 12:40 PM)Mr. Robot Wrote: [\[CITE\]](#) Hopefully it will save a lot of troubles with users asking the questions we ask - that's why I would like to get a little team going on discord to help with it, as one thing we might take for granted, another might not understand.

Hopefully, it will, but most new users just make a new thread, either way. At least that's what happened with the rat section regardless of all the tutorials. It did bring down the amount of the threads by a little though so, this SHOULD help with any of those threads in here too.

xx 0x0 xx - December 11, 2016, 12:23 pm

subscribed this is crazy thing to do i like that you always come with amazing things bro

lyrant - December 12, 2016, 10:23 am

Great post very useful information

Renestey - December 12, 2016, 12:32 pm

Subscribed, so far seems very promising and can't wait to see this come together, what do you think about mapping via drone?

Shaq - December 12, 2016, 1:25 pm

Subscribed as well, I'm excited to see how this goes and maybe help out where possible.

Not Your Average Orange - December 12, 2016, 2:57 pm

Pretty cool, but I can't find the subscribe button, do I have to be upgraded?

Edit: Nevermind, found it, it's at the very end of the thread. (And you do have to be upgraded)

deltaxflux - December 13, 2016, 7:02 am

I recommend to replace zanti with csploit

Mr. Robot - December 13, 2016, 7:06 am

(Dec 13, 2016 08:02 AM)deltaxflux Wrote: [\[CITE\]](#) I recommend to replace zanti with csploit
I disagree entirely.

OctoberzVeryOwn - December 13, 2016, 8:44 am

Posting to come back to this!

BlackSwN - December 14, 2016, 7:20 am

Posting here to come back. Thank you Mr. Robot

THC - December 14, 2016, 7:22 am

An interesting addition to this thread would be a section detailing how to find vulnerable devices running in your area.

This can be accomplished by using a web spider such as shodan.io and then filtering it for local results, based on your city or state.

Modern day Hippy - December 14, 2016, 7:23 am

such a great thread as always from Mr. Robot.

Ty for this guide

Mr. Robot - December 14, 2016, 8:11 am

(Dec 14, 2016 08:22 AM)M.D. Wrote: [\[CITE\]](#) An interesting addition to this thread would be a section detailing how to find vulnerable devices running in your area.

This can be accomplished by using a web spider such as shodan.io and then filtering it for local results, based on your city or state.

There will only ever be 1 or two devices on average that you wont be able to not find vulnerabilities for.

TheChi?f - December 14, 2016, 8:33 am

Subscribed to this. Will read back in a few.

?ane - December 14, 2016, 8:35 am

Subscribed to this, thanks for the well thought out tutorial Mr.Robot!

yorickx - December 14, 2016, 9:06 am

Good luck making this tutorial, cant wait for it

THC - December 14, 2016, 9:28 am

(Dec 14, 2016 09:11 AM)Mr. Robot Wrote: [\[CITE\]](#) There will only ever be 1 or two devices on average that you wont be able to not find vulnerabilities for.

But regardless it's sometimes fun to do from home

Billie Joe - December 15, 2016, 6:12 pm

im glad you are not in my city because you are being a nuisance doing this

gilles - December 16, 2016, 9:18 am

Posting to come back here, looks good so far good luck OP !

Cryptic5 - December 17, 2016, 2:33 am

Posting here to get back to! This looks very interesting

Mad76e - December 18, 2016, 7:57 am

(Dec 11, 2016 12:22 PM)Mr. Robot Wrote: [\[CITE\]](#) snip

How is it going mr.robot? need any help?

Mr. Robot - December 18, 2016, 12:26 pm

(Dec 18, 2016 08:57 AM)Mad76e Wrote: [\[CITE\]](#) How is it going mr.robot? need any help?

For the most part it's good, looking at a January release.

???? - December 18, 2016, 3:28 pm

keep doing this sir it is v interesting

but how do learn all of these? add perhaps a video tutorial and article or 2 per step sir

also what devices do need for this?

am need like a linux laptop or a blueberry pi maybe?

mrjokacly - December 19, 2016, 8:48 am

keep up the good work and have fun putting all of them them together

Papa Cuda - December 19, 2016, 8:48 am

Posting to come back. Nice thread Mr. Robot, and congrats on ub3r.

str0wn3dlt - December 19, 2016, 10:50 am

Keep doing this

Posting there to come back later, definety gonna use this :)

????Kosdff - December 19, 2016, 10:51 am

Posted here again for updates :3

xdavididhu - December 19, 2016, 12:10 pm

Looking forward for the full tutorial, nice work!

Mi2414 - December 19, 2016, 12:14 pm

Nice collection of resources, wish there were alternatives to some of the android apps for iOS but probably not unless you are jail broken.

egyy - December 19, 2016, 12:24 pm

Super dope tutorial so far. Nice work!

???? - December 19, 2016, 12:27 pm

(Dec 18, 2016 04:28 PM)Scorpi0n Wrote: [\[CITE\]](#) keep doing this sir it is v interesting

but how do learn all of these? add perhaps a video tutorial and article or 2 per step sir

also what devices do need for this?

am need like a linux laptop or a blueberry pi maybe?
ansir

Furorem - December 19, 2016, 12:44 pm

Dear Mr. Robot

Please can you go back to the Hollywood and make bunch of new episodes for us? i will beg you. I have thinkd twice to go an Detox cause this situation is akward and i feel like i can end my life.

Btw, damn nice kit.
Spoiler [\(Click to View\)](#)

Blake- - December 19, 2016, 10:52 pm

I really like this one. Posting to come back for updates. :)

quirky - December 23, 2016, 12:35 am

IMHO you missed the best tool for wardriving . talking about bedside-ng :) tweaking the atheros chipset with fcsfail monitor, you get handshakes in no time :)

Star-Lord - December 28, 2016, 7:20 am

Posting to come back for updates.

moorbes - December 28, 2016, 8:42 am

Posting so I can keep track of this :)

Le Anonimo - December 28, 2016, 10:28 am

Wanna work with you on these topics please PM me with you s.k.y.p.e. handle .. I am for your positive reply hope you will caught me soon

Kodaz - February 3, 2017, 3:44 pm

Really interested to see this thread finished... Has a few things I haven't used before.

JELLY?IsH - February 5, 2017, 11:42 am

This is amazing. I hope you continue with adding more info here.

Mr. Robot - February 5, 2017, 12:08 pm

(Feb 5, 2017 12:42 PM)whiteSEC Wrote: [\[CITE\]](#) This is amazing. I hope you continue with adding more info here.

I will be, looking for some micro tutorials made by other members to assist otherwise we are looking at the end of this month for release.

Wifi Pineapple - February 5, 2017, 12:25 pm

Mr. Robot' pid='54020979' dateline='1486325285']

I will be, looking for some micro tutorials made by other members to assist otherwise we are looking at the end of this month for release.

[/quote]

You should change wifite to something that doesn't say automated. When I read automated, I think you type a few words and then you leave it alone - you're thinking of beside-ng - where wifite actually needs the user input.

beside-ng you just type that plus the interface and it finds, deauths, and saves cap file by itself as well as finding new APs if you move to far from range

:) enjoy

Edit: Forgot to add that it's a really good tutorial. I've read it and linked it to people numerous times.