

Forum:[Hack Forums](#)

Thread: [CHALLENGE: with all network info, collect network traffic](#)

redax2882 - June 14, 2017, 6:55 pm

I have the TARGET's Wifi name, MAC address, Wi-Fi password, etc.

...but I am several miles away and on a different network.

Can I add the TARGET to my Wireshark to collect their packets remotely?

deltaxflux - June 14, 2017, 9:43 pm

(Jun 14, 2017 06:55 PM)redax2882 Wrote: [\[CITE\]](#) I have the TARGET's Wifi name, MAC address, Wi-Fi password, etc.

...but I am several miles away and on a different network.

Can I add the TARGET to my Wireshark to collect their packets remotely?

Bring your card in monitor mode and listen carefully. Deauth your targets and look in wireshark for the eapol protokoll

pomwtin - June 15, 2017, 4:09 am

Go to his location, get into router panel and if router supports setting up VPN then simply set up one you are running. Then you'll be able to monitor traffic from location far away

Rotely - June 15, 2017, 9:12 am

try to go to location and try

provider - June 16, 2017, 5:40 am

(Jun 15, 2017 04:09 AM)pomwtin Wrote: [\[CITE\]](#) Go to his location, get into router panel and if router supports setting up VPN then simply set up one you are running. Then you'll be able to monitor traffic from location far away
good idea

redax2882 - June 29, 2017, 10:54 am

(Jun 16, 2017 05:40 AM)provider Wrote: [\[CITE\]](#) I can go to the location and get into the router (easy). I also have a TorGuard subscription. How do I redirect traffic using that?

good idea

Mr. Robot - June 29, 2017, 10:59 am

(Jun 15, 2017 04:09 AM)pomwtin Wrote: [\[CITE\]](#) Go to his location, get into router panel and if router supports setting up VPN then simply set up one you are running. Then you'll be able to monitor traffic from location far away
I'd have to say you are almost correct.

It'd be better if the router supports VPN to setup a VPN on your own machine/network and route it through rather than sharing the same VPN service that you would pay for or use freely.

The overall best way to do this would be:

You have:
Wifi name, MAC address, Wi-Fi password.

zANTI on a mobile device (man in the middle attack) which will collect all http passwords/images/urls

Use 2 battery packs, occasionally go over and swap over the pack while the other is charging.

Or if they use LAN/ETHERNET you could use a LANturtle:

<https://hakshop.com/products/lan-turtle>

Plug it into their machine, ethernet into the turtle. Remote shell and access to the PC/network.

OR a pineapple:

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

Same as zANTI more or less.

OR if you have access to their PC for a few seconds, you can use a USB rubber ducky which will work like a keyboard and type really fast to execute code/scripts:

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

(you can also build one for only \$3 or so using an arduino micro, I have a thread on it if you need it)

Video

redax2882 - June 29, 2017, 12:32 pm

(Jun 29, 2017 10:59 AM)Mr. Robot Wrote: [\[CITE\]](#) The overall best way to do this would be:

You have:

Wifi name, MAC address, Wi-Fi password.

OR a pineapple:

Same as zANTI more or less.

This looks to be the best route... With the pineapple, can I basically leave it on the property and then collect it a day or two later? Then I would decipher the packets?

Mr. Robot - June 29, 2017, 1:26 pm

(Jun 29, 2017 12:32 PM)redax2882 Wrote: [\[CITE\]](#) This looks to be the best route... With the pineapple, can I basically leave it on the property and then collect it a day or two later? Then I would decipher the packets?

Packets would already be "deciphered" as you say with login information and other shit.

redax2882 - June 29, 2017, 1:29 pm

(Jun 29, 2017 01:26 PM)Mr. Robot Wrote: [\[CITE\]](#) Packets would already be "deciphered" as you say with login information and other shit.

If I have access to the LAN, is there a way to collect (for example) passwords without waiting for them to be used live?

Mr. Robot - June 29, 2017, 1:37 pm

(Jun 29, 2017 01:29 PM)redax2882 Wrote: [\[CITE\]](#) If I have access to the LAN, is there a way to collect (for example) passwords without waiting for them to be used live?

You can recover what's already on the PC but anything else you would need to wait.

redax2882 - June 29, 2017, 4:17 pm

(Jun 29, 2017 01:37 PM)Mr. Robot Wrote: [\[CITE\]](#) You can recover what's already on the PC but anything else you would need to wait.
If it's a Mac, what's the best to do recover what's already on it with only having access through the LAN?