

Forum:[Hack Forums](#)

Thread: [Tutorial SSHStrip MITM Attack](#)

StreetSquirrel - December 22, 2018, 2:12 am

For those of you who don't know ssl stripping is a technique used to downgrade https into http. Https unlike http uses an SSL (secure Socket Layer) to transfer data. We will rip the S away so we are able to manipulate and intercept data, which is called a man in the middle attack (MITM)

For this tutorial we will need Kali Linux with a chip set that supports monitor mode. Promiscuous mode if you are on a wired connection.

If these modes aren't supported, a WiFi adapter will do fine.

<https://null-byte.wonderhowto.com/how-to/buy-best-wireless-network-adapter-for-wi-fi-hacking-2018-0178550/>

Now we begin.

Boot into Kali and open a terminal. We will change to the home directory and install our script, easy-creds. Type the following commands.

Code \$ cd ~

\$ git clone https://github.com/brav0hax/easy-creds.git

Now we can navigate to the easy-creds folder and change the executable permission and run the installer. Type the following commands.

Code \$ cd easy-creds

\$ sudo chmod +x installer.sh

\$ sudo ./installer.sh

The script will ask what OS we are on.

Code Please choose your OS to install easy-creds

1. Debian/Ubuntu and derivatives
2. Red Hat or Fedora
3. Microsoft Windows
4. Exit

Choice:

Choose Debian/Ubuntu and press enter. It will ask for the path you'd like to install easy-creds in. Just use /opt for now.

easy-creds will now begin to install all the dependencies.

If there is an error, unable to install libs. Don't worry, this is typical. As long as one of them installs correctly you're good to go.

Now we will run our script. Type in easy-creds and hit enter. You should now be looking at a menu.

Code 1. Prerequisites & Configurations

2. Poisoning Attacks

3. FakeAP Attacks

4. Data Review

5. Exit

q. Quit current poisoning session

Choice:

Select FakeAP Attacks. After that choose FakeAP Attack Static.

Now you click no for sidejacking attack.

Code Interface connected to the internet (ex. eth0):

^Since I'm using WiFi I will enter my interface as wlan0. This may vary for you.

You will be greeted with this.

Code PHY Interface Driver Chipset

phy0 wlan0 iwlwifi Intel Corporation Dual Band Wireless-AC 3168NGW [Stone Peak] (rev 10)

Wireless interface name (ex. wlan0):

^Now we will enter our interface name. Again, mine is wlan0.

Code ESSID you would like your rogue AP to be called, example FreeWiFi:

^ This is asking what you want to name your fake hot spot. The name should be convincing so that people actually join.

Now we will be broadcasting on channel 11. So type that in and hit enter.

Code Your interface has now been placed in Monitor Mode

phy0 wlan0mon iwlwifi Intel Corporation Dual Band Wireless

^Your interface should now be in monitor or promiscuous mode. You will now enter the name of your new interface. Mine is wlan0mon.

The next step is up to you. There is no need to change the MAC address for me so I'm going to select no.

Now we are going to choose a tunnel interface name. We are just going to choose at0. Type at0 and press enter.

We do not have a dhcpd.conf file to use. Press no and enter.

Code Network range for your tunneled interface, example 10.0.0.0/24:

If you haven't noticed by now we have used a lot of the default settings. The same applies here, 10.0.0.0/24 and then press enter.

Code Enter the IP address for the DNS server, example 8.8.8.8:

Once again, we will be using 8.8.8.8, after you press enter 5 windows should pop up. From here you should be able to see who joins your fake hot spot, what they are searching, and the passwords they enter. All in plain text.

I hope you guys enjoyed this tutorial and have some success. I've been on the rode for 5 days now, this works pretty good at the hotels.

Let me know if you see any mistakes or have some ideas:)

sh4moon - December 22, 2018, 6:46 am

good tutorial. this can also be a rogue access point attack. you would just have to clone the target access point and deauth clients. people who write tutorials don't get enough credit.

Sitrep - December 22, 2018, 5:25 pm

Great tutorial, you explained it really good and the overall layout of the tutorial was easy to read. Great job!

I'll try this out as soon as I have time :)

StreetSquirrel - December 23, 2018, 8:33 am

(Dec 22, 2018 06:25 PM)Sitrep Wrote: [\[CITE\]](#) Great tutorial, you explained it really good and the overall layout of the tutorial was easy to read. Great job!

I'll try this out as soon as I have time :)

Good luck!

charon112 - December 27, 2018, 7:23 pm

Well i tried it, and it was amazing! It worked really well

StreetSquirrel - December 28, 2018, 12:14 am

(Dec 27, 2018 08:23 PM)charon112 Wrote: [\[CITE\]](#) Well i tried it, and it was amazing! It worked really well

I'm glad for you bro!

CheckMyNuts - December 28, 2018, 11:55 am

Nice tutorial, just need WiFi adapter for my virtual machine

StreetSquirrel - December 28, 2018, 12:17 pm

(Dec 28, 2018 12:55 PM)reksai33 Wrote: [\[CITE\]](#) Nice tutorial, just need WiFi adapter for my virtual machine

I just use live usb

CheckMyNuts - December 28, 2018, 12:21 pm

(Dec 28, 2018 01:17 PM)StreetSquirrel Wrote: [\[CITE\]](#) I just use live usb

You have kali Linux on live usb? so you can do it directly, right?

StreetSquirrel - December 28, 2018, 12:29 pm

(Dec 28, 2018 01:21 PM)reksai33 Wrote: [\[CITE\]](#) You have kali Linux on live usb? so you can do it directly, right?

Yup yup

CheckMyNuts - December 28, 2018, 12:30 pm

(Dec 28, 2018 01:29 PM)StreetSquirrel Wrote: [\[CITE\]](#) Yup yup

Thanks mate

saisrujan - December 30, 2018, 10:19 pm

Great Tutorial

I appreciate your effort

StreetSquirrel - December 30, 2018, 10:36 pm

(Dec 30, 2018 11:19 PM)saisrujan Wrote: [\[CITE\]](#) Great Tutorial

I appreciate your effort

:)

darkdoctor - January 2, 2019, 2:46 pm

Can you make a video tutorial please?

StreetSquirrel - January 2, 2019, 3:16 pm

(Jan 2, 2019 03:46 PM)darkdoctor Wrote: [\[CITE\]](#) Can you make a video tutorial please?

I wish, you cant figure it out?