

Forum: [Hack Forums](#)

Thread: [Simple Man in the middle attack on windows.](#)

Mr. Robot - December 22, 2016, 12:21 pm

So very simple and basic MiTM attack on windows.

Download

www.winpcap.org/install/

Download

<http://nighthawk.software.informer.com/download/?ca8e7c2>

(you can compile it yourself from the github)

Download

<https://sourceforge.net/projects/etherwatch/>

NightHawk - simple man in the middle with arpspoof for windows, similar to cain and abel but easier to use and navigate. Shows http logins. Doesn't re-arp itself from what I can see which can cause internet to stop after 10 minutes or so.

Winpcap - is the driver/file you need to allow your card to do this kind of activity.

Etherwatch - for monitoring images traveling through your network.

After installing winpcap drivers, we can go ahead and open up nighthawk and choose the adapter connected to the internet at the top and choose advanced mode.

Then we want to hit Scan Network to find the IPs of machines on your LAN.

Once we have decided which computer/phone/device we want to intercept, we click the ipv4 address of it in the "Target 1 box" and in the "Target 2 box" we want to choose your router/gateway IP. To find this we can open up CMD and type in ipconfig -

Once we have chosen the gateway and the target, we can hit "Start Sniffer" and "Start ARP spoofing"

Next we can click on the "Sniffer" tab at the top and wait for any http login forms.

On the device you are intercepting, you can go to <http://aavtrain.com/> and type in a username and password, and it will show up in the sniffer tab on your PC.

- One issue with etherwatch is loading sites such as imgur.com with https will crash it.
If that is all working and you are now MiTM you can open up etherwatch - Install it and run it.

Once open, choose your network card and it will start monitoring everything that happens through your adapter - which will mean the MiTM you have running will collect the images too.

With etherwatch you can move images around and WARNING: Potential SPAM or INFECTED LINK the IP or to only monitor images from that IP.

ze-slade - December 22, 2016, 12:23 pm

Looks like a pretty good tutorial, It's tempting to try this out. I never got into mitm attacks, but I always wanted to try one.

Mr. Robot - December 22, 2016, 12:25 pm

(Dec 22, 2016 01:23 PM)ze-slade Wrote: [\[CITE\]](#) Looks like a pretty good tutorial, It's tempting to try this out. I never got into mitm attacks, but I always wanted to try one.

This is a very basic one and wasn't going to put it up as the same can be accomplished with say cain and abel.

The main purpose it to show it can be done, while not as stable as running one on linux - it can be achieved and I will be hopefully working with other users in 2017 to make a completed tool that works 10x faster and better.

These tools are quite outdated and were never really complete so that's unfortunate as I think MiTM attacks are one of the best tools for network infiltration and monitoring.

Megabear - December 22, 2016, 12:26 pm

Woah.

This is dope Robot.

=)

I am gonna try this out soon on my windows.

Thanks for helping the community out. :)

ze-slade - December 22, 2016, 12:27 pm

(Dec 22, 2016 01:25 PM)Mr. Robot Wrote: [\[CITE\]](#) This is a very basic one and wasn't going to put it up as the same can be accomplished with say cain and abel.

The main purpose it to show it can be done, while not as stable as running one on linux - it can be achieved and I will be hopefully working with other users in 2017 to make a completed tool that works 10x faster and better.

These tools are quite outdated and were never really complete so that's unfortunate as I think MiTM attacks are one of the best tools for network infiltration and monitoring. Interesting, that's great to hear you'll be working on a better tool, are you planning on selling it or making it free?

fannas1 - December 22, 2016, 12:28 pm

Posting to come back and try this tutorial out. Thank you OP very interested in this.

ZuGgY - December 22, 2016, 12:29 pm

Thanks for this wonderful tutorial as always!

Mr. Robot - December 22, 2016, 12:30 pm

(Dec 22, 2016 01:27 PM)ze-slade Wrote: [\[CITE\]](#) Interesting, that's great to hear you'll be working on a better tool, are you planning on selling it or making it free?

I had plans on selling it for reasonably cheap maybe \$5-\$20 for a fully working one with modules for code injection and fun scripts similar to what zANTI runs (replacing downloads, flipping images, replacing images)

ze-slade - December 22, 2016, 12:32 pm

(Dec 22, 2016 01:30 PM)Mr. Robot Wrote: [\[CITE\]](#) I had plans on selling it for reasonably cheap maybe \$5-\$20 for a fully working one with modules for code injection and fun scripts similar to what zANTI runs (replacing downloads, flipping images, replacing images)

Makes sense, good luck with your project and any future ones to come!

Mr. Robot - December 22, 2016, 1:37 pm

Would appreciate for people to try this out and post back results.

DatNigguh - December 22, 2016, 7:20 pm

I plan on it in a week or so buddy, thanks for the tutorial and I'd be interested in purchasing a solid tool from ya!

Mr. Robot - June 8, 2018, 5:28 am

(Dec 22, 2016 08:20 PM)DatNigguh Wrote: [\[CITE\]](#) I plan on it in a week or so buddy, thanks for the tutorial and I'd be interested in purchasing a solid tool from ya!

Not a problem, still working on this tool years later. No help and no clue as to what I am doing. Learning as I go.

Aries Devil - June 10, 2018, 6:46 am

nice tut man...keep it up

actual155 - June 22, 2018, 5:50 pm

Nice Tutorial it seems very useful for monitoring other people who shouldn't be on my network

Bossbitch24 - June 22, 2018, 6:12 pm

Looking for a legit spammer that have bank logs

sapalapa - June 27, 2018, 11:59 pm

Do you know why it did not list the Ip of my router(Default Gateway), at Target2 text field?