

Forum:[Hack Forums](#)

Thread: [Influence | Using MiTMf | MiTM, DNS & ARP Spoofing](#)

SysAdmin - February 10, 2018, 4:05 pm

Welcome to the MiTMf tutorial. In this post, I will explain how to use Man-in-The-Middle Framework on Linux to conduct DNS and ARP Spoofing

Introduction

First of all, we need to acquire MiTMf. You will also need to do this if you are running Kali, as it does not come pre-installed. To do this, we run the command;

Code apt-get install mitmf

Once the package installs, it can simply be run by using the command;

Code mitmf

You are greeted with a usage wall of text, there are a ton of options which you should look and play through once you get this package. It is a powerful tool, so use it wisely. We are going to be using the following options in our attack;

Code --spooft - Loads plugin spoof

--arp - Redirects traffic using ARP Spoofing

--gateway - Specifies gateway IP

--targets - Specifies hosts to poison

--dns Proxy/Modifies DNS Queries

-i The interface you would like the spoof to run on

These are the standard options, there are a ton more that will help you out with different situations, such as --hsts, that will partially help you to bypass HSTS and --inject, which allows you to inject JavaScript or HTML code.

The Attack

Let's get our hands dirty. I will be using my Kali Laptop (Running on 192.168.1.12) to perform a MiTM attack on my Personal Windows PC (192.168.1.4). I will need my gateway address to fool the gateway that I am the PC, and Vice Versa. The IP of my gateway is 192.168.1.1. I will not be including the DNS Poisoning on the current attack, but I will explain how to use it later on.

I will be using the following command to perform a MiTM Attack with MiTMf:

Code mitmf --spooft --arp -i wlan0 --gateway 192.168.1.1 --targets 192.168.1.4

To break it down: mitmf (Package), --spooft (Load the plugin spoof), --arp (Redirect traffic using ARP Spoofing), -i (Interface) --gateway (Gateway IP), --targets (Target IP's)

If it works, you should then see something similar to this:

Screenshot [\(Click to View\)](#)

MiTMf automatically starts SSLstrip, to try and break down HTTPS into HTTP. All traffic that goes from 192.168.1.4 to the gateway, will be shown in the Terminal. You can also use Wireshark to analyze the packets in detail that are going through your connection by monitoring traffic through the

interface you are using in the command. I was downloading a game on Steam while MiTMf was running, so it was picking up lots of traffic. Notice how SSLstrip forced Imgur's HTTPS to get downgraded to HTTP:

Traffic shown on Terminal [\(Click to View\)](#)

Using arp -a on Windows, I was able to spot the spoofed address from the attacking machine:

You can stop mitmf by pressing CTRL-C in the Terminal. It should re-establish the connection between the Gateway and the Targets automatically.

DNS Spoofing

DNS Spoofing is achieved very easily, we will be adding --dns to the very same command we used in the previous attack.

Code `mitmf --spooft --arp -i wlan0 --gateway 192.168.1.1 --targets 192.168.1.4 --dns`

But this time, we need to edit a file, so we can tell mitmf on where it should point the spoofed DNS. mitmf.conf is located in /etc/mitmf. Let's say we wanted to redirect all traffic of the victim from imgur.com to 192.168.1.12;

Save the configuration file and start mitmf by using the command above. You should see something similar to this:

MiTMf DNS Spoofing [\(Click to View\)](#)

As soon as it ran, I tried to access imgur.com and voila! mitmf immediately cooked a response from imgur.com to 192.168.1.12. It timed out, as I had nothing running on the IP, but the attack was successful.

Conclusion

This kind of attack will only work if you have access to an internal network. This was done in an enclosed environment with two computers and a network that I personally own to show how a MiTM Attack actually works. I would like to thank everyone that took their time to read this thread. Commentary and Suggestions are very appreciated. Cheers!

CyberStrike - February 10, 2018, 7:57 pm

Good stuff well written and the screen shots definitely add to it.

skynet-7 - February 11, 2018, 7:10 am

Thank for this guide, good one. ;)

But I think MITMf is not usefull too much, because of the sites that you want the information (like facebook, google, instegram) works on HSTS, and it's not so easy to bypass it)mitmf don't do it). MITMf can pass HTTPS only.

But one thing I like in MITMf its the java script inject pluggin, wich you can wait until the target for one time will surf in HTTP protocol, and then you can inject any java script you want from the browser. :)

SysAdmin - February 11, 2018, 7:19 am

(Feb 11, 2018 08:10 AM)skynet-7 Wrote: [\[CITE\]](#) Thank for this guide, good one. ;)

But I think MITMf is not usefull too much, because of the sites that you want the information (like facebook, google, instegram) works on HSTS, and it's not so easy to bypass it)mitmf don't do it). MITMf can pass HTTPS only.

But one thing I like in MITMf its the java script inject pluggin, wich you can wait until the target for one time will surf in HTTP protocol, and then you can inject any java script you want from the browser. :)

You can avoid HSTS by using DNS Spoofing and cloning a website. Look into the Social Engineering Toolkit.

Baud - February 11, 2018, 10:51 am

(Feb 11, 2018 08:10 AM)skynet-7 Wrote: [\[CITE\]](#) But I think MITMf is not usefull too much, because of the sites that you want the information (like facebook, google, instegram) works on HSTS, and it's not so easy to bypass it)mitmf don't do it).

MITMf can pass HTTPS only.

On the paper MiTMf supports HSTS bypass through the --hsts option, I used to use it a couple years ago and it worked like a charm, especially on mobile, while the results were mixed on desktop. I don't know if it was updated to support more recent browser versions since then.

vladic4t - February 21, 2018, 11:11 am

(Feb 11, 2018 08:19 AM)SysAdmin Wrote: [\[CITE\]](#) You can avoid HSTS by using DNS Spoofing and cloning a website. Look into the Social Engineering Toolkit.

I think this will neither work because the DNS Spoofing makes a mitm attack and so if the mitm attack cannot bypass hsts or any website on nowadays browsers this will definitely not work. (I made this on my lab and it didn't work)

Any suggestions?

SysAdmin - February 21, 2018, 12:02 pm

(Feb 21, 2018 12:11 PM)vladic4t Wrote: [\[CITE\]](#) I think this will neither work because the DNS Spoofing makes a mitm attack and so if the mitm attack cannot bypass hsts or any website on nowadays browsers this will definitely not work. (I made this on my lab and it didn't work)

Any suggestions?

Worked fine for me with the --hsts option.