

Forum: [Hack Forums](#)

Thread: [\[GUIDE\] MiTM Attack with Ettercap](#)

Unknown69841 - January 20, 2021, 3:58 am

Original Post on Hackers-arise.com:

<https://www.hackers-arise.com/post/2017/08/28/mitm-attack-with-ettercap> [GUIDE] MiTM Attack with Ettercap Welcome back, my rookie cyber warriors!

In this tutorial we will use a GUI MitM tool known as Ettercap.

Ettercap is probably the most widely used MiTM attack tool (followed closely behind by Cain and Abel, which we will look at in the later tutorial).

Ettercap was developed by Albert Ornaghi and Marco Valleri. It basically a suite of tools to simplify MiTM attacks.

Ettercap enables us to place ourselves in the middle between two machines and then;infect the traffic with malware

- delete traffic

- sniff passwords

- provide fake certificates for HTTPS

- DNS spoof

The principles and techniques of a MiTM attack remain the same as with arpspoof with the small exception of the ip_forward. Unlike arpspoof, ettercap does not use ip forwarding in the Linux kernel, but instead uses it own module to forward IP packets.

It important to note that ettercap requires root privileges to open its Layer 2 (datalink) sockets. In addition, as you might expect, it can slow down communication between the two target systems as it does its own processing.

Ettercap is GUI based tool built into Kali so need to download and install anything, so let's get started doing a MiTM attack with Ettercap.

Step #1: Start ettercap

Let's view the help file for ettercap by typing;

```
kali > ettercap -h
```

As you can see, ettercap has a significant help file for running it from a command line, but the only thing we need from here is the switch to run it in graphical mode. In the bottom line of the screenshot (not the bottom line of the actual help file as I have truncated it in the interest of space), you can see the -G switch. This after the command ettercap will launch the ettercap GUI.

```
kali > ettercap -G
```

When we do, the ettercap GUI will start as seen below.

The first step in launching our MiTM attack is to start sniffing. Go to pulldown menu that says "Sniff" and click on "Unified Sniffing".

When we do that, it opens a new window asking us what interface we want to use and defaults to eth0.

When we click "OK", ettercap launches it sniffing and loads its plugins.

Our next step to find the hosts on the network. Click on the "Hosts" tab and you will see a menu that includes "Scan for Hosts". Click on it and ettercap will begin scanning the network for hosts.

Now, using that same "Hosts" tab, click on "Hosts List". This will display all the hosts that ettercap has discovered on your network as seen in the screenshot below.

Now, select one of the hosts that will be the target of this attack in the window by clicking on it and then click on "Add to Target 1" at the bottom of the window. When you do so, ettercap will add that host as the first target in our MiTM attack as seen in the screenshot below.

Next, select the second host in this attack and then click "Add to Target 2".

Finally, go to the menu above and click on MITM tab and the drop down menu will have a selection called "ARP Poisoning" as seen in the screenshot below.

Select it and it will open a pop window like below. Select "Sniff remote connections".

When we press OK, ettercap will begin ARP poisoning and you will see ettercap respond in its main windows with the message below.

Now, we have successfully placed ourselves between the two targets systems and all their traffic must flow through us. This is where the fun begins as we can now delete, manipulate, impersonate and view all their traffic.

Altering the Traffic

As I mentioned above, the real risk in a MiTM attack is that the attacker can eavesdrop on the Internet traffic as well as alter it, if they want. In this section, now that we are between the two systems we will demonstrate the risks of MiTM attack. We will use the MiTM attack to edit/alter the Internet traffic as seen by the target. In this way, the attacker can actually alter the content of websites, alter the content of an email, change the pictures seen by the target in their Internet traffic, delete specific Internet traffic packets, etc. The message should be clear, when we have placed ourselves in the middle, the target is at our mercy!

Step #2: Alter the Traffic

In this next section, we will be altering the traffic from an internal corporate Intranet site. This site is used by all the employees for corporate announcements, scheduling, etc. Although this scenario is within a corporate Intranet within a LAN, the technique and effect would be the same over the wider Internet. In our scenario, the manager has posted a new starting time for the following day because of a very heavy work load. As a result, he wants everyone to begin work at 6 am and he posts this to the corporate intranet site for all the employees to see. Our attacker has malicious intentions toward the target and wants to alter the message to the target so that they instead come to work late, at 11 am. This is likely to have negative repercussions for the target from the manager, exactly what the attacker wants.

Step #3, Create the Intranet Site

The corporate Intranet announcement page looks like the screenshot below. Everyone in the department will see it and although they are disappointed in the earlier start time, they adjust their schedule to help with the additional workload. Our attacker doesn't want the target to see this message, but rather an altered message to mislead him as to the new starting time.

Original Post on Hackers-arise.com:

<https://www.hackers-arise.com/post/2017/08/28/mitm-attack-with-ettercap>

No copy of Guide just repost! ? Thanks