# Man-in-the-Middle Lab

Thomas Martin

March 6, 2019

## Objectives

If an adversary can place themselves between communicating parties, without being detected, they can do a great deal of damage. Kali provides some very powerful tools for performing Man-in-the-Middle (MitM) attacks.

## Task 1: Configure VMs

For this exercise, we will run two virtual machines. For the *Target* machine, we do not need any special tools or software (it needs a browser). For convenience, we will use our OpenVAS Kali VM. For the *Attacker*, we will use the original Kali VM. Make sure each VM has been allocated 2GB of memory (this is less important if you are running installed VMs). Boot both VMs, using the NAT Network mode. Make sure the Target and Attacker VMs can both access the internet, and can ping each other.

## Task 2: Run Ettercap

Before we run Ettercap in the Attacker VM, we need to change some of the configuration details. Run the command:

`nano /etc/ettercap/etter.conf`

Immediately, you will see a line starting `ec_uid`. Replace the existing value (65534) with 0. Use CTRL-W to search for the string `iptables`. The following two lines start with `#redir`. Remove the `#` from both lines and save with CTRL-O. Exit with CTRL-X.

In the both the Target and Attacker VMs, check the status of the ARP table:

`arp -a`

Make sure you have these values later for reference.

In the Attacker VM, run Ettercap with the command:

`ettercap -G`

Go to Options, and make sure "Promisc mode" has been ticked. Go to "Sniff" - "Unified Sniffing". Select `eth0` for the Network Interface and click OK.

Go to “Hosts” - “Scan for hosts”. It should find four hosts. You can see what was found by selecting “Hosts” - “Hosts list”. Select “Start” and “Start sniffing”. Select “MitM” - “ARP Poisoning”, tick the box for “Sniff remote connections”, and click OK.

Go back to the Target VM and re-check the ARP table. Compare any differences.

Open a new terminal in the Attacker VM and run:

```
driftnet -i eth0
```

If you switch back to the Target VM, open a browser and start visiting sites, you will see any images loaded will appear in the driftnet window back in the Attacker VM (it may help if you make the driftnet window larger). Note that any secure HTTPS site will display a certificate warning. You may wish to try to find HTTP only sites to test (such as `http://42ndstreet.org.uk/` or `http://photobucket.com/`). Any images can be saved by clicking on them. And while only the most recent images are displayed, driftnet can be configured to download all images automatically.

Close driftnet and run the following command:

```
urlsnarf -i eth0
```

With this command, for any URLs that are requested in the Target VM, all the details will be listed in Kali. If you enter text in fields, they may be visible as GET parameters. You can see an example of this by using the search feature on `http://photobucket.com/` (but you will have to pay careful attention as a single search results in a great many requests.

## Wireshark

Beyond just performing these man-in-the-middle attacks, we can use the existing tools in Kali to observer how ettercap is performing them. Restart both VMs and start Wireshark running in the Attacker VM. To do so, just execute the command `wireshark` in a terminal, dismiss the error message. Start capturing packets on `eth0`. Run the same mitm attack in ettercap as described above (you only need to go as far as the ARP Poisoning stage) . Look through the packet capture and see if you can identify how the attack is performed.

## Extended Task

Experiment with the “dns spoof” plugin and try to use it to redirect the victim. You’ll need to modify the `/etc/ettercap/etter.dns` file.

Download a Windows 7 VM from:

```
https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/
```

Install the vulnerable apps that have been made available on Moodle. Go through Chapter 8 of Penetration Testing by Georgia Weidman (also available on Moodle) and perform the exploits on the vulnerable VM.

## Summary

This was a very simple example of a Man-in-the-Middle attack. Ettercap has many other interesting features, and there are other tools and techniques to achieve the same ends.