Arpspoof MITM - A Man in The Middle Attack with Kali Linux

Contents

Time required: 60 minutes

Lab Requirements

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

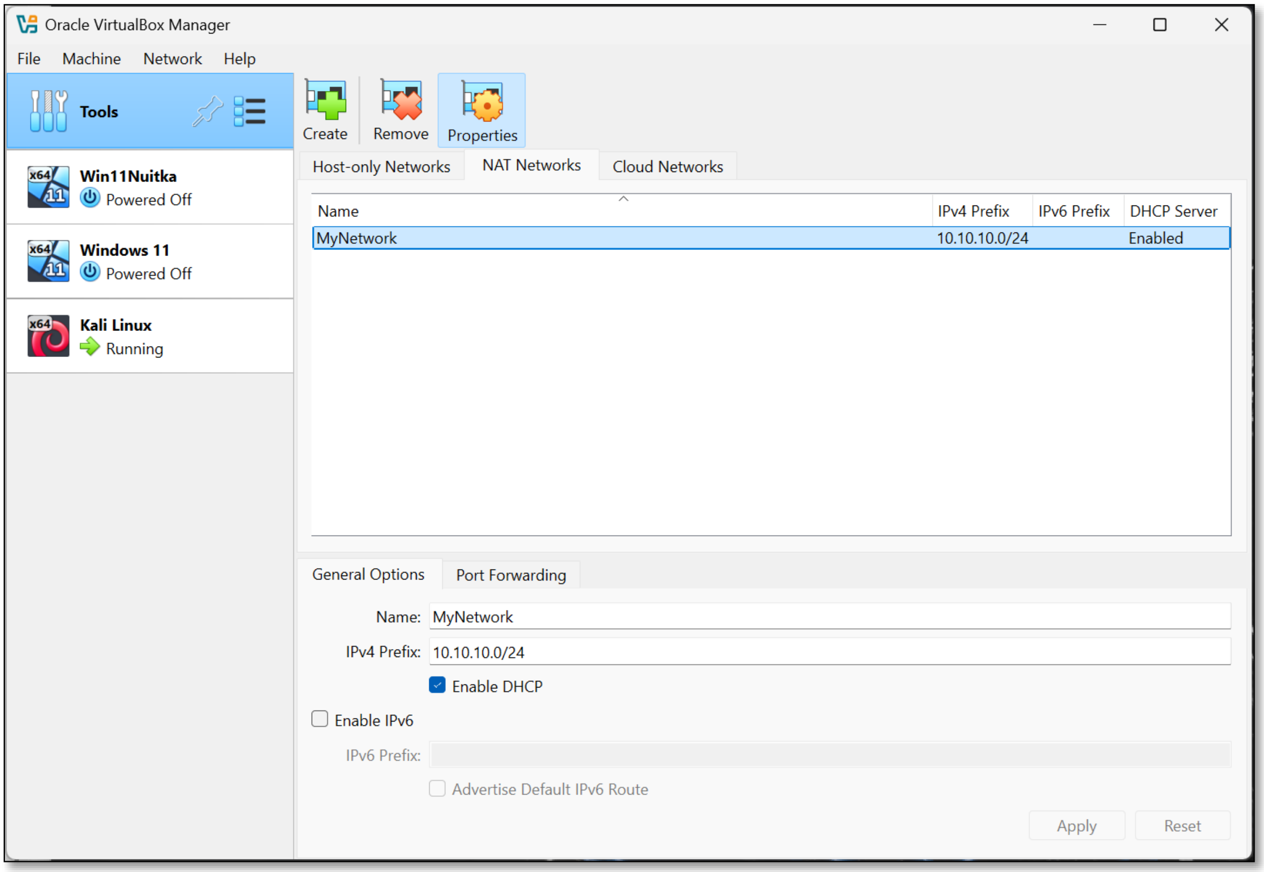
1. Kali Linux VM
2. Windows VM
3. Both VM's on a user created NAT network

Video walkthrough: VirtualBox User Created NAT

Create a NAT Network

For some activities in this class, we want to use a user created NAT Network. This is similar to putting our computers behind their own firewall. This network will isolate our VM's from the local network.

4. **Oracle VM VirtualBox Manager → Tools → Network Manager**
5. Click **NatNetworks** → Click **Create.**
6. **Name: MyNetwork**
7. **IPv4 Prefix: 10.10.10.0/24**



Name	IPv4 Prefix	IPv6 Prefix	DHCP Server
MyNetwork	10.10.10.0/24		Enabled

Name: MyNetwork

IPv4 Prefix: 10.10.10.0/24

☑ Enable DHCP

□ Enable IPv6

IPv6 Prefix:

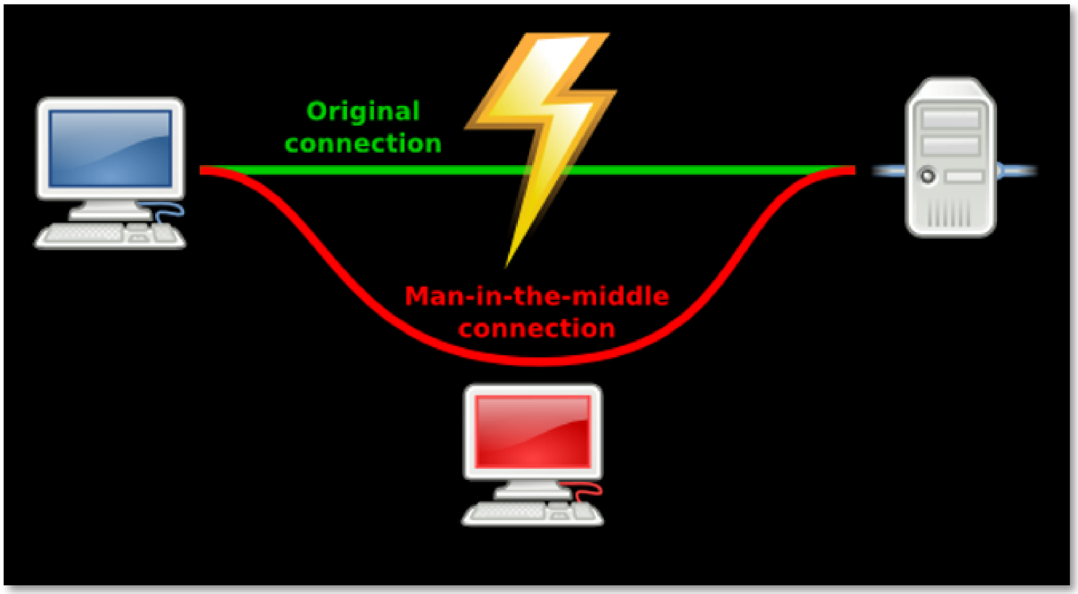
□ Advertise Default IPv6 Route

8. **In Oracle VM VirtualBox Manager:** Right Click each Virtual Machine → **Settings**.
9. **Network → Attached to**: **NatNetwork**

Man in the Middle (MITM)

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 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 Router you're using.

```
ip route show
```

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

Insert a screenshot:

Click or tap here to enter text.

2: Obtain the IP configuration from the Victim

You need to get the IP of your Victim.

Nmap is an open source tool to scan networks.

1. Open a terminal.
2. Do a quick scan of your local network. Substitute your network information.

```
sudo nmap -sn 10.10.1.0/24
```

3. **Insert a screenshot:**

Click or tap here to enter text.

4. On the Windows VM, go to a command prompt and confirm the IP address.

3: Turn on Packet Forwarding in Kali Linux

This is very important because if your machine isn't exchanging packets, the attack will result in a failure as your internet connection will be disrupted. By enabling the packet forwarding, you disguise your local machine to act as the network router.

In Kali Linux, to turn on packet forwarding, run the following command:

```
sudo sysctl net.ipv4.ip_forward=1
```

4: Redirect Packets to From Victim to Kali with arpspoof

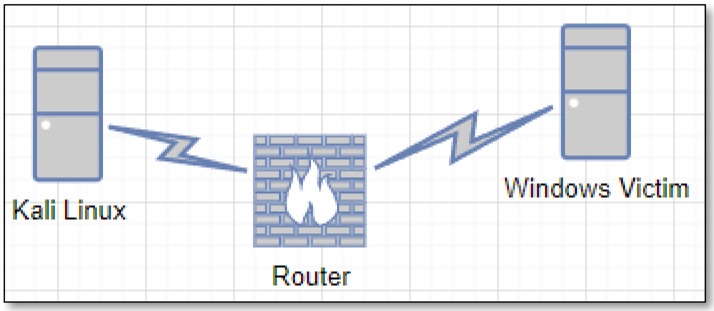
Arpspoof is a Linux utility that lets you expropriate traffic to a machine of your choice from a switched LAN. Arpspoof is a simple tool to redirect network traffic on the local network.

dsniff contains several tools to listen to and create network traffic. We are going to use arpspoof - Send out unrequested (and possibly forged) arp replies.

Install dsniff

```
sudo apt install dsniff
```

To find your network interface name, use **ip a** The network interface name in VirtualBox will be eth0. This is the first ethernet adapter.



This diagram shows normal network communication.

You are going to tell the Victim that Kali Linux is the router.

Use the following syntax to start intercepting packets from the Victim to your Router:

```
sudo arpspoof -i <Network Interface Name> -t <Victim IP> <Router IP>
```

This has enabled the monitoring the incoming packets from the Victim to the Router. Leave this terminal running.

Insert a screenshot:

Click or tap here to enter text.

5: Intercept Packets from the Router to the Victim

You're doing here the same as the previous step, except it's just reversed. Leaving the previous terminal open as it is, open up a new terminal to start extracting packets from the Router. Type the following command with your network interface name and router IP:

```
arpspoof -i <Network Interface Name> -t <Router IP> <Victim IP>
```

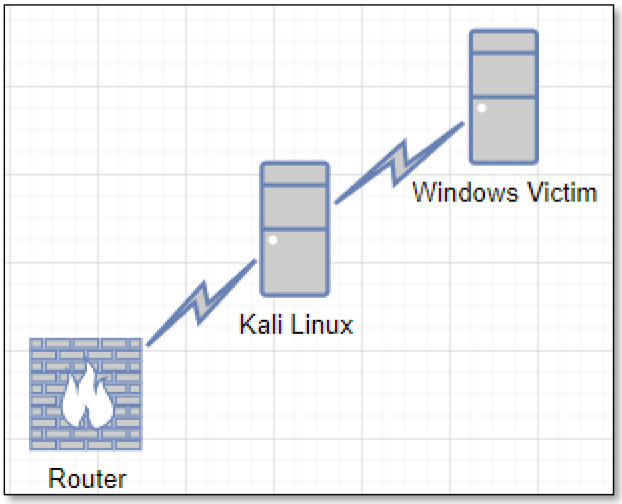
We switched the position of the arguments in the command we used in the previous step.

You are now in the middle of the communication between the Victim and the Router.

Insert a screenshot:

Click or tap here to enter text.

6: Kali Linux is The Default Gateway for the Victim



At this point, the victim machine thinks that the Kali Linux attack machine is the router.

1. Go to the Windows 11 command prompt: arp -a
2. You should see that the Kali Linux machine and the default gateway have the same MAC address.
3. Insert a screenshot:

Click or tap here to enter text.

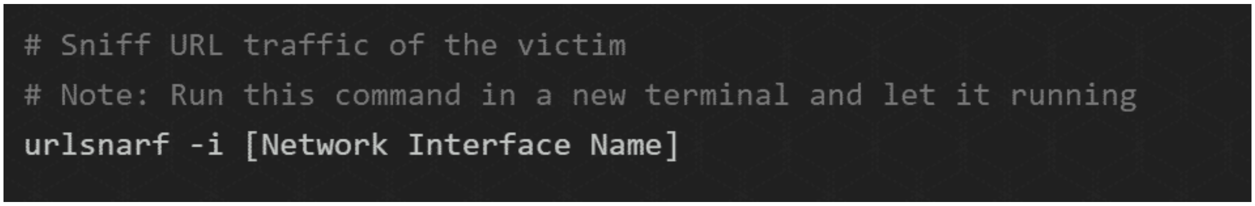
7: Sniffing URLs information from victim navigation

You can also sniff out the website's URL that our Victim often visits. The program we're going to use is a command-line tool known as **urlsnarf**. It sniffs out and saves the HTTPs request from a designated IP in the Common log format. Fantastic utility to perform offline post-processing traffic analysis with other network forensics tools.

Let the other two terminals keep running. Start a new terminal.

The syntax you'll put in the command terminal to sniff out the URLs is:

```
sudo urlsnarf -i [Network interface name]
```



```
# Sniff URL traffic of the victim
# Note: Run this command in a new terminal and let it running
urlsnarf -i [Network Interface Name]
```

As long as each terminal is functional and you've accidentally not closed one of them, Kali will capture all http traffic. There are very few web sites that use http, most use https. We will use vulnweb.com, which uses http port 80.

1. On the Windows VM → go to vulnweb.com
2. On Kali → the urlsnarf terminal should show traffic to and from vulnweb.com
3. **Insert a screenshot:**

Click or tap here to enter text.

8: Stopping the Attack

Once you're satisfied with what you've got your hands on, you may stop the attack by closing each terminal. You can use the Ctrl+C shortcut to go about it quickly.

In Kali → disable packet forwarding.

Type in the following command in the terminal:

```
sudo sysctl -w net.ipv4.ip_forward=0
```

9: Back to Normal

Everything is back the way it was.

1. Go to the Windows 11 command prompt: arp -a
2. You should see that the Kali Linux machine and the default gateway have different MAC addresss.
3. Insert a screenshot:

   Click or tap here to enter text.

Summary

NOTE: This is not a script, it is a summary of the commands used.

```
# Enable port forwarding
sudo sysctl -w net.ipv4.ip_forward=1

# Spoof connection between Victim and Router
# Note: Run this command in a new terminal and let it run
sudo arpspoof -i [Network Interface Name] -t [Victim IP] [Router IP]

# Same step but inverted
# Note: Run this command in a new terminal and let it run
sudo arpspoof -i [Network Interface Name] -t [Router IP] [Victim IP]

# Sniff URL traffic of the victim
# Note: Run this command in a new terminal and let it run
sudo urlsnarf -i [Network Interface Name]
# This should show traffic to and from www.vulnweb.com

# Disable port forwarding once you're done with the attack
sudo sysctl -w net.ipv4.ip_forward=0
```