**Laboratory Exercise 5 – IP and MAC Spoofing**

**1. Overview**

For this lesson, students will use the Cyber Range: Kali Linux with Metasploitable (2018) environment to complete IP spoofing, MAC spoofing. Students will also use the Kali and Vulnerable Windows (64bit) VMs environmentto complete and examine a MITM attack called ARP poisoning.

**2. Resources required**

This exercise requires a Kali Linux VM running in the Cyber Range.

**3. Initial Setup**

For this exercise, you will log in to your Cyber Range account and select the Kali Linux with Metasploitable (2018) environment, then click “start” to start your environment and “join” to get to your Linux desktop login. Log in using these credentials:

Username: **student**

Password: **student**

**4. Tasks**

**Task 1: IP Spoofing using nmap**

Nmap has an option to let you scan a host using a spoofed IP. To spoof the IP during a nmap scan, complete the following:

Ip: 10.1.71.229/20

Meta ip: 10.1.78.205/20

Fake : 204.120. 0.15

Use the technique we have introduced in Lab 3 to find out your own IP address, and the Metasploitable IP address.

1. Open Wireshark. When it loads, choose eth0 by double clicking eth0 and then filter using ip.addr == <spoofed IP> && ip.addr == <target IP>, where <spoofed IP> is any valid but fake IP you want to use and <target IP> is the target Metasploitable IP address. NOTE: You will need to open Wireshark as root.
2. Open a terminal and type the following: nmap -S <spoofed IP> -e eth0 -PN -F <Target IP >
3. In my case:

nmap -S 10.1.1.1 -e eth0 -PN -F 10.1.144.241

Quick reminder of options:

-S the spoof (i.e., fake) IP address

-e specifies the interface

-PN asks nmap do not ping before scanning, such that your real IP is not revealed.

-F is sets the fast scan option (top 100 ports)

**Question 1 (10 pts):** attach a screenshot of the captured packet in Wireshark. The screenshot should clearly show the packet sent from the spoofed IP to the target IP. Verbally explain what you have done and how do you interpret the results.

**First, as a root using sudo su, we initialized the Metasploit database and started the Metasploit framework as well. After verifying that the database had connectivity with db\_status, we verified that we were working in the Metasploit able workspace. Through this we found the ip address, and in another terminal (using grep) we found the Metasploit able machine and IP Address or the Target address in this case. Wireshark was then running and the listed above commands were executed to send the packet from the spoofed IP address into the target ip address which happened by filtering through eth0.**

A picture containing text, screenshot, monitor, computer

Description automatically generated

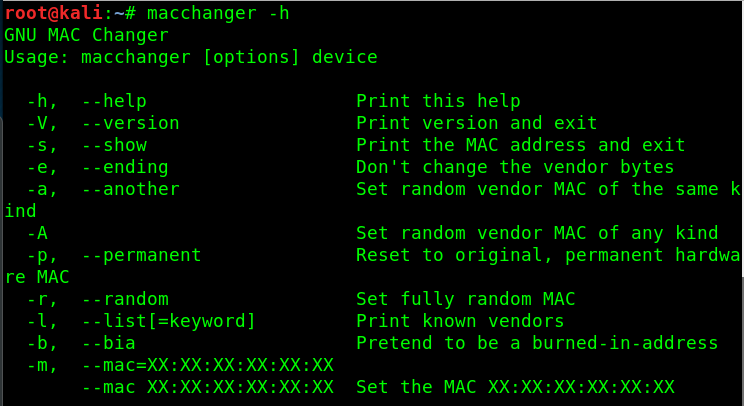
**Question 2 (5 pts):** Note that in Wireshark, you can only find packets send from the spoofed IP address to the target IP address, but not packets on the reverse direction (that is, send from the target IP to the spoofed IP). What might be the reason?

**We may not be able to find packets sent from the target IP to the spoofed IP address because the spoofed IP is perhaps valid yet fake, or perhaps there is a connectivity issues due to software faults or checks.sudo**

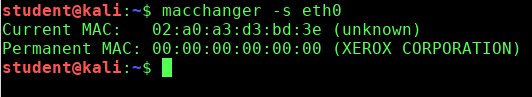
**Task 2: Mac Spoofing with Macchanger**

Many organizations will prevent individuals from accessing their systems by using MAC filtering. This may work in some cases; however, many hackers will sniff the network and find a valid MAC address then spoof that address using a program like Macchanger. The first thing we want to do is look at the options under the help menu.

* Type macchanger -h and press enter



* Type macchanger -s eth0 to see the current MAC address of the device you are on (yours could be different)



As stated above, an attacker will look for a valid MAC address on the network to spoof. There are many ways to complete this task. For now, we will use nmap.

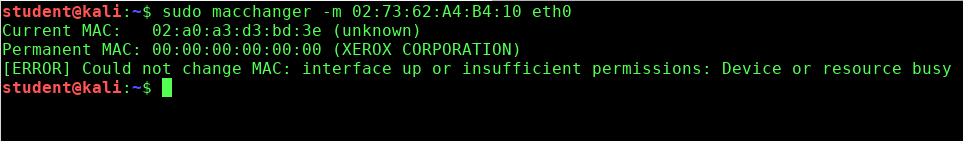
* Open a new terminal tab and become root.
* Use the nmap commands in Lab 3 to find the MAC address of the Metasploitable machine. Hint: you may want to filter for the keyword “open” to find the machine with an open port, and display a few more lines (such as 4 lines) before and after where the keyword appears.

Return to the macchanger tab and complete the follow command

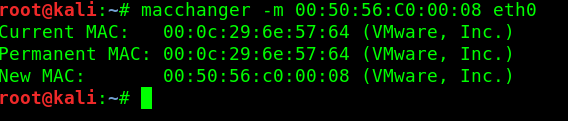
* sudo macchanger -m <Metasploitable MAC Address> eth0

You may get an error due to the Cyber Range preventing MAC spoofing. Remember though, an attacker will not be using internal resources that belong to the organization. They will have a device of their own. I have also provided a screenshot of the expected output.

Cyber Range Output



Expected Output if it were not limited by the Cyber Range environment:



**Question 3 (10 pts):** submit a screenshot showing the Metasploitable machine’s MAC address that you have found. Submit another screenshot showing your attempt to spoof the MAC and the error message gave by Cyber Range. Verbally explain what you have done and how do you interpret the results.

* **I first went to the termianal window with the metasploit framework running, and used the db\_nmap Metasploitable IP and db\_nmap -F -sS -n -v –open –reason Metasploitable IP, command. Afterwards, in new terminal, I became root and used msfconsole and workspace metasploitable, as well as the db\_nmap -p- -sS -n -v –open -max-err-timeour 100ms –reason <target IP> in order to retrieve the MAC address as shown in the first screenshot. Then, it was just a matter of using the given command “sudo macchanger -m <Metasploitable MAC Address> eth0” to get the error statement limited by the Cyber Range environment.**

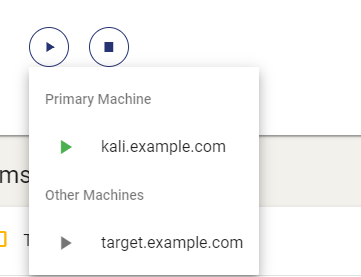
A computer screen capture

Description automatically generated with medium confidenceText

Description automatically generated

**Task 3: ARP spoofing for internal MIM attack**

Close and shut down the current Kali Linux with Metasploitable (2018) environment. For this task, we will use the Kali and Vulnerable Windows7(64) VMs Environment.On the courses page, select this environment, then open **both** virtual machines by powering them up and clicking on the play button for each VM. There is a screenshot below showing the two VMs. Each machine will open in a new tab.



**NOTE**: Once on the Windows (target.example.com) desktop, a one-time “Windows Activation” window may pop up. If it does, just bypass this by selecting “Ask Me Later” or just select the Cancel button; we're not registering this OS since this is for temporary, educational use.   
  
***IMPORTANT****: For “Windows Activation”, DO NOT select “Activate Now” or this will cause problems and you'll have to ask your instructor to reset your VMs.*

On the Kali (kali.example.com) VM, open a terminal and complete the following:

* Type sudo apt-get update and wait it finish. This will update the package lists in the Linux such that new packages can be found.
* Type sudo apt-get install dsniff and press enter.
* Type y if you get a prompt and hit enter.

Dsniff is the package that contains ARPspoof.

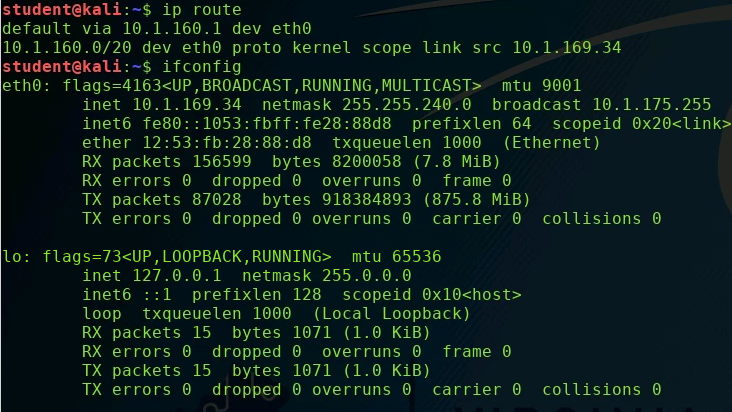
* Find the default gateway by typing ip route and pressing enter.
* Find your interface by typing ifconfig and pressing enter.

As you can see in the screenshots below, my default gateway is 10.1.160.1 and my IP address is 10.1.169.34. You will have different IP addresses.

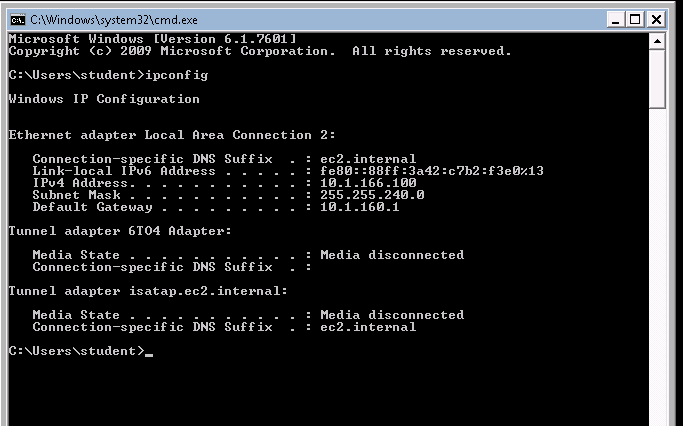
IP: 10.1.134.161

Getaway: 10.1.128.1

Take 10.1.131.176

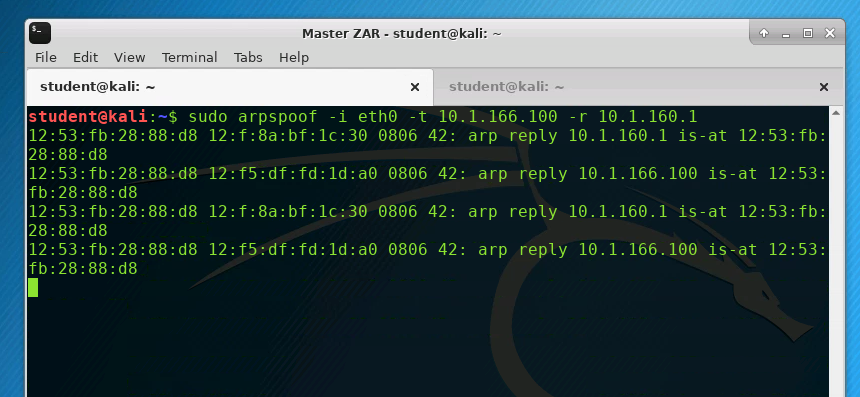


Next, we need to get our target IP address. Switch to the Windows VM tab, open a command prompt, type ipconfig and press enter. In my case, the IP is 10.1.166.100 as shown in the screenshot below. Take note of YOUR target’s IP address.



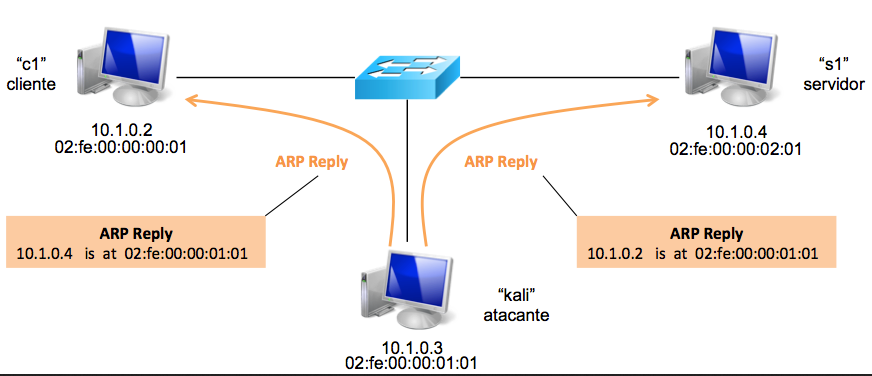
Switch back to the Kali VM and return to the terminal. Looking at the command below, replace the first IP address (target) with your default Windows VM IP and the second IP with your default gateway IP.

* Type sudo arpspoof -i eth0 -t <Target IP> <Default Gateway IP>
* In my case, sudo arpspoof -i eth0 -t 10.1.166.100 10.1.160.1



To break this down, the attacker is sending an ARP reply to the network stating that the attacker’s MAC address is associated with the IP address of the default gateway. Such that if the victim is to send a packet to the IP of the default gateway, the victim’s Link layer will actually send the packet to the attacker because it thinks that the attacker’s MAC address is associate with the IP address. When the attacker receives the packet, the attacker can forward it to the real gateway, and in the meanwhile inspect and even modify the packet.

These above steps can’t be implemented in the Cyber Range environment and we will stop the lab here.



Source: <https://raw.githubusercontent.com/cletomcj/vnx-sdn/master/noarpspoof/ARP_spoofing_2_esquema.png>

To sniff the network requests that are passing through the victim’s machine, we can use Wireshark on the Kali VM.

* Open Wireshark
* When Wireshark loads, choose eth0 by double clicking eth0.
* In the filter box, type arp and press enter.
* You should be able to see multiple ARP packets that advertising the default Gateway’s IP is associated with the MAC address of your own machine.

**Question 4 (10 pts):** submit a screenshot that shows your default gateway, a screenshots that shows the IP address of the Windows machine, and a screenshot that shows you use Wireshark to captures all the ARP packets. The ARP packet should clearly show that it is send from your machine, to the Windows machine, and advertising your machine’s MAC address is associated with the default gateway’s IP. Verbally explain what you have done and how do you interpret the results.

**The first step was opening both parts of the Kali windows cyber range program, then typing the following commands listed above :**

* **Type sudo apt-get update and wait it finish. This will update the package lists in the Linux such that new packages can be found.**
* **Type sudo apt-get install dsniff and press enter.**
* **Type y if you get a prompt and hit enter.**
* **Find the default gateway by typing ip route and pressing enter.**
* **Find your interface by typing ifconfig and pressing enter.**

**Then after going to the Windows VM tab, I was able to aquire the 3 necessary addresses for the completion of task 3 which was**

**IP: 10.1.134.161**

**Getaway: 10.1.128.1**

**Target 10.1.131.176**

**Only when using the final Type sudo arpspoof -i eth0 -t <Target IP> <Default Gateway IP> command, was the networks sniffed.**

A screenshot of a computer

Description automatically generated with medium confidenceA screenshot of a computer

Description automatically generated with medium confidence

A computer screen capture

Description automatically generated with medium confidence