Network Penetration Testing Methodology-Perimeter Devices

1 Hr 39 Min Remaining

**Exercise 1: Scanning with Nmap against Defenses**

**Scenario**

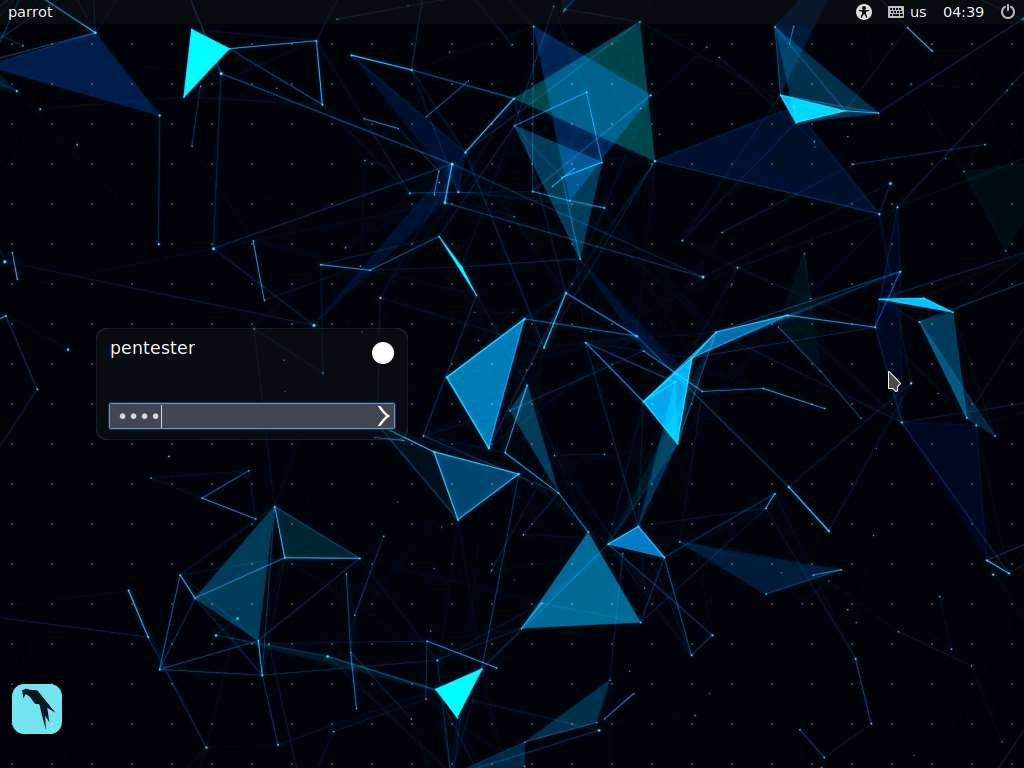
One of the most popular open source scanning tools on the market is Nmap. As you may have discovered, it is an effective tool. We have also, on numerous occasions, discovered that if there are defenses in place such as firewalls or filters, conducting scans becomes more challenging.

During a penetration test, it is imperative that you use a tool to identify open ports and the services attached to that port. There are a number of tools available, and we will start with the most popular tool on the market that is free and open source: Nmap. Nmap also has options that give it better success when encountering filters.

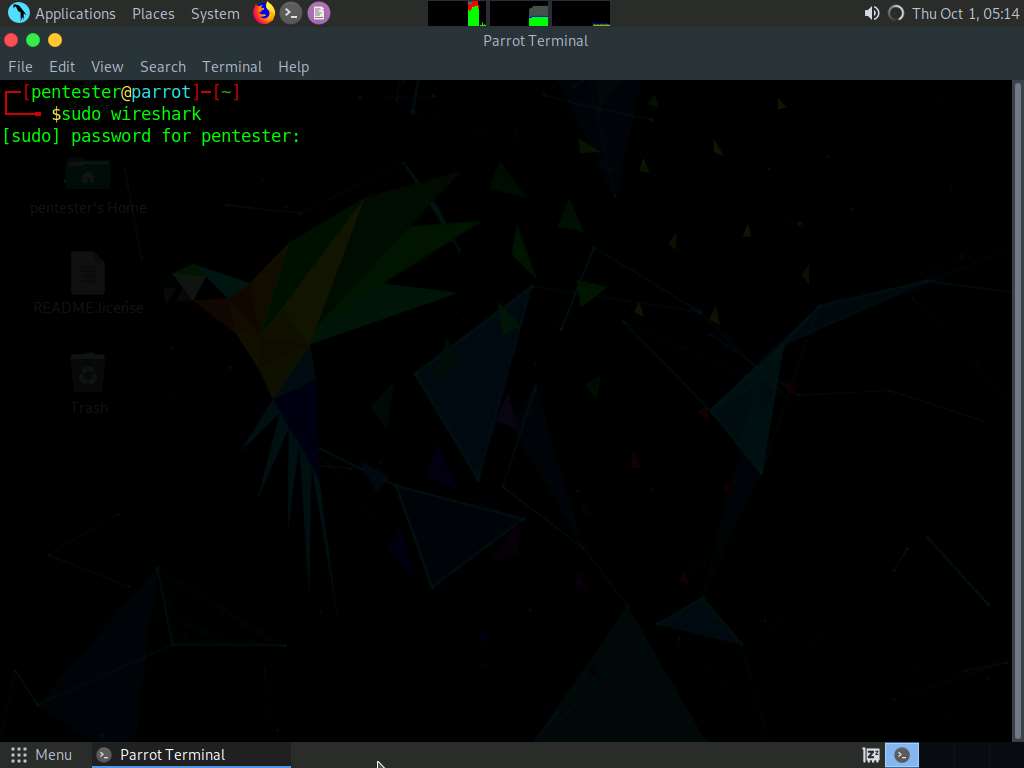
The objective of this lab is to help students use Nmap, and then attempt advanced options to scan through a filter. In this lab, you will:

* Scan for a target
* Observe and troubleshoot the scan
* Attempt advanced options to scan through a filter

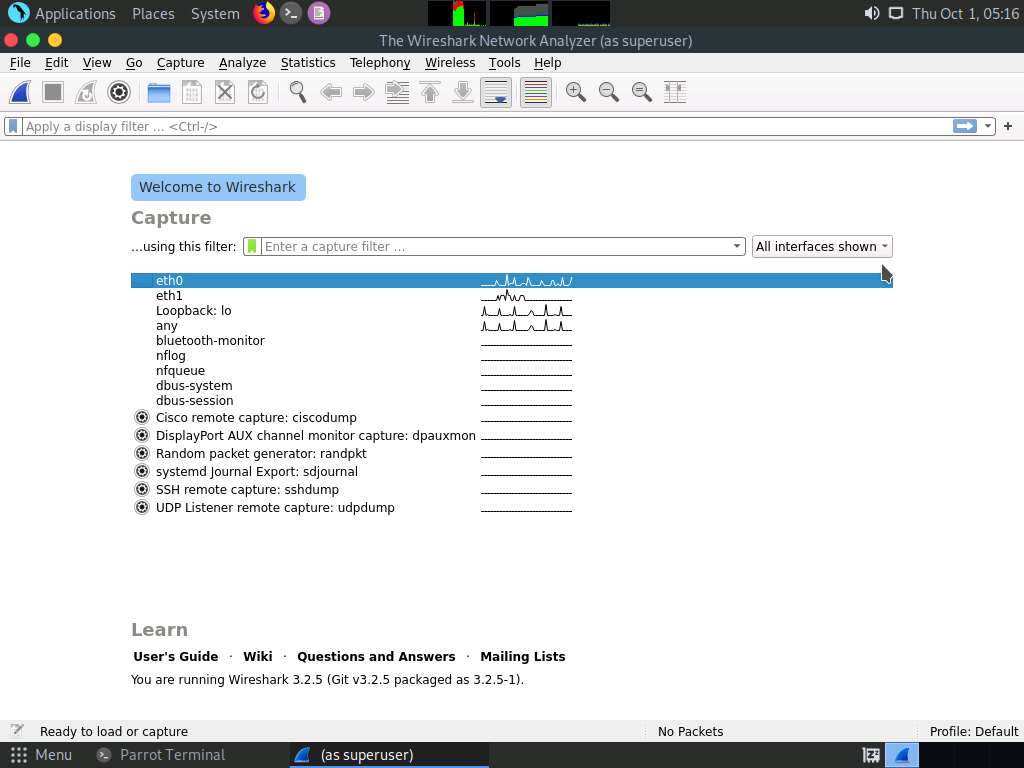
1. Click [Parrot](https://labclient.labondemand.com/Instructions/2e9ecc61-2e0e-4b61-931e-5ada85a820dd?rc=10). Parrot logon screen appears, type **toor** in the Password field and press **Enter**.



1. You are now ready to test the rules. First, start a **protocol analyzer** when you begin to test the rules. Start Wireshark, launch a terminal and type **sudo wireshark** and press **Enter**. Type **toor** when prompted for Password and press **Enter**.

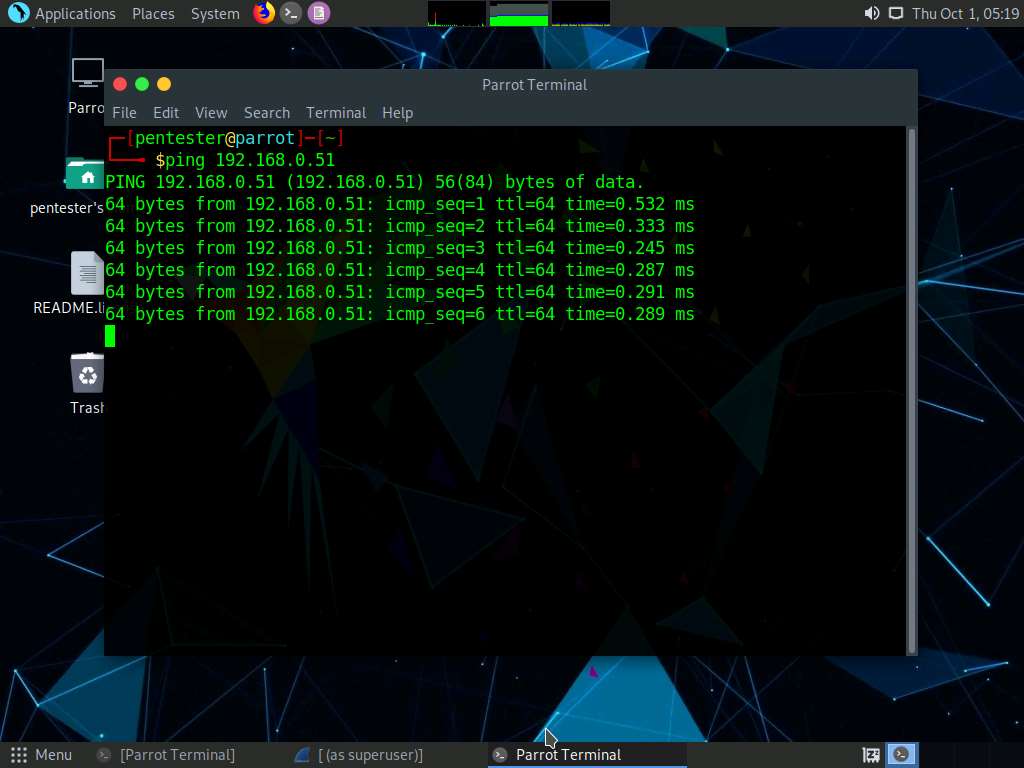


1. Double-click **eth0** interface to start capturing. Minimize the Wireshark window.

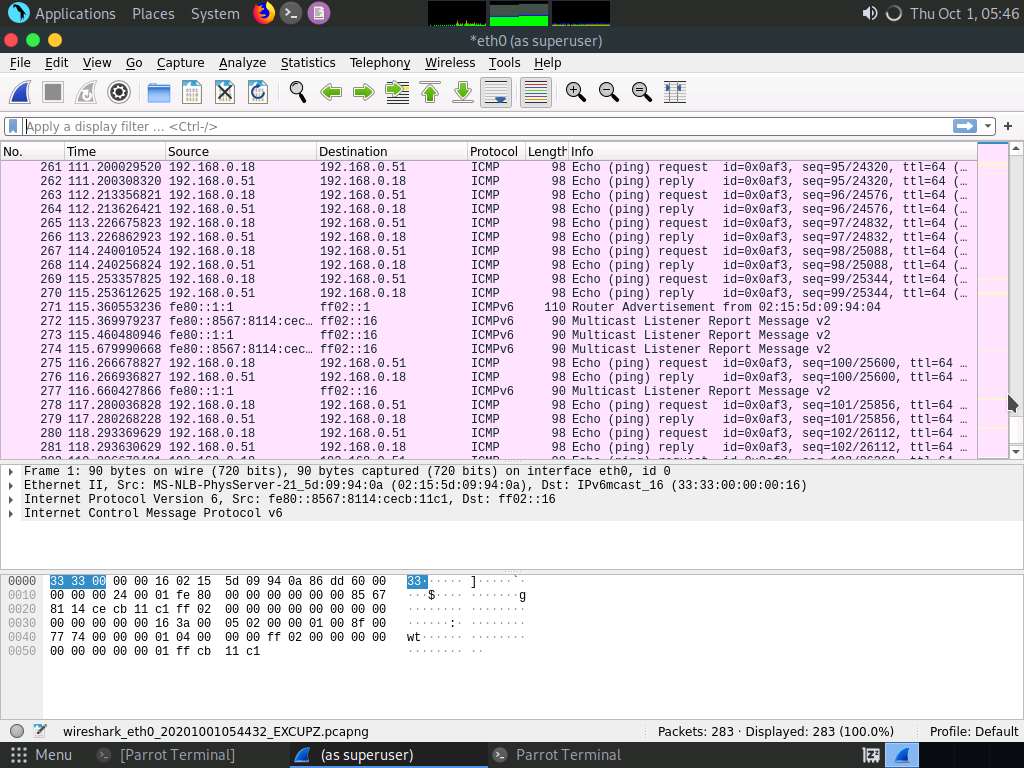


1. Now, launch a new terminal window and type **ping 192.168.0.51** and press **Enter**. Switch to **Wireshark** window to view the capture.

192.168.0.51 is the IP addres of **RPC Server Ubuntu** machine

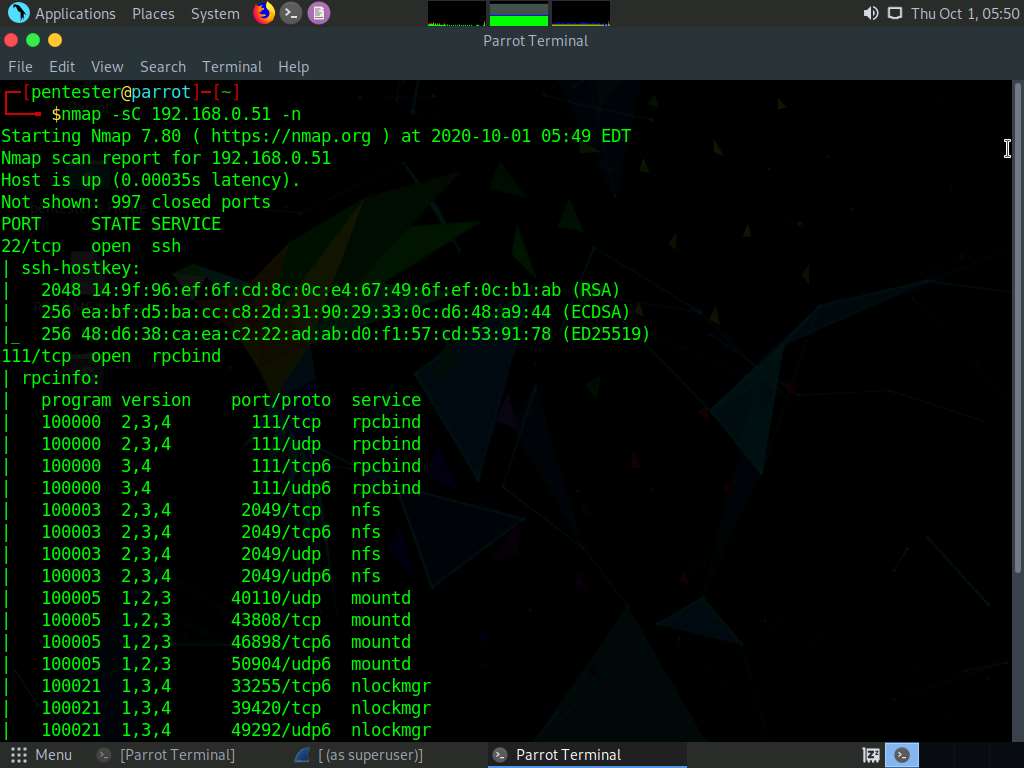


1. Click **Stop Capturing Packets** button in the menu bar to stop the packet capture. Take a few minutes to review the packets in Wireshark, as shown in the screenshot.

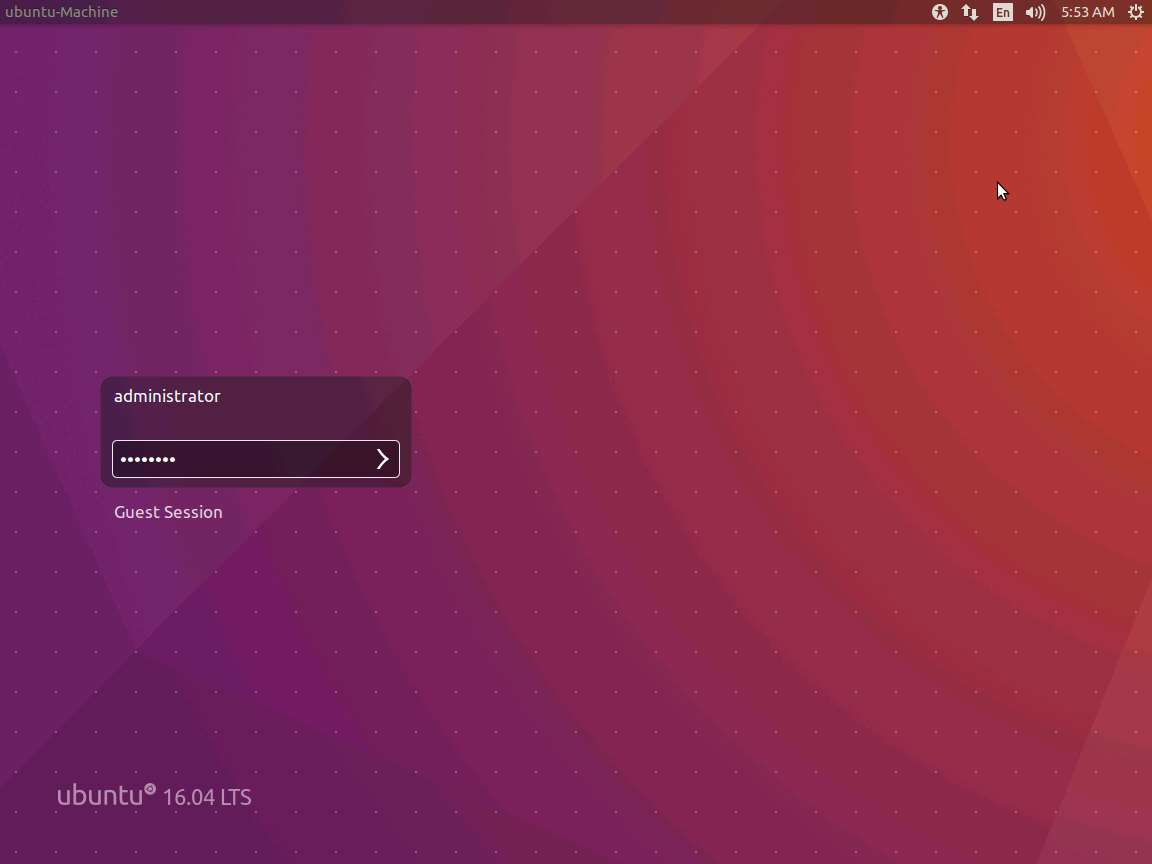


1. You have not set up any protections as of yet, so you should be able to ping. As soon as you **enable protections**, this will change. Part of advanced techniques is identifying what is in between us and a target, or what is on the target that is preventing us from connecting to it. At the current setting, the **iptables** are allowing all traffic.
2. Launch a terminal window, type **nmap -sC 192.168.0.51 -n** and press **Enter**, as shown in the screenshot.

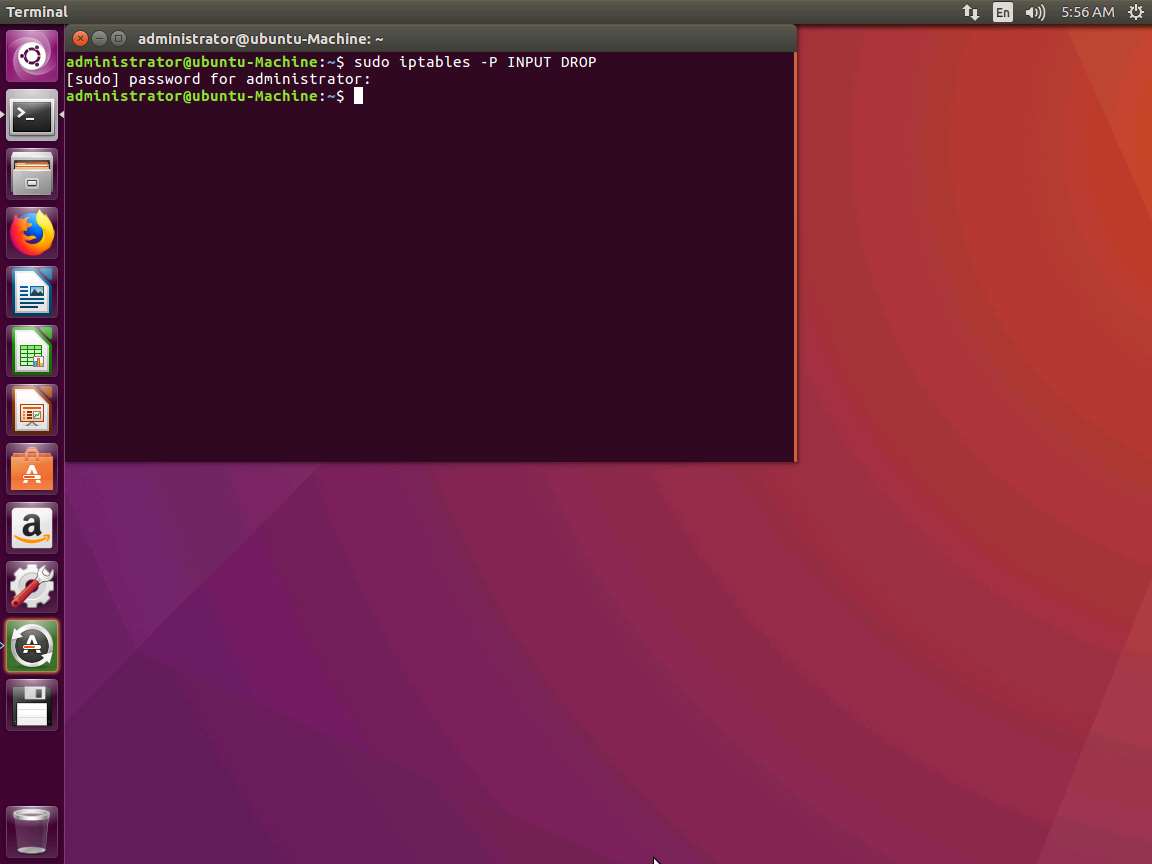
192.168.0.51 is the IP addres of **RPC Server Ubuntu** machine



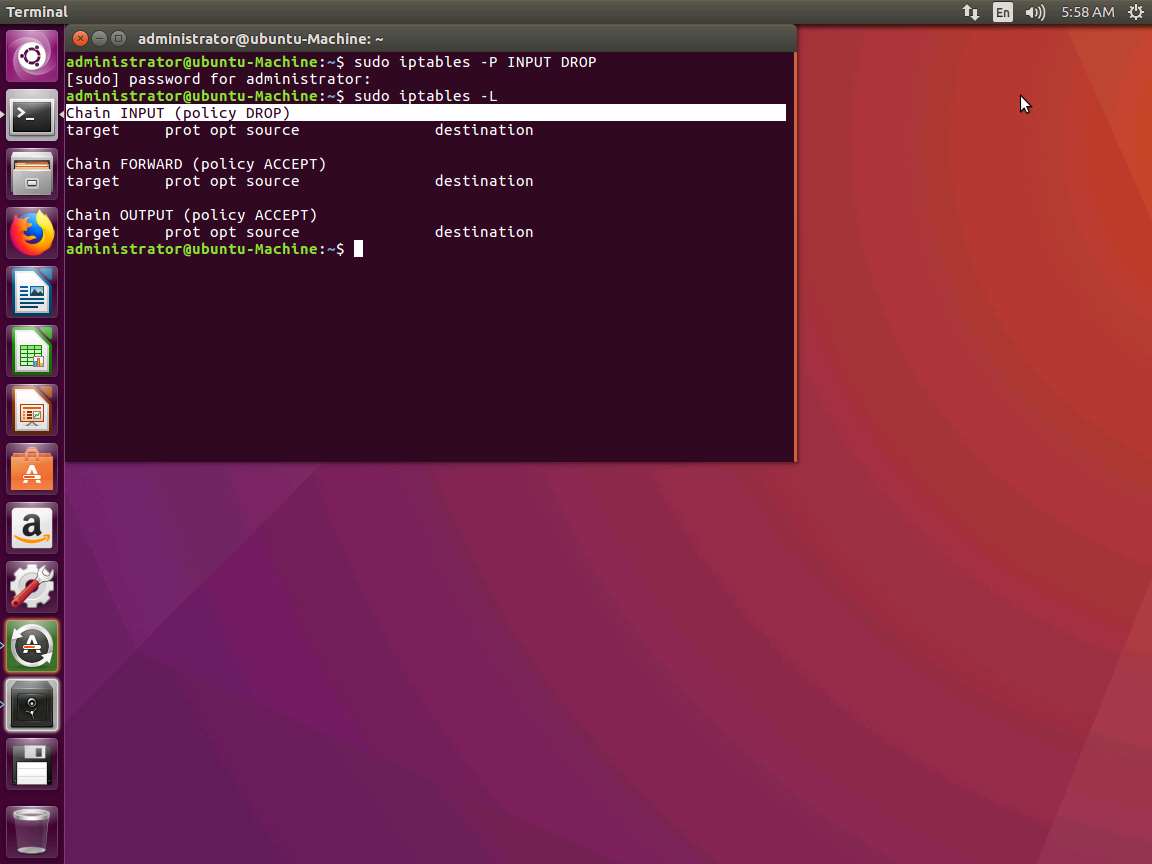
1. Switch to **RPC Server Ubuntu** machine, by default **administrator** user profile in selected, type **Infinit3** in the Password field and press **Enter** to logon.



1. Once you are logged into machine launch a terminal and type **sudo iptables -P INPUT DROP**. Type **Infinit3** and press **Enter** when prompted for the password.

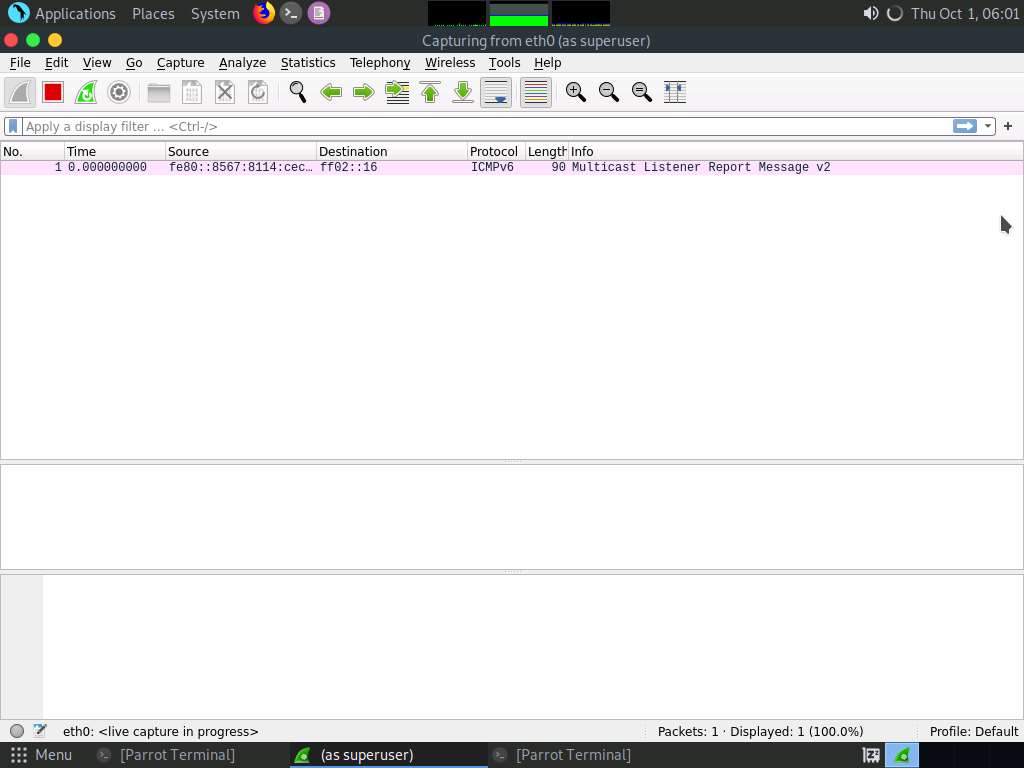


1. Once you have entered the rule, all **inbound packets** will be **blocked**. To see your rule, type **sudo iptables -L** and press **Enter**, type **Infinit3** and press **Enter** when prompted for the password.

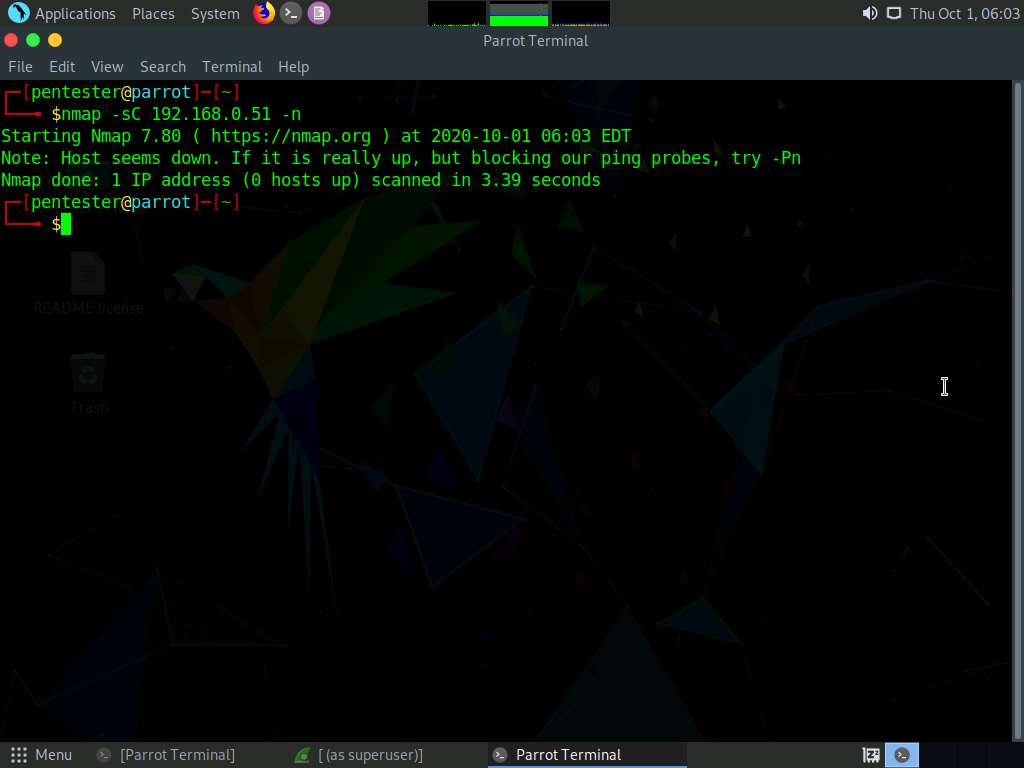


1. Switch to [Parrot](https://labclient.labondemand.com/Instructions/2e9ecc61-2e0e-4b61-931e-5ada85a820dd?rc=10), and maximize the Wireshark and click **Start capturing packets** (Shark Fin Icon) to start the new packet capture. Leave the Wireshark window running.

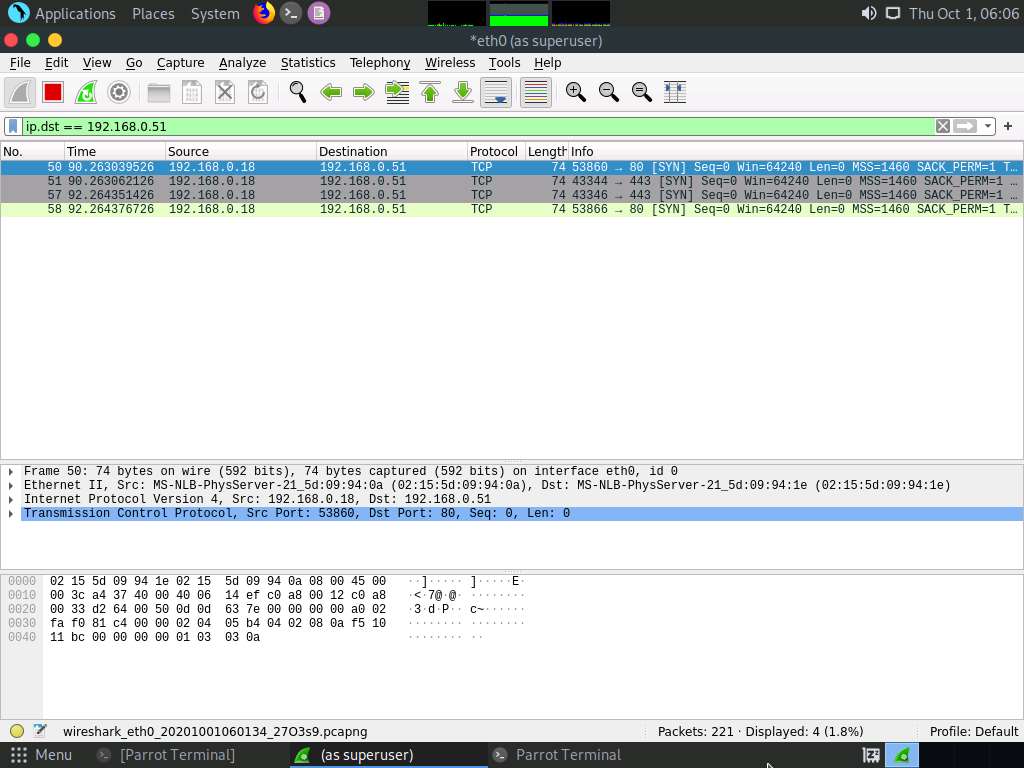
If Unsaved packets popup appears, click **Continue without Saving**.



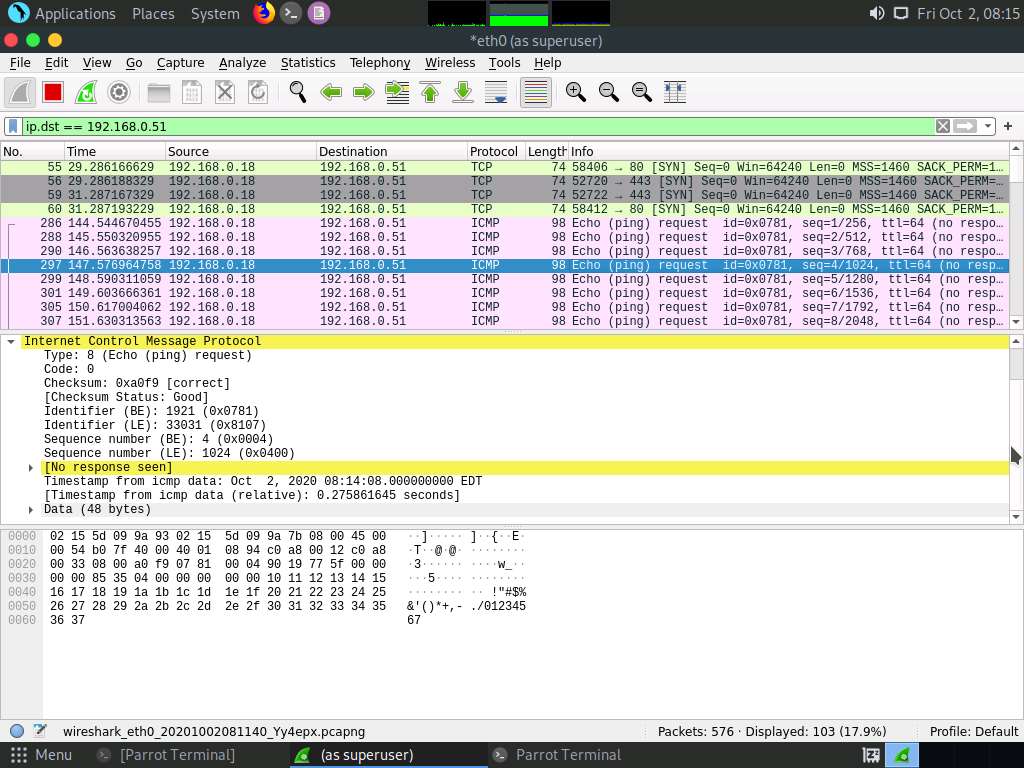
1. Launch a new Terminal, and then type **nmap -sC 192.168.0.51 -n** and press **Enter**. As the screenshot shows, this configuration reduces the attack surface to zero. This occurs when you are working from the perimeter. The tester will often face different types of obstacles. As a result, you must first evaluate them, and then detect any weaknesses or go through the administrator’s configuration.



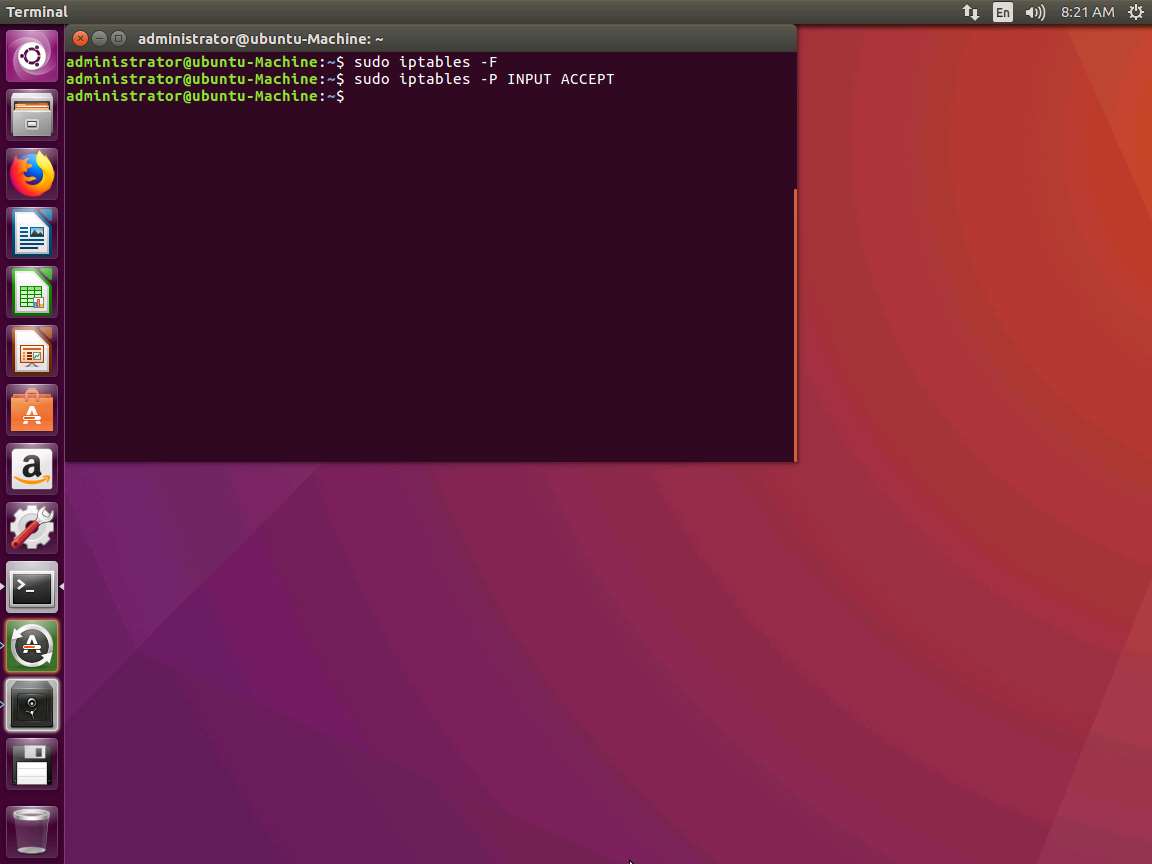
1. Maximize the Wireshark window and then type **ip.dst == 192.168.0.51** in the Filter field and press **Enter** to apply the filter. Have a look at the captured traffic and then clear the Filter.



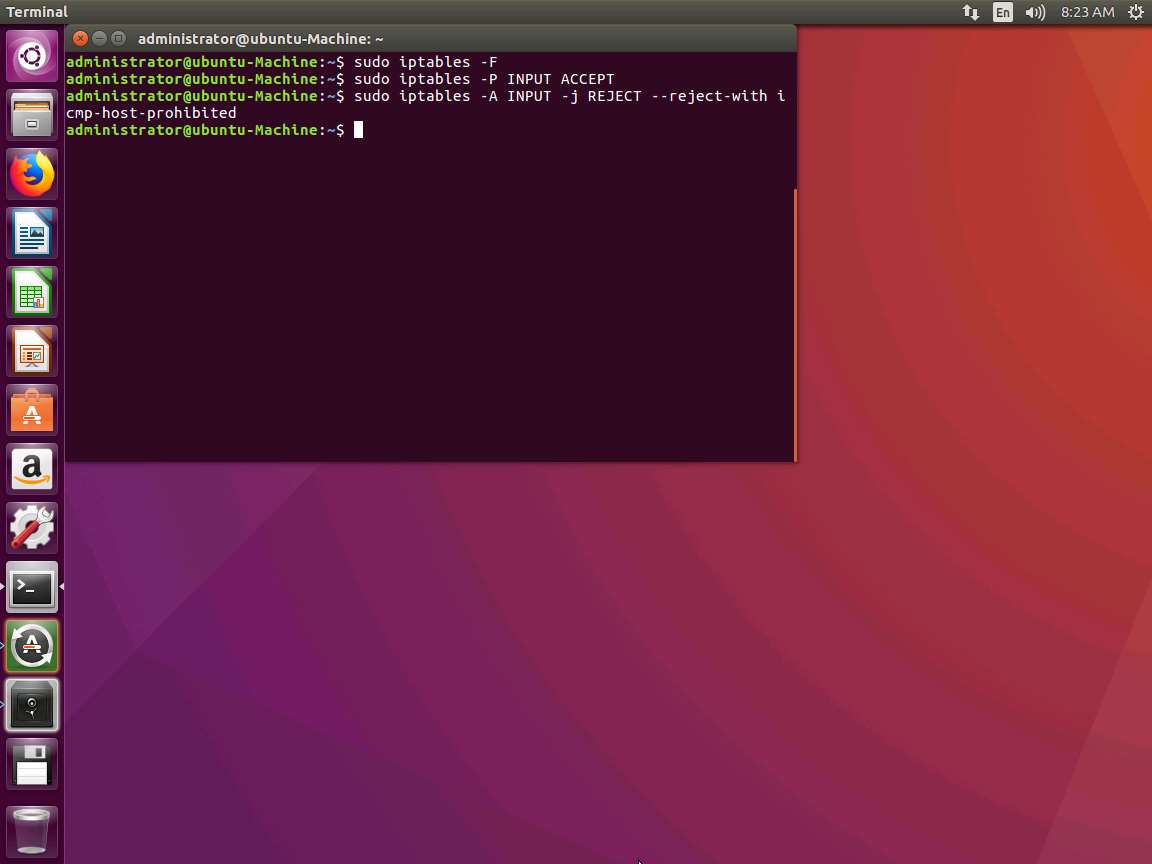
1. Launch a new Terminal, and then type **ping 192.168.0.51** and press **Enter**, and then switch to Wireshark window to view packet capture, you can see the message in the packet capture states that **no response** from the Target machine.



1. At the current setting, the iptables are appropriately configured to not respond. With most devices, they are not set this way by default. Change the configuration of the iptables to reflect a typical configuration for Cisco or any other router vendor. When you scan an **access control list** (ACL), you will receive an **Internet Control Message Protocol** (ICMP) packet of code **3** type **13**.
2. Configure the iptables settings to emulate a filtering devices response. Switch to **RPC Server Ubuntu** machine and in the terminal window type the following commands and press **Enter**:
   * **sudo iptables -F**
   * **sudo iptables –P INPUT ACCEPT**

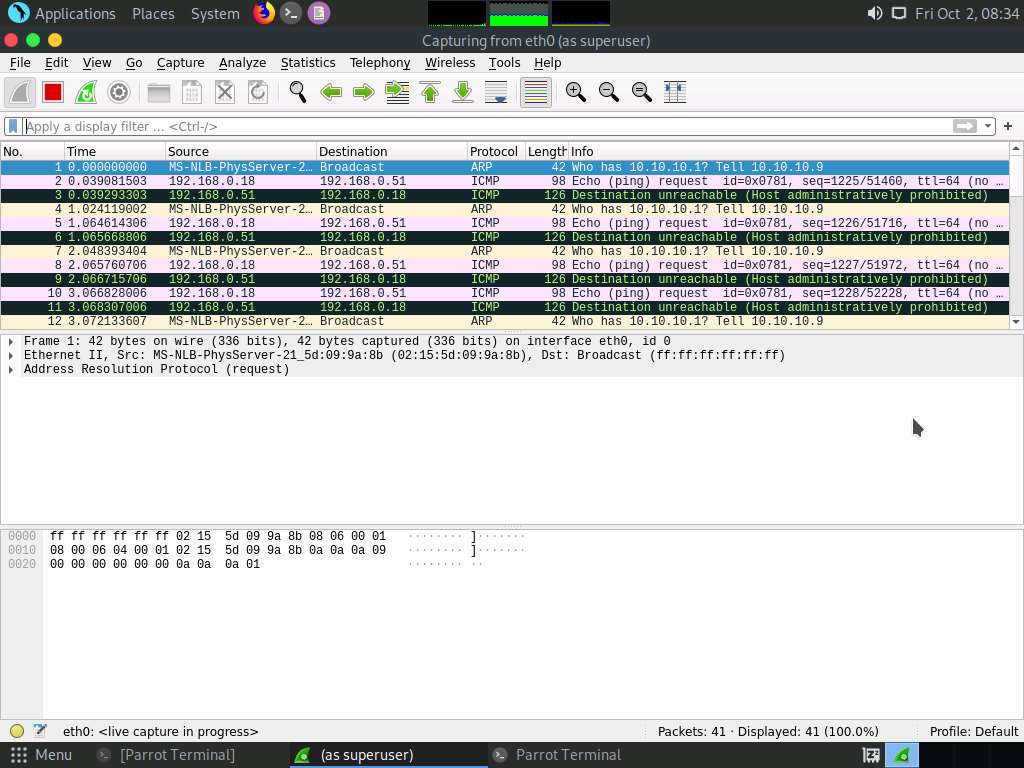


1. Set up something similar to this ACL behavior in the iptables. Type **sudo iptables -A INPUT -j REJECT --reject-with icmp-host-prohibited** and press **Enter**.

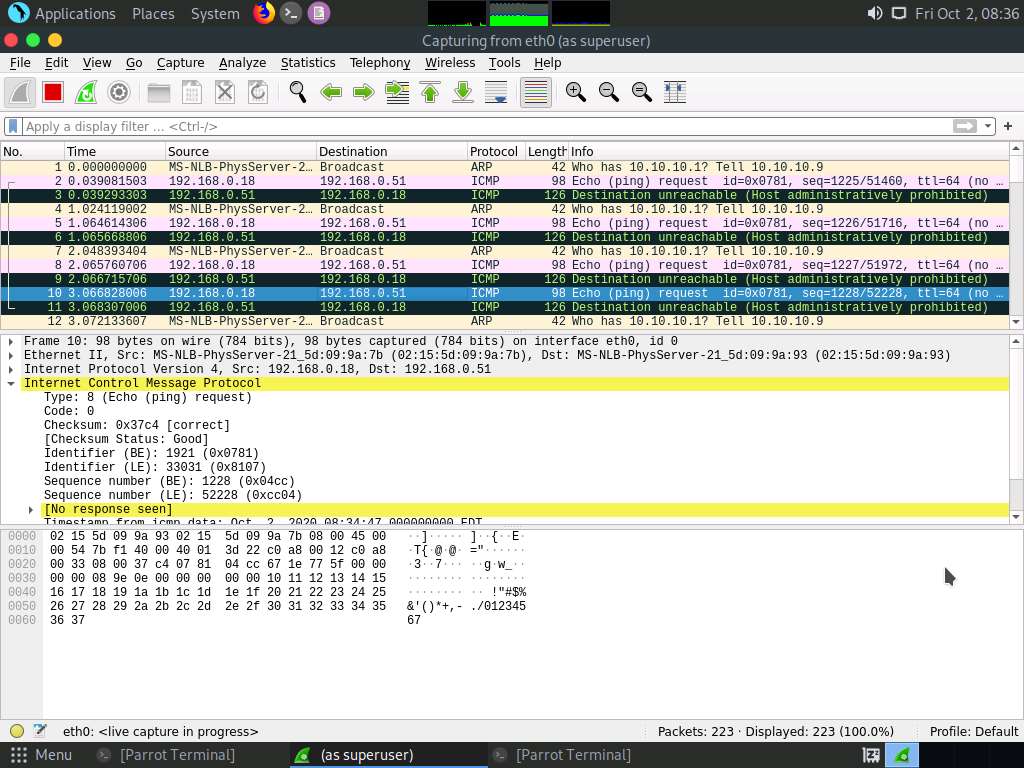


1. Switch to [Parrot](https://labclient.labondemand.com/Instructions/2e9ecc61-2e0e-4b61-931e-5ada85a820dd?rc=10), and maximize the Wireshark and click **Start capturing packets** (Shark Fin Icon) to start the new packet capture. Leave the Wireshark window running.

If Unsaved packets popup appears, click **Continue without Saving**.



1. Conduct the Nmap scan (**nmap -sC 192.168.0.51 -n**), and then review the information in Wireshark.



1. Once a filter is in place, you must determine a method into it (see next lab exercise for the relevant instructions). This concludes the lab exercise. Close all the windows that were opened in both the machines.