Exercise 11: Identify Target System OS with TTL and TCP Window Sizes using Wireshark

Scenario

Identifying the OS used on the target host allows an attacker to figure out the vulnerabilities the system possess and the exploits that might work on a system to further carry out additional attacks.

Attacker can identify the OS running on the target machine by looking at the Time To Live (TTL) and TCP window size in the IP header of the first packet in a TCP session.

Sniff/capture the response generated from the target machine using packet-sniffing tools like Wireshark and observe the TTL and TCP window size fields.

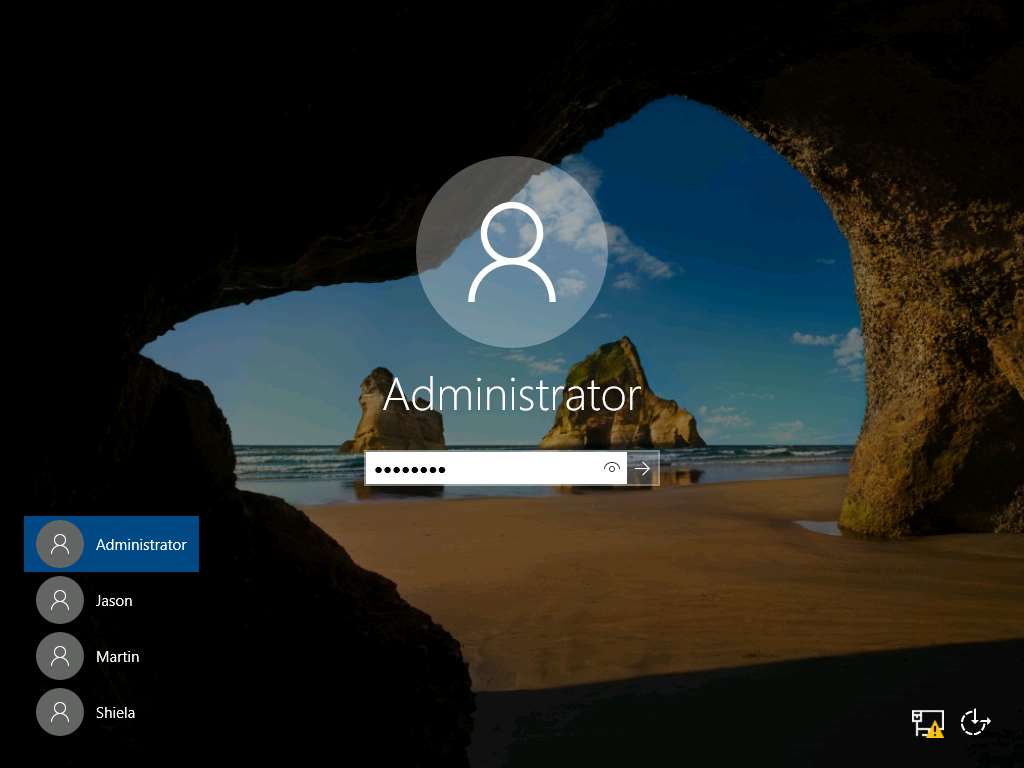
**Lab Duration**: **5** Minutes

1. Click Windows Server 2016 machine, click Ctrl+Alt+Delete link.

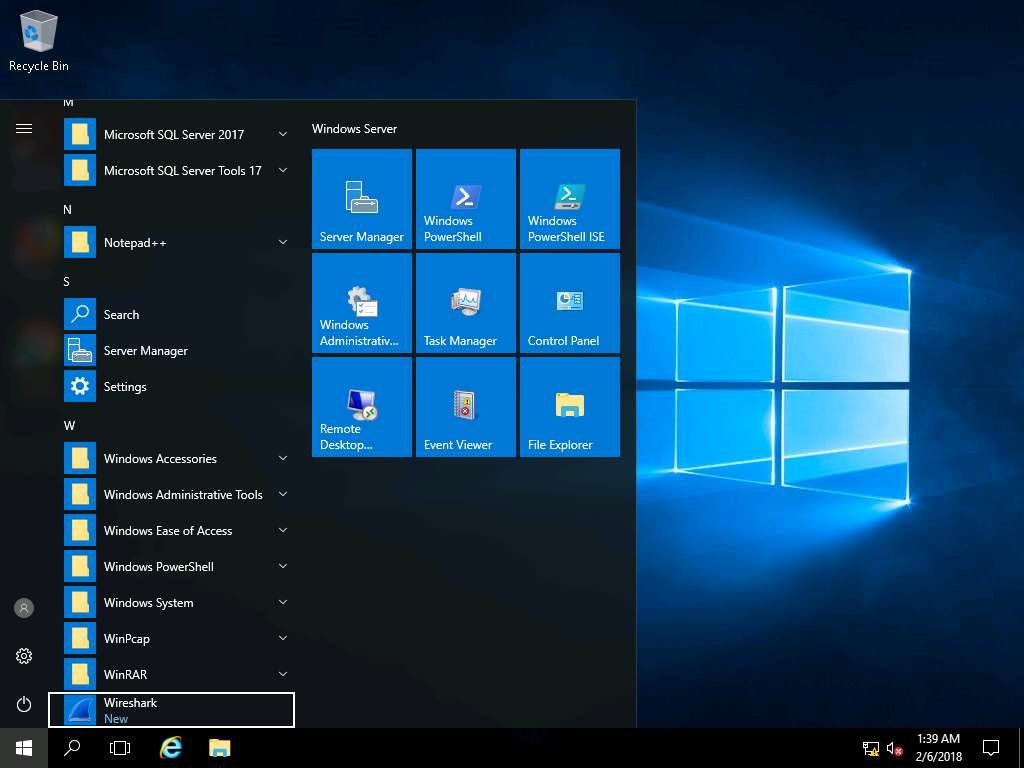
If you are already logged in to the Windows Server 2016 machine, skip to the Step no. 3 of this lab.



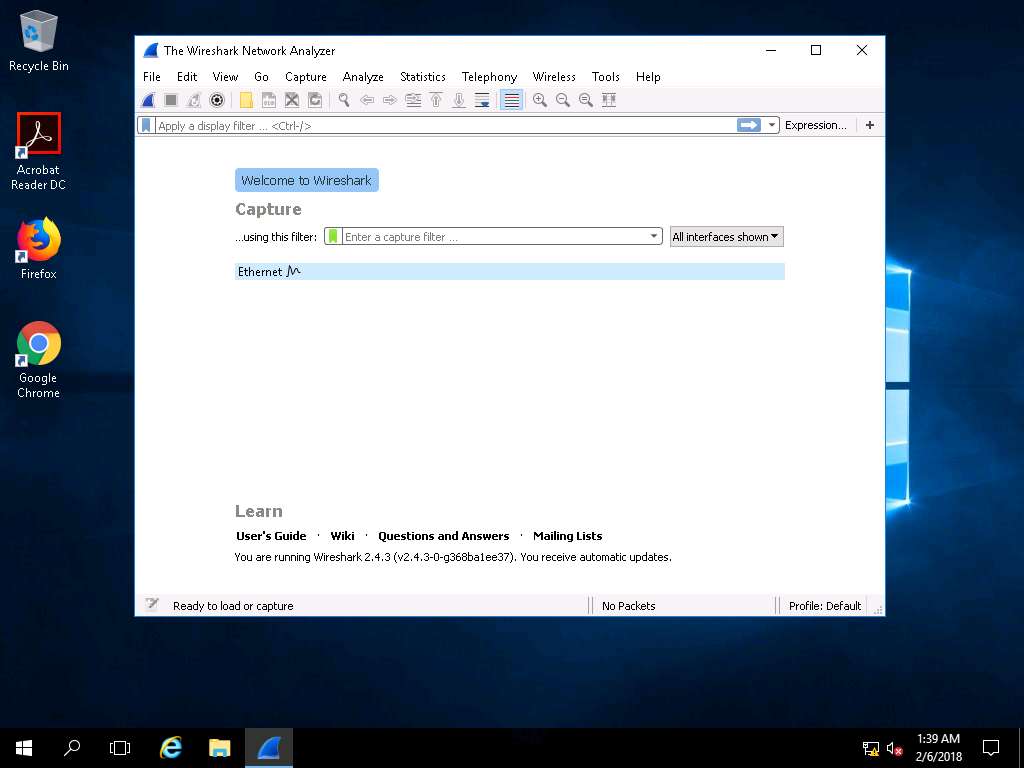
1. By default **Administrator** user account is selected, click Pa$$w0rd and press **Enter** to login.



1. Launch the **Wireshark** application from the **Start** menu.



1. The wireshark main application window appears, double-click on the **Ethernet** interface to start capturing network packets.



1. Now, click Windows 10 machine, click Ctrl+Alt+Delete link.

If you are already logged in to the Windows Server 2016 machine, skip to the Step no. 7 of this lab.



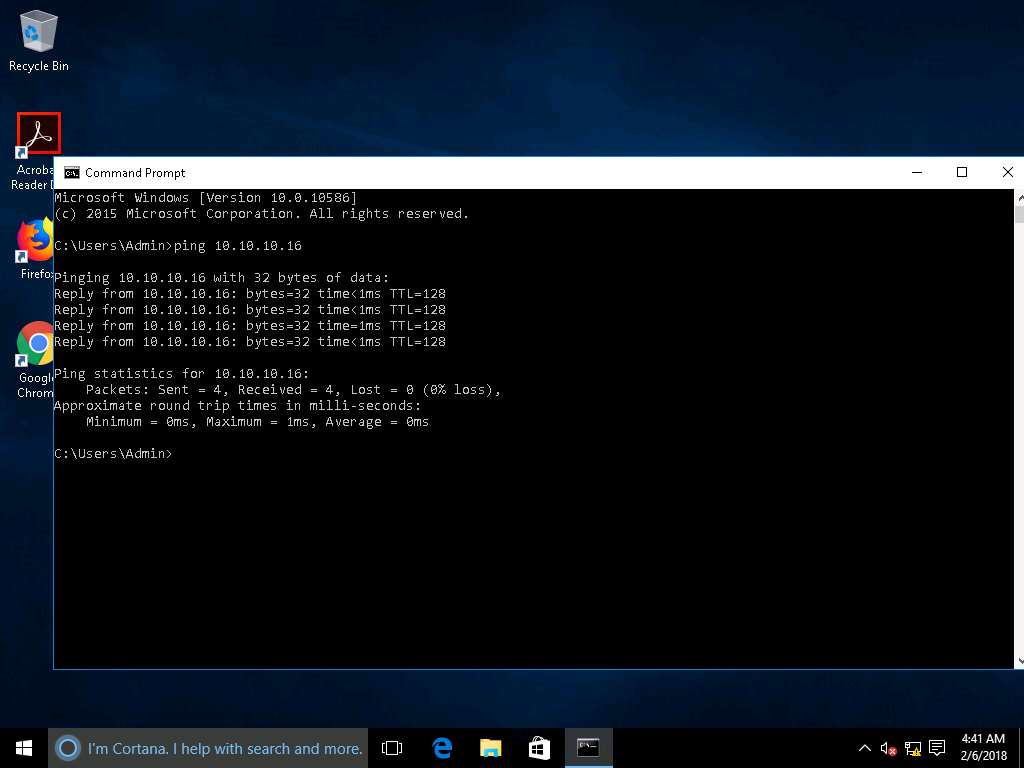
1. By default **Admin** user account is selected, click Pa$$w0rd and press **Enter** to login.



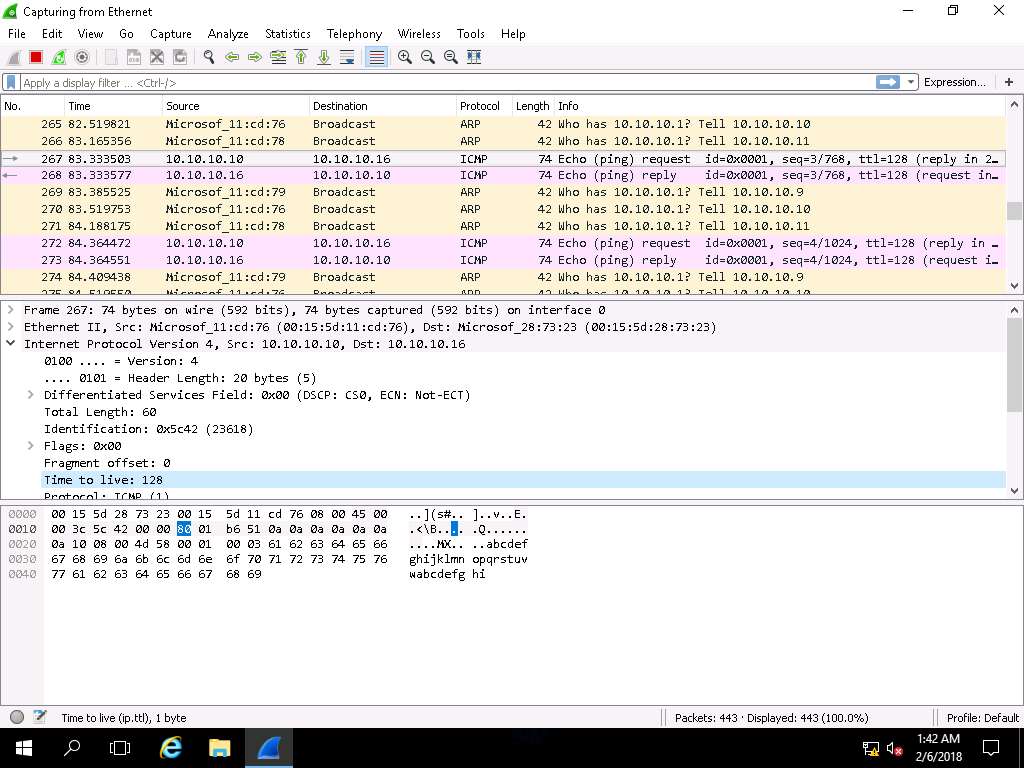
1. **Right-click** the start-menu icon and click **Command Prompt** from the context menu.



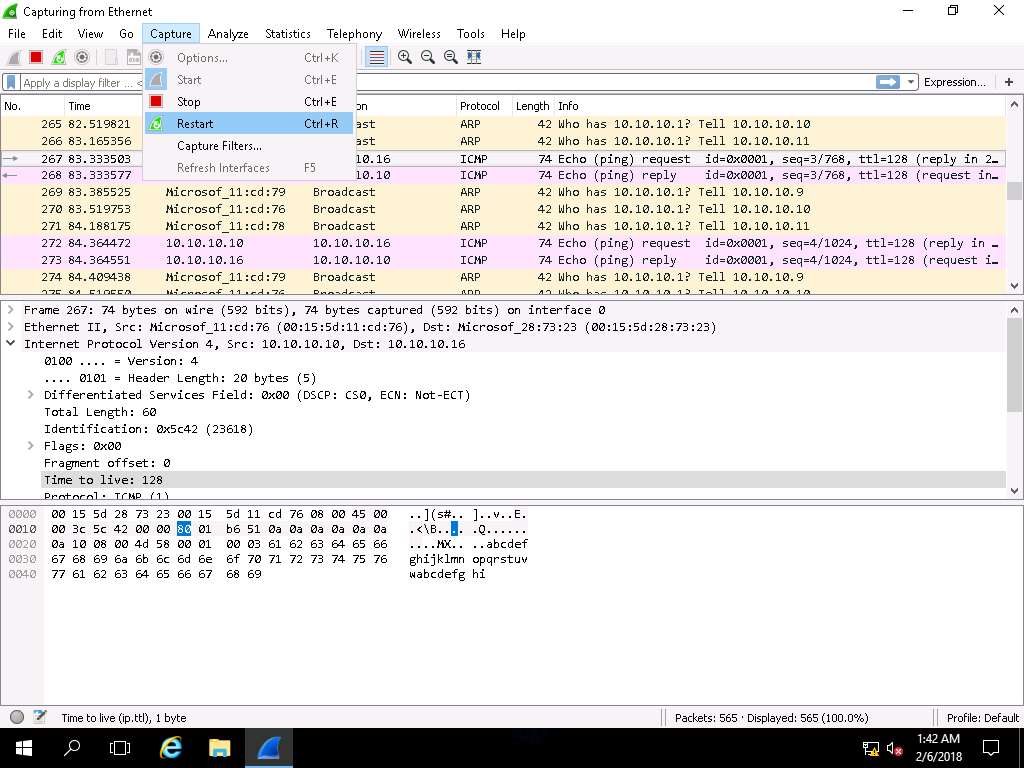
1. In the command prompt window type **ping 10.10.10.16** and press **Enter** to ping the Windows Server 2016 machine.



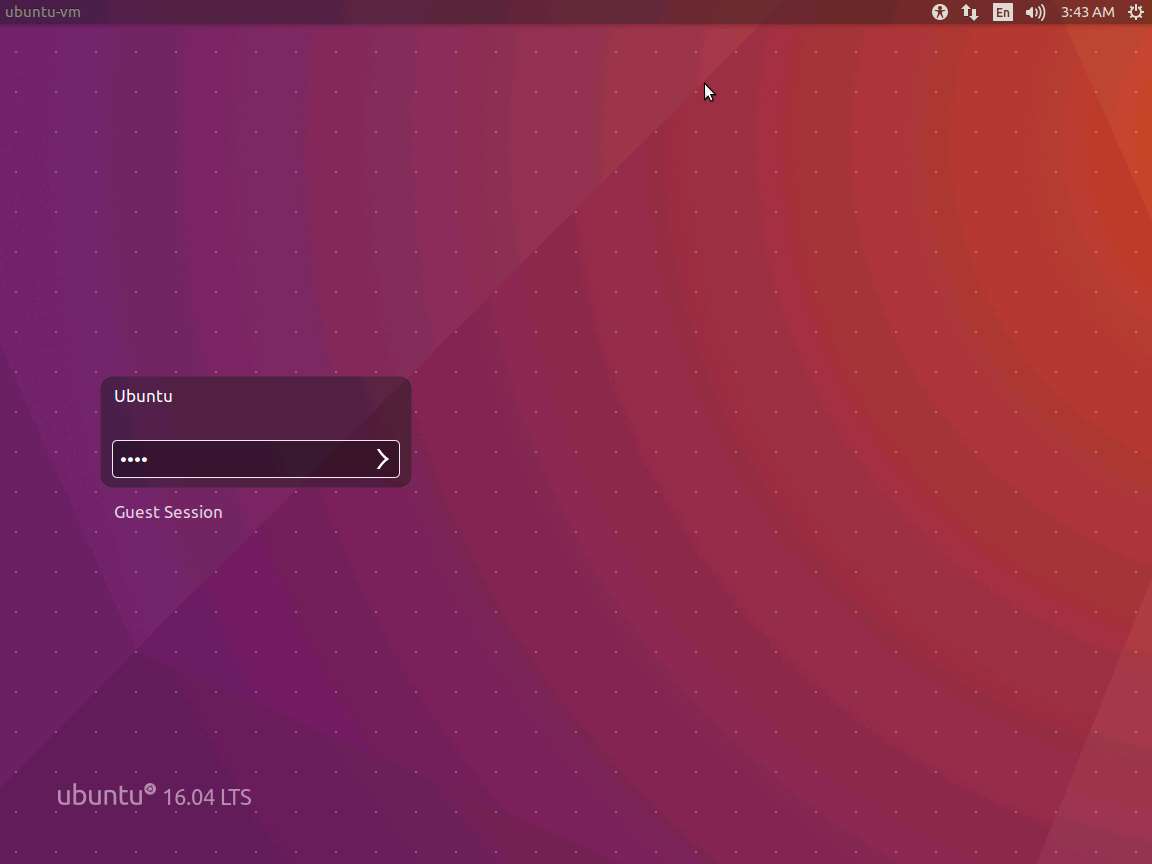
1. Switch back to the **Windows Server 2016** machine and select the **ICMP** packet from windows 10. Expand the **Internet Protocol Version 4** heading in the **Packet Details** pane and note down the **Time to live** value.



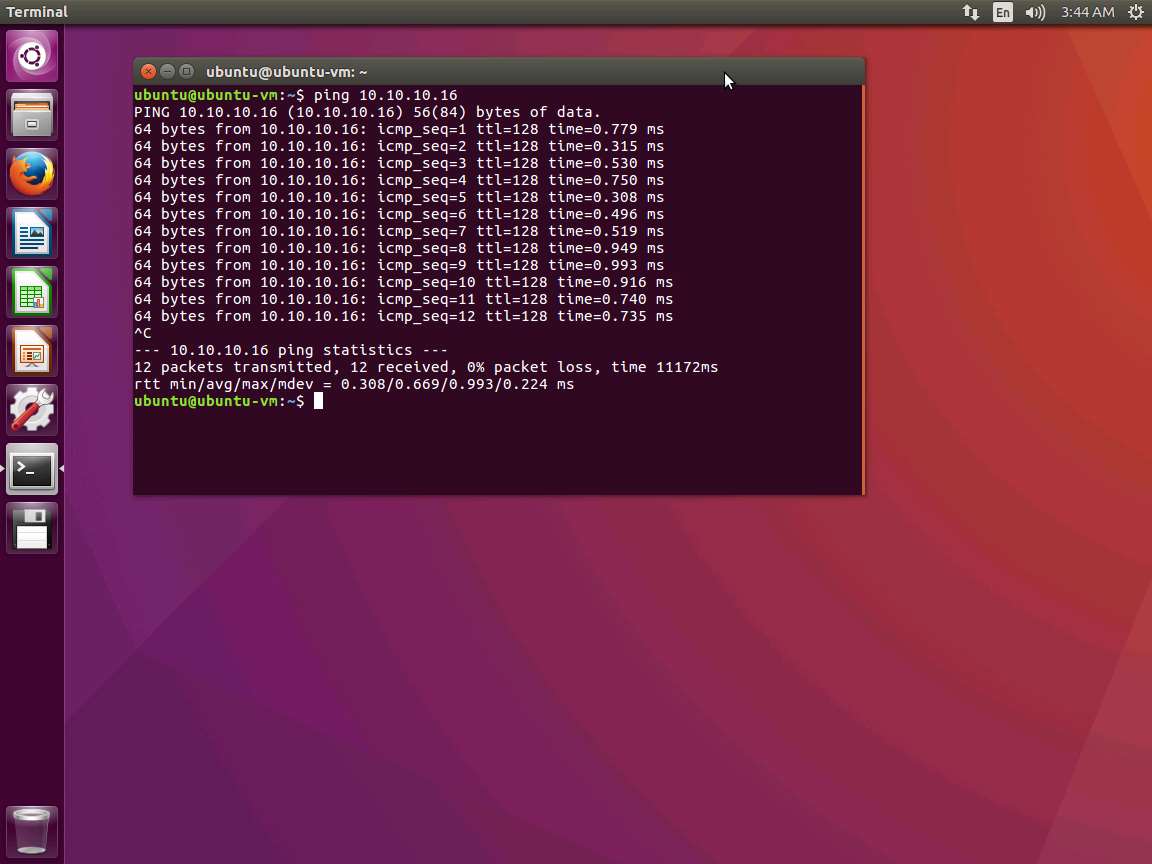
1. Click **Capture--> Restart** from the menu bar. If a prompt appears, click **Continue Without Saving** button.



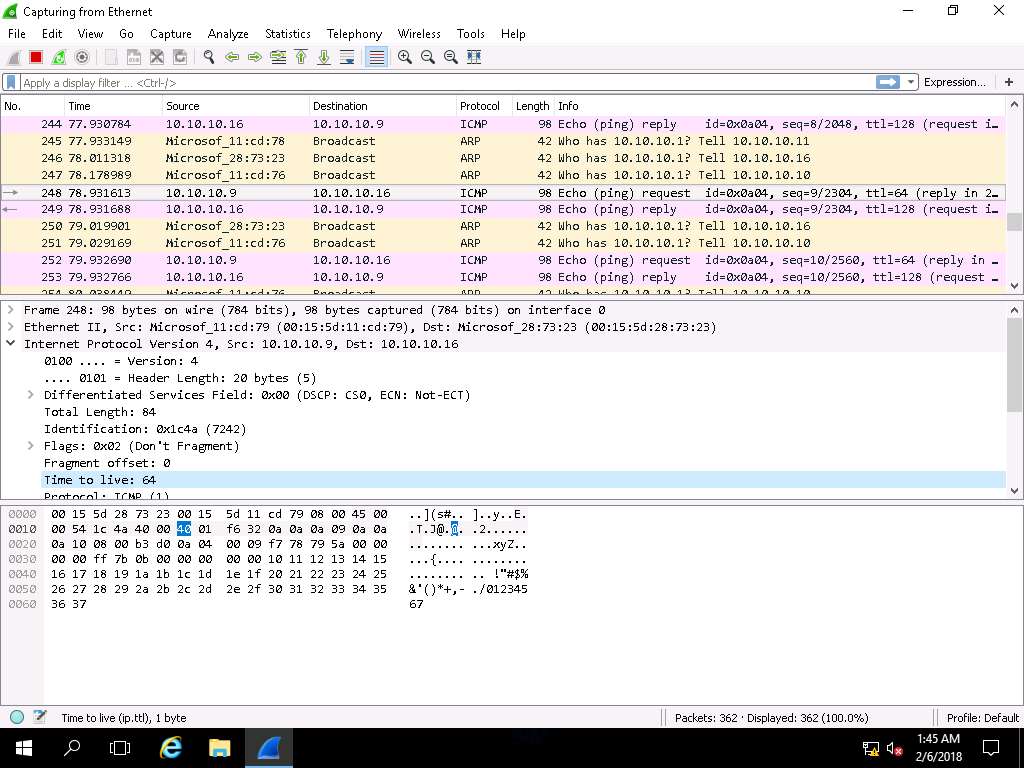
1. Click Ubuntu and type **toor** in the Password field and press **Enter**.



1. In the Ubuntu machine, open a command terminal and type **ping 10.10.10.16** and press **Enter.** After a few packets have been sent press **Ctrl+C** to stop pinging the machine.



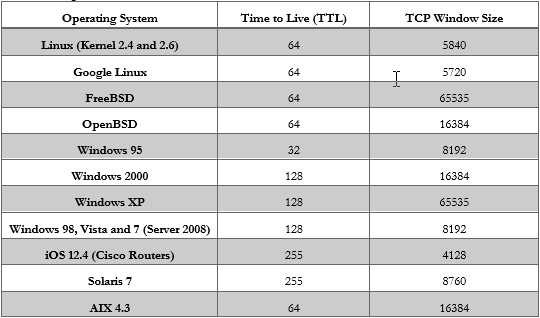
1. Switch back to the **Windows Server 2016** machine, click Windows Server 2016 and select the **ICMP** packet from Ubuntu. Expand the **Internet Protocol Version 4** heading in the **Packet Details** pane and note down the **Time to live** value.



1. Compare the different Time to Live values to identify the OS of the target machines.

Refer to the table in the screenshot for more details.

Close all application windows after the lab is finished.



In this lab you learned how to sniff/capture the response generated from the target machine using packet-sniffing tools like Wireshark and observe the TTL and TCP window size fields to determine the OS of the target machines.