Network Penetration Testing Methodology-Perimeter Devices

1 Hr 38 Min Remaining

**Exercise 2: Identifying and Bypassing a Firewall**

**Scenario**

Attackers are constantly searching for vulnerable clients to penetrate their network through IP spoofing to damage or steal data. The attackers can access packets through a firewall by spoofing the IP address. If attackers are able to capture network traffic, as explained in the previous lab, they can perform Trojan attacks, registry attacks, password hijacking attacks, etc., which can be disastrous for an organization’s network.

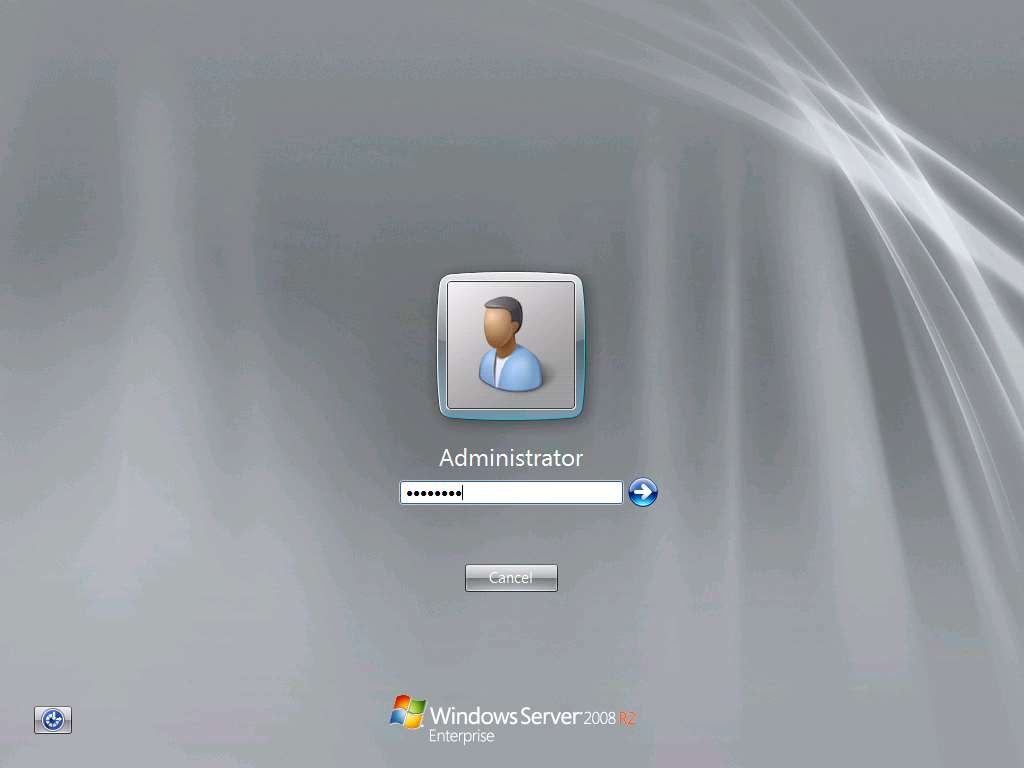
Therefore, as a network administrator you should be able to identify attacks by extracting information from captured traffic such as source and destination IP addresses, protocol type, header length, source and destination ports, etc. and compare these details with modeled attack signatures to detect if an attack has occurred.

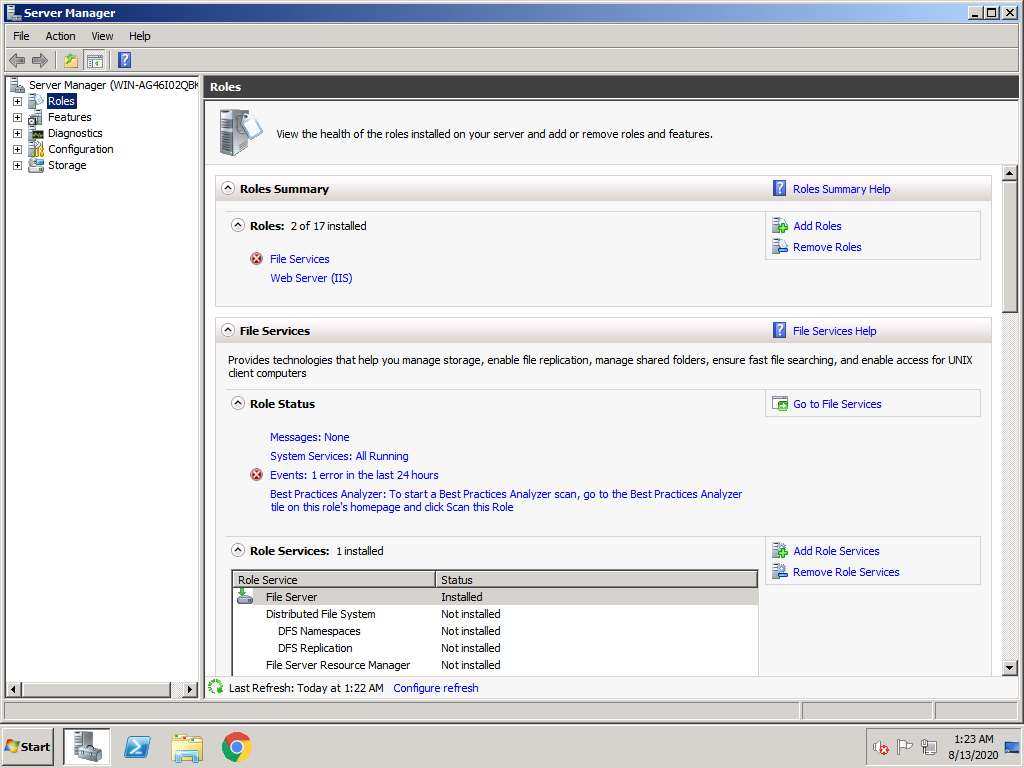
**Lab Duration**: **15** Minutes

1. Click [Web Server](https://labclient.labondemand.com/Instructions/2e9ecc61-2e0e-4b61-931e-5ada85a820dd?rc=10) click [Ctrl+Alt+Delete](https://labclient.labondemand.com/Instructions/2e9ecc61-2e0e-4b61-931e-5ada85a820dd?rc=10).

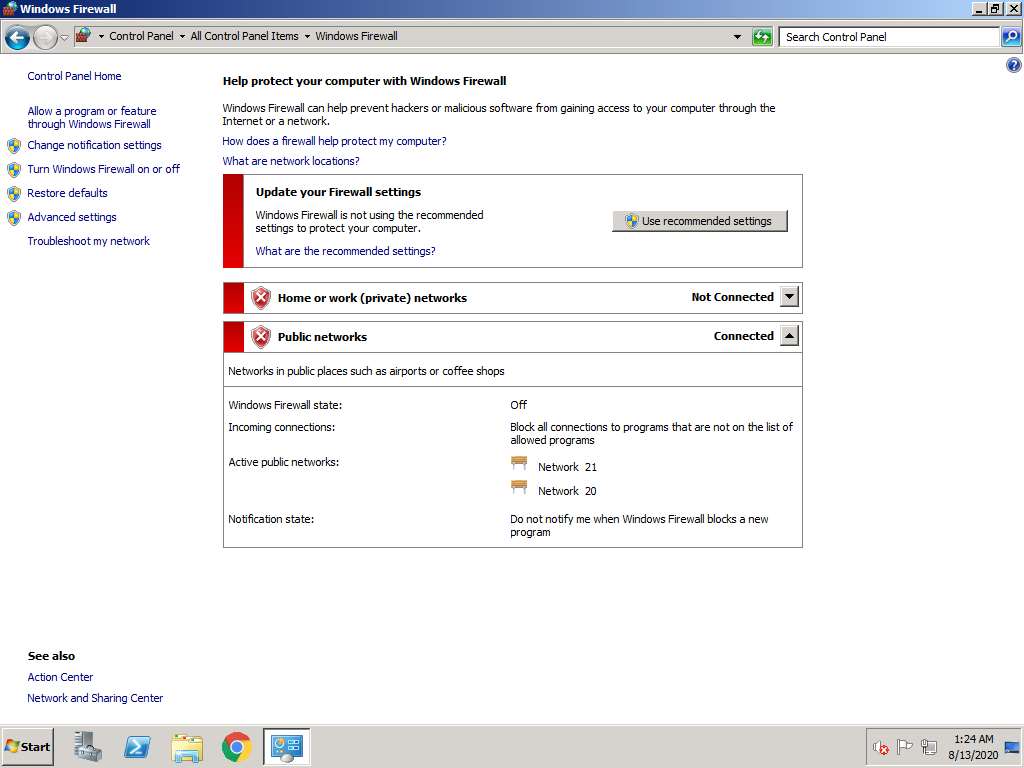


1. In th password field click Pa$$w0rd and click **Login** button or press **Enter**. Close the **Server Manager** window that appears.

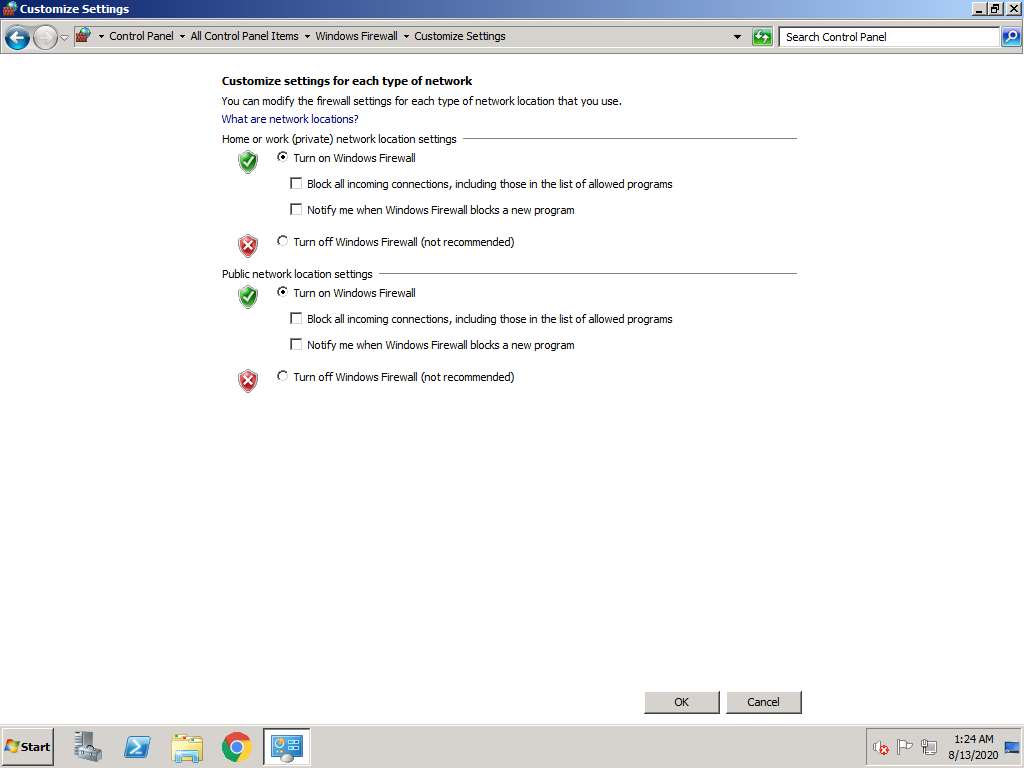




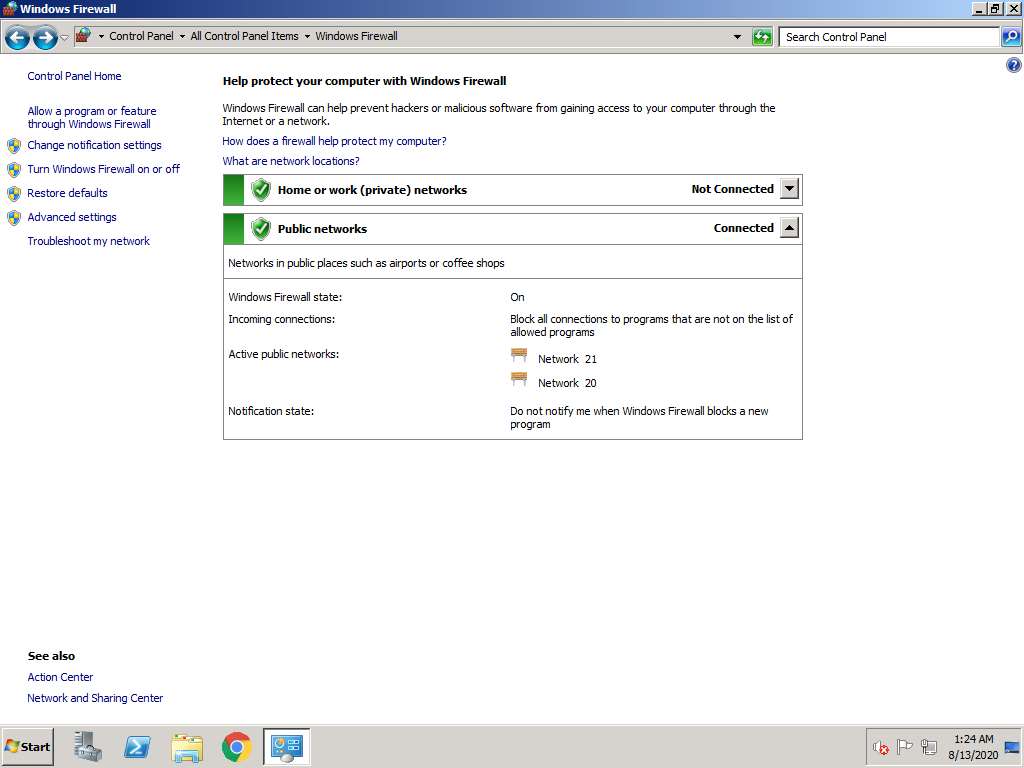
1. Navigate to **Start** menu and click **Control Panel**. Click **Windows Firewall** link in Control Panel. When **Windows Firewall** control panel appears, click **Turn Windows Firewall on or off** in Windows Firewall in the left pane.



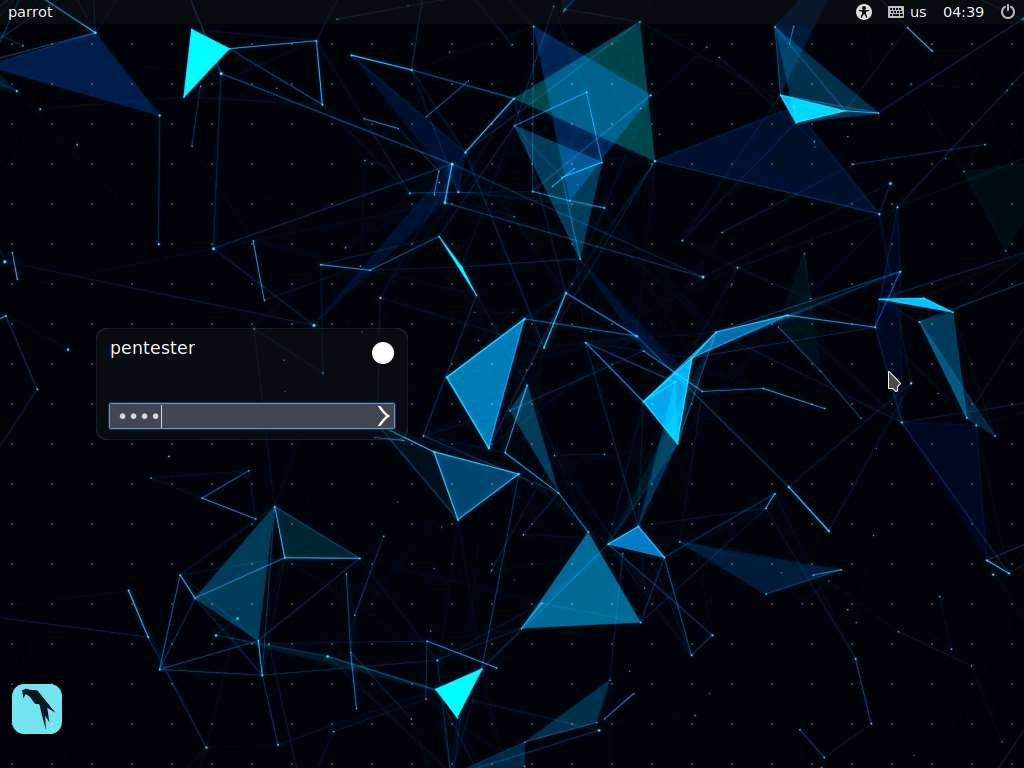
1. Now, to customize the settings of windows firewall, choose **Turn on Windows Firewall** radio button in both network location settings and click **OK**.



1. Now, Windows Firewall is **ON** in **Web Server** machine.

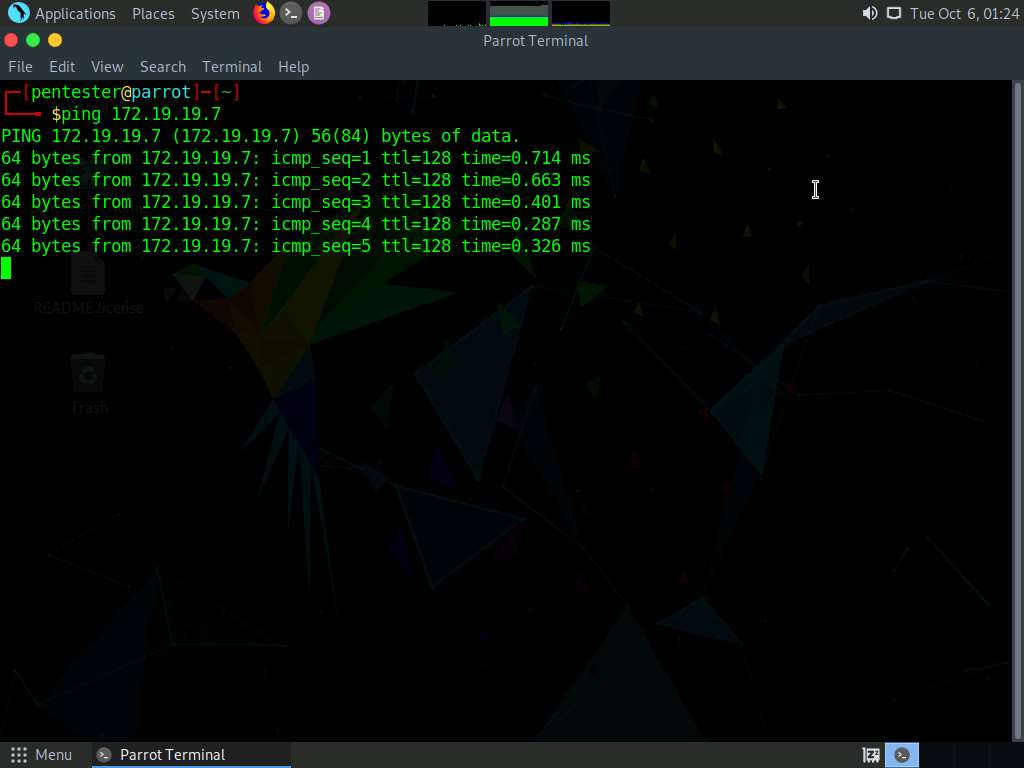


1. Click [Parrot](https://labclient.labondemand.com/Instructions/2e9ecc61-2e0e-4b61-931e-5ada85a820dd?rc=10). Parrot logon screen appears, type **toor** in the Password field and press **Enter**.



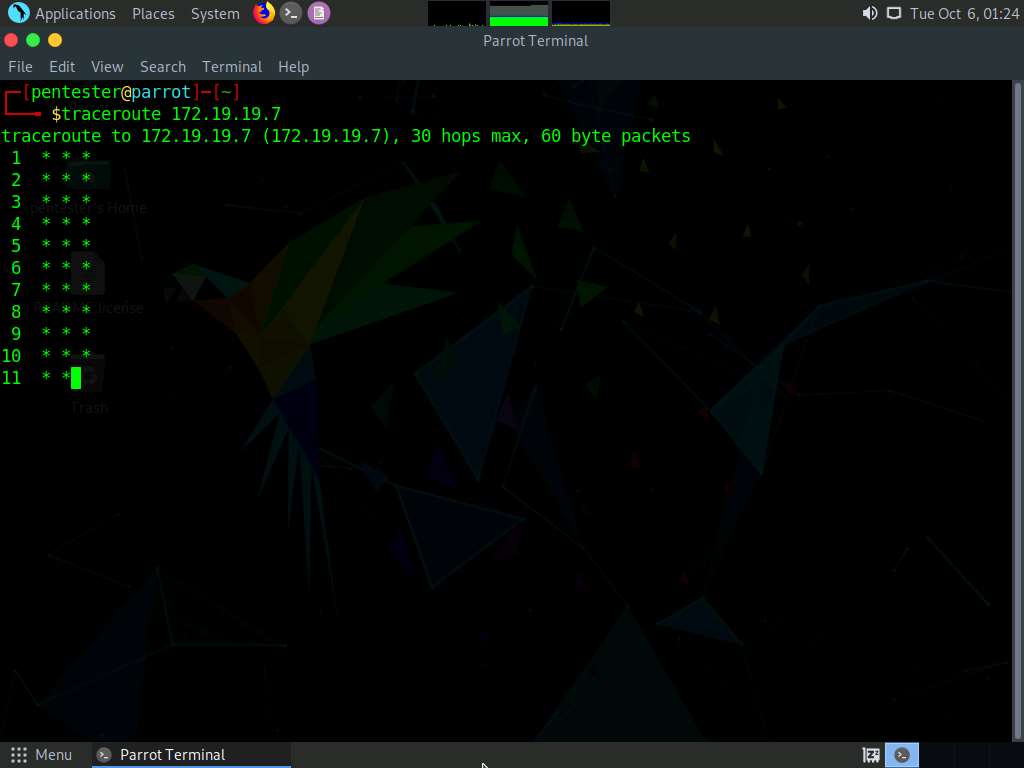
1. Click **Terminal** icon from the taskbar to launch.
2. Now check the connectivity between the Attacker Machine (**Parrot**) and the Victim Machine (**Web Server**). To check, type **ping 172.19.19.7** in the terminal and press **Enter**. If the ping is successful, meaning the remote machine is replying with 64 bytes of memory, then press **Ctrl+C** to stop pinging the machine.

Ping command is not enough to bypass the travel packets between two machines.

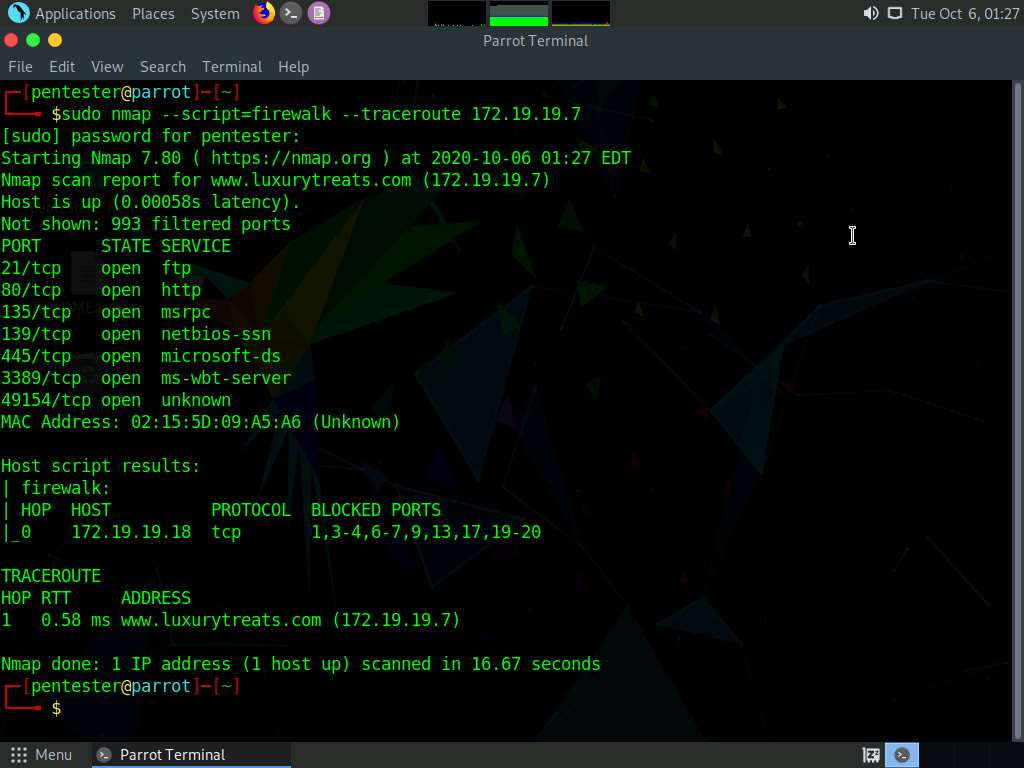


1. Now perform traceroute to the victim's machine, now launch another command terminal window and type **traceroute 172.19.19.7** and press **Enter**. After performing traceroute, no results will be displayed as **Windows Firewall** is turned on as shown in the screenshot below: Press **Ctrl+C** on the keyboard to stop the traceroute command.

Traceroute command will track the packet travelling between two machines.



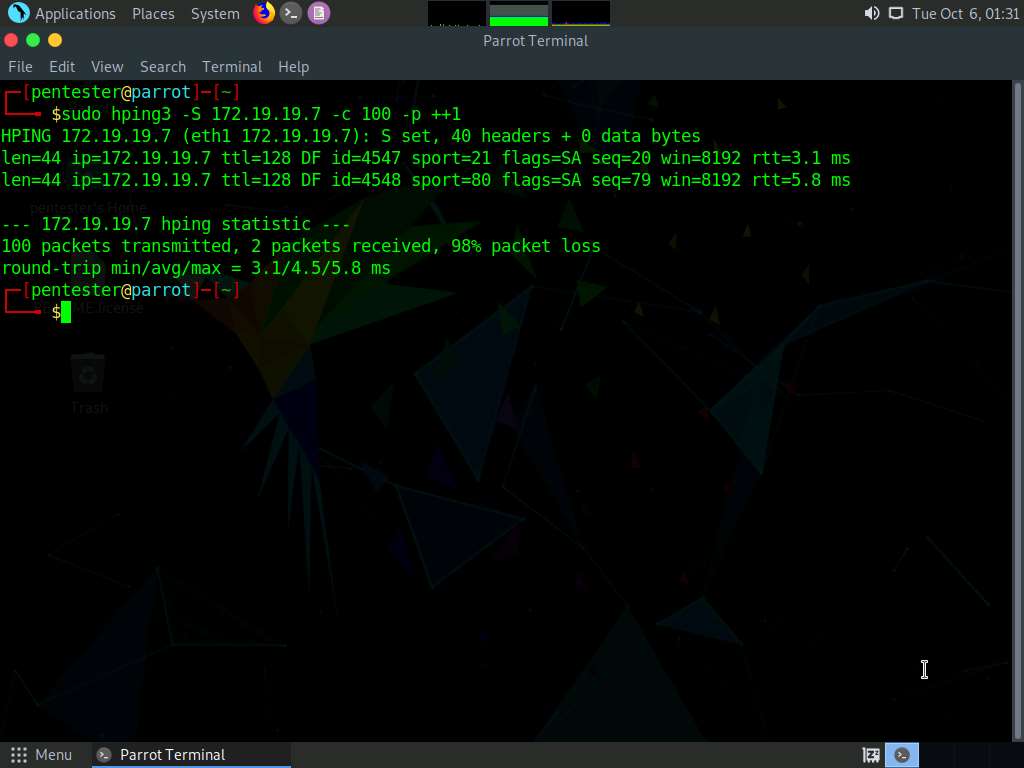
1. Now, type following command **sudo nmap --script=firewalk --traceroute 172.19.19.7** and press **Enter**, type **toor** and press **Enter** when prompted for Password. This command will check for the open ports on the target machine, as shown in the screenshot. This displays open ports on the victim's machine, filtered ports under Host script results, and Traceroute details.



1. Now, type **sudo hping3 -S 172.19.19.7 -c 100 -p ++1** and press **Enter** type **toor** and press **Enter** if prompted for Password. Hping begins to ping each port in incremental order till port **100** and displays the response packets for the ports that respond to the requests. In hping statistic, you can see out of **100** packets only **2** packets are transmitted to victim’s machine and the rest 98 packets’ transfer fails. The **2** packets which passed through the firewall from port **21** and **80** and other packets are filtered by the firewall. You can use these two open ports to perform your penetration testing.

The scan takes about 5 minutes to finish.

-S switch is for setting SYN TCP flag.



1. Close all the windows.

In this lab you have learned how to Identify and Bypassing firewall.