Network Penetration Testing Methodology-Internal

6 Hr 43 Min Remaining

Instructions Resources Help  100%

Exercise 5: Performing Passive OS Fingerprinting to Obtain Remote Operating System Information

Scenario

Active OS fingerprinting involves sending a packet to the designated system in a network and examining the response to identify the operating system. Passive OS fingerprinting, in contrast to active OS fingerprinting, is the process of identifying the operating system by inspecting the initial Time To Live (TTL) in the IP header and the TCP window size (the size of the receive window) of the first packet sent from a host in TCP session, i.e. the SYN or SYN+ACK packet.  
As a penetration tester, you need to have knowledge of how to perform passive OS fingerprinting in a network.  
In this lab, you will learn how to perform passive OS fingerprinting using p0f tool.

**Lab Duration**: **15** Minutes

1. Click [Parrot](https://labclient.labondemand.com/Instructions/52f4d542-434e-4a10-8f51-0c2b8ca1d32b?rc=10). Parrot lock screen appears.



1. By default **pentester** is selected as the **user**. Type **toor** in the Password field and press **Enter**.

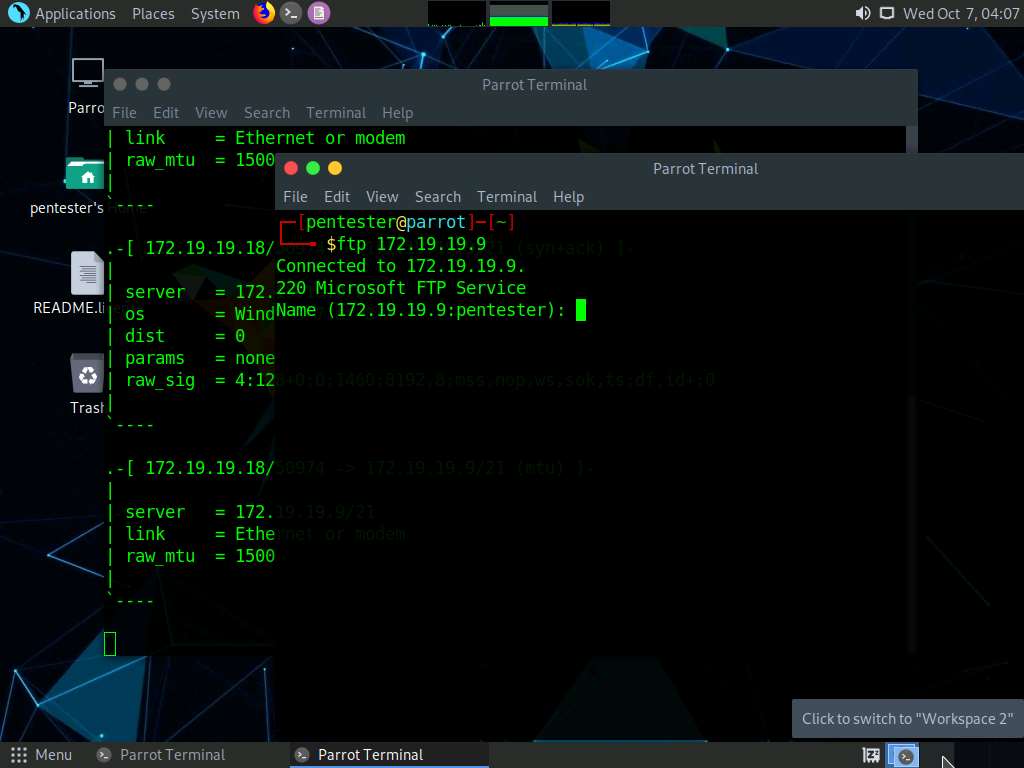


1. In this lab, we will try to retrieve operating system related information from a machine hosting an FTP server, using a tool named **p0f**.
2. Now, launch a command line terminal, type **sudo p0f -i any -p -o /tmp/sniff.log** and press **Enter**. Type **toor** and press **Enter** when prompted for password. **p0f** begins to listen on all the interfaces of Parrot, and whenever it captures a packet, it decodes the header information and guesses the operating system.
   1. The **-i** switch corresponds to the interface
   2. By setting the **-p** switch, we are setting the tool to run in promiscuous mode.
   3. We are setting the **p0f** tool to store the output (**-o**) in **/tmp** location inside a file named **sniff.log**.

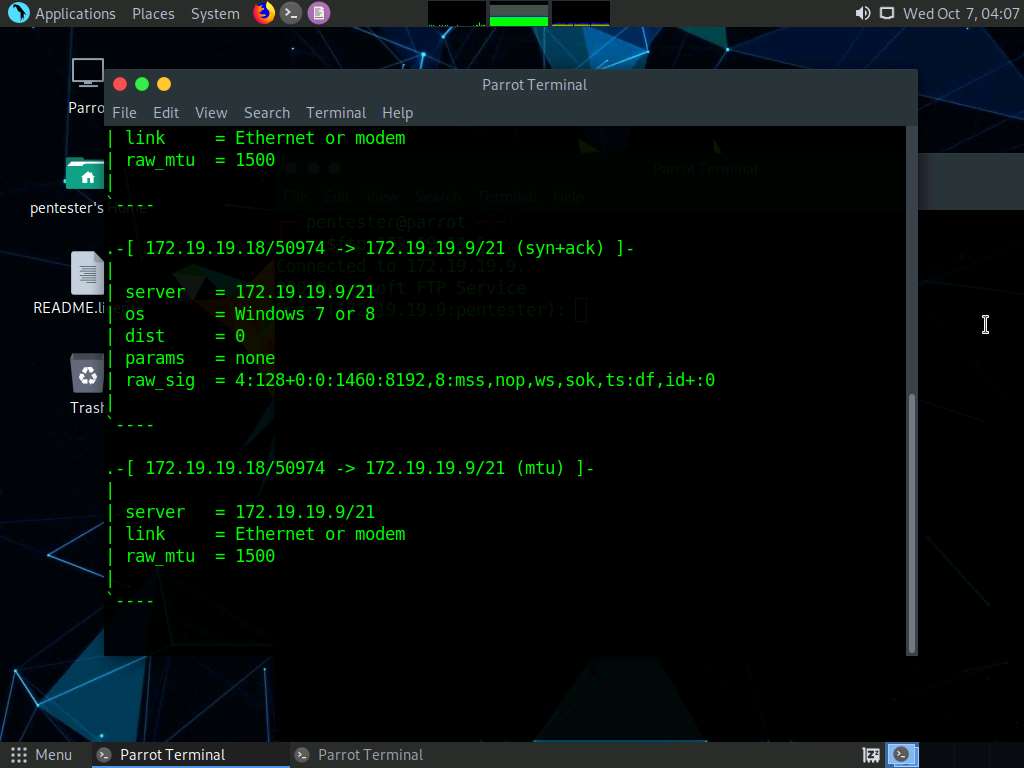


1. Now, launch another command line terminal, type **ftp 172.19.19.9** and press **Enter**. This will ask you to enter login credentials. By doing so, the client i.e., Parrot machine will send the request and the machine hosting the FTP server will respond to the query.

**172.19.19.9** is the IP address of the machine hosting the FTP server.



1. Switch to the command line terminal where p0f is running and scroll up the window. You will observe that p0f has analyzed all the requests and responses and decoded them to display information such as **OS**, **raw signature** and **raw mtu**. In this lab, p0f identified the operating system as **Windows 7 or 8** (or its equivalent). Scroll down the window to view the header information of each packet decoded by the tool.



Thus, you have learned how to perform passive OS fingerprinting using p0f tool.