Network Penetration Testing Methodology-Perimeter Devices

1 Hr 36 Min Remaining

**Exercise 5: Proxychains**

**Scenario**

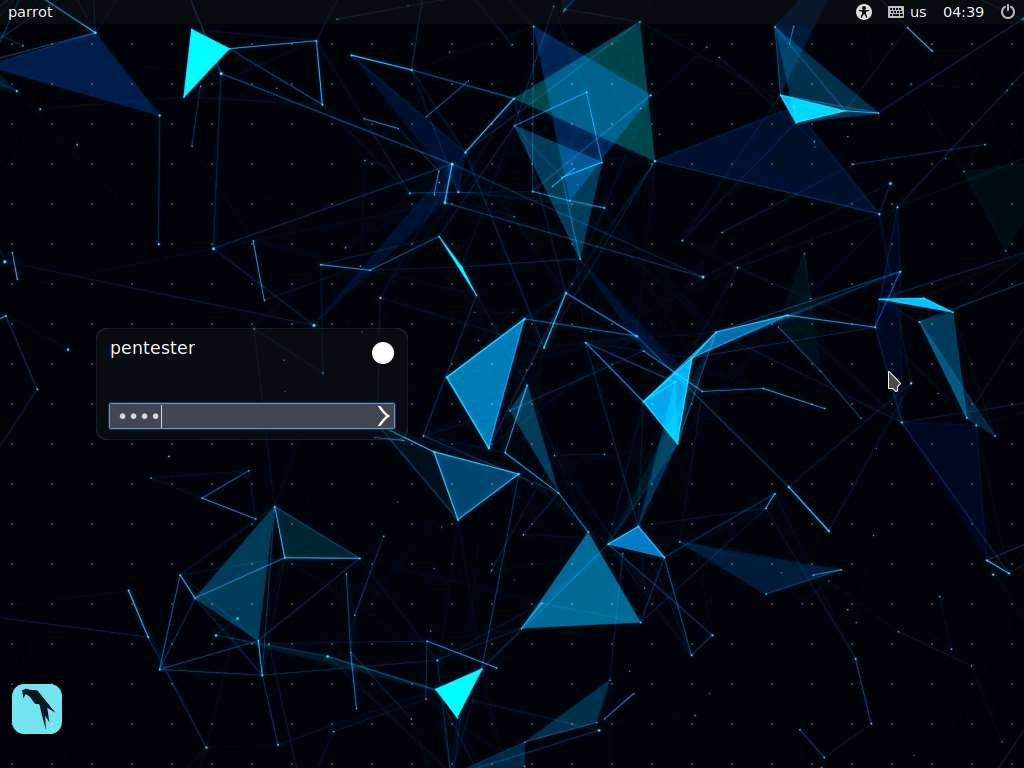
In this lab, you will:

* Use proxychains to conduct a scan

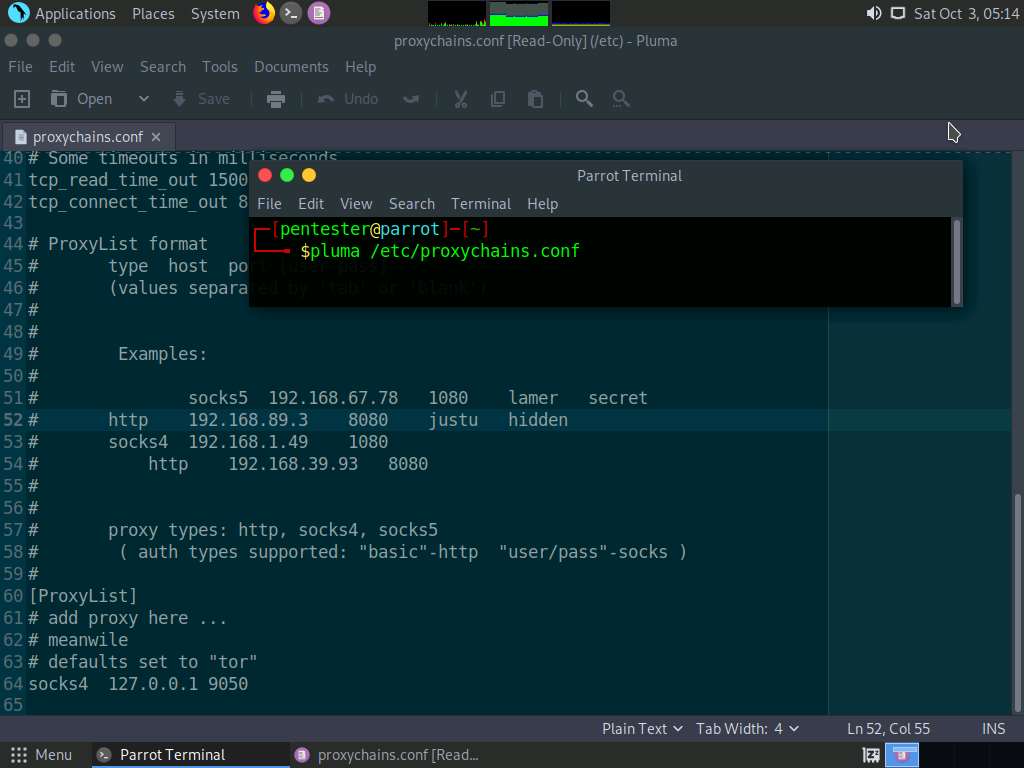
**Lab Duration**: **10** Minutes

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**.

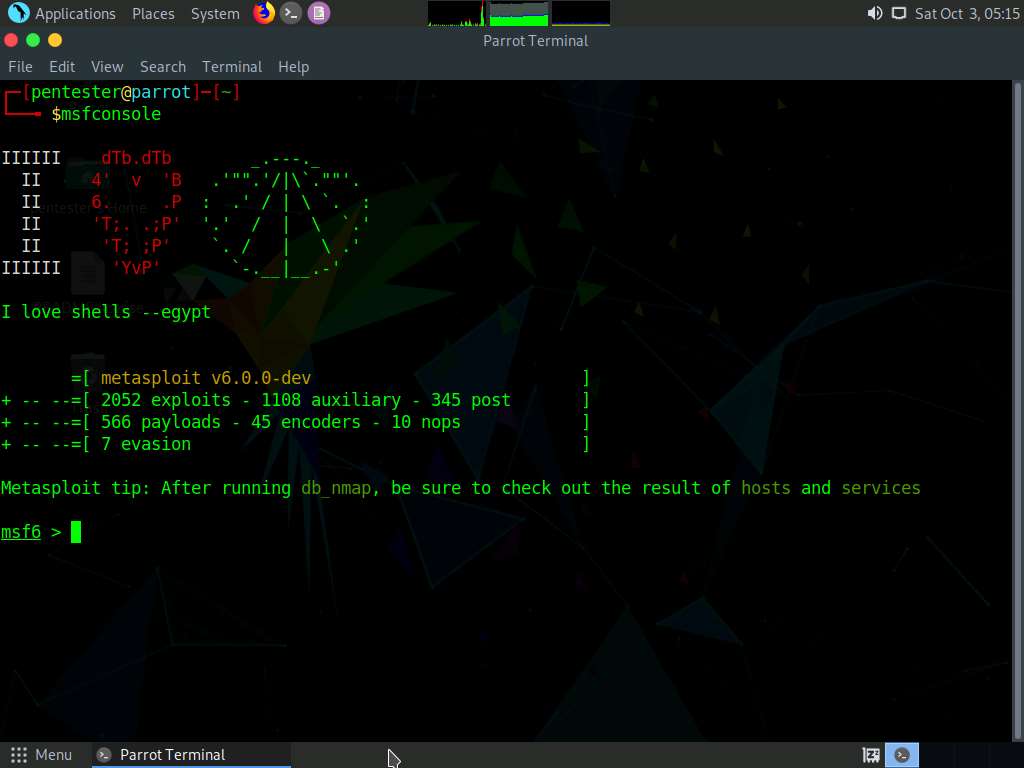
If you are already logged in skip to **step 2**.



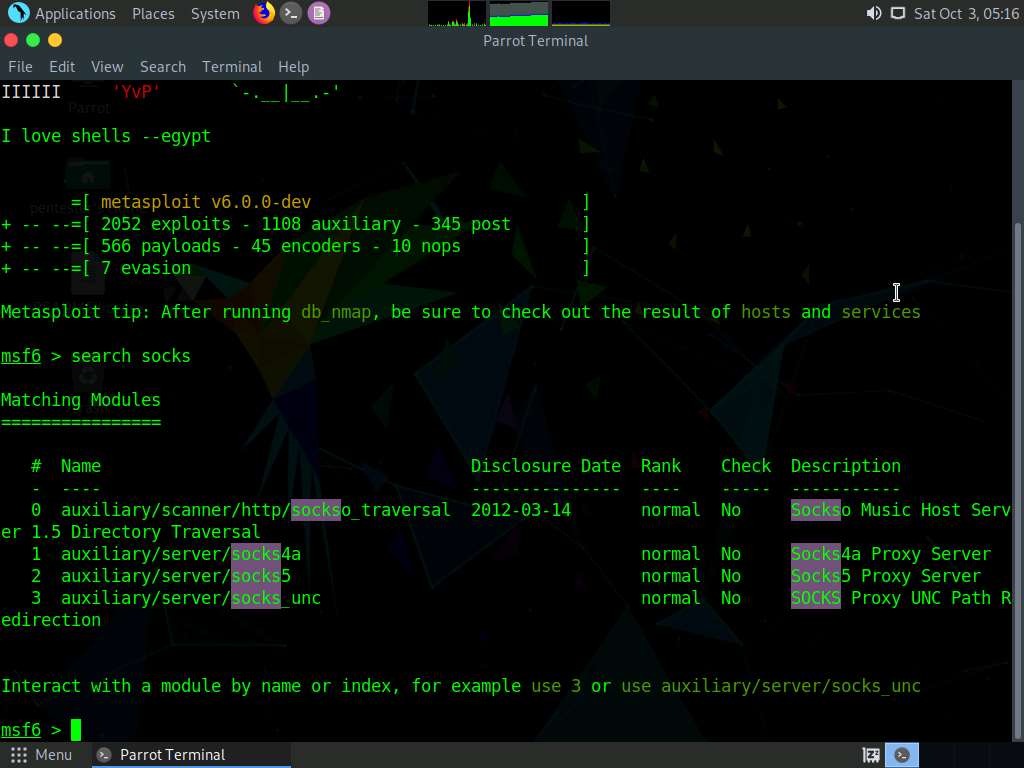
1. Launch a terminal window, type **pluma /etc/proxychains.conf**, and press **Enter**. Carefully review the information and note the configuration at the bottom. Although this serves our purpose for the lab, you may add more information to the file. Close the text editor window.



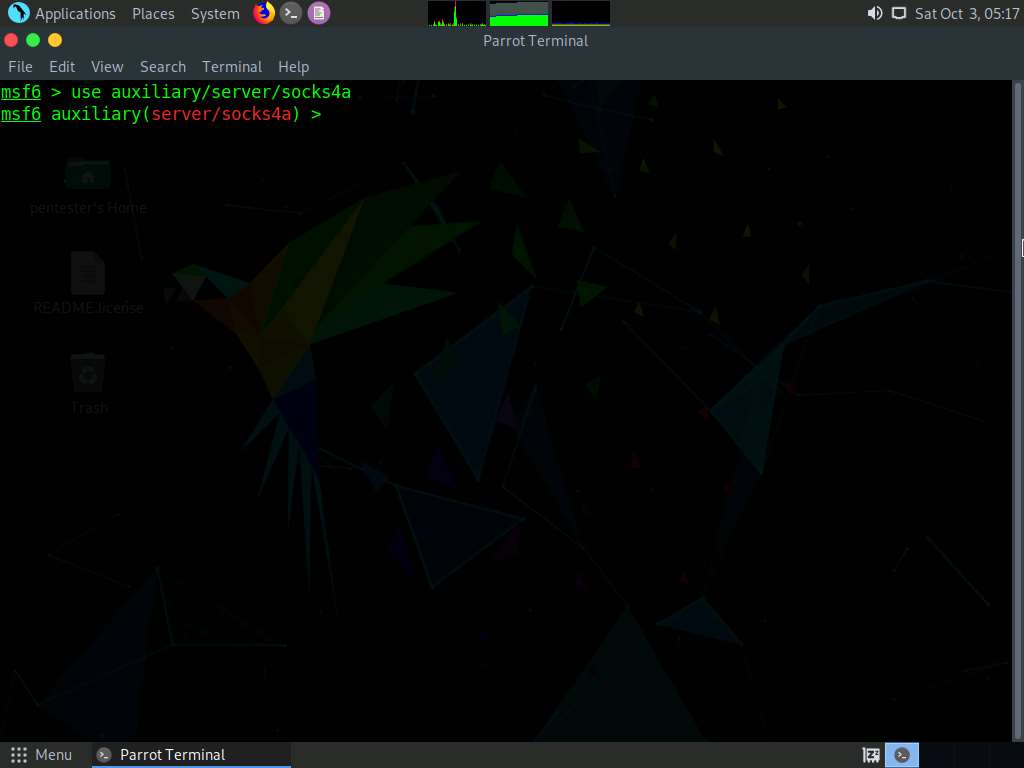
1. In the terminal window type **msfconsole** and press **Enter** to launch Metasploit Framework.



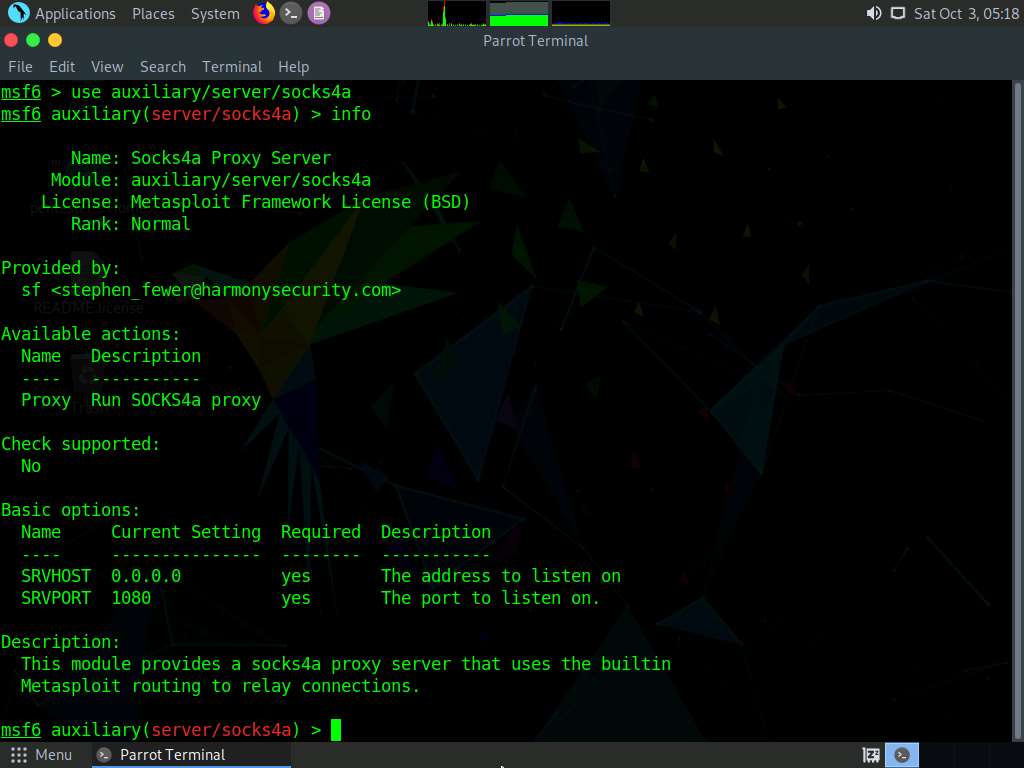
1. In the msfconsole type **search socks** and press **Enter**.



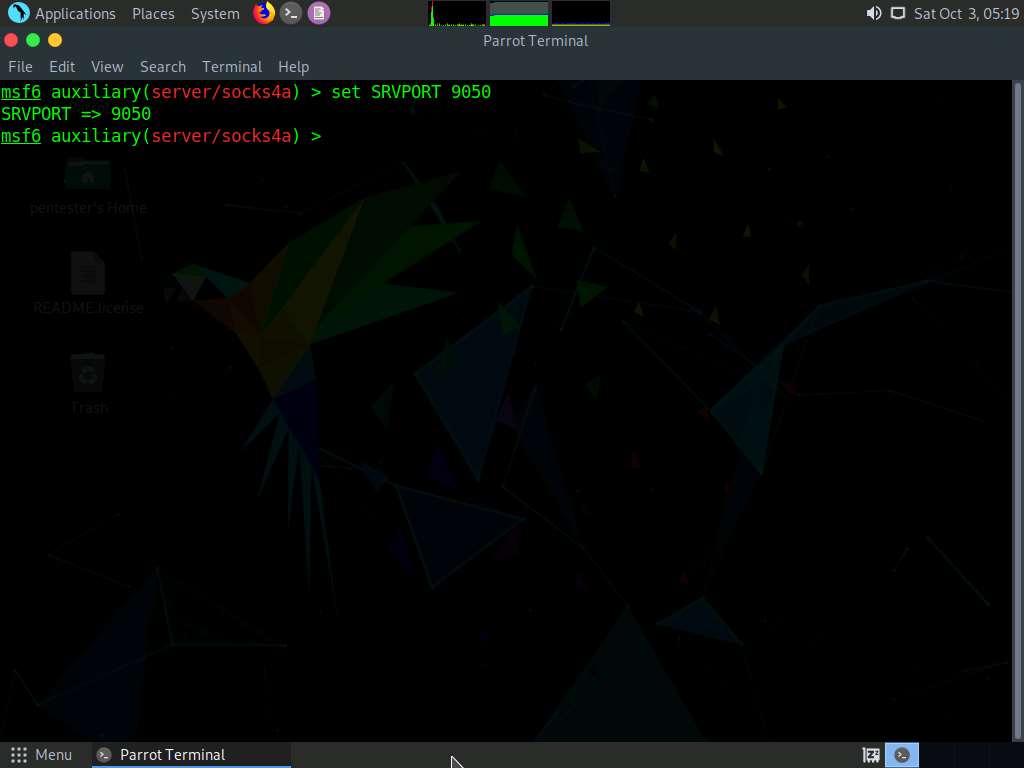
1. Select the server; type **use auxiliary/server/socks4a** and press **Enter**.



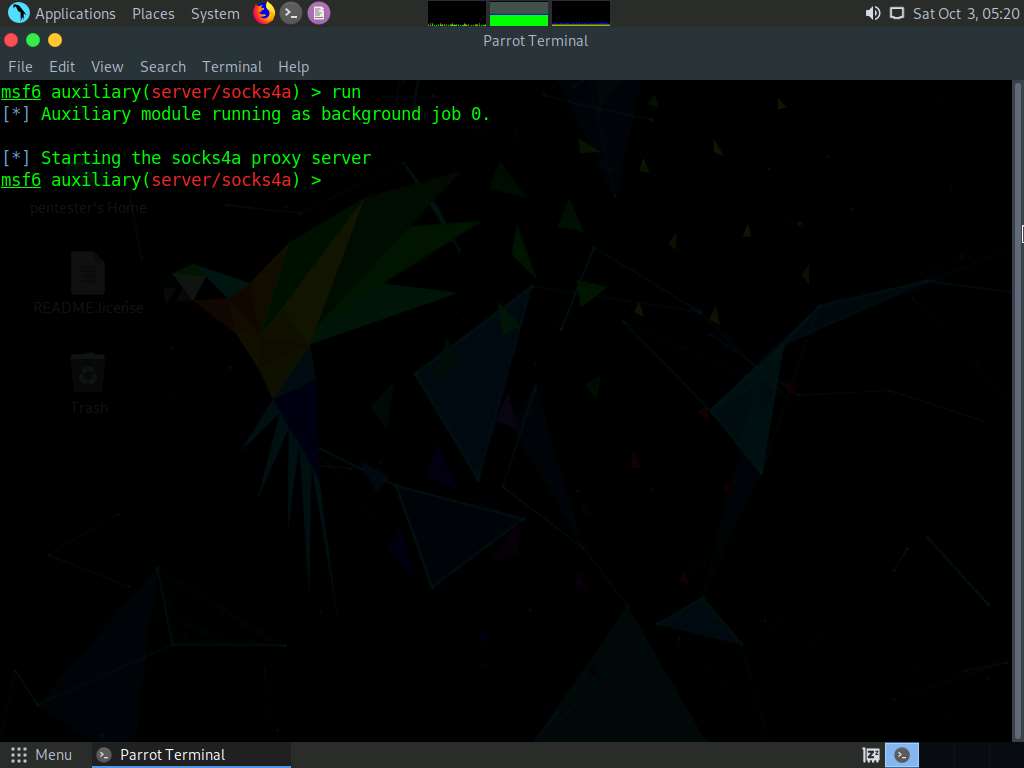
1. Once the module is loaded, type **info** and press **Enter** to read about the module.



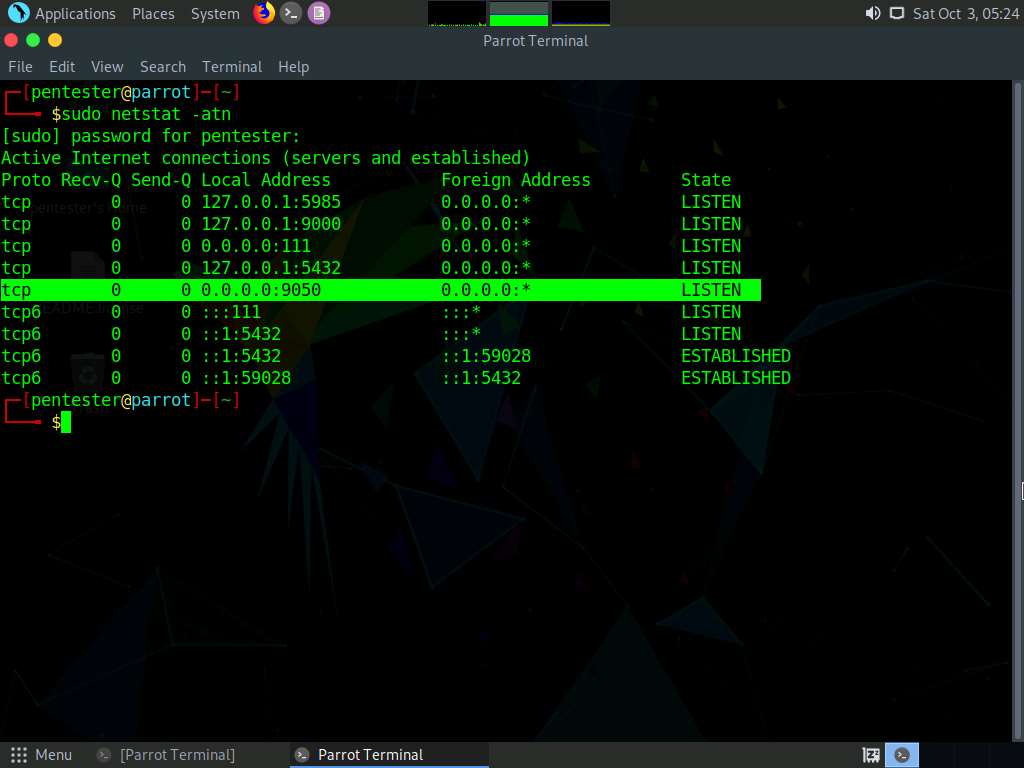
1. To set up the port, type **set SRVPORT 9050** and press **Enter**.



1. Type **run** and press **Enter** to run the server.



1. To verify whether Server is running or not, open a new terminal window and type **sudo netstat -atn** and press **Enter** type toor and press Enter when prompted for password. You should see the port open and listening.



1. Run **proxychains**, type **sudo proxychains nmap -sT 192.168.0.51** and press **Enter**.

192.168.0.51 is the IP address of the **RPC Server Ubuntu** machine.

