Network Penetration Testing Methodology-Internal

6 Hr 42 Min Remaining

Instructions Resources Help  100%

Exercise 7: Scanning with DMitry

Scenario

To begin the lab, a proficient tester may use any tool depending on his or her personal preference. The objective of this lab is to help students use the DMitry tool. The following activities are included in this lab:

• Start the DMitry tool

• Setup the network environment

• Scan and review the data from the DMitry tool

**Lab Duration**: **5** Minutes

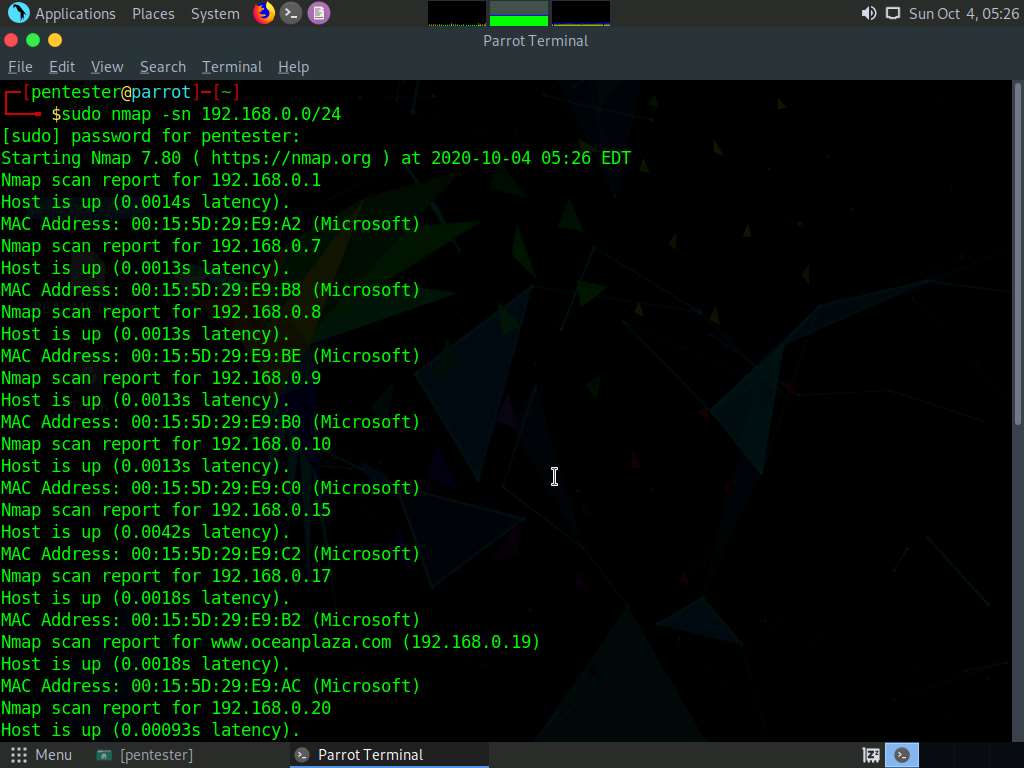
1. Click [Parrot](https://labclient.labondemand.com/Instructions/52f4d542-434e-4a10-8f51-0c2b8ca1d32b?rc=10). Parrot lock screen appears.



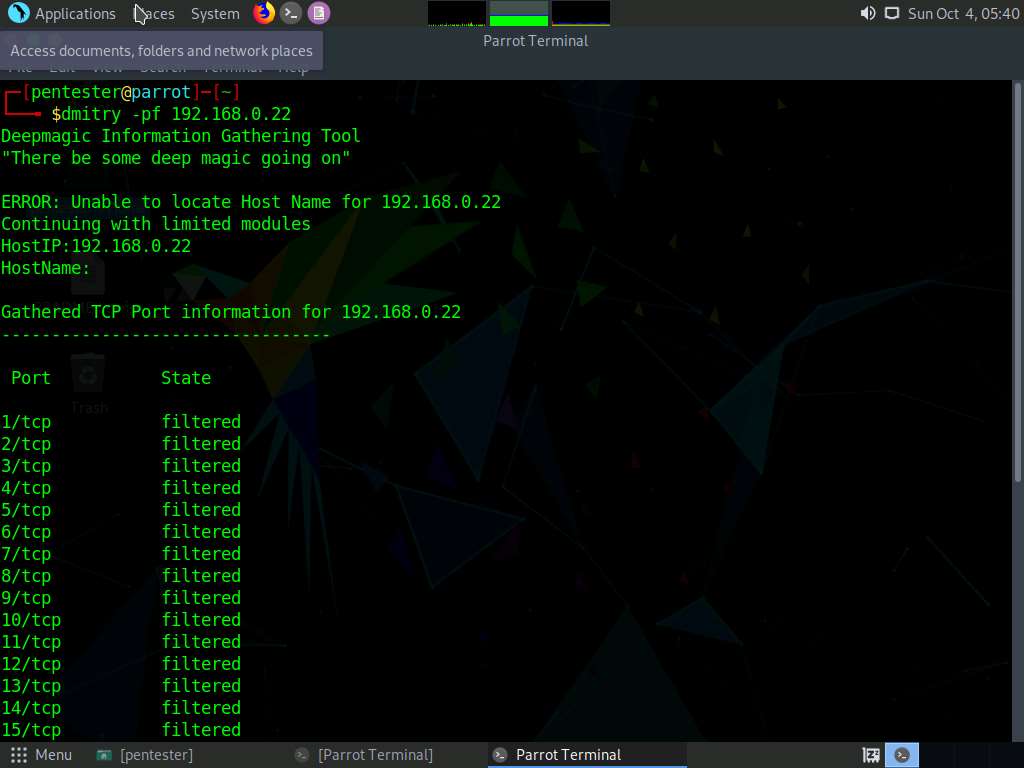
1. By default **pentester** is selected as the **user**. Type **toor** in the Password field and press **Enter**.

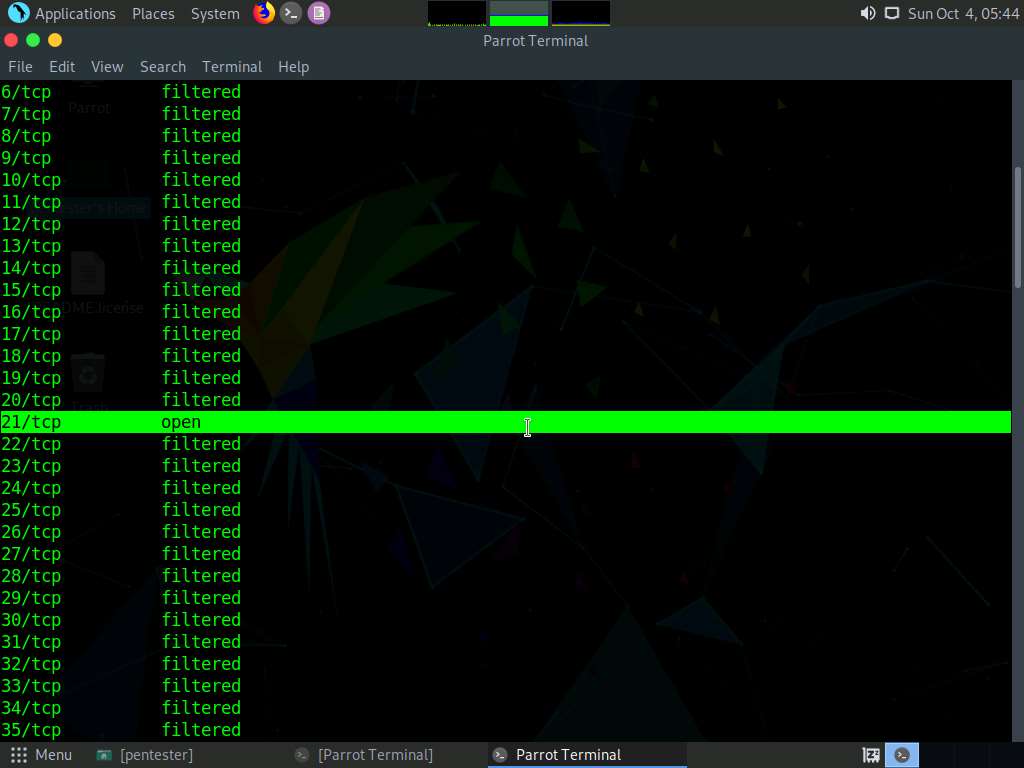


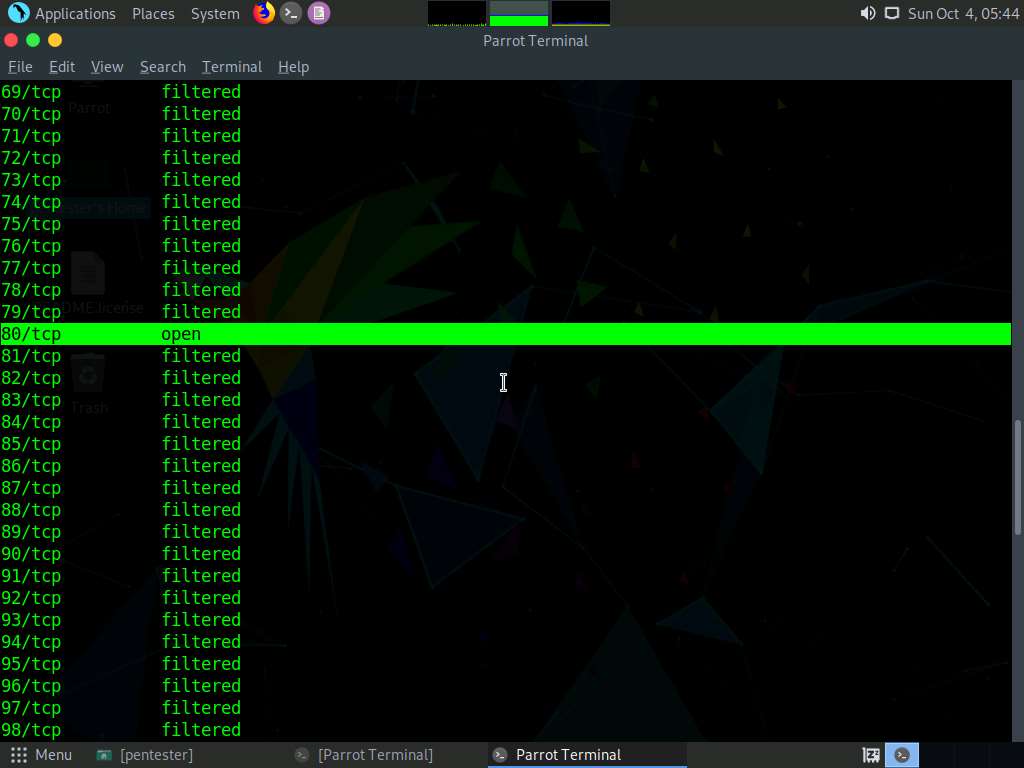
1. Obtain the list of targets using the following scanning methodology: a. Live Systems b. Ports c. Services d. Enumeration e. Identify vulnerabilities f. Exploitation
2. Enter **sudo nmap -sn 192.168.0.0/24**. Type **toor** if you are asked to enter the password. An example of a partial output from the command is shown in the screenshot.



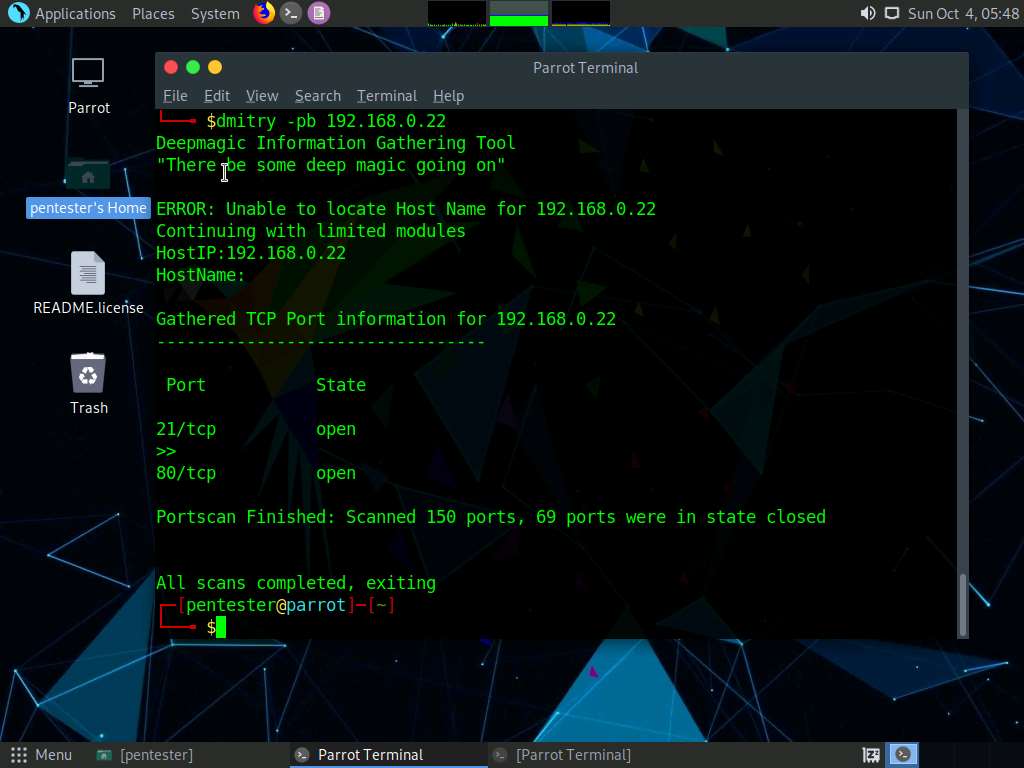
1. The scan reveals a selection of targets, records information about the targets, and determines which ones to target. Since you have used the Nmap tool, switch to another tool. Note that this module requires proficiency in at least two to three tools for each step of the process.
2. Open a terminal window and enter **dmitry -pf 192.168.0.22**, as shown in the screenshot.







1. The DMitry tool, a port scanner, provides all port information (for more information about the tool, please see the main page)
2. In the terminal window, enter **dmitry -pb 192.168.0.22**, as shown in the screenshot



1. You are now viewing a banner grab as well as port scan, as shown in the above screenshot
2. If there is time, continue using the tool and explore more options.
3. This concludes the lab exercise.