Network Penetration Testing Methodology-Internal

6 Hr 48 Min Remaining

Instructions Resources Help  100%

Exercise 1: Scanning with Netdiscover

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 Netdiscover tool. This tool has higher ease-of-use. In this lab, you will

* Start the Netdiscover tool
* Explore the different scan options
* Scan and review the data from Netdiscover

**Lab Duration**: **10** Minutes

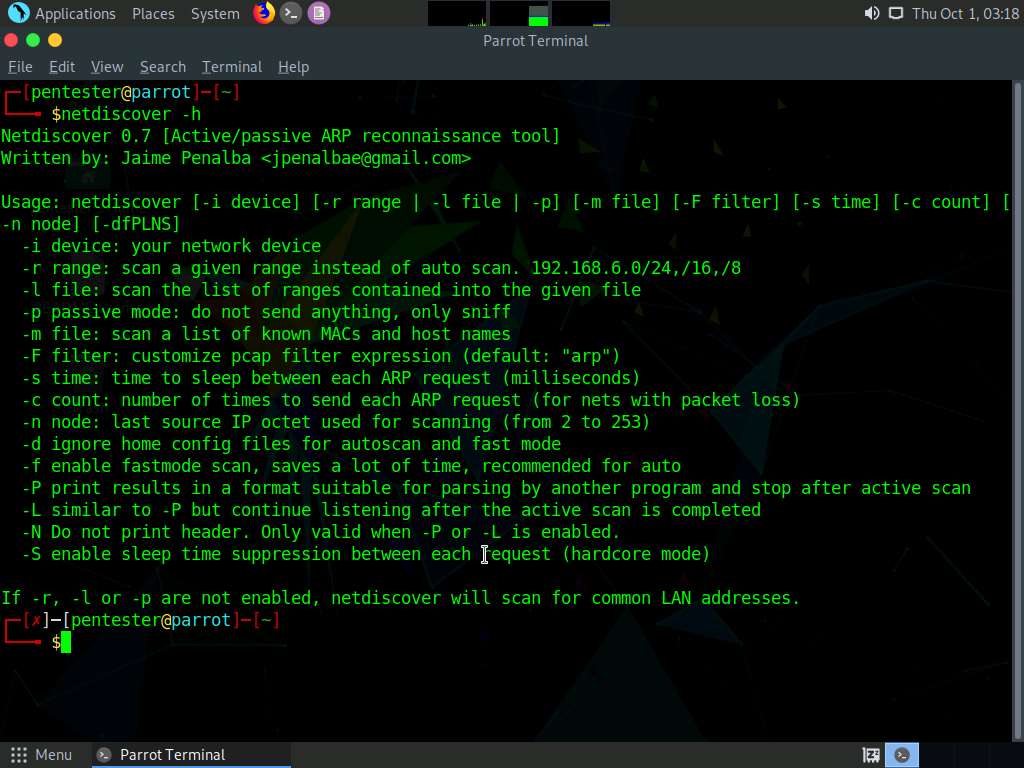
1. Click [Parrot](https://labclient.labondemand.com/Instructions/52f4d542-434e-4a10-8f51-0c2b8ca1d32b?rc=10). Parrot lock screen appears.



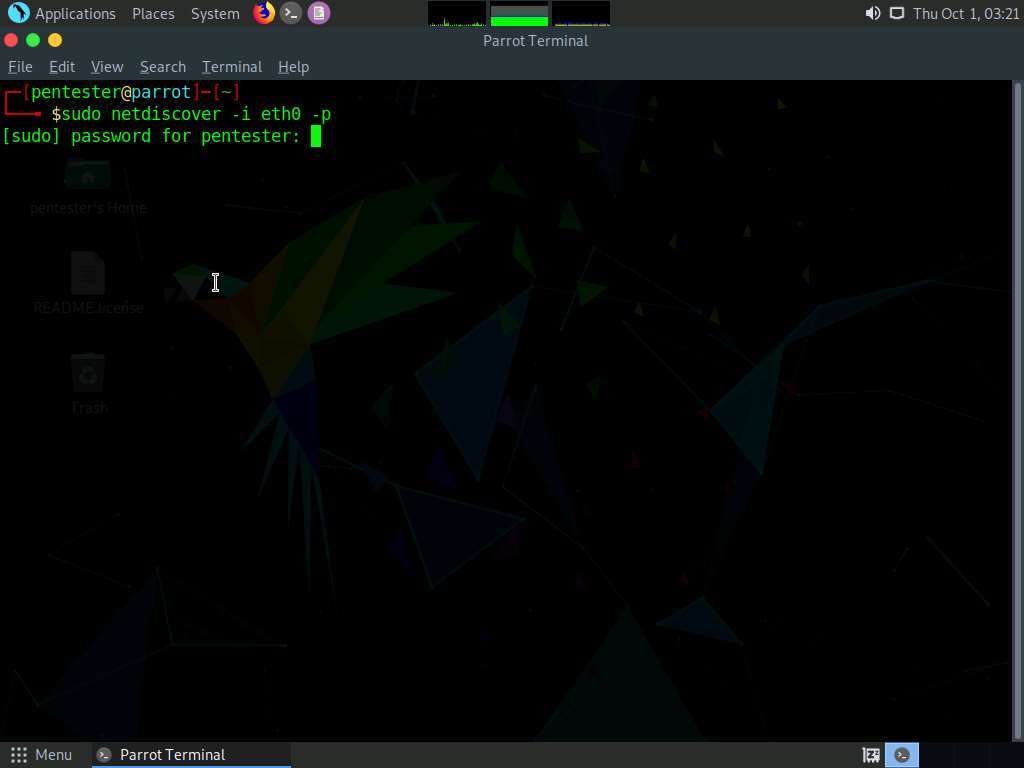
1. By default **pentester** is selected as the **user**. Type **toor** in the Password field and press **Enter**.



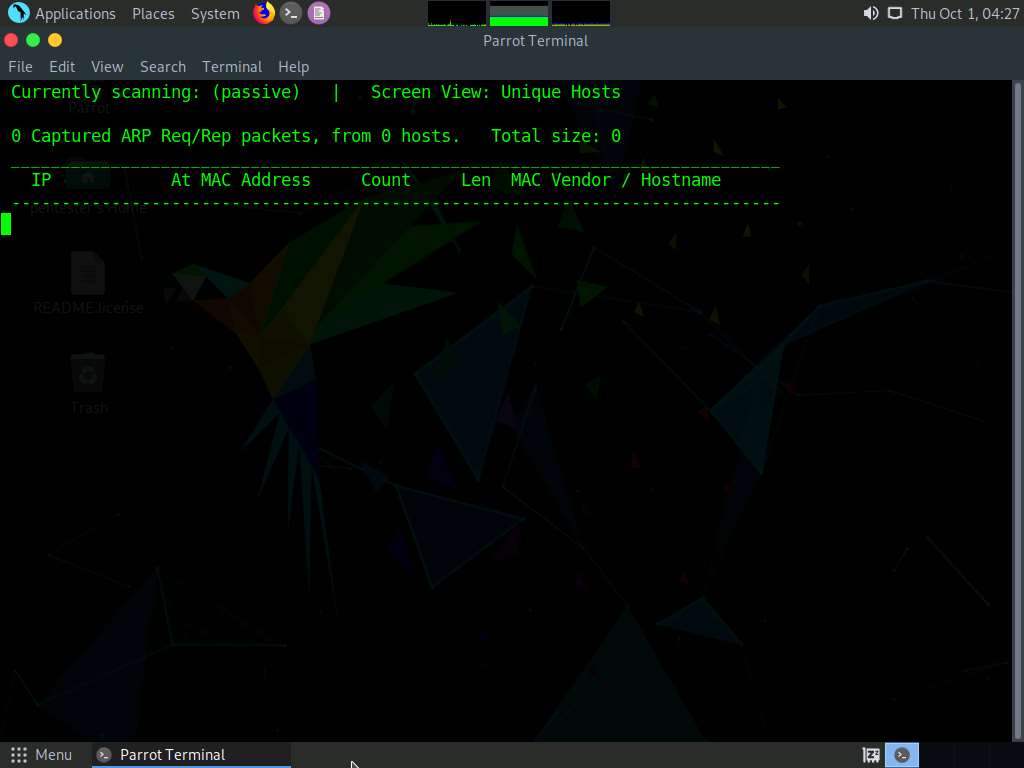
1. Open a terminal window and enter **netdiscover -h**. This will display the netdiscover commands as shown in the screenshot:



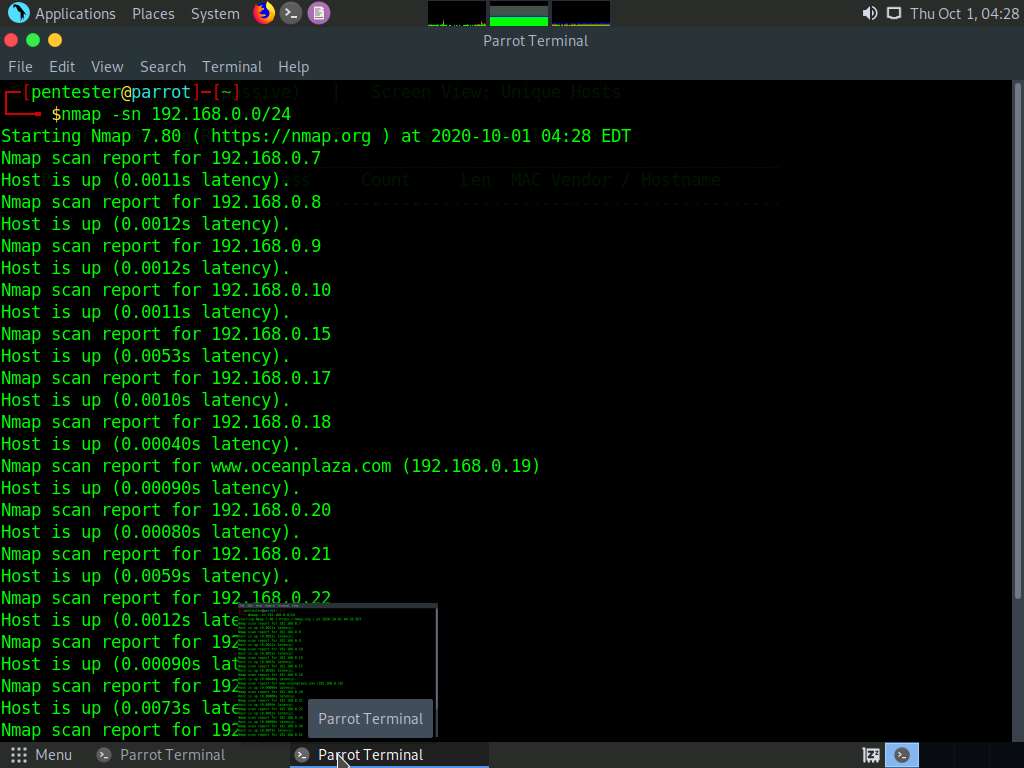
1. This tool allows the user to discover live systems. In the terminal window, enter **sudo netdiscover -i eth0 -p**. If you are asked to enter a password, enter **toor**.



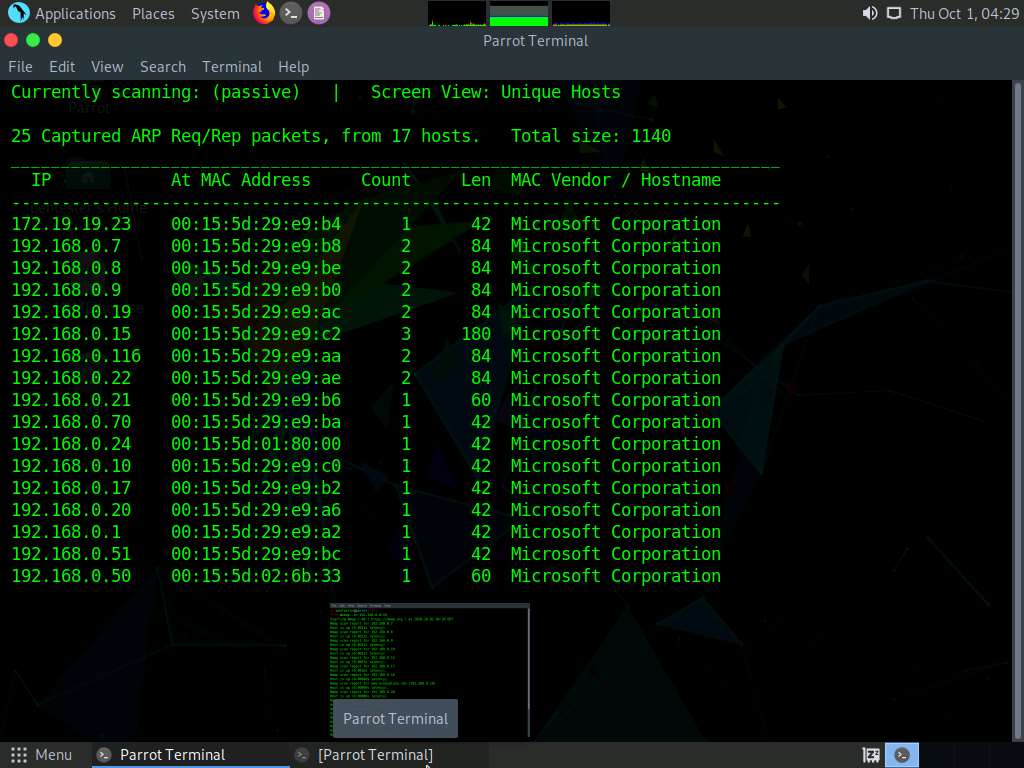
1. In the passive option, targets are generated slowly. It takes a lot of time to display the result. To save time, you can create your own traffic by doing a ping sweep using nmap which is demonstrated in the next step.



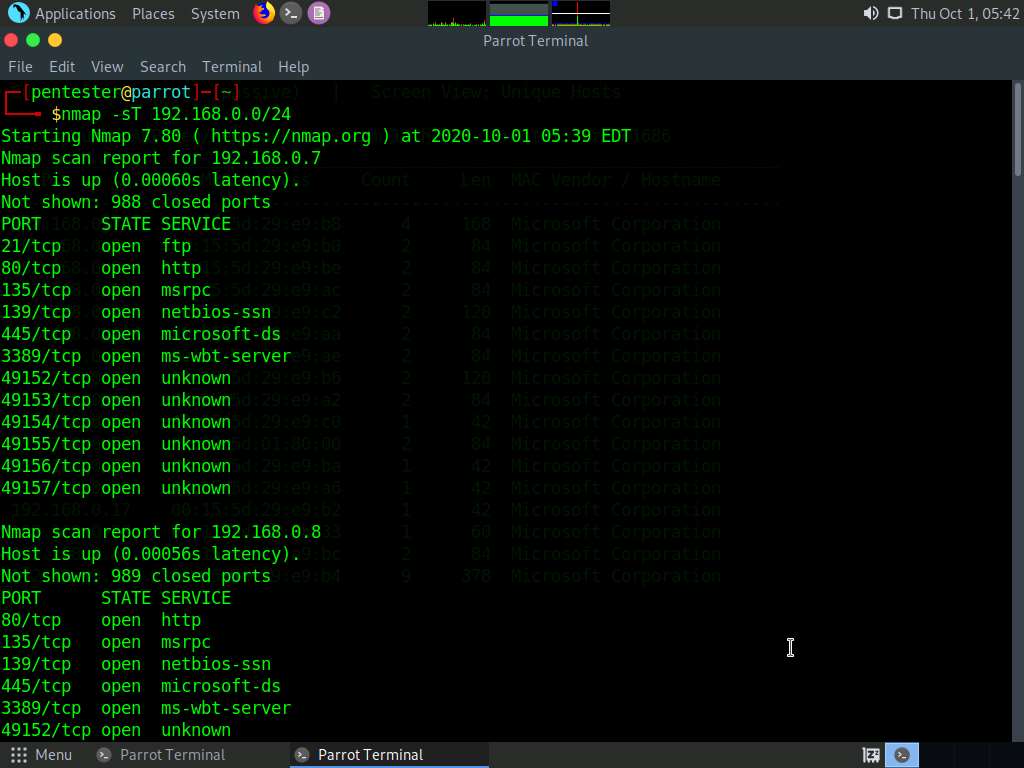
1. In a new terminal window, enter an nmap ping sweep to generate traffic. To do a ping sweep, type **nmap -sn 192.168.0.0/24** and press **Enter**.



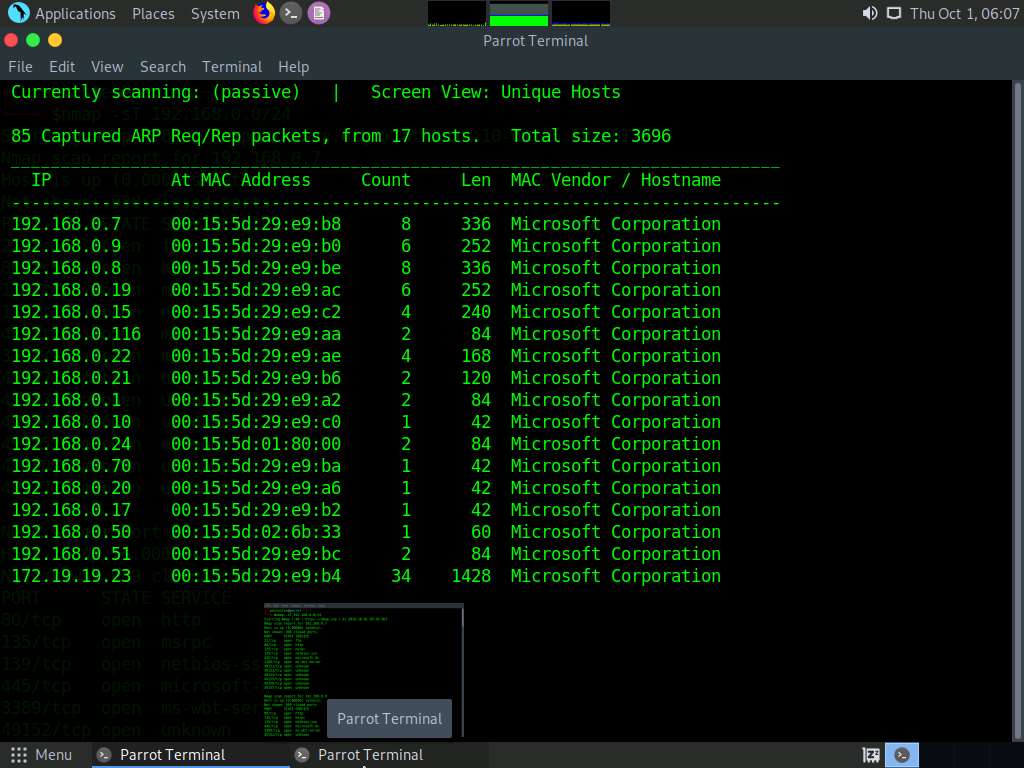
1. Switch back to netdiscover window to view the output



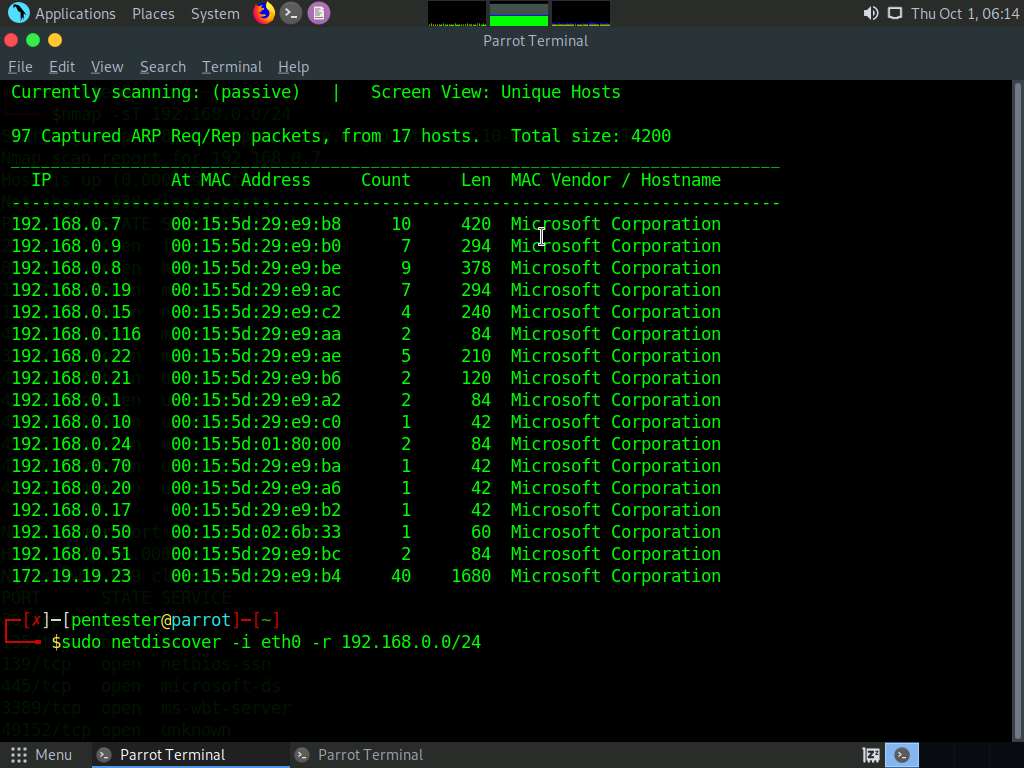
1. At times, some machines may not be discovered due to reasons such as the existence of a firewall or some other filter. At such situation, you may use a Transmission Control Protocol (TCP) scan to confirm the existence of the new machine. To perform a TCP scan, enter the command **nmap -sT 192.168.0.0/24**.



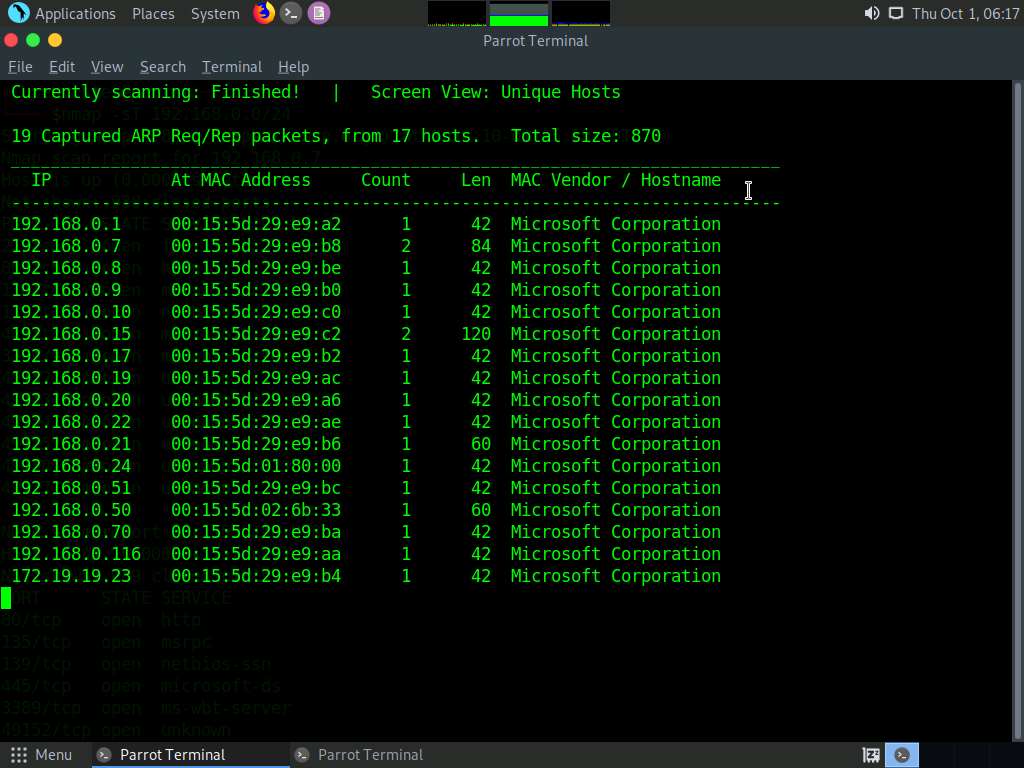
1. Note that you have not scanned all 65,536 ports, which is preferable. Depending on the target machines' settings, access to and data obtained from this machine may be limited. Upon scan completion, switch back to netdiscover window to view the output. In this lab, the netdiscover output remains the same, as no new machines were discovered during the nmap scan.



1. If stealth is not part of the scope of the test and a passive scan is unnecessary, an active scan is the best choice. To discover targets, use Netdiscover as a scanner. To search for the network for targets, exit the current netdiscover scan, type **sudo netdiscover -i eth0 -r 192.168.0.0/24** in the terminal window and press **Enter**. If you are asked to enter a password, enter **toor**.



1. The targets will be displayed on the screen after some time, as shown in the screenshot. (To speed up the process, you can run a nmap ping sweep scan.)



1. This new method validates your live and target machines. This concludes the lab exercise.