Network Penetration Testing Methodology-Internal

6 Hr 43 Min Remaining

Instructions Resources Help  100%

Exercise 4: Using Workspaces and db\_nmap

Scenario

In this lab, you will

* Conduct the task of creating workspaces
* Use db\_nmap contained within the Metasploit Framework
* Store and retrieve the scan results from the tool
* Import the results into a Metaploit module

**Lab Duration**: **10** Minutes

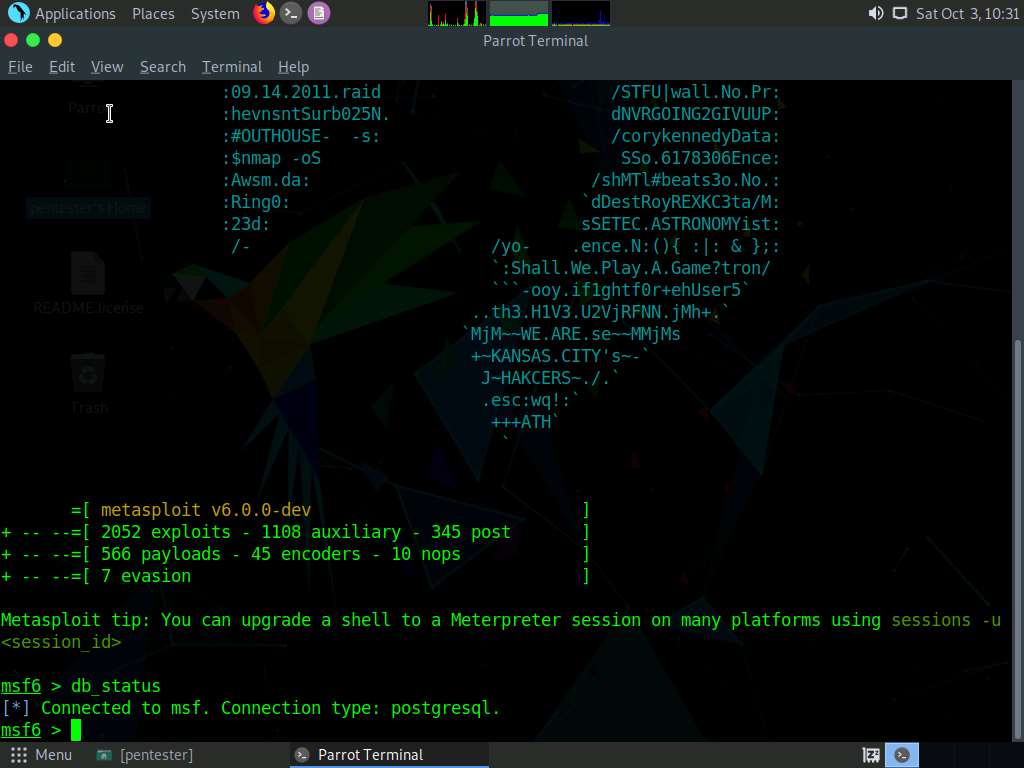
1. Click [Parrot](https://labclient.labondemand.com/Instructions/52f4d542-434e-4a10-8f51-0c2b8ca1d32b?rc=10). Parrot lock screen appears.



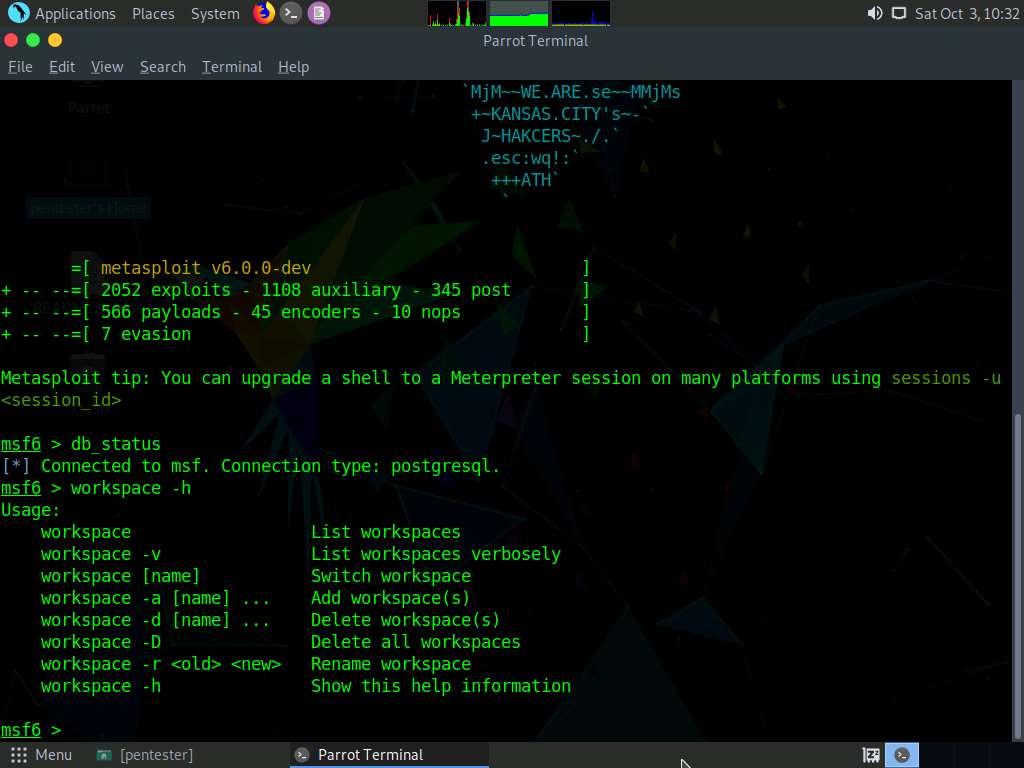
1. By default **pentester** is selected as the **user**. Type **toor** in the Password field and press **Enter**.



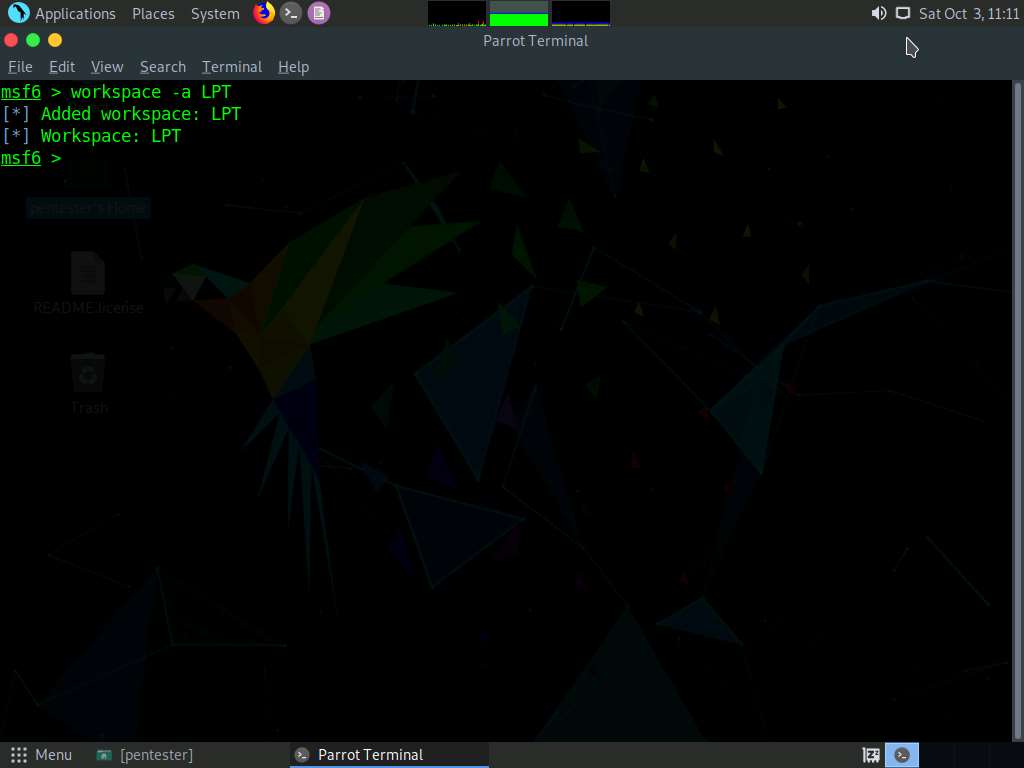
1. Log in to the Parrot machine and open a terminal window. Set up and initialize the **sql server**. In the terminal window, type **sudo service postgresql start** and press **Enter**. Enter the password **toor** if you are required to. The postgresql command initializes the **PostgreSQLdatabase** service.
2. After the database is launched, type **sudo msfdb init** press **Enter**. Enter the password **toor** if you are required to. The **msfdb init** command initializes and creates the PostgreSQL database for Metasploit.
3. If a database appears to be already configured, a message to skip initialization appears; ignore the message.
4. Once the databases are created and initialized, we can quickly fire up Metasploit using the command **sudo msfconsole**. Enter the password **toor** if you are required to.
5. To find out the status of the database, type **db\_status** in the terminal window, as shown in the screenshot.



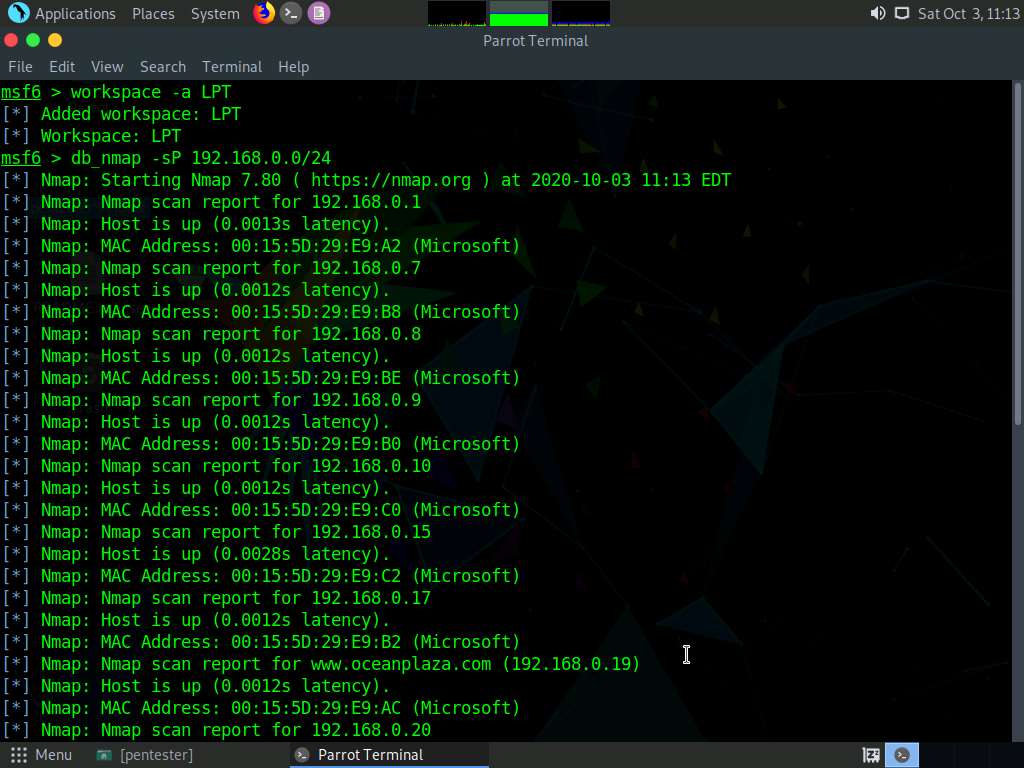
1. The Metasploit tool has different workspaces; type **workspace -h** to see the different commands available for the workspace. Once you have reviewed them, continue.



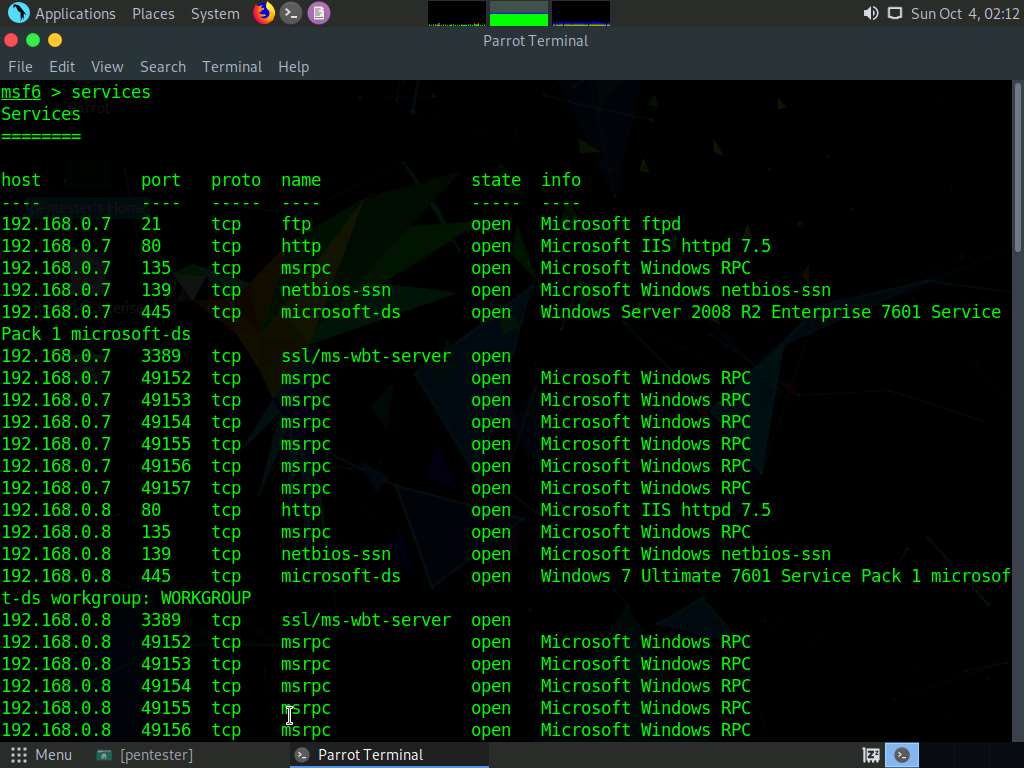
1. Create a workspace for your data by typing **workspace -a LPT**. You now have a workspace setup. You are ready to use the built-in Nmap database within Metasploit.



1. Next, use the tool to conduct the scanning methodology. Enter **db\_nmap -sP 192.168.0.0/24**, as shown in the screenshot.



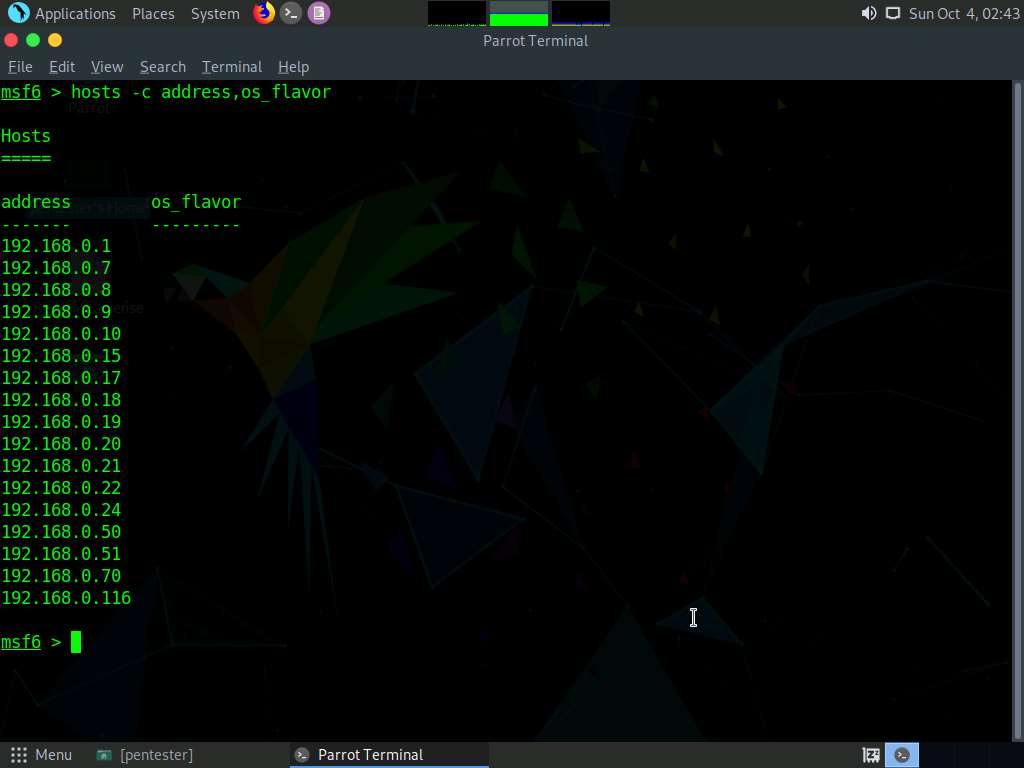
1. Once the scan is complete, move to the next step; type **db\_nmap -sS 192.168.0.2-30**.
2. Once the scan is complete, move to the next step; type **db\_nmap -sV 192.168.0.2-30**.
3. Once the scan is complete, move to the next step; type **db\_nmap -A 192.168.0.2-30**.
4. You have now conducted the bulk of the scanning methodology. Sufficient data have been stored in the workspace. To examine the database information, type **services** and press **Enter**, as shown in the screenshot.



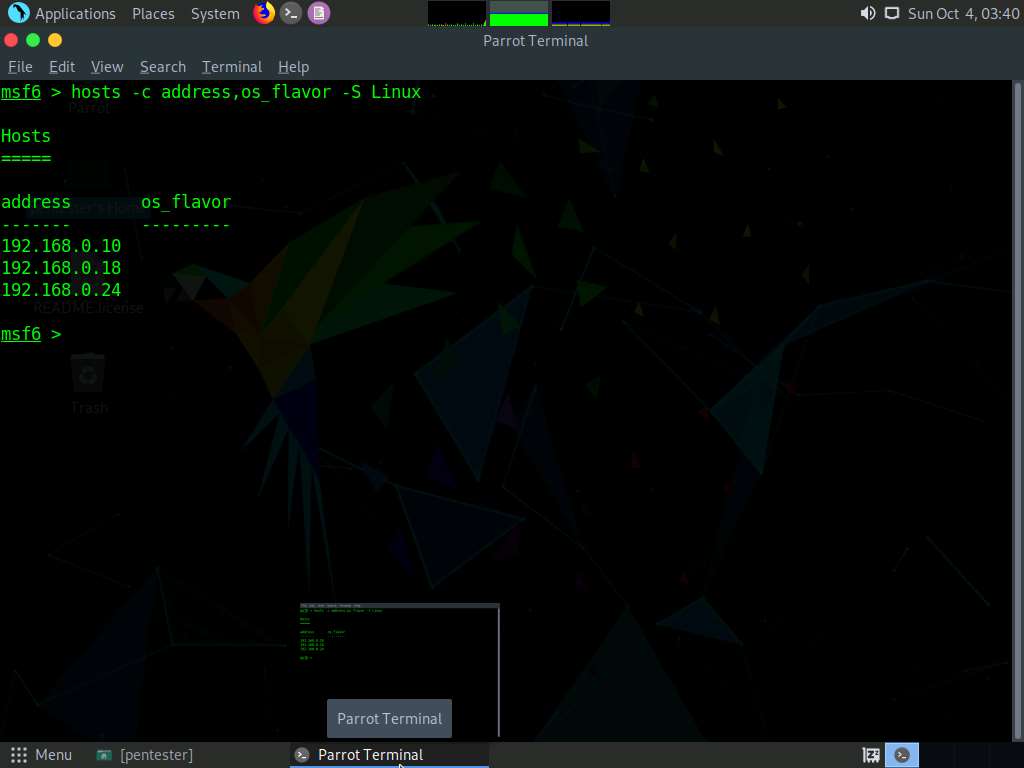
1. The results show all services from the scans; this is the start of the target database, and works well for penetration testing.
2. Next, examine the database list of hosts; type **hosts**, as shown in the screenshot.



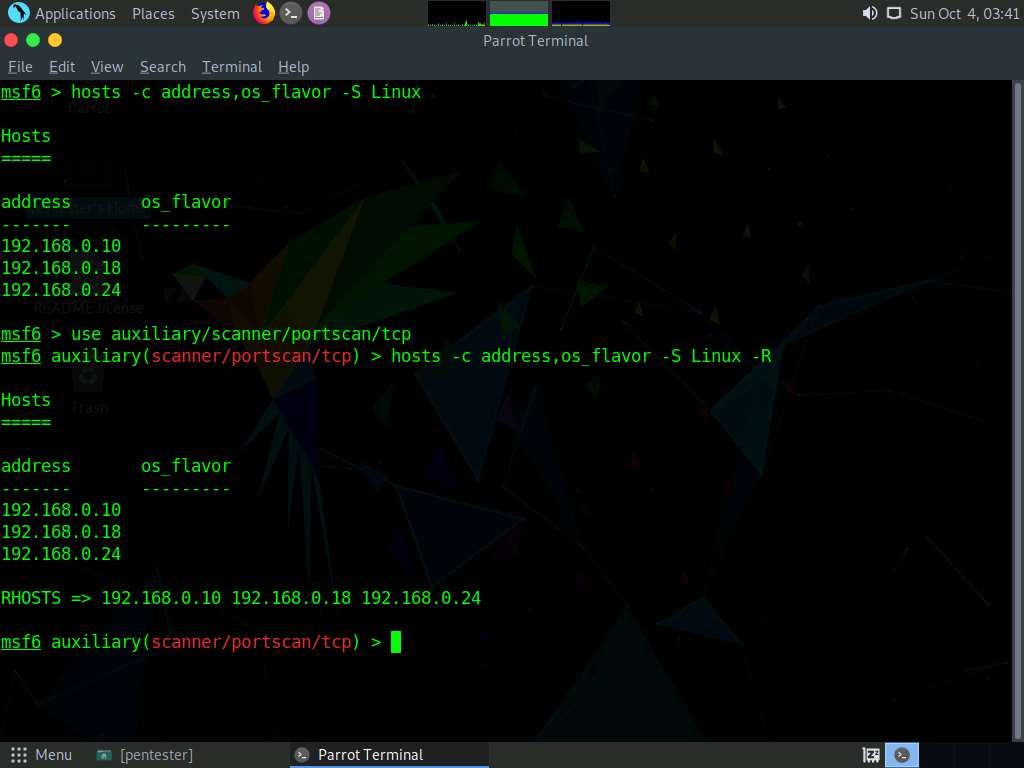
1. Because of the virtual environment, you may not receive the most accurate data. Additional analysis is needed to better clarify the targets.
2. Enter **host -h** to see the different available options. Query the “hosts’” command to display only the IP address and OS type using the “-c” switch.
3. Type **hosts -c address,os\_flavor** and press **Enter**, as shown in the screenshot.



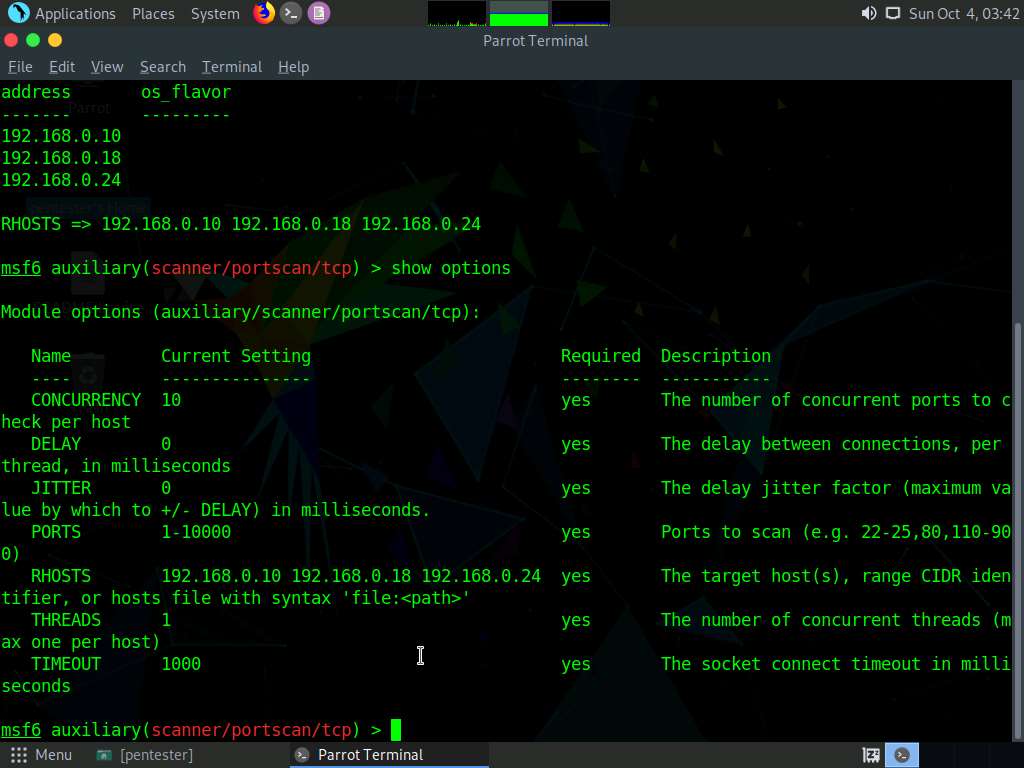
1. Note that you can also search all entries for a specific target. If you wish to find only Linux-based machines from the scan, use the “-S” option. This option can be combined with our previous example to fine-tune the results. Type **hosts -c address,os\_flavor -S Linux**.



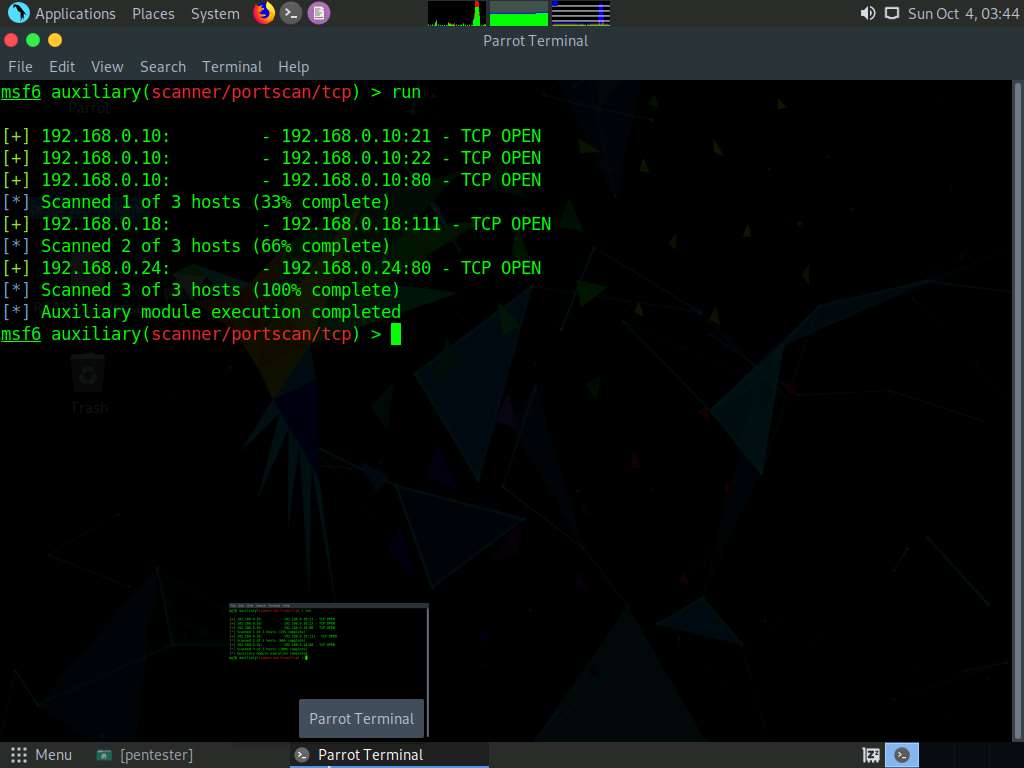
1. Next, import the results of the scans into a Metasploit Module. Type **use auxiliary/scanner/portscan/tcp** and press **Enter**.
2. Input the data into the scanner by using the R option; type **hosts -c address,os\_flavor -S Linux -R** and press **Enter**, as shown in the screenshot.



1. The above command will import the results in the host table into RHOSTS; you can view this by entering **show options**. Note that there might be extra hosts in the database.



1. Once you are ready, type **run** and press **Enter**. The scan will be conducted against the target added to the database, as shown in the screenshot.



1. You have diverse search options; for this, type **services -c name,info -S http** and press **Enter**. This will search the hosts for services with HTTP in the name.
2. There are many combinations for searching. You can use specific ports or port ranges, or the full or partial service name when using the “-s” or “-S” switches, as well as for all hosts or a select few. However, you may need to experiment with these features in order to obtain the desired results.
3. As you have seen in this exercise, we have many options to work with when using the database capability within Metasploit; therefore, you are encouraged to research on your own.
4. This concludes the lab exercise.