Network Penetration Testing Methodology-Internal

6 Hr 41 Min Remaining

Instructions Resources Help  100%

Exercise 8: Create a Python Script to Grab the Banner of the ssh Service

Scenario

In this lab, you will create a python script to grab the banner of the secure shell (SSH) service.

**Lab Duration**: **10** Minutes

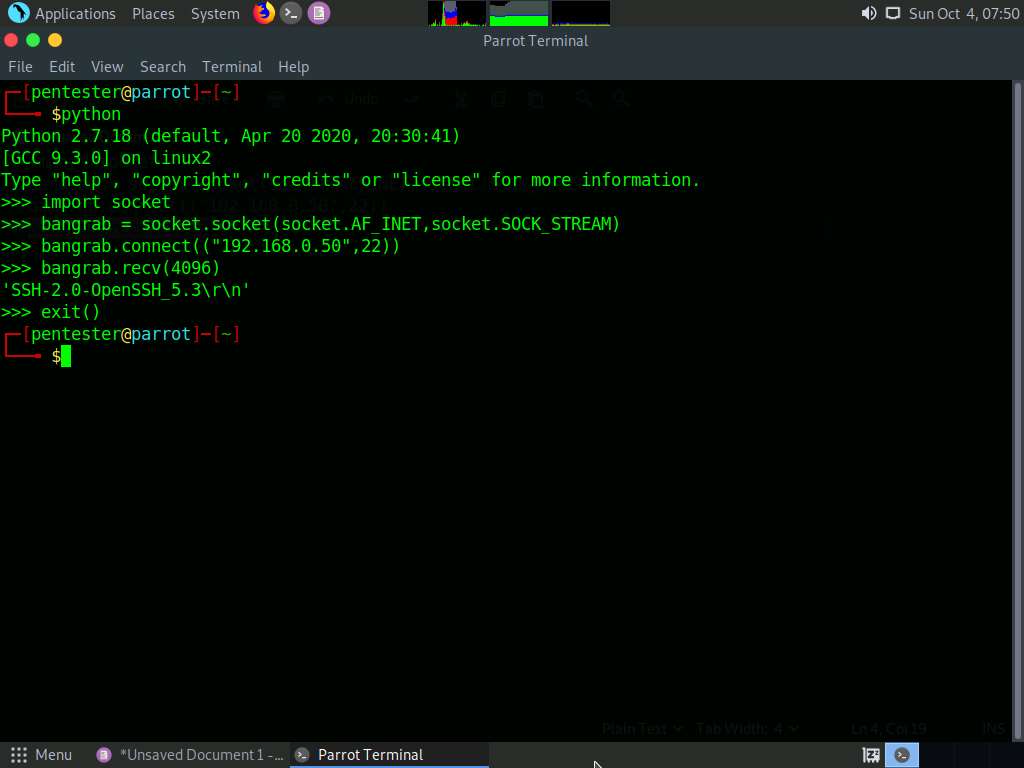
1. Click [Parrot](https://labclient.labondemand.com/Instructions/52f4d542-434e-4a10-8f51-0c2b8ca1d32b?rc=10). Parrot lock screen appears.



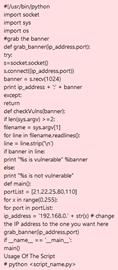
1. By default **pentester** is selected as the **user**. Type **toor** in the Password field and press **Enter**.



1. Open a terminal window on the Parrot machine and enter the following code



1. As you review the image, consider the following explanation:
   * The **import statement** helps obtain the required socket library
   * The **bangrab** is a variable that stores the content of the created socket
   * The **socket type** is a TCP socket base on the SOCK\_STREAM
   * Once the socket is created, you can access and manipulate the socket using the appropriate **function calls**
   * The **connect function** is used to identify the address and port for the connection
   * The **receive statement** receives the data from the socket
2. This process is used to extract the banner of any port, provided you change the number of the connecting port
3. For a more robust type of banner grabbing tool, you can refer to the following code:



1. Please see the appendix for select coding examples.