Network Penetration Testing Methodology-Internal

6 Hr 41 Min Remaining

Instructions Resources Help  100%

Exercise 9: Use Metasploit to Detect Version of HTTP

Scenario

In this lab, you will

• Take an exploit from the Metasploit and review it

**Lab Duration**: **10** Minutes

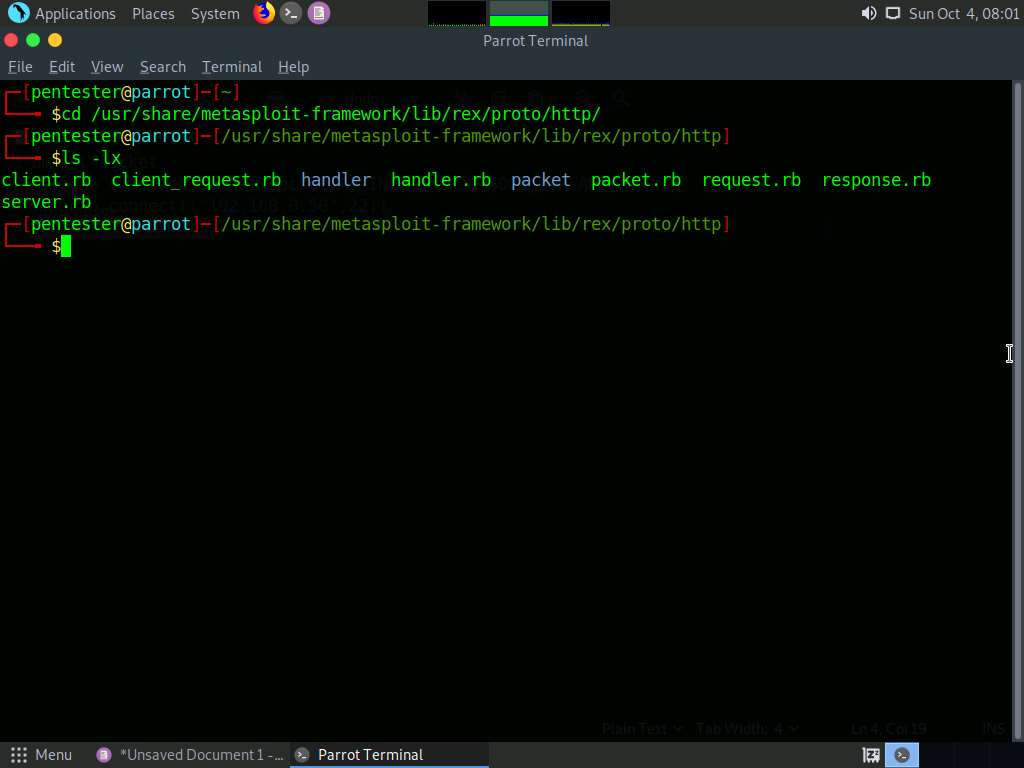
1. Click [Parrot](https://labclient.labondemand.com/Instructions/52f4d542-434e-4a10-8f51-0c2b8ca1d32b?rc=10). Parrot lock screen appears.



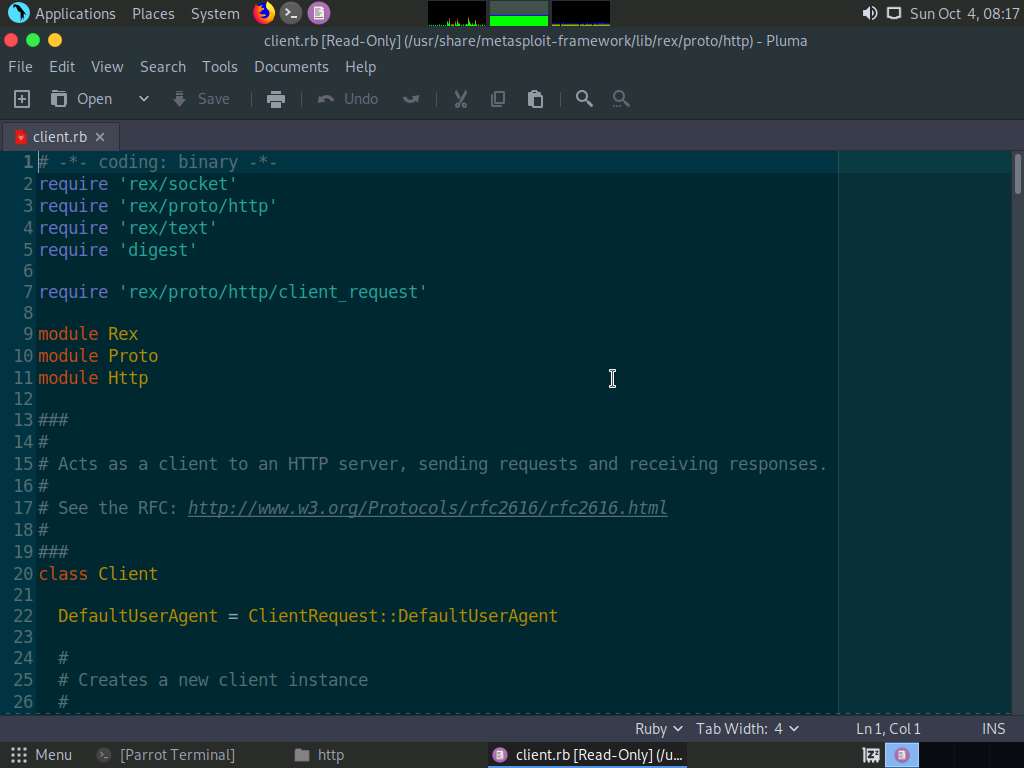
1. By default **pentester** is selected as the **user**. Type **toor** in the Password field and press **Enter**.



1. Open a terminal window on the Parrot machine
2. The module you investigate is the one that is used to detect the version of **http**. Review the **Metasploit** core info; type **cd /usr/share/metasploit-framework/lib/rex/proto/http** and press **Enter** in the terminal window
3. Enter **ls -lx**



1. All these files contain a variety of **HTTP** methods, which include functions to set up a connection, the **GET** and **POST** request, and response handling.
2. To open the module, navigate to **Places**, select **File System**, and navigate to **/usr/share/metasploit-framework/modules/auxiliary/scanner/http**. In the **HTTP** folder, scroll down and right-click on **http\_version.rb**, and then click on **Open With Pluma** from the context menu.
3. Carefully review the information. Next, explore mixin. Once the review is done, close the text editor window.
4. Navigate to **Places**; select **File System** and navigate to **/usr/share/metasploit-framework/lib/rex/proto/http**. In the **http** folder, right-click on **client.rb**, and then click on **Open With Pluma** from the context menu.
5. This is the code for the mixin; there are the routines that you will need for handling the sockets in order to conduct tasks to extract the data from the site.
6. An example of an excerpt of the code is shown in the screenshot:



1. The key to this routine is in the defined class:
   * self.hostname = host
   * self.port = port.to\_i
   * self.context = context
   * self.ssl = ssl
   * self.ssl\_version = ssl\_version
   * self.proxies = proxies
   * self.username = username
   * self.password = password
2. Once you have reviewed the file, close all open windows. As the class shows, you have covered most requirements when acting as a client for a web server.
3. This is the process you should follow when you are working as a practitioner and professional security and penetration tester. Always investigate the code that is being used BEFORE you ever deploy it on a site.
4. This concludes the lab exercise.