Network Penetration Testing Methodology-Internal

6 Hr 37 Min Remaining

Instructions Resources Help  100%

Exercise 17: Search for Exploits using Searchsploit

Scenario

The objective of this lab is to help students use SearchSploit for searching exploits. In this lab, you will

• Start SearchSploit

• Search for exploits

**Lab Duration**: **5** Minutes

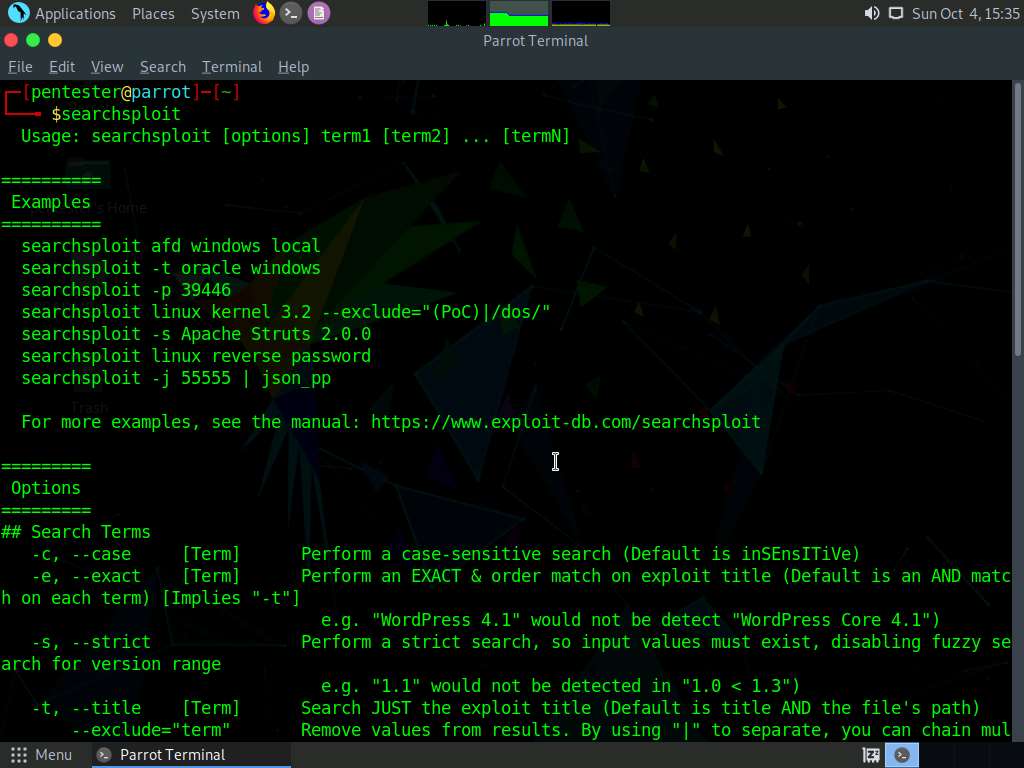
1. Click [Parrot](https://labclient.labondemand.com/Instructions/52f4d542-434e-4a10-8f51-0c2b8ca1d32b?rc=10). Parrot lock screen appears.



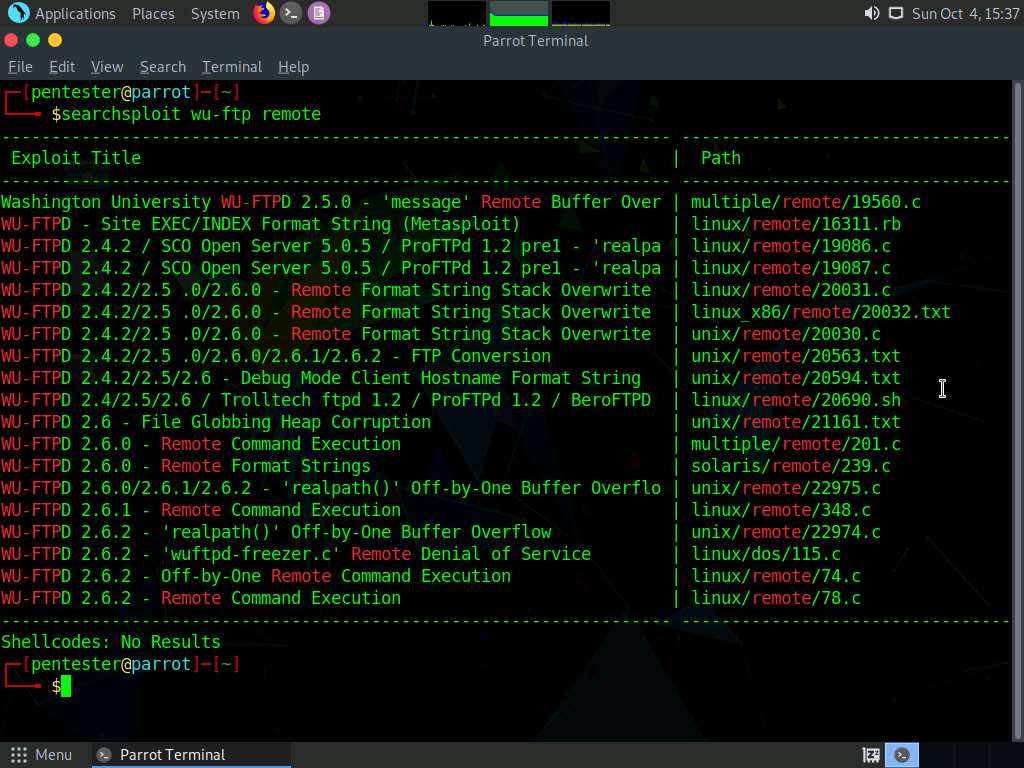
1. By default **pentester** is selected as the **user**. Type **toor** in the Password field and press **Enter**.



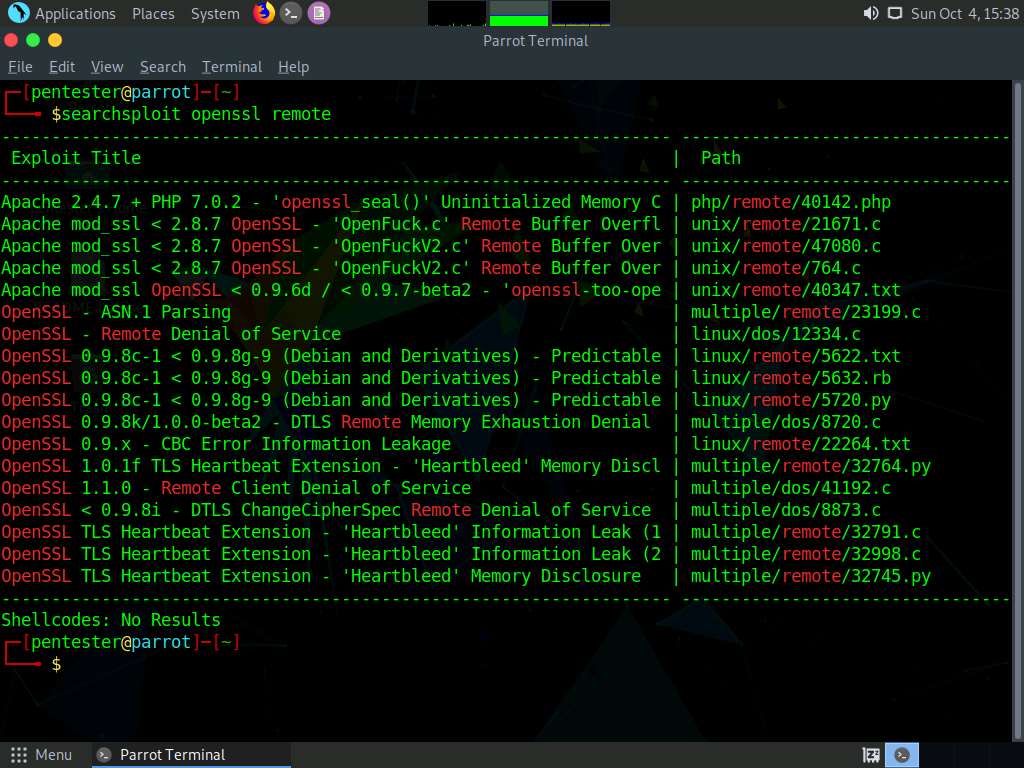
1. Open the terminal window, type **searchsploit** and press **Enter**. This will output the options for the command.



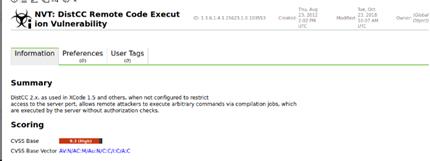
1. You may search for up to three terms. In a terminal window, type **searchsploit wu-ftp remote** and press **Enter**.
2. This will remotely search for a Washington University FTP exploit. Although it is rare that we will run into this version of FTP, it is possible; importantly, the process is key, as it does not change for any additional searches. The output of this command is shown in the screenshot.



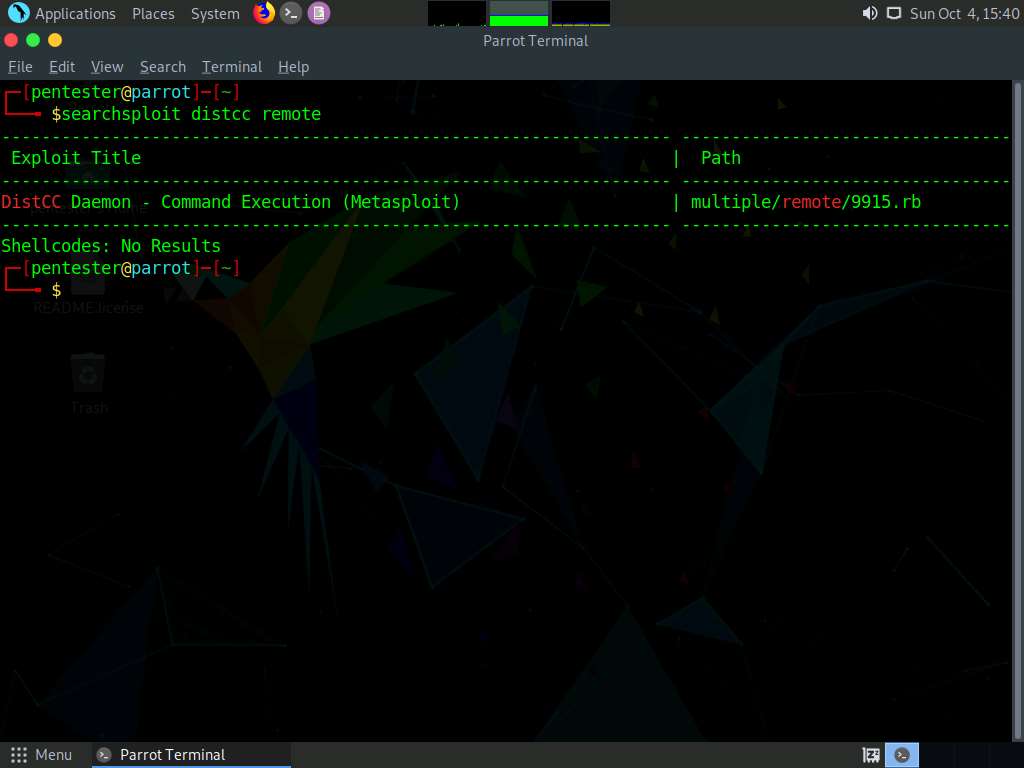
1. Search for the code or script version that you are comfortable with and continue.
2. Next, explore the source code, compile and build the code, and check if you can exploit the vulnerability discovered. Remember that 100% exploitation is not possible, so there are no guarantees. You will also search from within the exploit framework of Metasploit in a later exercise.
3. Next, enter another search; enter **searchsploit openssl remote**.



1. Next, explore the versions and check if any of the exploits match the version discovered.
2. This is why the target database is important. Take your time to complete the recon step and explore the corresponding data. Greater scrutiny increases accuracy and, thus, eases the task of exploiting the target.
3. Next, search for the distccd vulnerability discovered in the OpenVAS search.



1. This is an old vulnerability, but the process itself is key. The command used to run the software also allows access to the daemon with the **–allow** option.
2. An example of the SearchSploit results are shown in the screenshot.



1. As the exploit shows, the code is in Ruby, and it is a Metasploit module. Next, use Metasploit to use the exploit.
2. This concludes the lab exercise.