Network Penetration Testing Methodology-External

1 Hr 6 Min Remaining

Instructions Resources Help  100%

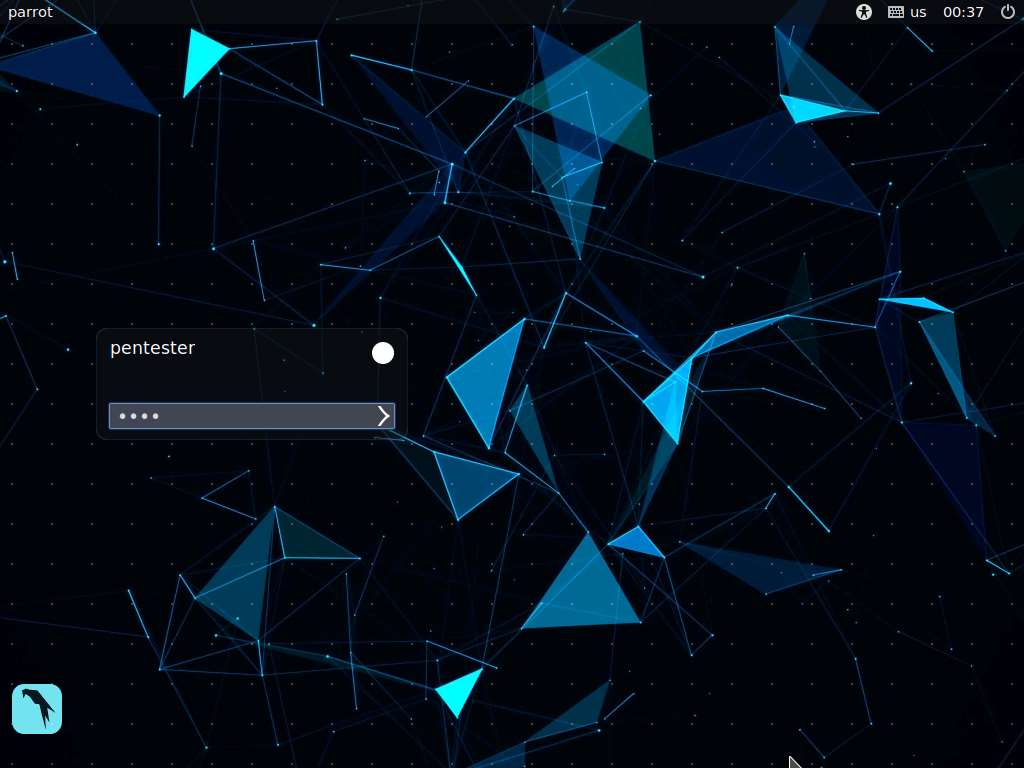
Exercise 4: Perform Web Application Scanning with WMAP

Scenario

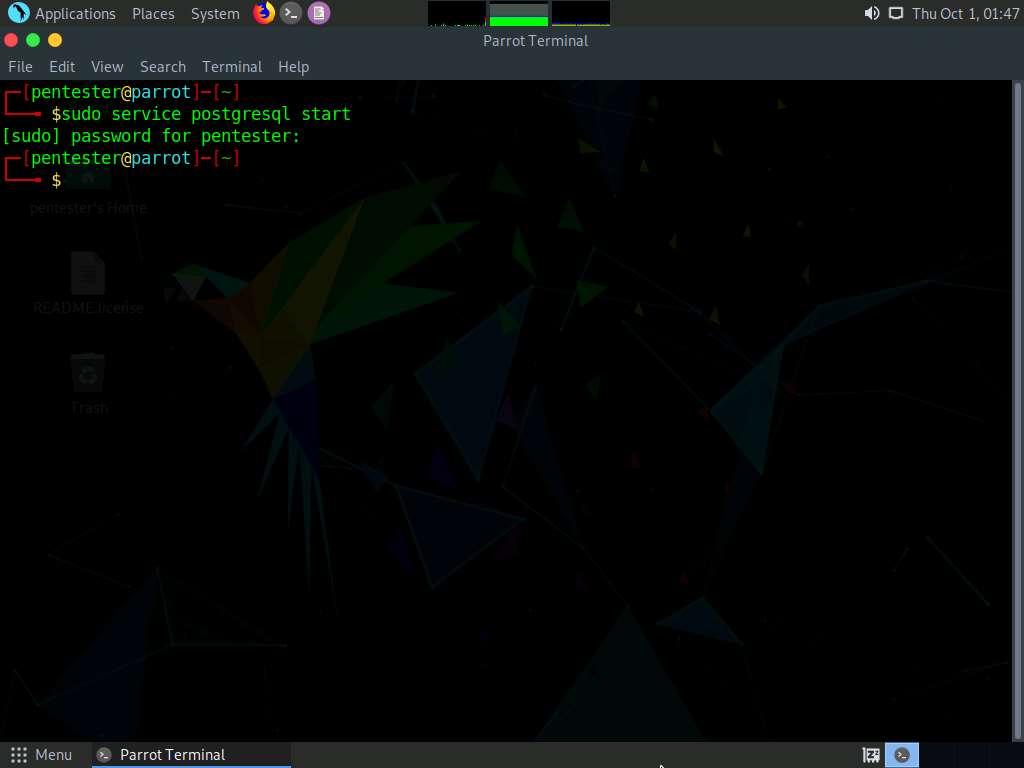
The WMAP tool is used for web application scanning from within the Metasploit console.In this lab you will

* Use the tool WMAP that is part of the Metasploit tools
* Scan a web servers with WMAP

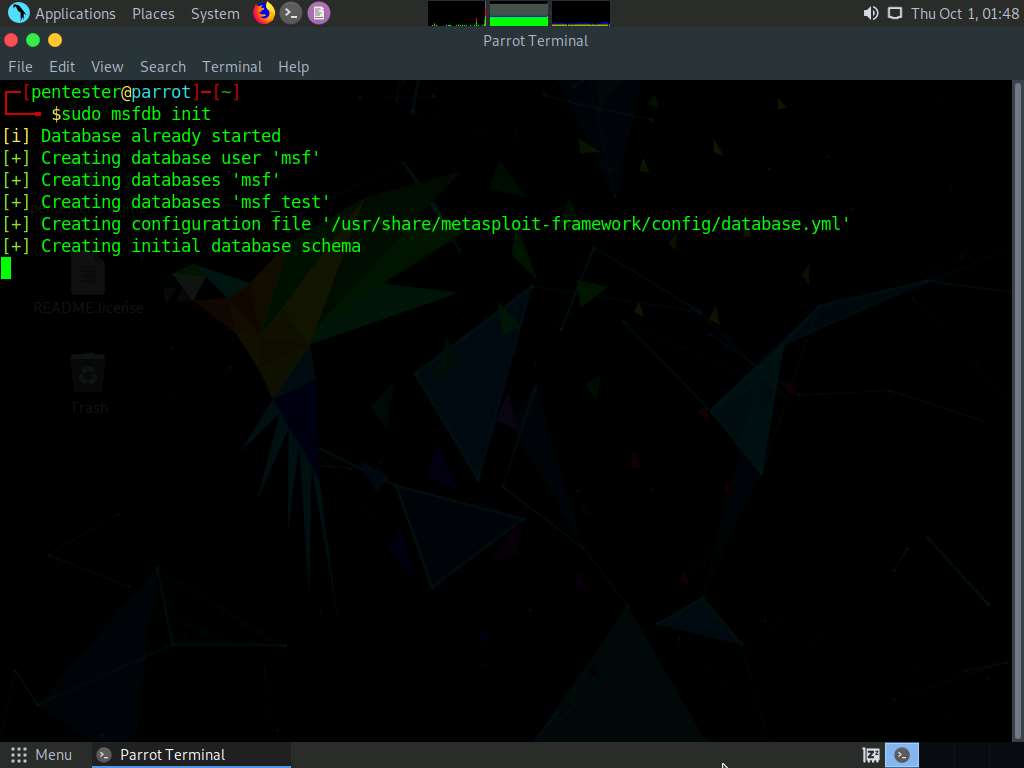
1. Click [Parrot](https://labclient.labondemand.com/Instructions/d51b1821-8ebe-4479-bf4b-33b56a1978d1?rc=10). Parrot logon screen appears, type **toor** in the Password field and press **Enter**.



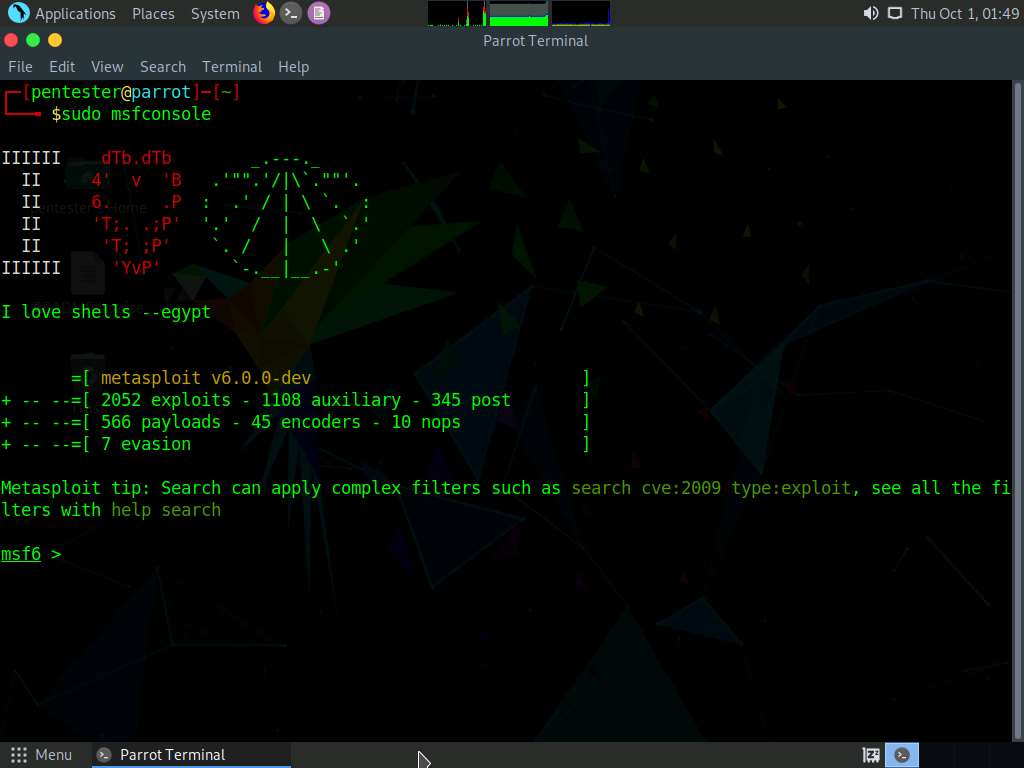
1. The WMAP tool is used for web application scanning from within the Metasploit console, as we did before, we have to setup the database before launching the console, so let us do that now. Open a terminal window and type **sudo service postgresql start** and press **Enter**. Type **toor** when prompted for Password and press **Enter**.



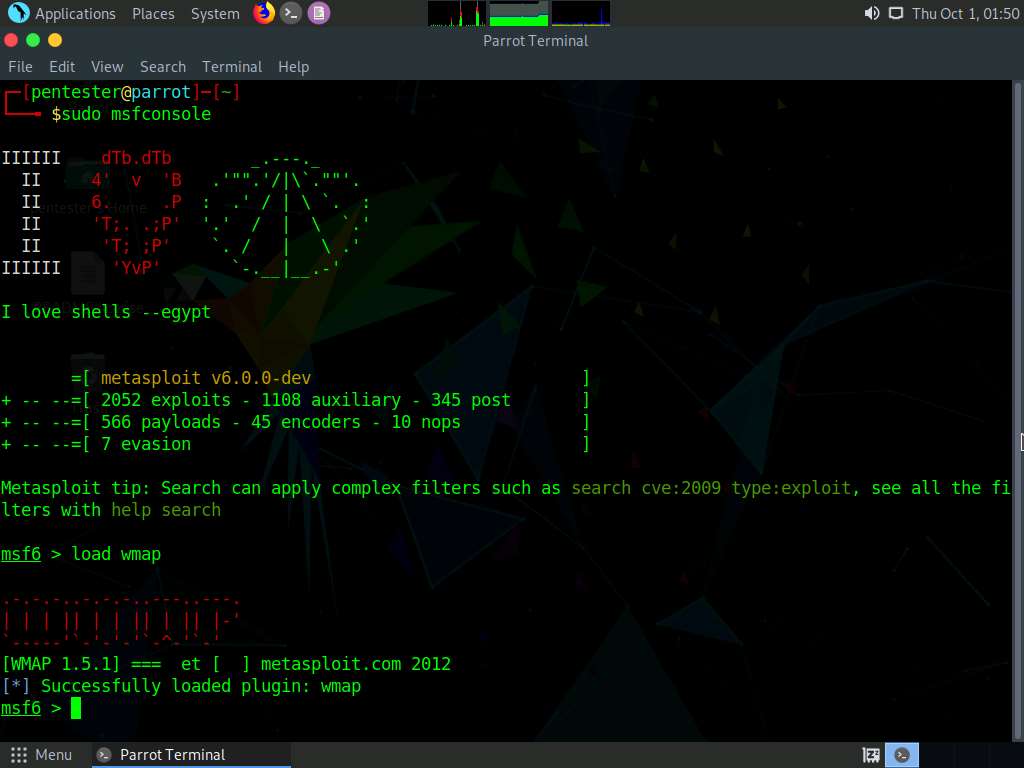
1. If this is the first time running Metasploit, then we need to run **msfdb init** but if it is not the first time, then we can launch the console. Type **sudo msfdb init** and press **Enter**.



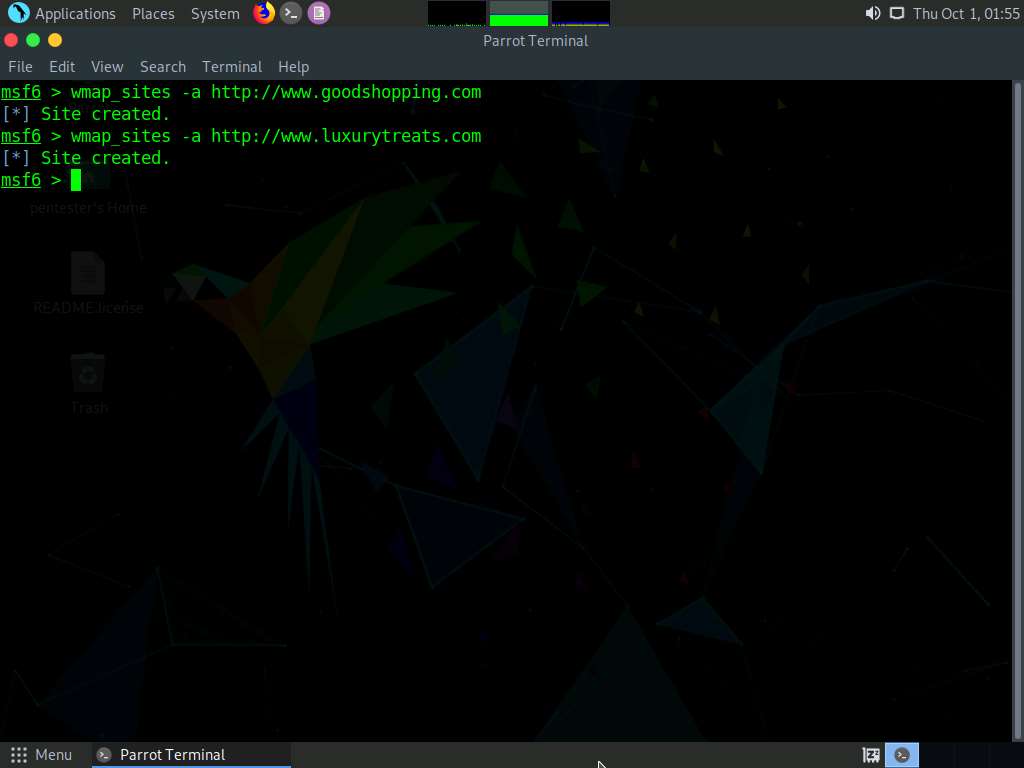
1. Type **sudo msfconsole** and press **Enter** to launch the metasploit framework.



1. Once msfconsole opens we now have to load the wmap too, type **load wmap** and press **Enter**. This will load the tool, once the tool is loaded we can now setup the scans with it.

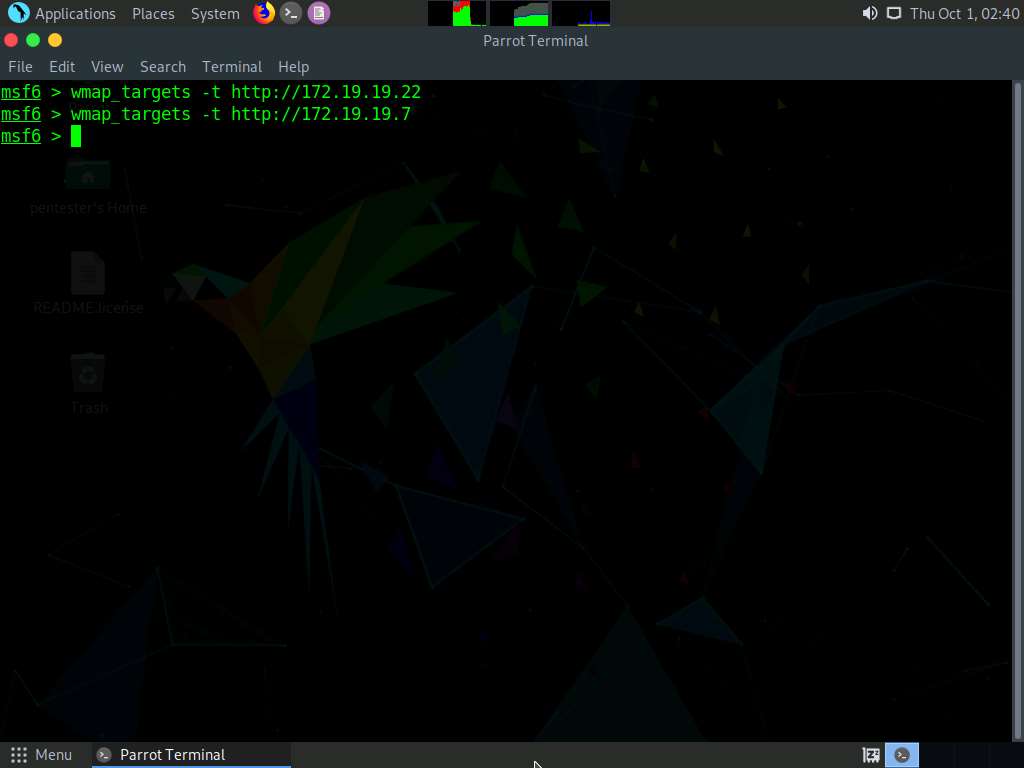


1. The next thing we have to do is add the sites, type **wmap\_sites -a http://www.goodshopping.com** and press **Enter** to add the first site. Once the one site is added, add another site, type **wmap\_sites -a http://www.luxurytreats.com** and press **Enter** to add the second site.

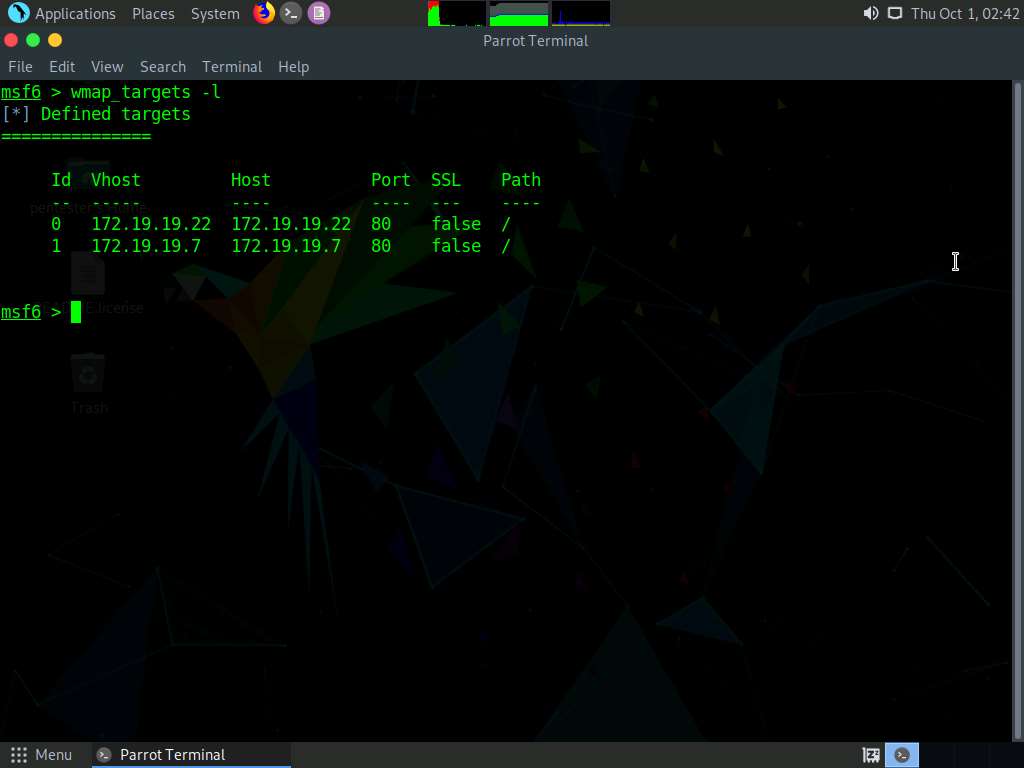


1. Now we want to add our two targets, type **wmap\_targets -t http://172.19.19.22** and press **Enter**. Enter the 2nd target, type **wmap\_targets -t http://172.19.19.7** and press **Enter**.

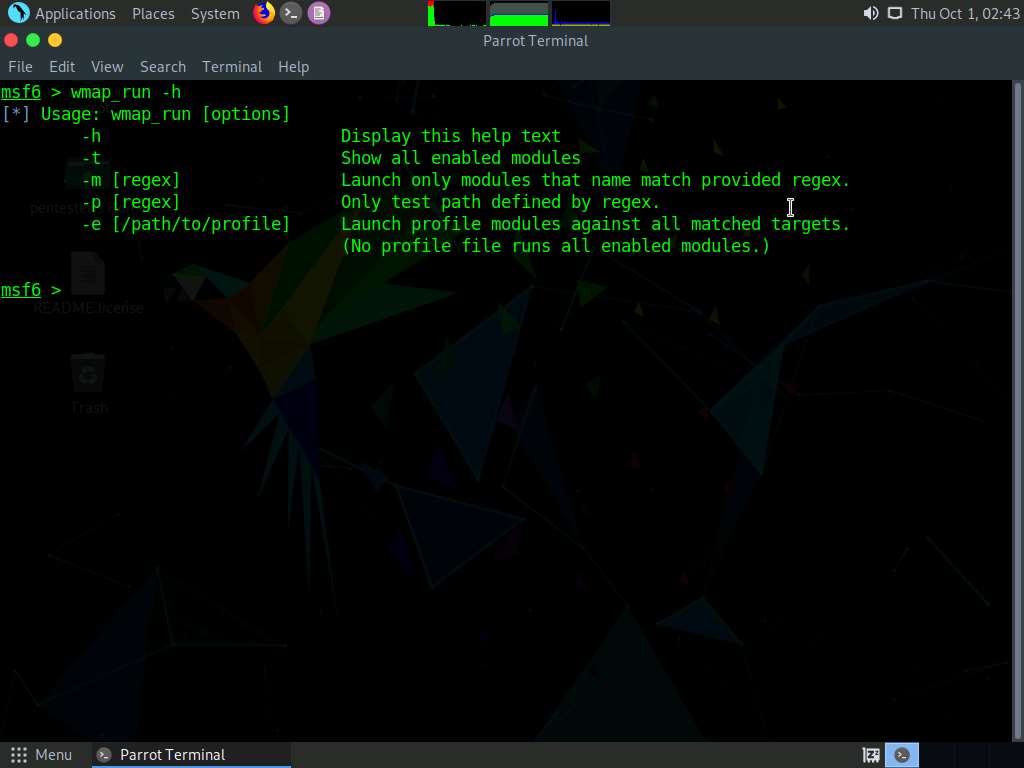
**172.19.19.22** is the IP address of the machine where www.goodshopping.com is hosted and **172.19.19.7** is the IP address of the machine where www.luxurytreats.com is hosted.



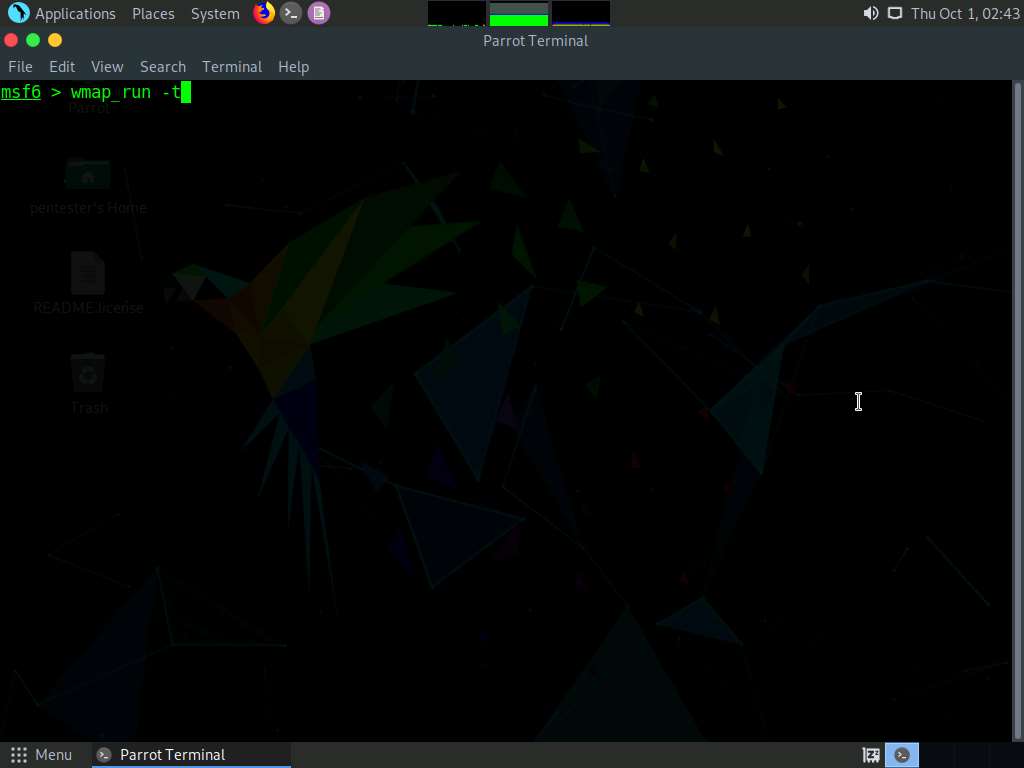
1. To view the targets type **wmap\_targets -l** and press **Enter**.

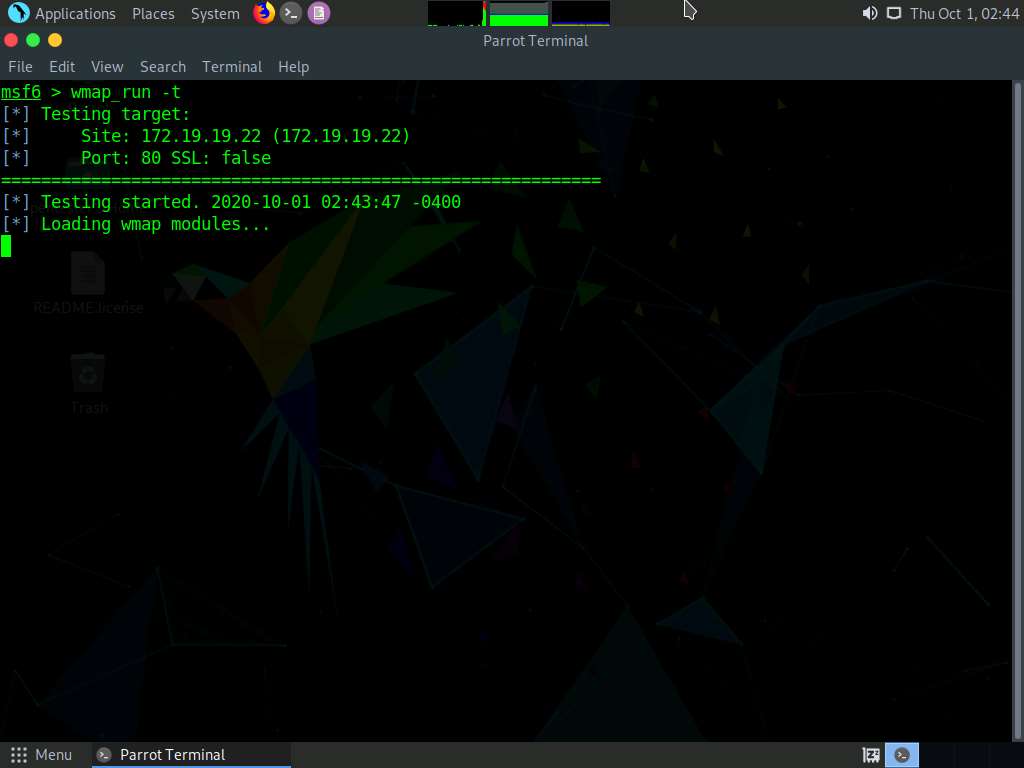


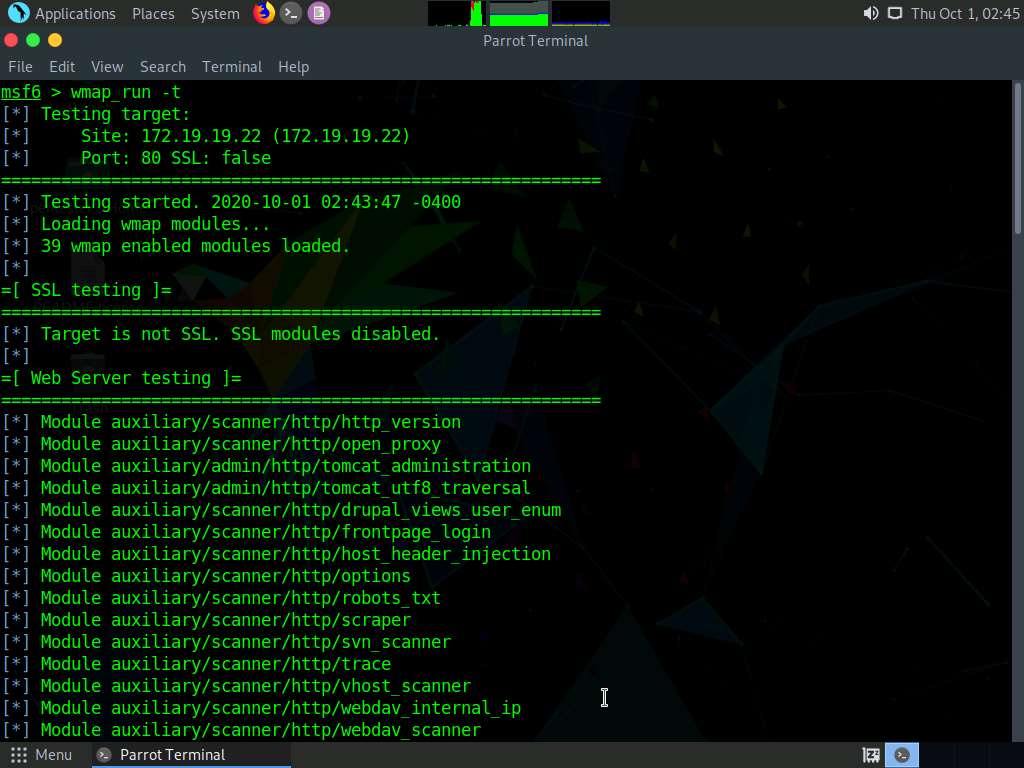
1. The next thing to do, is look at the options for the wmap\_run command, type **wmap\_run -h** and press **Enter**.

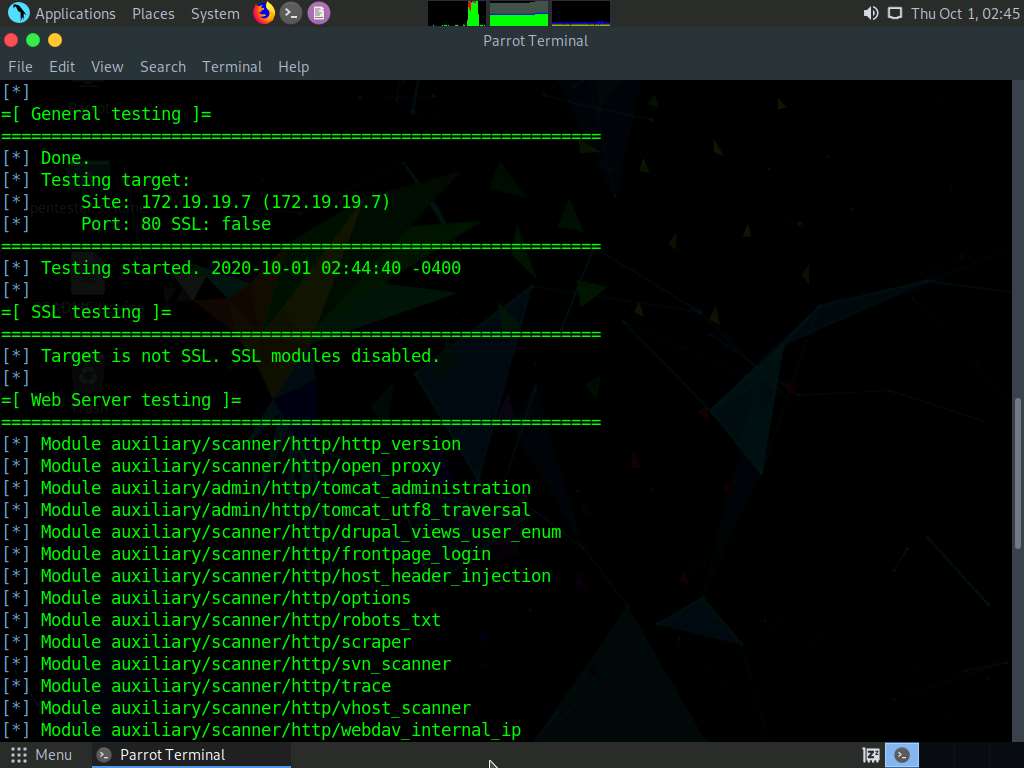


1. We now need to run the modules that we are going to use to test the target, type **wmap\_run -t** and press **Enter**. Once the command has completed, take a few minutes and review the information from the lab, as you can see there are many modules that have been loaded based on the site.

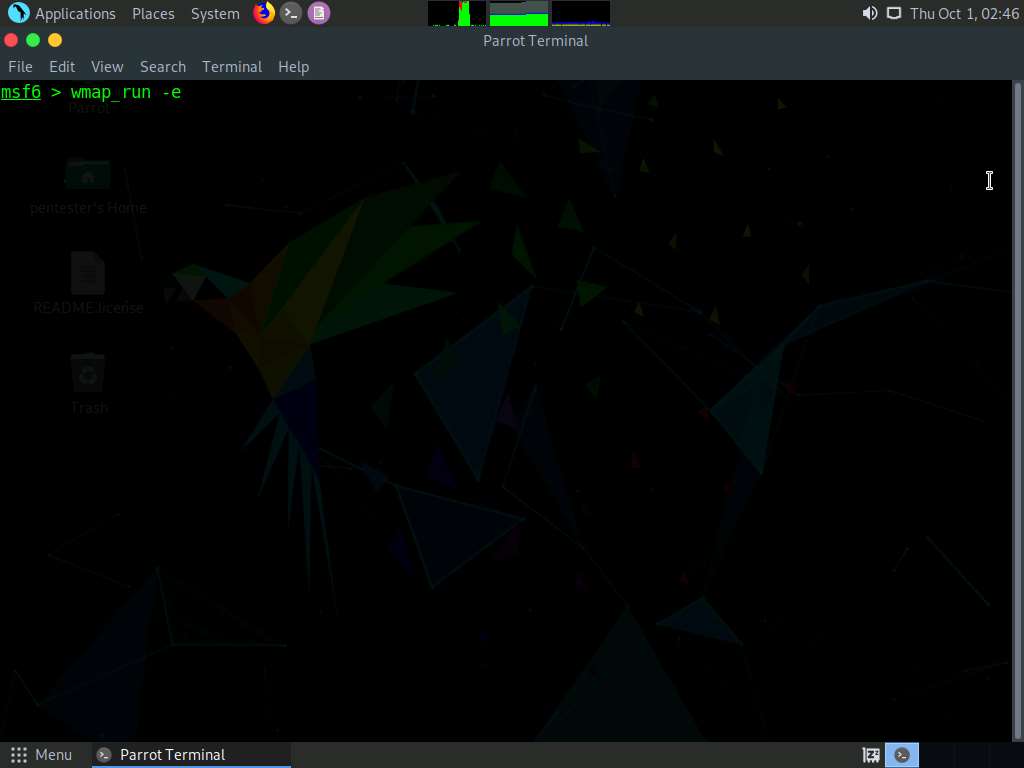


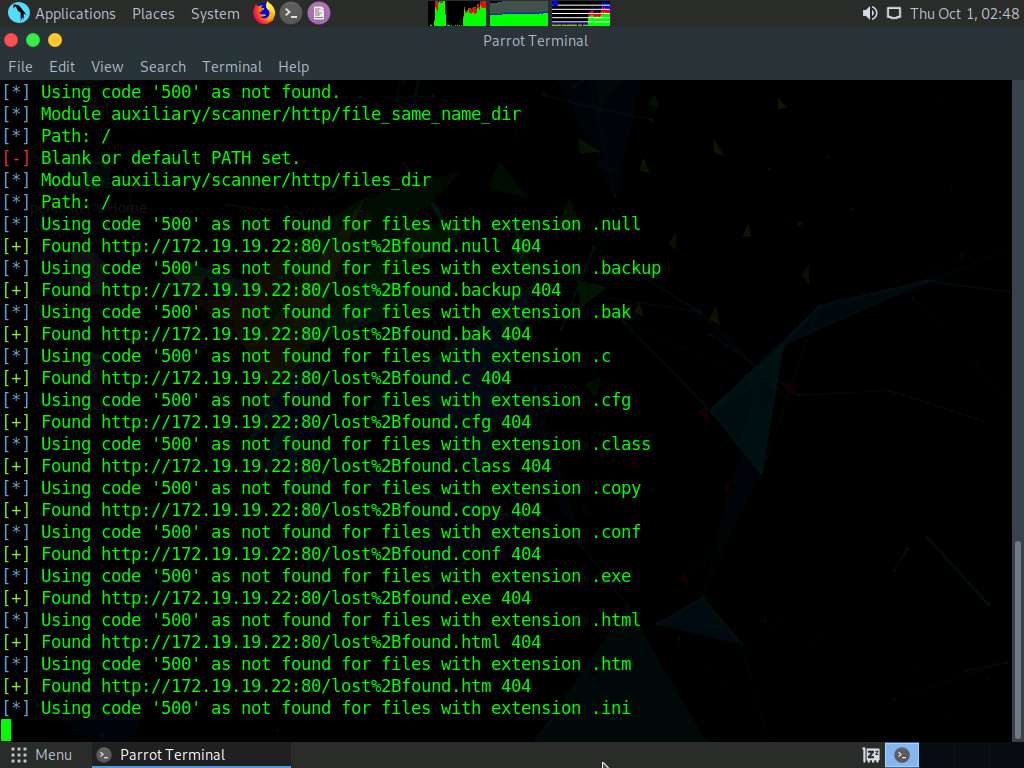


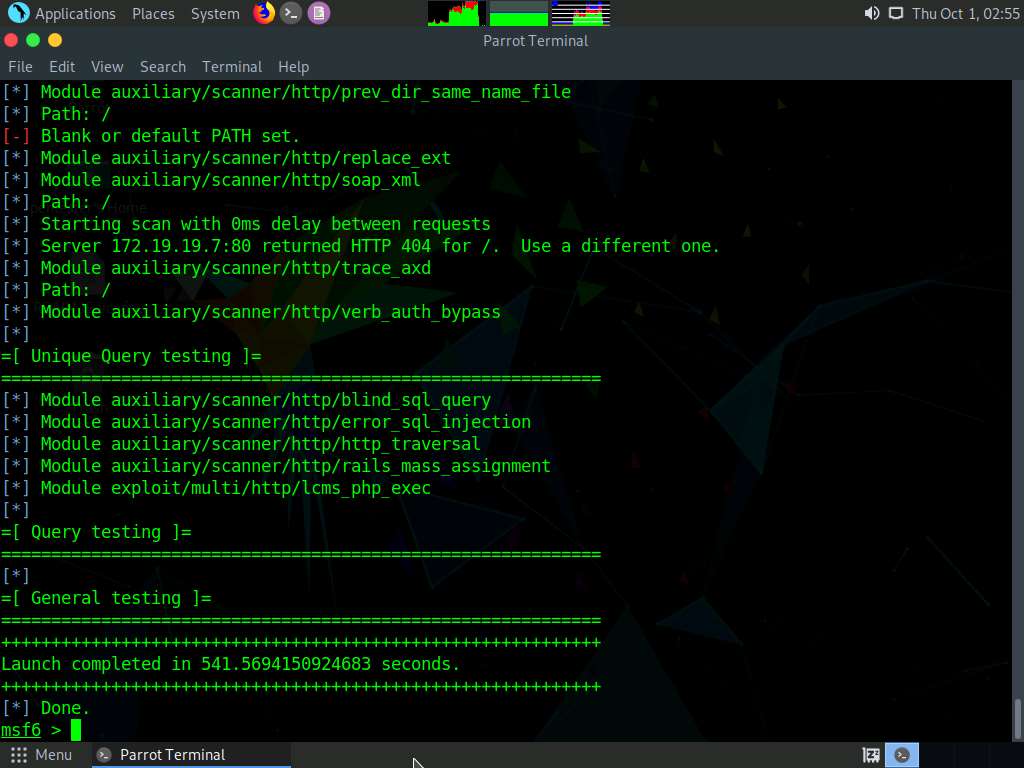




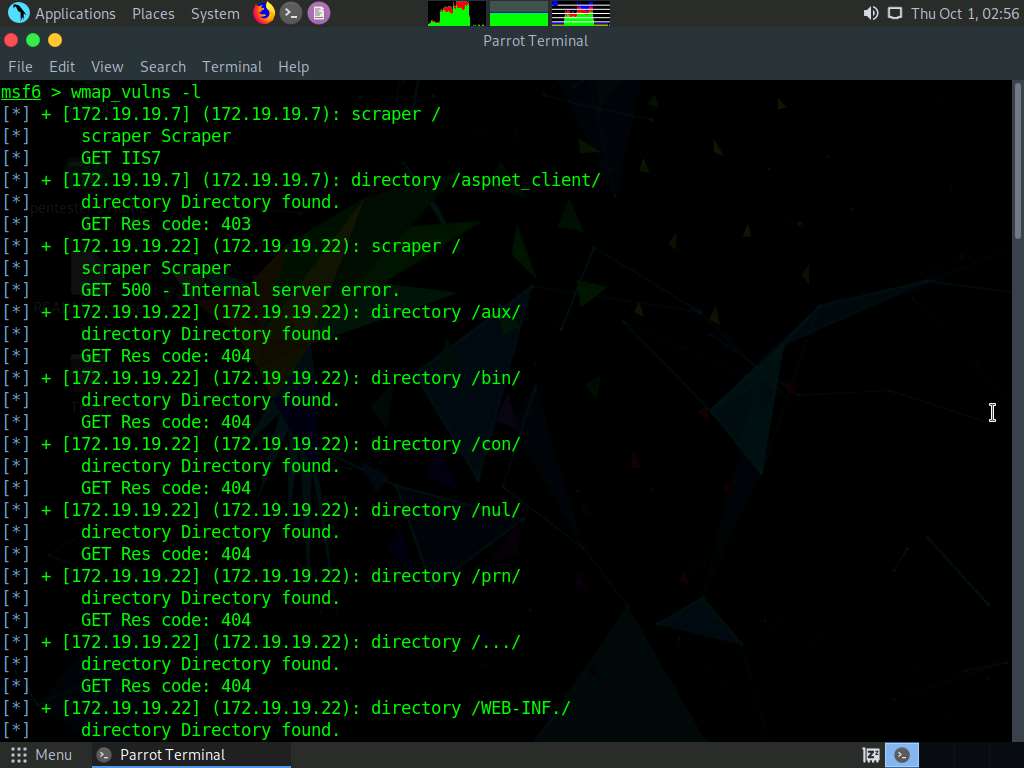
1. Once you have finished reading about the modules, it is now time to run the assessment, type **wmap\_run -e** and press **Enter**. Once the scan has completed, you can review the results of the scan and take a few minutes to look for where the attack surface of the target it, and the vector you think you can use to attack these targets. You can press **Ctrl+C** to terminate the scan, as it will take lot off time to complete since there are a lot of modules.
2. As the scan results show, the **WMAP tool** is not perfect, but it is another tool we can use to compliment our normal web scanning tools like **Nikto** and **Vega**.



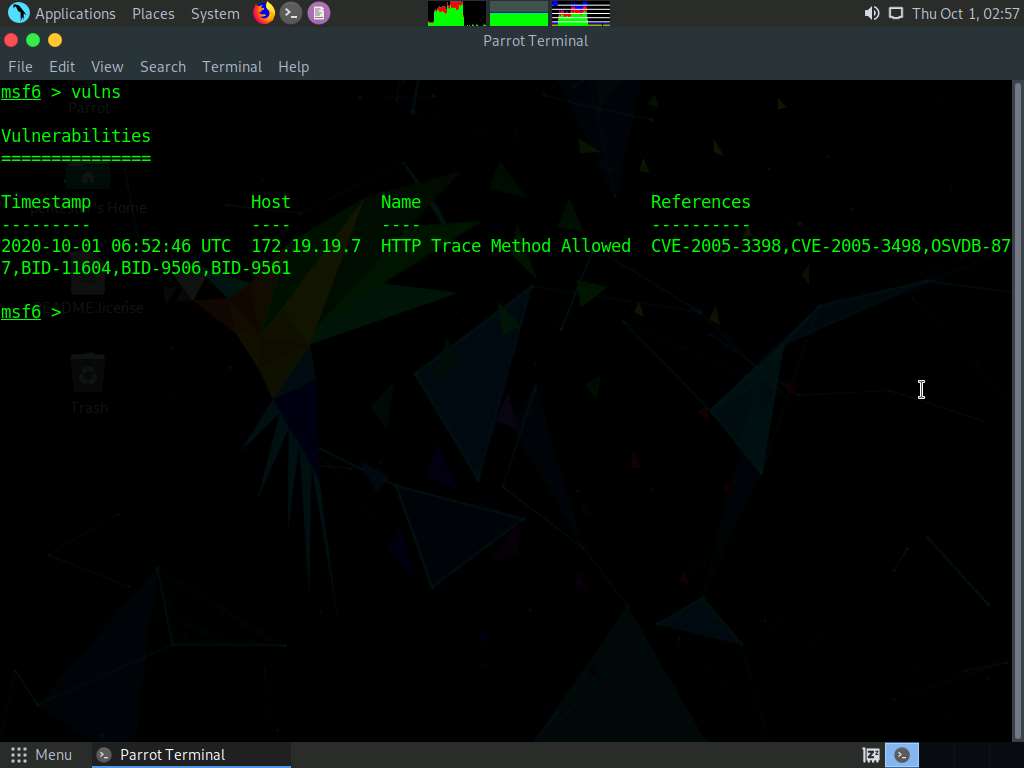




1. To look at the vulnerabilities that have been written to the database, type **wmap\_vulns -l** and press **Enter**.



1. You can also display the vulnerabilities by typing **vulns** and press **Enter**.



1. We have accomplished what we wanted to in this lab, so we can clean up from the exercise and close all programs.

In this lab you have learnt how to:

* Use the tool WMAP that is part of the Metasploit tools
* Scan a web servers with WMAP