Network Penetration Testing Methodology-External

1 Hr 7 Min Remaining

Instructions Resources Help  100%

Exercise 3: Enumerate a Wordpress Site

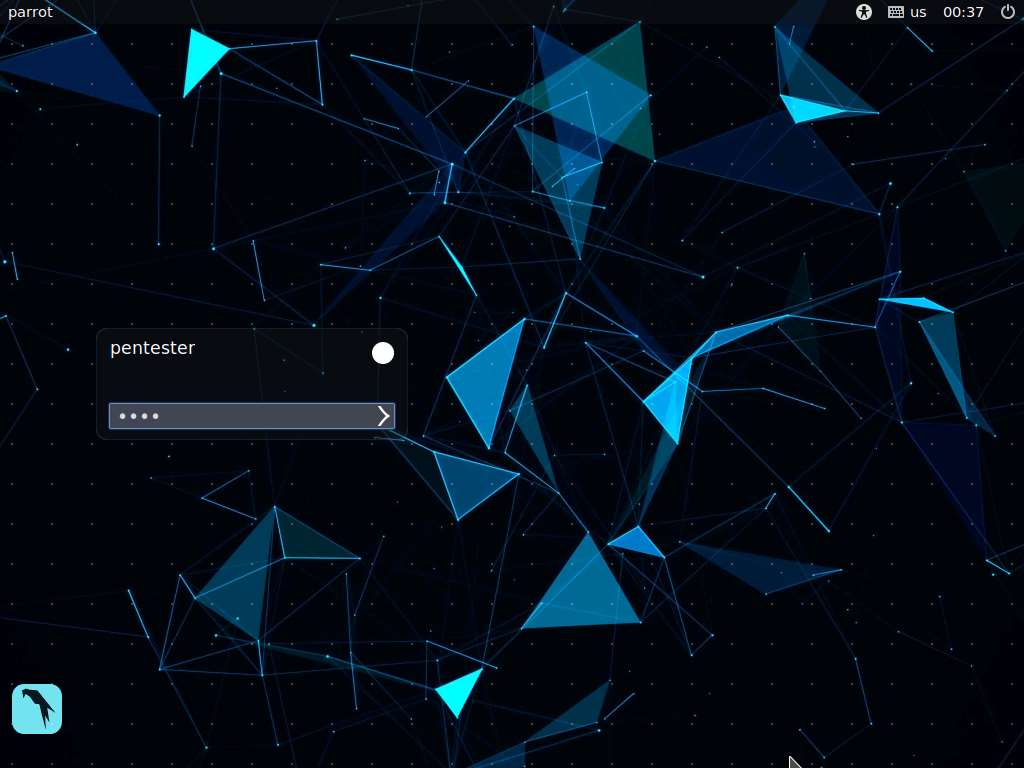
Scenario

In this lab, you will:

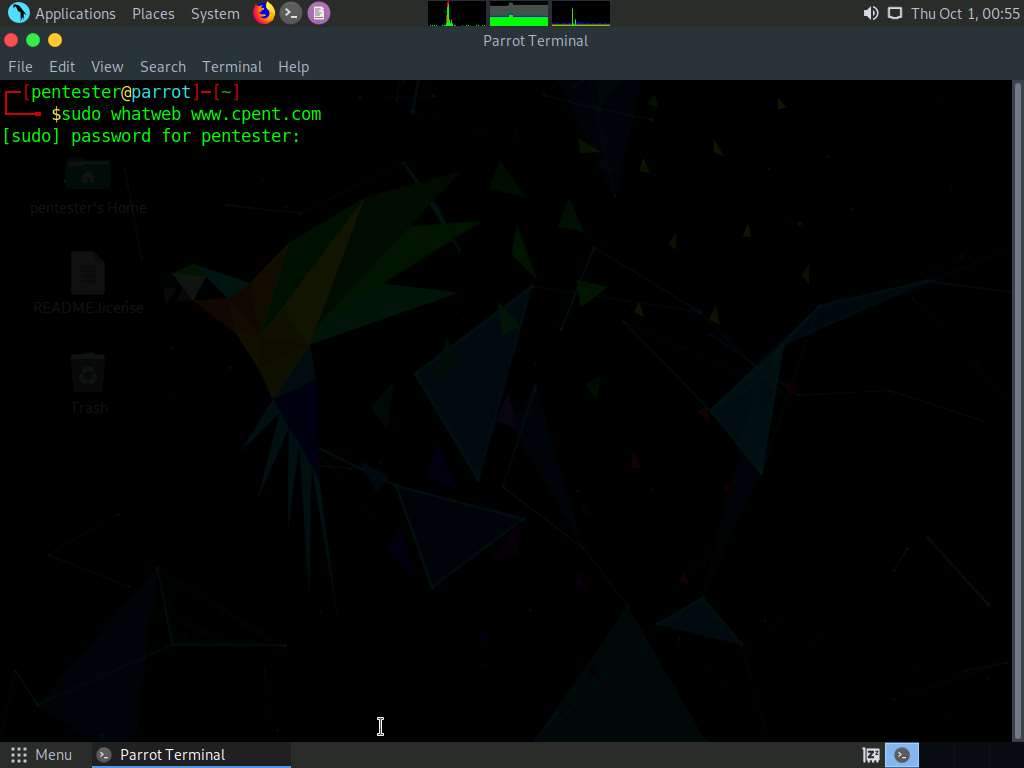
* Use the wpscan tool
* Enumerate a Wordpress site

**Lab Duration**: **25** Minutes

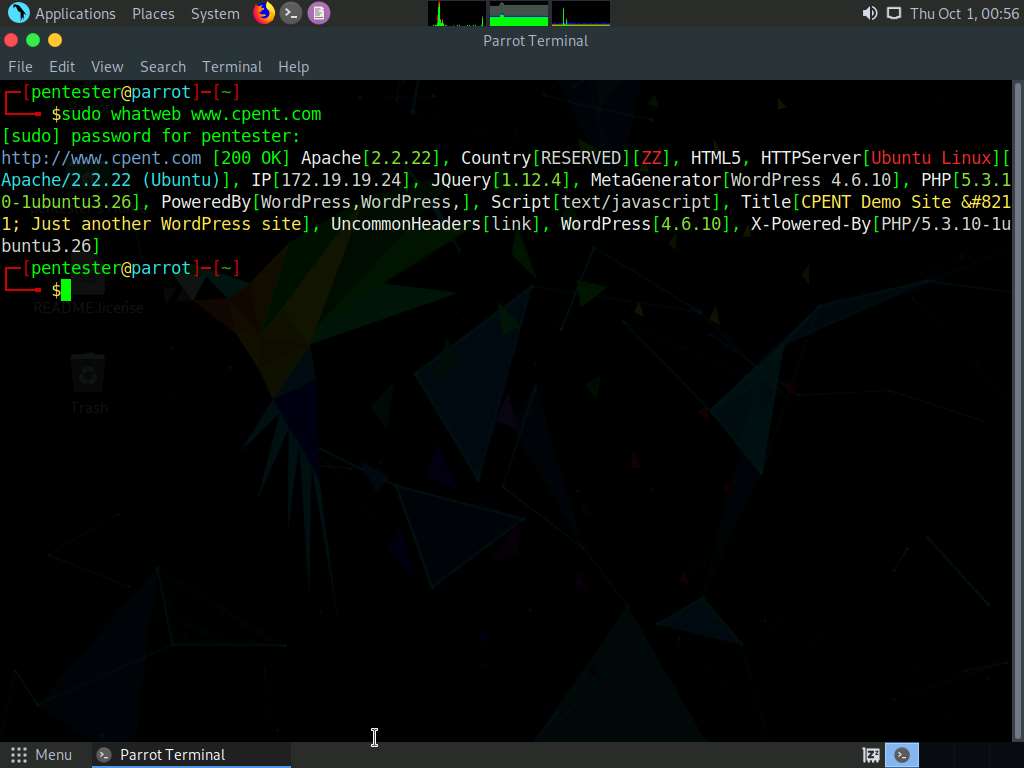
1. Click [Parrot](https://labclient.labondemand.com/Instructions/d51b1821-8ebe-4479-bf4b-33b56a1978d1?rc=10). Parrot logon screen appears, type **toor** in the Password field and press **Enter**.



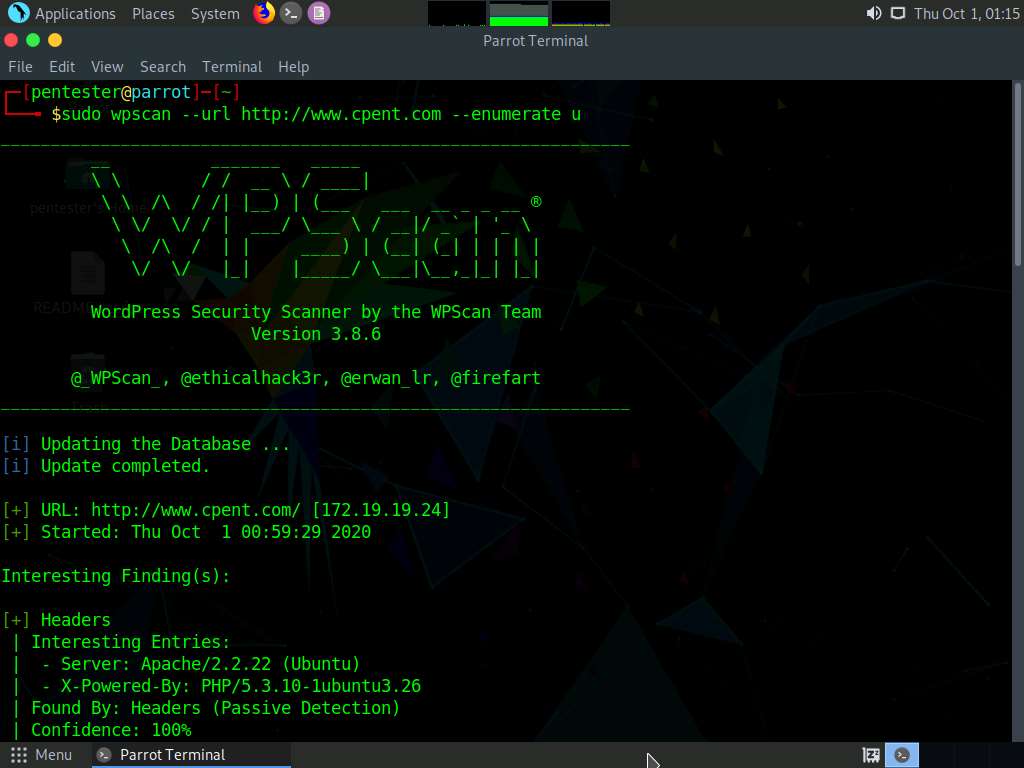
1. Use the **wpscan** tool to scan a website that is running **Wordpress**. First, scan the site to check what installed software and version number come up.
2. Launch a Terminal, and type **sudo whatweb www.cpent.com** and press **Enter**. Type **toor** when prompted for Password and press **Enter**.

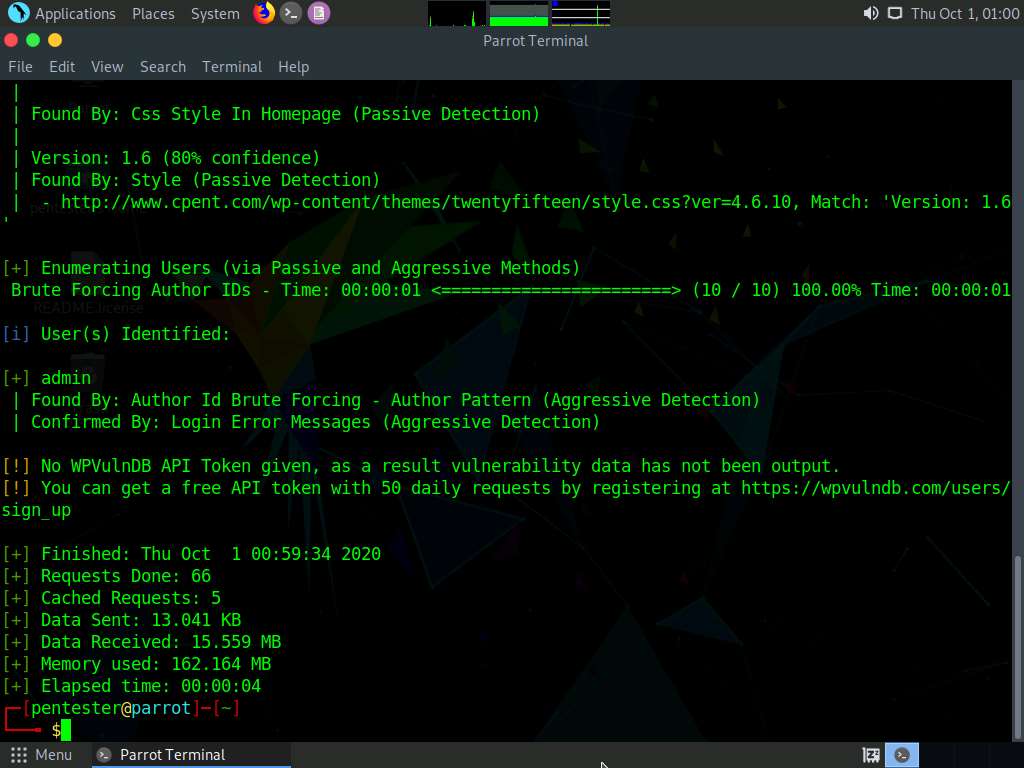


1. Record the information as required onto your target database. Once you are successful, search for vulnerabilities using the version of **Wordpress** available, which is **4.6.10**.

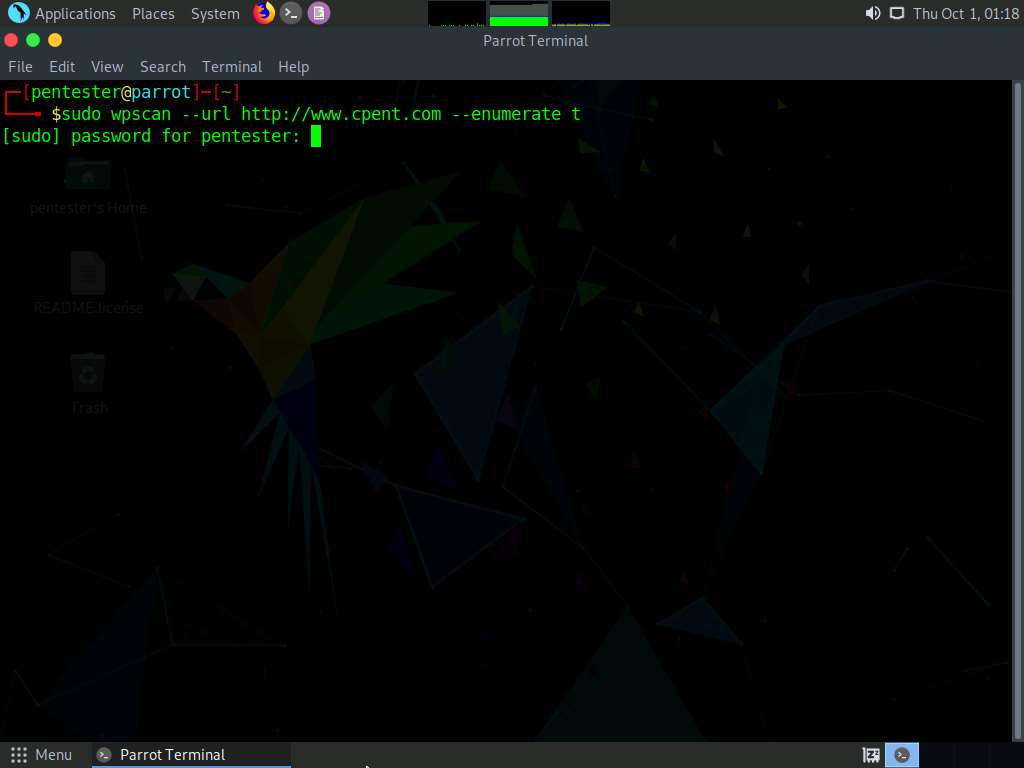


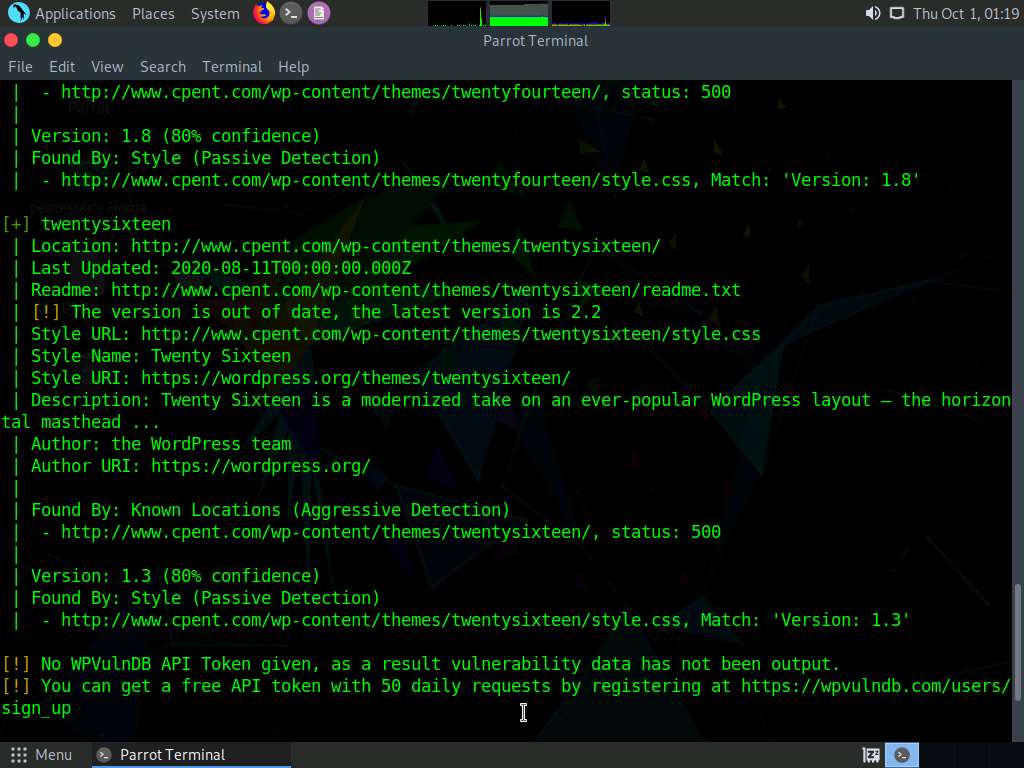
1. Next, scan the Wordpress website with **whatweb** tool. In the terminal type **sudo wpscan --url http://www.cpent.com --enumerate u** and press **Enter**. Type **toor** if prompted for Password and press **Enter**. This will enumerate the users, if there exists any.



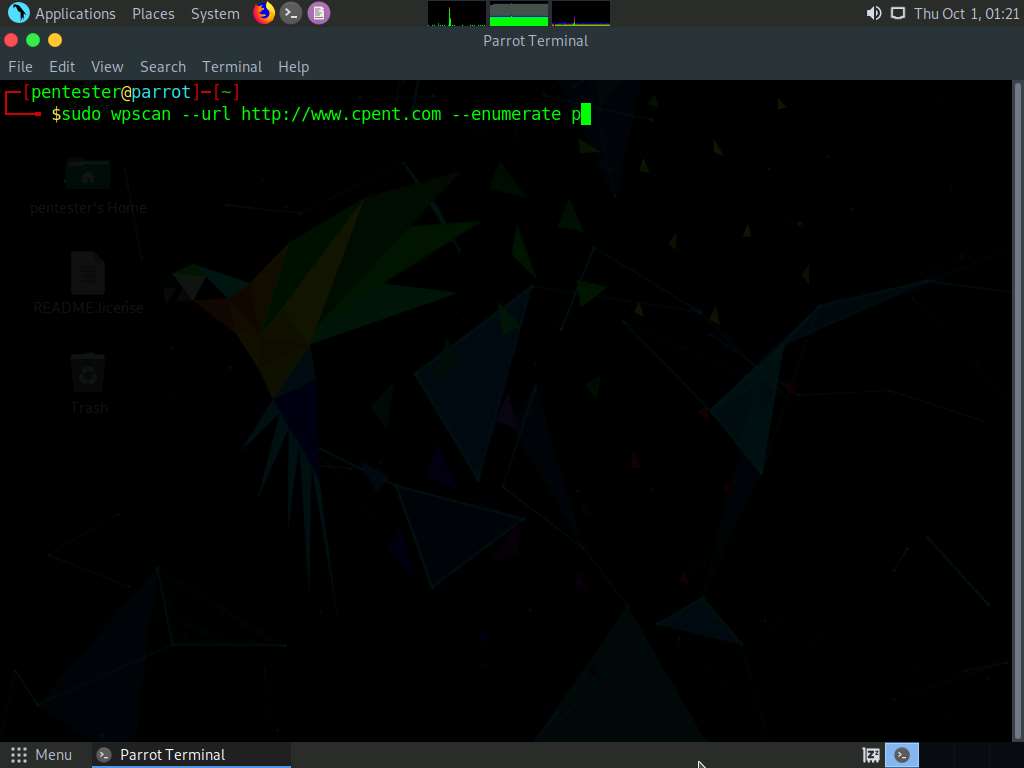


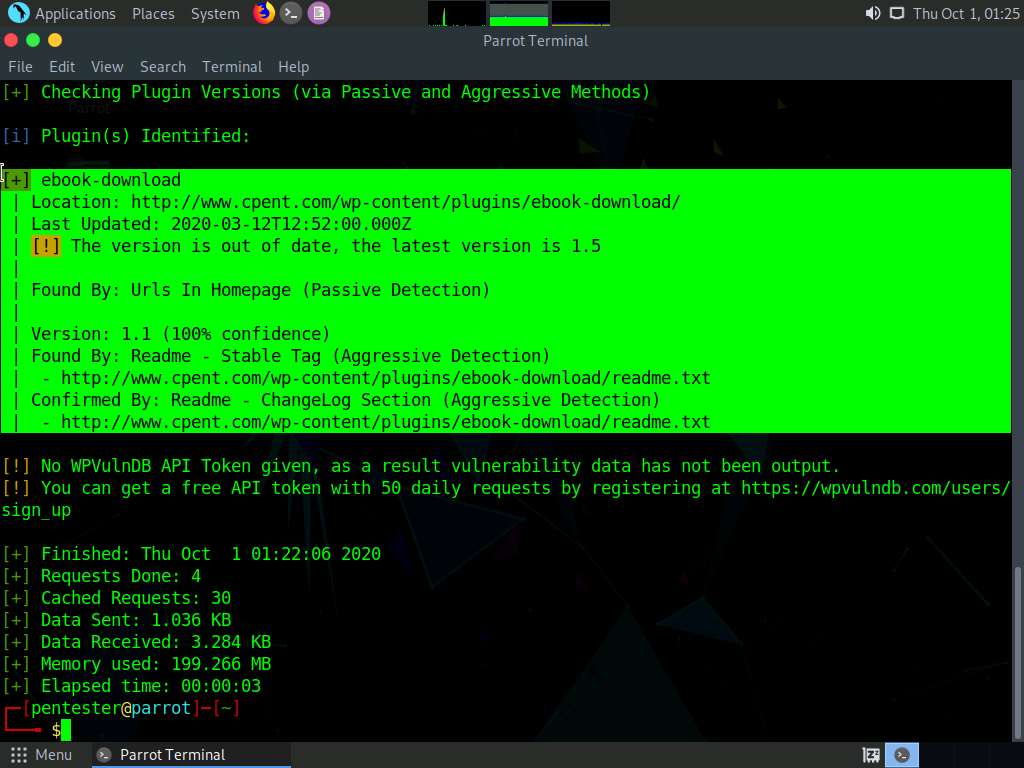
1. Type **sudo wpscan --url http://www.cpent.com --enumerate t** and press **Enter**. Type **toor** if prompted for Password and press **Enter**. This will enumerate the installed themes, if there exists any. Explore all themes that appear.





1. Now, enumerate the plugins. Type **sudo wpscan --url http://www.cpent.com --enumerate p** and press Enter. Type **toor** if prompted for Password and press **Enter**. This will enumerate the installed plugins in the wordpress site, if there exists any.





1. As noted earlier, the process itself is key; once you follow the steps, the data can be enumerated irrespective of the target version.