DIRBUSTER VULNERABILITY SCANNER Software Guide

cloud academy
A QA COMPANY

DIRBUSTER VULNERABILITY SCANNER

This guide covers the basics of using DirBuster, the directory buster. Dirbuster is used once you have scanned an IP address and found any vulnerabilities. DirBuster will help you map out the application.

Why use DirBuster?

Building a directory of the target site is useful in finding as many potential points of entry to the target. This could be done manually, by going through the website and making a note of every page on the site. However, there is a potential for a high error rate; site directories could be wrongly taken down, or missed altogether.

DirBuster automates this process, and builds a map of the site for you, and finds any potential hidden sites.

Install DirBuster

DirBuster comes pre-installed on Kali Linux.

If you need to install DirBuster, enter into your terminal the following line:

```
sudo apt-get install dirbuster
```

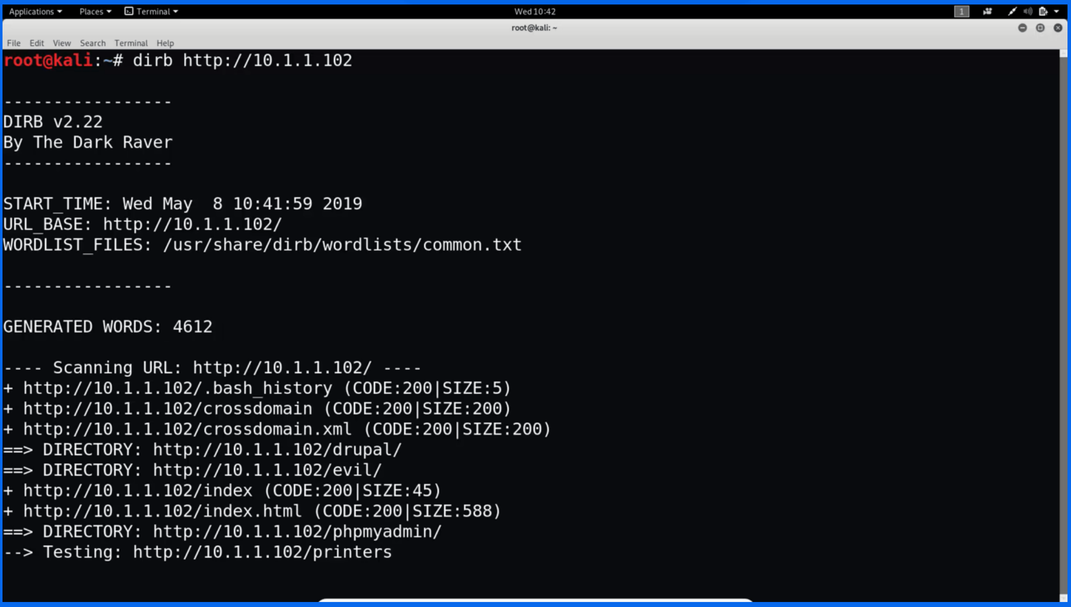
Spider a Website

Spidering, also known as web crawling, is the process of using a script or program to go through a website to get data on the site. This process isn't limited to penetration testing; search engines crawl through websites to get information using a particular search term.

DirBuster uses a similar process and attempts to find hidden pages. It then presents this back.

To launch a spider, you'll need the target IP address. Then enter the following command:

```
dirb [enter target IP address]
```



```
root@kali:~# dirb http://10.1.1.102

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed May  8 10:41:59 2019
URL_BASE: http://10.1.1.102/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.1.1.102/ ----
+ http://10.1.1.102/.bash_history (CODE:200|SIZE:5)
+ http://10.1.1.102/crossdomain (CODE:200|SIZE:200)
+ http://10.1.1.102/crossdomain.xml (CODE:200|SIZE:200)
==> DIRECTORY: http://10.1.1.102/drupal/
==> DIRECTORY: http://10.1.1.102/evil/
+ http://10.1.1.102/index (CODE:200|SIZE:45)
+ http://10.1.1.102/index.html (CODE:200|SIZE:588)
==> DIRECTORY: http://10.1.1.102/phpmyadmin/
--> Testing: http://10.1.1.102/printers
```