Dirb — A web content scanner

Ajay Manoharan · Follow
Published in Tech Zoom · 3 min read · Oct 30, 2017

Dirb Using Kali Linux

What is Dirb

DIRB is a command line based tool to brute force any directory based on wordlists. DIRB will make an HTTP request and see the HTTP response code of each request

How it works

It internally has a wordlist file which has by default around 4000 words for brute force attack. There are a lot of updated wordlists available over the internet which can also be used. Dirb searches for the words in its wordlist in every directory or object of a website or a server. It might be an admin panel or a subdirectory that is vulnerable to attack. The key is to find the objects as they are generally hidden.

How to get it?

Donwload Dirb via Github : https://github.com/seifreed/dirb
Download Dirb via Sourceforge : https://sourceforge.net/projects/dirb/

Note : I used Kali Linux and Dirb comes pre-installed with Kali.

Purpose of Dirb in Security testing:

Purpose of DIRB is to help in professional and web application auditing in security testing. DIRB looks for almost all the web objects that other generic CGI scanners can't look for. It doesn't look for vulnerabilities but it looks for the web contents that can be vulnerable.

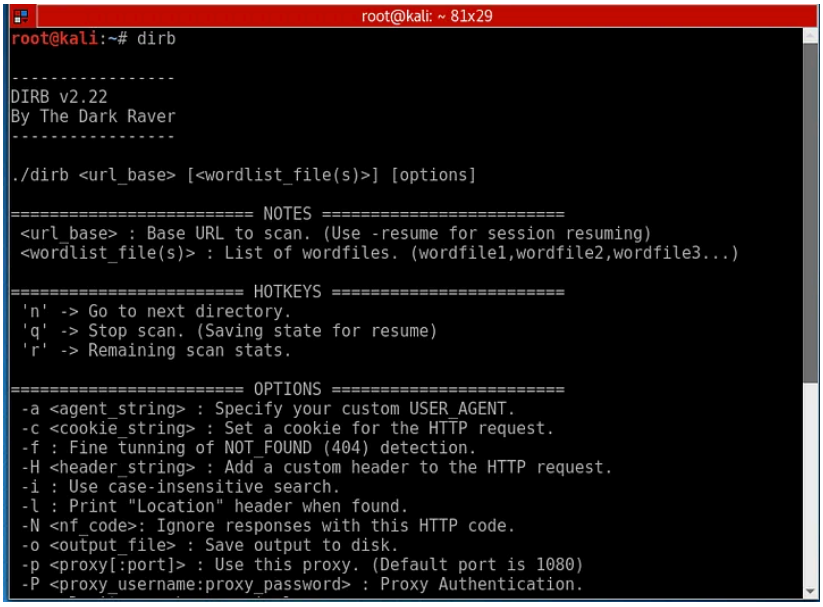
Using Dirb:

Step 1 — Open Terminal

Step 2 — Start Dirb

Once we have a terminal open, go ahead and type **dirb** to get the help screen.

Kali> dirb



As you can see in this screenshot above, DIRB's syntax is very simple with multiple options. In its simplest form, we only need to type the command **dirb** followed by the **URL**of the website we are testing.

Kali> dirb URL

Step 3 — Dirb for simple hidden object scan

with the Dirb's default word list file it searches the URL for 4612 Object types. Let's try it on test site, webscantest.com.

kali > dirb http://webscantest.com

```
root@kali: ~ 81x29
root@kali:~# dirb http://webscantest.com/

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

START_TIME: Mon Oct 30 08:05:15 2017
URL_BASE: http://webscantest.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://webscantest.com/ ----
--> Testing: http://webscantest.com/.passwd
```

DIRB begins the scan looking for those keywords among the website objects.

```
root@kali:~# dirb http://webscantest.com/

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

START_TIME: Mon Oct 30 08:05:15 2017
URL_BASE: http://webscantest.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://webscantest.com/ ----
==> DIRECTORY: http://webscantest.com/business/
==> DIRECTORY: http://webscantest.com/cart/
==> DIRECTORY: http://webscantest.com/css/
+ http://webscantest.com/favicon.ico (CODE:200|SIZE:5430)
==> DIRECTORY: http://webscantest.com/icons/
==> DIRECTORY: http://webscantest.com/images/
```


The results list with the response code and the size of the file for each ping. Also, dirb starts searching the files of the folder which returns the response code as 200. It searches the entire folders with the wordlist and displays the results.

```
-----------------
END_TIME: Wed Feb 10 23:15:51 2016
DOWNLOADED: 54004 - FOUND: 113
root@kali:~#
```

Finally, when DIRB is done, it reports back the number of found objects (113 in this case). Note that in the help screen above, we can use the -o switch to send the results to an output file to save the results to a text file.

Testing for Special Vulnerable list

We can use DIRB to test for specific vulnerable objects within specific types of web technologies. Each web technology has different vulnerabilities. They are NOT all the same. DIRB can help us look for specific vulnerable objects specific to the particular technology.

In Kali, DIRB has specific wordlists to search for these vulnerable often hidden objects. You can find them at:

kali > cd /usr/share/dirb/wordlists/vuln

Then list the contents of that directory:

kali > ls -l

```
total 492
-rw-r--r-- 1 root root    230 Jun 29  2004 apache.txt
-rw-r--r-- 1 root root    259 Dec 30  2011 axis.txt
-rw-r--r-- 1 root root 122829 Aug 30  2007 cgis.txt
-rw-r--r-- 1 root root    706 Jun  7  2005 coldfusion.txt
-rw-r--r-- 1 root root   4648 Oct 26  2011 domino.txt
-rw-r--r-- 1 root root 135331 May 29  2013 fatwire_pagenames.txt
-rw-r--r-- 1 root root   1869 May 17  2011 fatwire.txt
-rw-r--r-- 1 root root    523 Apr  8  2010 frontpage.txt
-rw-r--r-- 1 root root   3896 Mar 16  2012 hpsmh.txt
-rw-r--r-- 1 root root  20644 May 13  2009 hyperion.txt
-rw-r--r-- 1 root root    485 May 31  2004 iis.txt
-rw-r--r-- 1 root root    365 May 24  2004 iplanet.txt
-rw-r--r-- 1 root root    395 Oct  9  2013 jboss.txt
-rw-r--r-- 1 root root   2148 Apr 29  2013 jersey.txt
-rw-r--r-- 1 root root    306 Jun  7  2005 jrun.txt
-rw-r--r-- 1 root root    465 Nov  9  2008 netware.txt
-rw-r--r-- 1 root root  29182 Sep 20  2013 oracle.txt
-rw-r--r-- 1 root root   2442 Jun 29  2012 ror.txt
-rw-r--r-- 1 root root  33300 Oct  1  2013 sap.txt
-rw-r--r-- 1 root root  44075 Sep 15  2011 sharepoint.txt
-rw-r--r-- 1 root root    970 Sep  7  2004 sunas.txt
-rw-r--r-- 1 root root    220 Oct 19  2003 tests.txt
-rw-r--r-- 1 root root   2474 Feb  1  2012 tomcat.txt
-rw-r--r-- 1 root root    536 Feb  6  2007 vignette.txt
-rw-r--r-- 1 root root   7117 Aug 27  2013 weblogic.txt
-rw-r--r-- 1 root root  12564 Jun 27  2013 websphere.txt
root@kali:/usr/share/dirb/wordlists/vulns#
```

As you can see above, there is a number of file list for each of the specific vulnerability to test. If your web server is Apache and you want to test it use apache.txt

To run

kali > dirb http://webscantest.com /usr/share/dirb/wordlists/vulns/apache.txt

Hacking Dirb

Written by Ajay Manoharan

86 Followers · Writer for Tech Zoom