专注APT攻击与防御

https://micropoor.blogspot.com/

DIRB官方地址：

http://dirb.sourceforge.net/

简介（摘自官方原文）：

DIRB is a Web Content Scanner. It looks for existing (and/or hidden) Web Objects. It basically works by launching a dictionary based attack against a web server and analizing the response.

介绍：

DIRB是一个基于命令行的工具，依据字典来爆破目标Web路径以及敏感文件，它支持自定义UA，cookie，忽略指定响应吗，支持代理扫描，自定义毫秒延迟，证书加载扫描等。是一款非常优秀的全方位的目录扫描工具。同样Kaili内置了dirb。

攻击机： 192.168.1.104 Debian

靶机： 192.168.1.102 Windows 2003 IIS

普通爆破：

1 root@John:~/wordlist/small# dirb http://192.168.1.102 ./ASPX.txt 2

3 ‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐

4 DIRB v2.22

5 By The Dark Raver

6 ‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐ 7

8 START\_TIME: Sun Feb 17 23:26:52 2019

9 URL\_BASE: http://192.168.1.102/

10 WORDLIST\_FILES: ./ASPX.txt 11

12 ‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐ 13

14 GENERATED WORDS: 822 15

16 ‐‐‐‐ Scanning URL: http://192.168.1.102/ ‐‐‐‐

17 + http://192.168.1.102//Index.aspx (CODE:200|SIZE:2749)

18 + http://192.168.1.102//Manage/Default.aspx (CODE:302|SIZE:203) 19

20 ‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐

21 END\_TIME: Sun Feb 17 23:26:56 2019

22 DOWNLOADED: 822 ‐ FOUND: 2

多字典挂载：

1 root@John:~/wordlist/small# dirb http://192.168.1.102 ./ASPX.txt,./DI R.txt

2

3 ‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐

4 DIRB v2.22

5 By The Dark Raver

6 ‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐ 7

8 START\_TIME: Sun Feb 17 23:31:02 2019

9 URL\_BASE: http://192.168.1.102/

10 WORDLIST\_FILES: ./ASPX.txt,./DIR.txt 11

12 ‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐ 13

14 GENERATED WORDS: 1975 15

16 ‐‐‐‐ Scanning URL: http://192.168.1.102/ ‐‐‐‐

17 + http://192.168.1.102//Index.aspx (CODE:200|SIZE:2749)

18 + http://192.168.1.102//Manage/Default.aspx (CODE:302|SIZE:203)

19 + http://192.168.1.102//bbs (CODE:301|SIZE:148)

20 + http://192.168.1.102//manage (CODE:301|SIZE:151)

21 + http://192.168.1.102//manage/ (CODE:302|SIZE:203)

22 + http://192.168.1.102//kindeditor/ (CODE:403|SIZE:218)

23 + http://192.168.1.102//robots.txt (CODE:200|SIZE:214)

24 + http://192.168.1.102//Web.config (CODE:302|SIZE:130)

25 + http://192.168.1.102//files (CODE:301|SIZE:150)

26 + http://192.168.1.102//install (CODE:301|SIZE:152) 27

28 (!) FATAL: Too many errors connecting to host

29 (Possible cause: EMPTY REPLY FROM SERVER) 30

31 ‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐

32 END\_TIME: Sun Feb 17 23:31:06 2019

33 DOWNLOADED: 1495 ‐ FOUND: 10

自定义UA：

1 root@John:~/wordlist/small# dirb http://192.168.1.102 ./ASPX.txt ‐a "M ozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"

2

3 ‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐

4 DIRB v2.22

5 By The Dark Raver

6 ‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐ 7

8 START\_TIME: Sun Feb 17 23:34:51 2019

9 URL\_BASE: http://192.168.1.102/

10 WORDLIST\_FILES: ./ASPX.txt

11 USER\_AGENT: Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.googl e.com/bot.html)

12

13 ‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐ 14

15 GENERATED WORDS: 822

16

17 ‐‐‐‐ Scanning URL: http://192.168.1.102/ ‐‐‐‐

18 + http://192.168.1.102//Index.aspx (CODE:200|SIZE:2735)

19 + http://192.168.1.102//Manage/Default.aspx (CODE:302|SIZE:203) 20

21 ‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐

22 END\_TIME: Sun Feb 17 23:34:54 2019

23 DOWNLOADED: 822 ‐ FOUND: 2

自定义cookie：

1 root@John:~/wordlist/small# dirb http://192.168.1.102/Manage ./DIR.txt ‐a "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.ht ml)" ‐c "ASP.NET\_SessionId=jennqviqmc2vws55o4ggwu45"

2

3 ‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐

4 DIRB v2.22

5 By The Dark Raver

6 ‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐ 7

8 START\_TIME: Sun Feb 17 23:53:08 2019

9 URL\_BASE: http://192.168.1.102/Manage/

10 WORDLIST\_FILES: ./DIR.txt

11 USER\_AGENT: Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.googl e.com/bot.html)

12 COOKIE: ASP.NET\_SessionId=jennqviqmc2vws55o4ggwu45 13

14 ‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐ 15

16 GENERATED WORDS: 1153 17

18 ‐‐‐‐ Scanning URL: http://192.168.1.102/Manage/ ‐‐‐‐

19 + http://192.168.1.102/Manage//include/ (CODE:403|SIZE:218)

20 + http://192.168.1.102/Manage//news/ (CODE:403|SIZE:218)

21 + http://192.168.1.102/Manage//include (CODE:301|SIZE:159)

22 + http://192.168.1.102/Manage//images/ (CODE:403|SIZE:218)

23 + http://192.168.1.102/Manage//sys/ (CODE:403|SIZE:218)

24 + http://192.168.1.102/Manage//images (CODE:301|SIZE:158) 25

26 (!) FATAL: Too many errors connecting to host

27 (Possible cause: EMPTY REPLY FROM SERVER) 28

29 ‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐

30 END\_TIME: Sun Feb 17 23:53:10 2019

31 DOWNLOADED: 673 ‐ FOUND: 6

自定义毫秒延迟：

1 root@John:~/wordlist/small# dirb http://192.168.1.102/Manage ./DIR.txt ‐a "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.ht ml)" ‐c "ASP.NET\_SessionId=jennqviqmc2vws55o4ggwu45" ‐z 100

2

3 ‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐

4 DIRB v2.22

5 By The Dark Raver

6 ‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐ 7

8 START\_TIME: Sun Feb 17 23:54:29 2019

9 URL\_BASE: http://192.168.1.102/Manage/

10 WORDLIST\_FILES: ./DIR.txt

11 USER\_AGENT: Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.googl e.com/bot.html)

12 COOKIE: ASP.NET\_SessionId=jennqviqmc2vws55o4ggwu45

13 SPEED\_DELAY: 100 milliseconds 14

15 ‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐ 16

17 GENERATED WORDS: 1153 18

19 ‐‐‐‐ Scanning URL: http://192.168.1.102/Manage/ ‐‐‐‐

20 + http://192.168.1.102/Manage//include/ (CODE:403|SIZE:218)

21 + http://192.168.1.102/Manage//news/ (CODE:403|SIZE:218)

22 + http://192.168.1.102/Manage//include (CODE:301|SIZE:159)

23 + http://192.168.1.102/Manage//images/ (CODE:403|SIZE:218)

24 + http://192.168.1.102/Manage//sys/ (CODE:403|SIZE:218)

25 + http://192.168.1.102/Manage//images (CODE:301|SIZE:158) 26

27 (!) FATAL: Too many errors connecting to host

28 (Possible cause: EMPTY REPLY FROM SERVER) 29

30 ‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐

31 END\_TIME: Sun Feb 17 23:55:50 2019

32 DOWNLOADED: 673 ‐ FOUND: 6

其他更多有趣的功能：

1 DIRB v2.22

2 By The Dark Raver

3 ‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐ 4

5 dirb <url\_base> [<wordlist\_file(s)>] [options] 6

7 ========================= NOTES =========================

8 <url\_base> : Base URL to scan. (Use ‐resume for session resuming)

9 <wordlist\_file(s)> : List of wordfiles. (wordfile1,wordfile2,wordfile 3...)

10

11 ======================== HOTKEYS ========================

12 'n' ‐> Go to next directory.

13 'q' ‐> Stop scan. (Saving state for resume)

14 'r' ‐> Remaining scan stats.

15

16 ======================== OPTIONS ========================

17 ‐a <agent\_string> : Specify your custom USER\_AGENT.

18 ‐b : Use path as is.

19 ‐c <cookie\_string> : Set a cookie for the HTTP request.

20 ‐E <certificate> : path to the client certificate.

21 ‐f : Fine tunning of NOT\_FOUND (404) detection.

22 ‐H <header\_string> : Add a custom header to the HTTP request.

23 ‐i : Use case‐insensitive search.

24 ‐l : Print "Location" header when found.

25 ‐N <nf\_code>: Ignore responses with this HTTP code.

26 ‐o <output\_file> : Save output to disk.

27 ‐p <proxy[:port]> : Use this proxy. (Default port is 1080)

28 ‐P <proxy\_username:proxy\_password> : Proxy Authentication.

29 ‐r : Don't search recursively.

30 ‐R : Interactive recursion. (Asks for each directory)

31 ‐S : Silent Mode. Don't show tested words. (For dumb terminals)

32 ‐t : Don't force an ending '/' on URLs.

33 ‐u <username:password> : HTTP Authentication.

34 ‐v : Show also NOT\_FOUND pages.

35 ‐w : Don't stop on WARNING messages.

36 ‐X <extensions> / ‐x <exts\_file> : Append each word with this extensi ons.

37 ‐z <millisecs> : Add a milliseconds delay to not cause excessive Floo d.

38

39 ======================== EXAMPLES =======================

40 dirb http://url/directory/ (Simple Test)

41 dirb http://url/ ‐X .html (Test files with '.html' extension)

42 dirb http://url/ /usr/share/dirb/wordlists/vulns/apache.txt (Test wit h apache.txt wordlist)

43 dirb https://secure\_url/ (Simple Test with SSL)

Micropoor