

**Introduction**

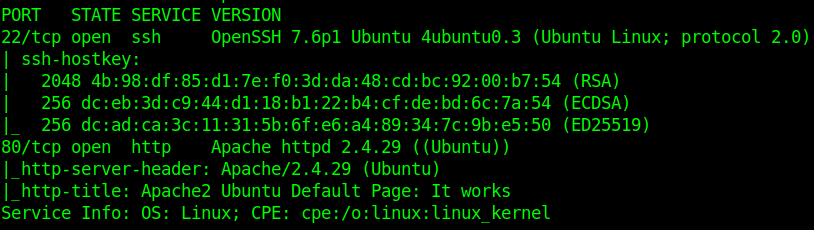
OpenAdmin est une box Linux dont l’adresse IP est 10.10.10.171.

Compétences mises en œuvre :

**Enumération** **initiale**

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

|  |
| --- |
| $ nmap -T4 -A 10.10.10.171 |



Deux ports sont ouverts :

* 22 pour un serveur ssh.
* 80 pour un serveur web.

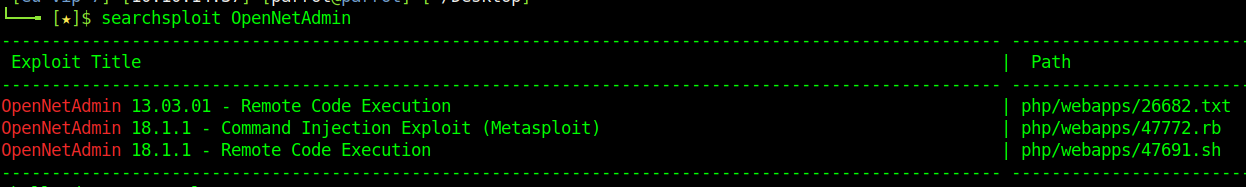
Nous lançons une énumération de fichier/dossier sur le port 80 avec dirsearch :

|  |
| --- |
| $ python3 dirsearch -w wordlist -u <http://10.10.10.171/> -x 403 -f -t 100 -e "html,php" |

**Obtenir un accès utilisateur**

La page <http://10.10.10.171>/ona est très intéressante, elle nous révèle qu’un OpenNetAdmin est installé sur la machine en version 18.1.1. En recherchant avec searchsploit, nous avons plusieurs exploits qui correspond :

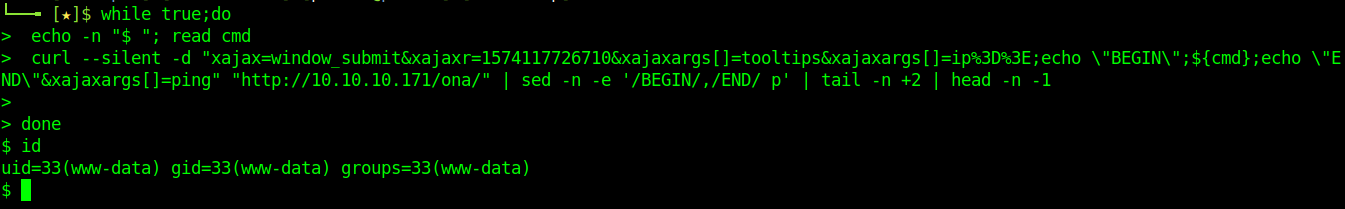
|  |
| --- |
| $ searchsploit OpenNetAdmin |



Nous allons tenter la RCE :

|  |
| --- |
| $ locate 47691.sh  $ cp /usr/share/exploitdb/exploits/php/webapps/47691.sh ./exploit .sh |

Malheureusement le script bash ne fonctionne pas en tant que script, il faut alors copier-coller en one-liner les commandes :



En explorant la base de données du site, on peut récupérer un login et un mot de passe :



En listant le dossier /home/, nous pouvons voir deux utilisateurs : jimmy et joanna. Le mot de passe vu plus tôt fonctionne sur jimmy en SSH. Le fichier user.txt étant dans le home de joanna, nous somme obligés de faire plus d’énumération afin de faire une élévation latérale.

**Obtenir un accès administrateur**

Bla