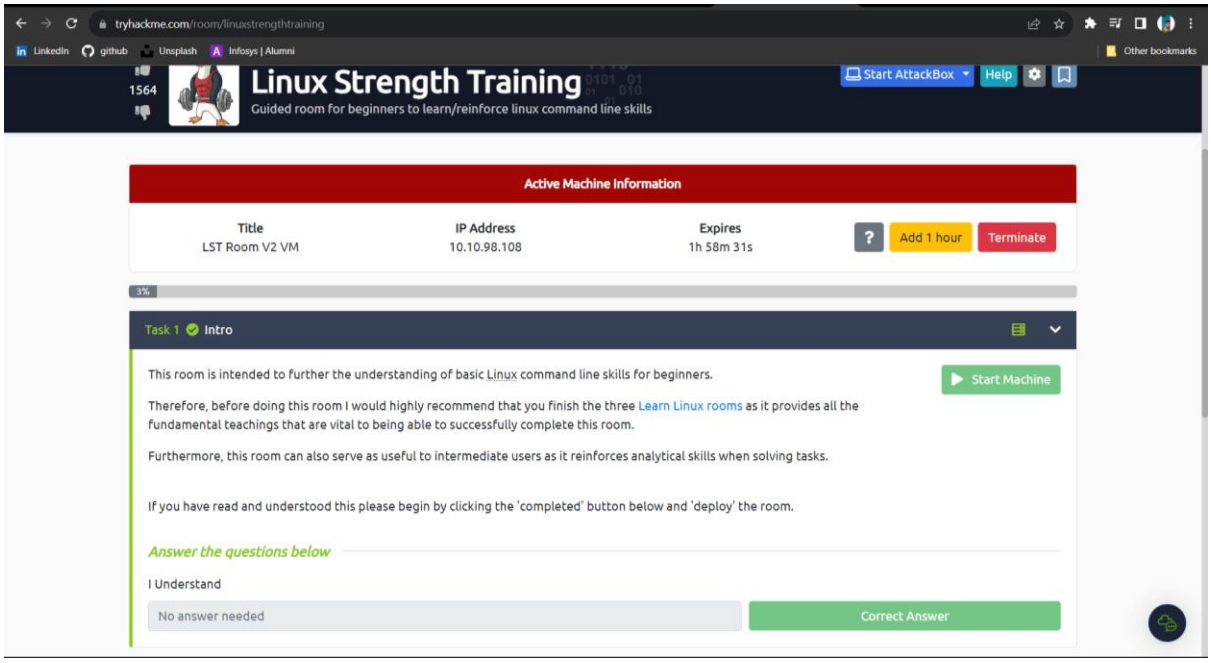
Assignment 2

THE CYBERHOST Cyber Security Intern

Task 1: Intro

First, we have to join the room to access the room then we just have to deploy the attached VM and start the Machine.



After starting the machine, we will get an IP Address after 60 seconds. And the task will be completed.

Task 2: Finding your way around Linux – overview

Q1. I have read and understood

A1. No answer needed

Q2. What is the correct option for finding files based on group

A2. -group

Q3. What is format for finding a file with the user named Francis and with a size of 52 kilobytes in the directory /home/francis/

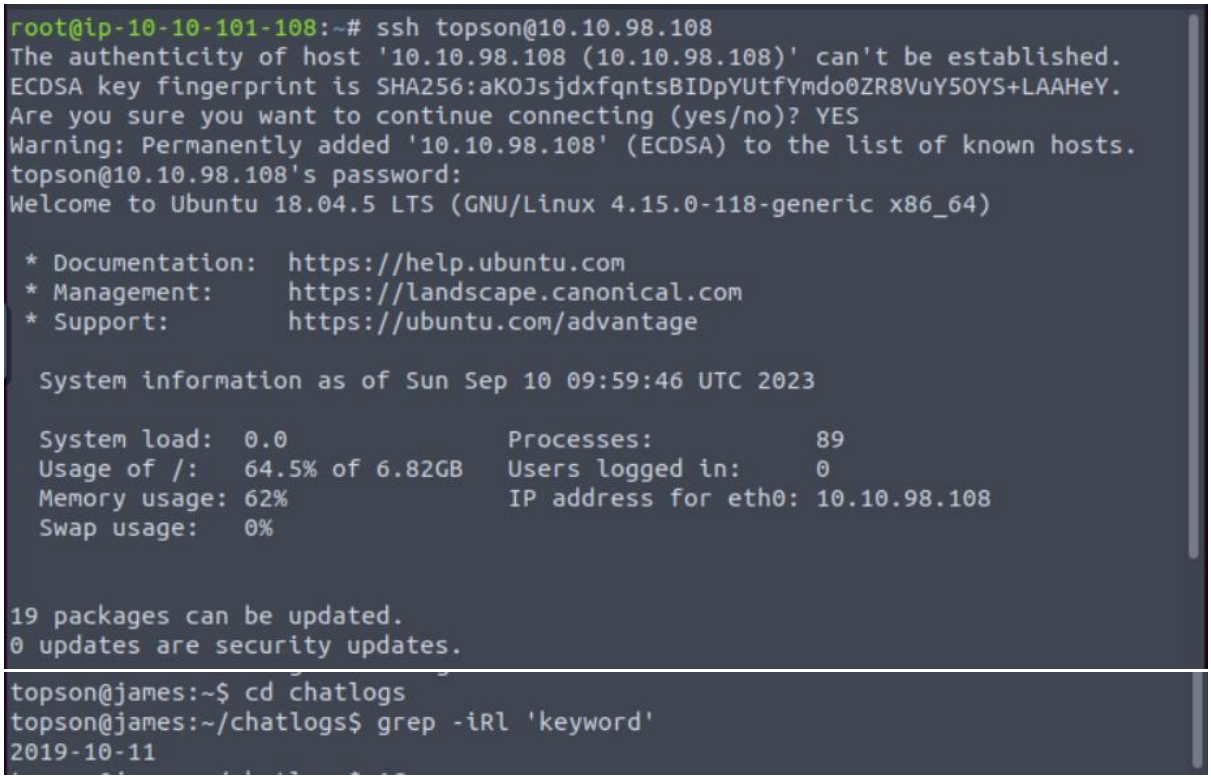
A3. find /home/francis/ -type f -user francis -size 52k

Combining the below two query we can get the answer to the question. First enter the username query then combine the query with size query.

Find files based on size	find [directory path] -type f -size [size]	find /home/Andy -type f -size 10c (c for bytes, k for kilobytes M megabytes G for gigabytes type:'man find' for full information on the options)
Find files based on username	find [directory path] -type f -user [username]	find /etc/server -type f -user john

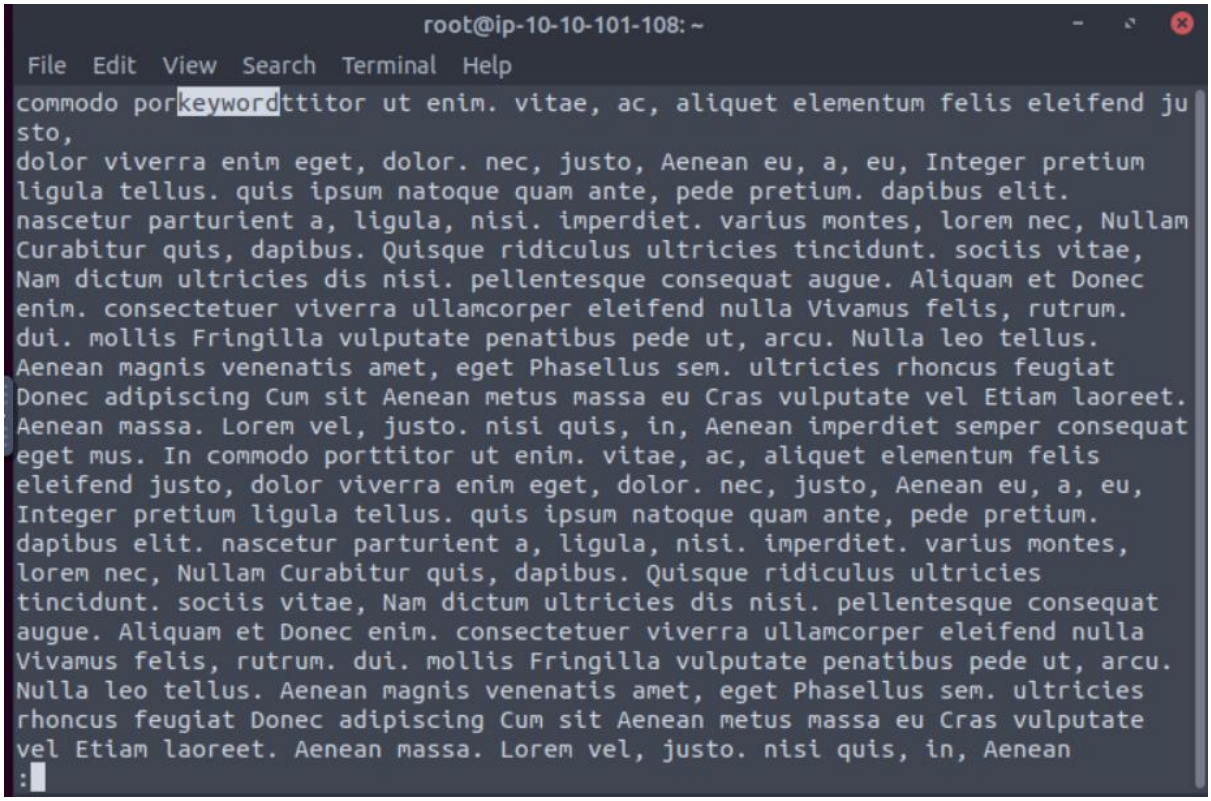
Q4. SSH as topson using his password topson. Go to the /home/topson/chatlogs directory and type the following: grep -iRl 'keyword'. What is the name of the file that you found using this command?

A4. 2019-10-11



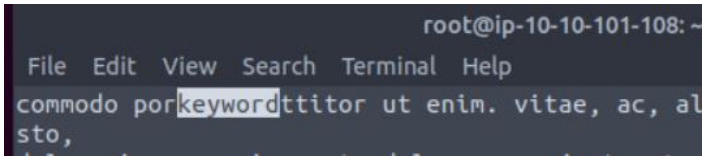
Q5. Type: less [filename] to open the file. Then, before anything, type / before typing: keyword followed by [ENTER]. Notice how that allowed us to search for the first instance of that word in the entire document. For much larger documents this can be useful and if there are many more instances of that word in the document, we would be able to hit enter again to find the next instance in the document.

A5. No answer needed.



Q6. What are the characters subsequent to the word you found?

A6. ttitor



Q7. Read the file named 'ReadMeIfStuck.txt'. What is the Flag?

A7. Flag{81726350827fe53g}

```
topson@james:~$ ls
billings  chatlogs     corperateFiles  ReadMeIfStuck.txt
channels  clientslogs  meetings        workflows
topson@james:~$ cat ReadMeIfStuck.txt
Looking for flag 1?:It seems you will have to think harder if you want to find t
he flag. Perhaps try looking for a file called additionalHINT if you can't find
it..
Looking for flag 2?: look for a file named readME_hint.txt
topson@james:~$
```

```
topson@james:~$ find / -type f -name additionalHINT 2>/dev/null
/home/topson/channels/additionalHINT
topson@james:~$
```

I used 2>/dev/null to avoid getting error messages.

```
topson@james:~$ cat /home/topson/channels/additionalHINT
try to find a directory called telephone numbers... Oh wait.. it  contains a spa
ce.. I wonder how we can find that....
topson@james:~$
```

```
topson@james:~$ find / -type d -name "telephone numbers" 2>/dev/null
/home/topson/corperateFiles/xch/telephone numbers
topson@james:~$
```

```
topson@james:~$ cd /home/topson/corperateFiles/xch
topson@james:~/corperateFiles/xch$ ls
 EguOYOKVD   kMnGQJxue   'telephone numbers'   YXNLOlwMF
 jFGmcDl     pMsBsgXdk    yikJfMW
topson@james:~/corperateFiles/xch$ cd telephone\numbers
-bash: cd: telephonenumbers: No such file or directory
topson@james:~/corperateFiles/xch$ cd telephone\ numbers
topson@james:~/corperateFiles/xch/telephone numbers$ ls
readME.txt
```

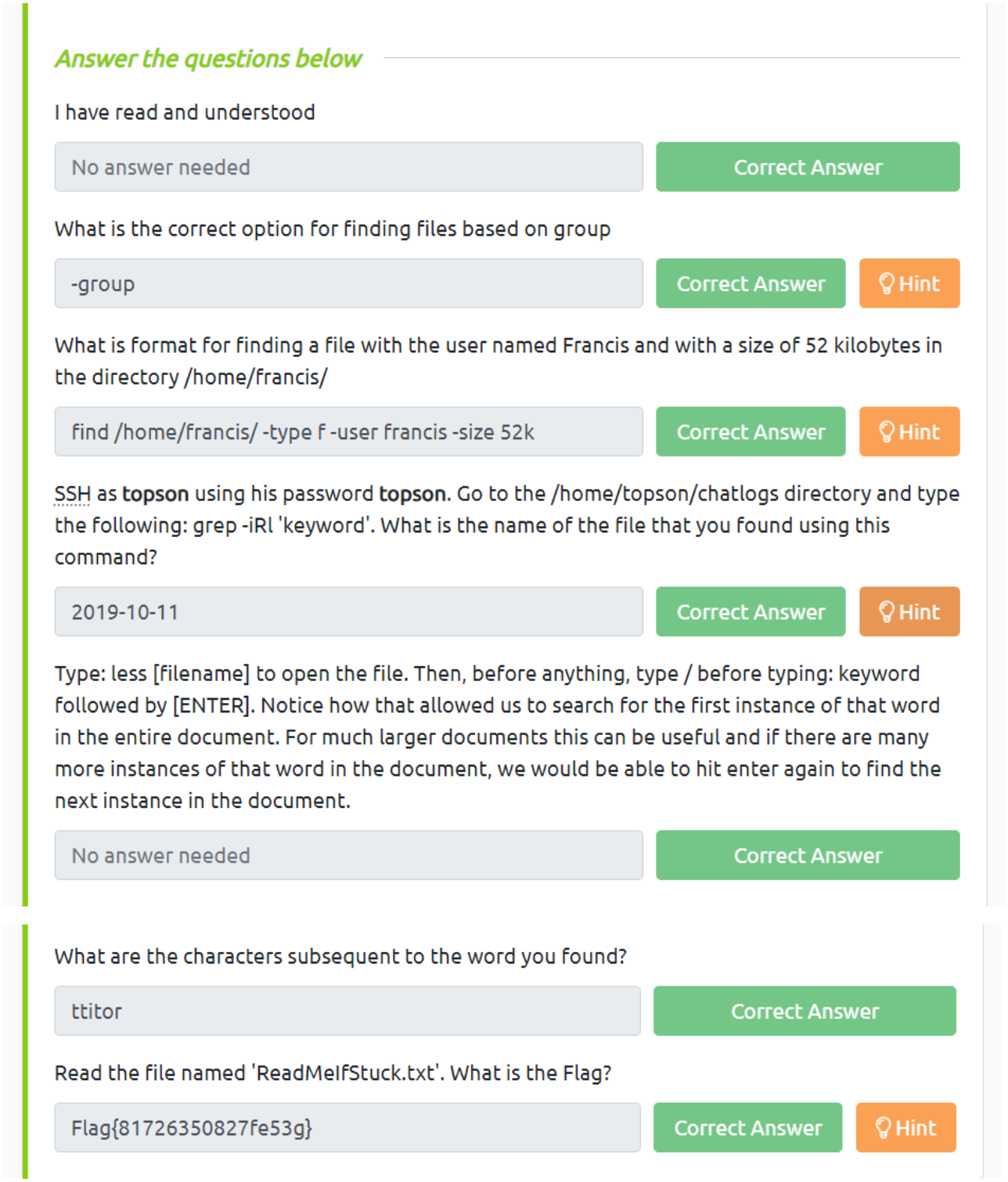
```
topson@james:~/corperateFiles/xch/telephone numbers$ cat cat readME.txt
cat: cat: No such file or directory
202-555-0150
202-555-0125
617-555-0115
+1-617-555-0115
+1-617-555-0186
+1-617-555-0138
use the Find command to find a file with a modified date of 2016-09-12 from the
/workflows directory
```

Then I tried to find the file which is modified between 2016-09-11 to 2016-09-13 and I found a file in workflows directory.

```
topson@james:~$ find / -type f -newermt 2016-09-11 ! -newermt 2016-09-13 2>/dev/nul
l
/home/topson/workflows/xft/eBQRhHvx
/usr/lib/python3/dist-packages/urllib3/packages/backports/makefile.py
/usr/lib/python3/dist-packages/urllib3/packages/backports/__init__.py
topson@james:~$
```

Then I entered the first file. And using less I found the answer.

```
tis adipisci labore nulla molestiae minus molestias nam veniam incidunt provident i
taque esse officia dolore placeat harum quo volFlag{81726350827fe53g}uptate quia se
d deleniti ad repellendus aut praesentium obcaecati facere natus architecto ullam m
axime qui earum sit perferendis rerum hic reprehenderit odit numquam vel dignissimo
```



Task 3: Working with files:

Q1. Hypothetically, you find yourself in a directory with many files and want to move all these files to the directory of /home/francis/logs. What is the correct command to do this?

A1. mv * /home/francis/logs

Q2. Hypothetically, you want to transfer a file from your /home/james/Desktop/ with the name script.py to the remote machine (192.168.10.5) directory of /home/john/scripts using the username of john. What would be the full command to do this?

A2. scp /home/james/Desktop/script.py john@192.168.10.5:/home/john/scripts

upload file to a remote machine	scp [filename] [username]@[IP of remote machine]:/[directory to upload to]	scp example.txt john@192.168.100.123:/home/john/

Q3. How would you rename a folder named -logs to -newlogs

A3. mv -logs -newlogs

rename files/folder	mv [current filename] [new filename]	mv ssh.conf NewSSH.conf

Q4. How would you copy the file named encryption keys to the directory of /home/john/logs

A4. cp "encryption keys" /home/john/logs

copy file/folder	cp [filename/folder] [directory] (remember, if the filename/folder name has spaces then you will need to encase the filename with speech marks such as cp "[filename with spaces]" [directory]. This applis to other commands such as mv.)	cp ssh.conf /home/newfolder

Q5. Find a file named readME_hint.txt inside topson's directory and read it. Using the instructions it gives you, get the second flag.

A5. Flag{234@i4s87u5hbn$3}

```
topson@james:~$ find / -type f -name readME_hint.txt 2>/dev/null
/home/topson/corperateFiles/RecordsFinances/readME_hint.txt
```

```
topson@james:~$ find / -type f -name -MoveMe.txt 2>/dev/null
/home/topson/corperateFiles/RecordsFinances/-MoveMe.txt
topson@james:~$
```

```
topson@james:~$ cd /home/topson/corperateFiles/RecordsFinances/
topson@james:~/corperateFiles/RecordsFinances$ ls
 ajkJji   GxPtUIo   january          -MoveMe.txt       uIkmHPN
 CeCJDJ   hHYDeM   '-march folder'   readME_hint.txt
topson@james:~/corperateFiles/RecordsFinances$
```

```
topson@james:~/corperateFiles/RecordsFinances$ mv -- -MoveMe.txt -march\ folder
topson@james:~/corperateFiles/RecordsFinances$ cd -- -march\ folder
topson@james:~/corperateFiles/RecordsFinances/-march folder$ ls
-MoveMe.txt  -runME.sh
topson@james:~/corperateFiles/RecordsFinances/-march folder$
```

```
topson@james:~/corperateFiles/RecordsFinances/-march folder$ ./-runME.sh
-MoveMe.txt exists.
Flag{234@i4s87u5hbn$3}
```

Answer the questions below

Hypothetically, you find yourself in a directory with many files and want to move all these files to the directory of /home/francis/logs. What is the correct command to do this?

mv * /home/francis/logs — Correct Answer

Hypothetically, you want to transfer a file from your /home/james/Desktop/ with the name script.py to the remote machine (192.168.10.5) directory of /home/john/scripts using the username of john. What would be the full command to do this?

scp /home/james/Desktop/script.py john@192.168.10.5:/home/john/scripts — Correct Answer

How would you rename a folder named -logs to -newlogs

mv -logs -newlogs — Correct Answer — Hint

How would you copy the file named encryption keys to the directory of /home/john/logs

cp "encryption keys" /home/john/logs — Correct Answer — Hint

Find a file named readME_hint.txt inside topson's directory and read it. Using the instructions it gives you, get the second flag.

Flag{234@i4s87u5hbn$3} — Correct Answer — Hint

Task 4: Hashing – Introduction

I downloaded the file in my windows. Then I opened the file and copy the text. And in my attach machine I created a text file named hash1 and paste the text inside the file.

Q1. Download the hash file attached to this task and attempt to crack the MD5 hash. What is the password?

A1. secret123

```
root@ip-10-10-252-162:~/Desktop# john --format=raw-md5 --wordlist=/usr/share/wor
dlists/rockyou.txt hash1
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
secret123        (?)
1g 0:00:00:00 DONE (2023-09-10 12:47) 5.000g/s 86400p/s 86400c/s 86400C/s extrem
o..goarmy
Use the "--show --format=Raw-MD5" options to display all of the cracked password
s reliably
Session completed.
root@ip-10-10-252-162:~/Desktop#
```

Q2. What is the hash type stored in the file hashA.txt

A2. Md4

```
sarah@james:~$ find / -type f -name hashA.txt 2>/dev/null
/home/sarah/system AB/server_mail/server settings/hashA.txt
sarah@james:~$
```

```
sarah@james:~$ cat /home/sarah/system\ AB/server_mail/server\ settings/hashA.txt

f9d4049dd6a4dc35d40e5265954b2a46sarah@james:~$
```

f9d4049dd6a4dc35d40e5265954b2a46

I'm not a robot

reCAPTCHA
Privacy - Terms

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
f9d4049dd6a4dc35d40e5265954b2a46	md4	admin

Q3. Crack hashA.txt using john the ripper, what is the password?

A3. Admin

```
root@ip-10-10-252-162:~/Desktop# john --format=raw-md4 --wordlist=/usr/share/wor
dlists/rockyou.txt hash1
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD4 [MD4 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
admin            (?)
1g 0:00:00:00 DONE (2023-09-10 13:15) 50.00g/s 998400p/s 998400c/s 998400C/s mon
te..johny
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
root@ip-10-10-252-162:~/Desktop#
```

Q4. What is the hash type stored in the file hashB.txt

A4. SHA-1

```
sarah@james:~$ find / -type f -name hashB.txt 2>/dev/null
/home/sarah/oldLogs/settings/craft/hashB.txt
sarah@james:~$
```

```
sarah@james:~$ cat /home/sarah/oldLogs/settings/craft/hashB.txt
b7a875fc1ea228b9061041b7cec4bd3c52ab3ce3sarah@james:~$
```

Q5. Find a wordlist with the file extention of '.mnf' and use it to crack the hash with the filename hashC.txt. What is the password?

A5. unacvaolipatnuggi

Q6. Crack hashB.txt using john the ripper, what is the password?

A6. letmein

```
root@ip-10-10-252-162:~# cd Desktop
root@ip-10-10-252-162:~/Desktop# john --format=raw-sha1 --wordlist=/usr/share/wo
rdlists/rockyou.txt hash1
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA1 [SHA1 256/256 AVX2 8x])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
letmein          (?)
1g 0:00:00:00 DONE (2023-09-10 13:13) 100.0g/s 51200p/s 51200c/s 51200C/s stupid
..letmein
Use the "--show --format=Raw-SHA1" options to display all of the cracked passwor
ds reliably
Session completed.
root@ip-10-10-252-162:~/Desktop#
```

Answer the questions below

Download the hash file attached to this task and attempt to crack the MD5 hash. What is the password?

secret123 — Correct Answer

SSH as **sarah** using: sarah@[10.10.98.108] and use the password: **rainbowtree1230x**

What is the hash type stored in the file hashA.txt

md4 — Correct Answer

Crack hashA.txt using john the ripper, what is the password?

admin — Correct Answer

What is the hash type stored in the file hashB.txt

SHA-1 — Correct Answer

Find a wordlist with the file extention of '.mnf' and use it to crack the hash with the filename hashC.txt. What is the password?

unacvaolipatnuggi — Correct Answer — Hint

Crack hashB.txt using john the ripper, what is the password?

letmein — Correct Answer

My 1 hour of Attach Machine is over so I'll use my Kali Linux

Task 5: Decoding base64

Q1. what is the name of the tool which allows us to decode base64 strings?

A1. base64

Q2. find a file called encoded.txt. What is the special answer?

A2. john

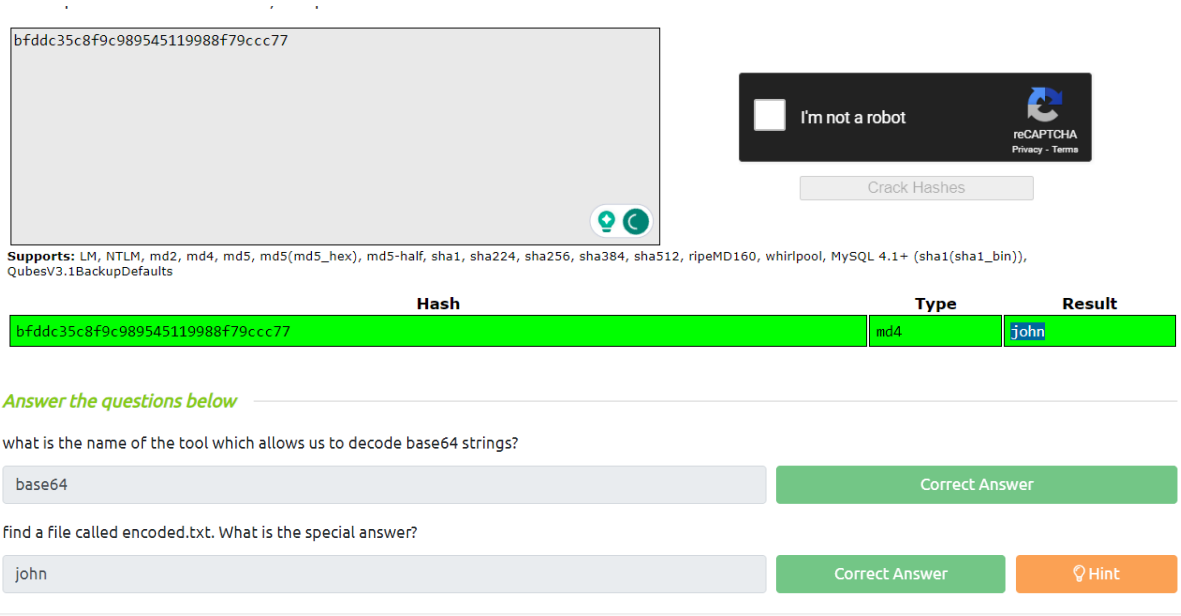
We found the file and we converted into base64 and store the output in a new file name decoded.txt

```
lYyB1dCBsZWN0dXMgcGxhY2VyYXQsIG9ybmFyZSBxdWFtIHZpdGFlLCBjb25zZWN0ZXR1ciBtaS4gTW9yYmkgbm9uIGxpYmVybyBmYWNpbGlzaXMsIHBvc3VlcmUgZXJh
dCBpZCwgc2VtcGVyIGxpYmVyby4gRXRpYW0gaW4gbWF1cmlzIGJpYmVuZHVtLCB2aXZlcnJhIGxhY3VzIG5lYywgcG9ydGEgbGVjdHVzLiA=
sarah@james:~$ cat /home/sarah/system\ AB/managed/encoded.txt | base64 -d >> decoded.txt
sarah@james:~$ ls
 decoded.txt   example.txt  'linuxconf backup'   logs   logs33   oldLogs   serverLx  'system AB'  'system mx'
sarah@james:~$ cat decoded.txt
```

Using less command we got the place of that answer

```
dignissim. Suspendisse ultrices condimentum nisi et
c special: the answer is in a file called ent.txt, t
e egestas dui, ut condimentum magna. Vestibulum tell
```

```
sarah@james:~$ find / -type f -name ent.txt 2>/dev/null
/home/sarah/logs/zhc/ent.txt
sarah@james:~$ cat /home/sarah/logs/zhc/ent.txt
bfddc35c8f9c989545119988f79ccc77
```



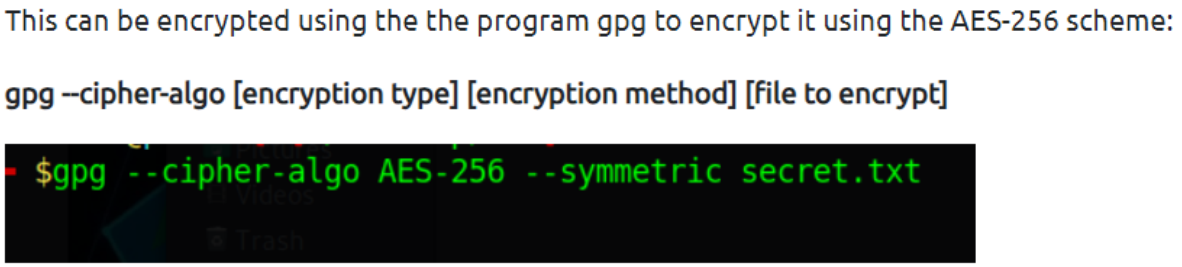
Task 6: Encryption/Decryption using gpg

Q1. Now try it for yourself. Make a random text file and enter some readable sentences in there before encrypting and decrypting it as illustrated above.

A1. No answer needed

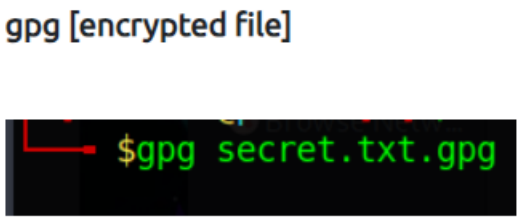
Q2. You wish to encrypt a file called history_logs.txt using the AES-128 scheme. What is the full command to do this?

A2. gpg --cipher-algo AES-128 --symmetric history_logs.txt



Q3. What is the command to decrypt the file you just encrypted?

A3. gpg history_logs.txt.gpg



Q4. Find an encrypted file called layer4.txt, its password is bob. Use this to locate the flag. What is the flag?

A4. Flag{B07$f854f5ghg4s37}

```
sarah@james:~$ find / -type f -name layer4.txt 2>/dev/null
/home/sarah/system AB/keys/vnmA/layer4.txt
sarah@james:~$ cat /home/sarah/system AB/keys/vnmA/layer4.txt
cat: /home/sarah/system: No such file or directory
cat: AB/keys/vnmA/layer4.txt: No such file or directory
sarah@james:~$ cat /home/sarah/system\ AB/keys/vnmA/layer4.txt
◆       ◆>◆◆◆!#◆◆sxG◆$qh^K◆n◆◆◆B◆Iv◆◆n}◆%3TT◆v◆!;◆=◆9u◆◆◆,◆◆>◆
                                                        ◆] [◆3◆8◆◆◆+◆VgEt◆RCS◆◆◆◆◆◆◆&S◆◆G;◆5◆▒Dk◆◆y◆_kVm*sarah@james:~$
```

```
sarah@james:~$ gpg /home/sarah/system\ AB/keys/vnmA/layer4.txt
gpg: keybox '/home/sarah/.gnupg/pubring.kbx' created
```

```
Enter new filename [layer4.txt]: l1dec.txt
sarah@james:~$ ls
 decoded.txt   example.txt   l1dec.txt  'linuxconf backup'   logs   logs33   oldLogs   serverLx  'system AB'  'system mx'
sarah@james:~$ cat l1dec.txt
1. Find a file called layer3.txt, its password is james.
```

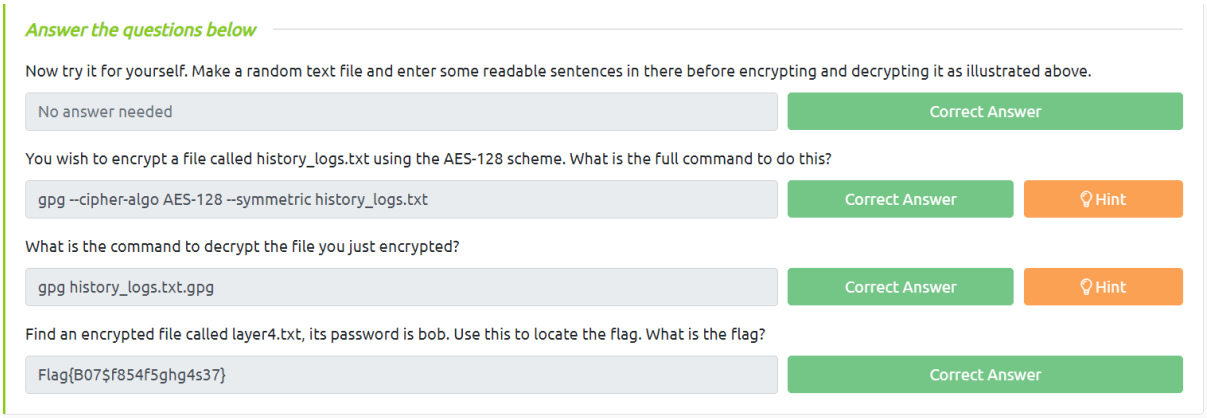
```
sarah@james:~$ find / -type f -name layer3.txt 2>/dev/null
/home/sarah/oldLogs/2014-02-15/layer3.txt
sarah@james:~$ cat /home/sarah/oldLogs/2014-02-15/layer3.txt
◆       ◆]/X◆◆B◆◆r◆S◆◆◆~)ju:n   $`S9|◆◆◆◆◆◆◆◆h◆◆!C◆T/
                                                !◆B◆◆t5_p◆◆f
                                                        ◆◆◆◆T>◆Ы(       ◆◆D◆◆j◆◆◆◆T      #◆◆c◆◆◆ş◆◆◆#◆)ц◆◆0>▒dmz◆◆◆◆◆sarah
@james:~$
```

```
@james:~$ gpg /home/sarah/oldLogs/2014-02-15/layer3.txt
gpg: WARNING: no command supplied.  Trying to guess what you mean ...
gpg: AES256 encrypted data
gpg: encrypted with 1 passphrase
gpg: /home/sarah/oldLogs/2014-02-15/layer3.txt: unknown suffix
Enter new filename [layer3.txt]: l3dec.txt
sarah@james:~$ ls
 decoded.txt   l1dec.txt  'linuxconf backup'   logs33    serverLx    'system mx'
 example.txt   l3dec.txt   logs                oldLogs  'system AB'
sarah@james:~$ cat l3dec.txt
1. Find a file called layer2.txt, its password is tony.
```

```
sarah@james:~$ find / -type f -name layer2.txt 2>/dev/null
/home/sarah/oldLogs/settings/layer2.txt
sarah@james:~$ cat /home/sarah/oldLogs/settings/layer2.txt
◆
        8◆~◆◆Й  v◆▒\`◆t◆◆◆◆◆◆N◆z0%◆Z◆]◆~◆◆|!)Z%JC◆SC◆◆◆N◆#9s|◆蘗◆◆@C◆;◆,◆{◆9(◆jCa:◆#v◆D◆◆s◆U◆+◆◆◆sм,Sr4ฺ◆◆ p◆◆S◆◆◆◆◆◆◆_◆□e>◆◆c
sarah@james:~$ gpg /home/sarah/oldLogs/settings/layer2.txt
gpg: WARNING: no command supplied.  Trying to guess what you mean ...
gpg: AES256 encrypted data
gpg: encrypted with 1 passphrase
gpg: /home/sarah/oldLogs/settings/layer2.txt: unknown suffix
Enter new filename [layer2.txt]: l2dec.txt
sarah@james:~$ ls
 decoded.txt   l1dec.txt   l3dec.txt          logs     oldLogs   'system AB'
 example.txt   l2dec.txt  'linuxconf backup'   logs33   serverLx  'system mx'
sarah@james:~$ cat l2dec.txt
MS4gRmluZCBhIGZpbGUgY2FsbGVkIGxheWVyMS50eHQsIGl0cyBwYXNzd29yZCBpcyBoYWNrZWQu
sarah@james:~$
```

```
MS4gRmluZCBhIGZpbGUgY2FsbGVkIGxheWVyMS50eHQsIGl0cyBwYXNzd29yZCBpcyBoYWNrZWQu
sarah@james:~$ cat l2dec.txt | base64 -d
1. Find a file called layer1.txt, its password is hacked.sarah@james:~$
```

```
sarah@james:~$ find / -type f -name layer1.txt 2>/dev/null
/home/sarah/logs/zmn/layer1.txt
sarah@james:~$ cat /home/sarah/logs/zmn/layer1.txt
◆       O◆04I◆◆D◆◆W/◆◆◆◆1D◆:e◆◆c◆◆◆◆}◆x◆ŋy◆◆%◆&◆◆K◆W◆◆◆N`P◆◆HX&.◆BW◆
 (◆n◆gC◆◆◆zOW/  Q◆◆◆sarah@james:~$ gpg /home/sarah/logs/zmn/layer1.txt
gpg: WARNING: no command supplied.  Trying to guess what you mean ...
gpg: AES256 encrypted data
gpg: encrypted with 1 passphrase
gpg: /home/sarah/logs/zmn/layer1.txt: unknown suffix
Enter new filename [layer1.txt]: final.txt
sarah@james:~$ ls
 dd.txt        example.txt   l1dec.txt   l3dec.txt          logs     oldLogs   'system AB'
 decoded.txt   final.txt     l2dec.txt  'linuxconf backup'   logs33   serverLx  'system mx'
sarah@james:~$ cat final.txt
Flag{B07$f854f5ghg4s37}
sarah@james:~$
```



Task 7: Cracking encrypted gpg files

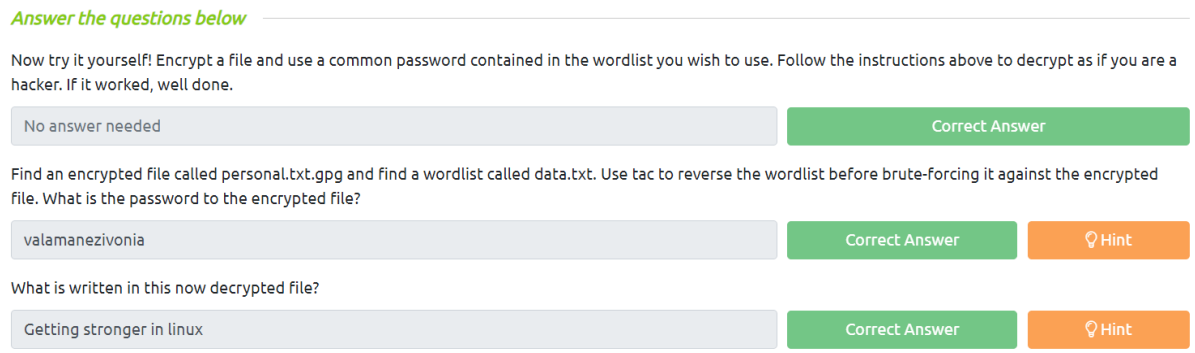
Q1. Now try it yourself! Encrypt a file and use a common password contained in the wordlist you wish to use. Follow the instructions above to decrypt as if you are a hacker. If it worked, well done.

A1. No answer needed.
Q2. Find an encrypted file called personal.txt.gpg and find a wordlist called data.txt. Use tac to reverse the wordlist before brute-forcing it against the encrypted file. What is the password to the encrypted file?

A2. Valamanezivonia

Q3. What is written in this now decrypted file?

A3. Getting stronger in linux



Task 8: Reading SQL databases

Q1. Find a file called employees.sql and read the SQL database. (Sarah and Sameer can log both into mysql using the password: password). Find the flag contained in one of the tables. What is the flag?

A1. Flag{13490AB8}

```
sarah@james:~$ find / -type f -name  employees.sql  2>/dev/null
/home/sarah/serverLx/employees.sql
```

```
sarah@james:~$ cd /home/sarah/serverLx
sarah@james:~/serverLx$ mysql -u sarah -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 4
```

```
mysql> show databases
    -> ;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| employees          |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
5 rows in set (0.00 sec)

mysql>
```

```
mysql> show tables;
+------------------------+
| Tables_in_employees    |
+------------------------+
| current_dept_emp       |
| departments            |
| dept_emp               |
| dept_emp_latest_date   |
| dept_manager           |
| employees              |
| salaries               |
| titles                 |
+------------------------+
8 rows in set (0.01 sec)

mysql> desc employees;
+------------+---------------+------+-----+---------+-------+
| Field      | Type          | Null | Key | Default | Extra |
+------------+---------------+------+-----+---------+-------+
| emp_no     | int(11)       | NO   | PRI | NULL    |       |
| birth_date | date          | NO   |     | NULL    |       |
| first_name | varchar(14)   | NO   |     | NULL    |       |
| last_name  | varchar(16)   | NO   |     | NULL    |       |
| gender     | enum('M','F') | NO   |     | NULL    |       |
| hire_date  | date          | NO   |     | NULL    |       |
+------------+---------------+------+-----+---------+-------+
6 rows in set (0.00 sec)
```

```
mysql> select * from employees where last_name like 'flags%';
Empty set (0.08 sec)

mysql> select * from employees where first_name like 'flag%';
Empty set (0.09 sec)

mysql> select * from employees where last_name like 'flag%';
+--------+------------+------------+-----------------+--------+------------+
| emp_no | birth_date | first_name | last_name       | gender | hire_date  |
+--------+------------+------------+-----------------+--------+------------+
| 499973 | 1963-06-03 | Lobel      | Flag{13490AB8} | M      | 1994-02-01 |
+--------+------------+------------+-----------------+--------+------------+
1 row in set (0.08 sec)
```

Answer the questions below

Find a file called employees.sql and read the SQL database. (Sarah and Sameer can log both into mysql using the password: password). Find the flag contained in one of the tables. What is the flag?

Flag{13490AB8} | Correct Answer | Hint

Task 9: Final Challenge

Q1. Go to the /home/shared/chatlogs directory and read the first chat log named: LpnQ. Use this to help you to proceed to the next task.

A1. No answer needed

Q2. What is Sameer's SSH password?

A2. thegreatestpasswordever000

```
(2020-08-13) Michael: once you find the configuration file and
consequently the wordlist directory, visit it. One of those wor
dlists must contain the password it used for the testing. All I
 remember is that the password began with ebq. You will need Sa
meer's account. His SSH password is: thegreatestpasswordever000
```

Q3. What is the password for the sql database back-up copy

A3. Ebqattle

Q4. Find the SSH password of the user James. What is the password?

A4. Vuimaxcullings

```
mysql> select * from employees where first_name like 'James';
+--------+------------+------------+-----------+--------+------------+
| emp_no | birth_date | first_name | last_name | gender | hire_date  |
+--------+------------+------------+-----------+--------+------------+
| 499996 | 1953-03-07 | James      | vuimaxcullings | M      | 1990-09-27 |
+--------+------------+------------+-----------+--------+------------+
1 row in set (0.09 sec)
```

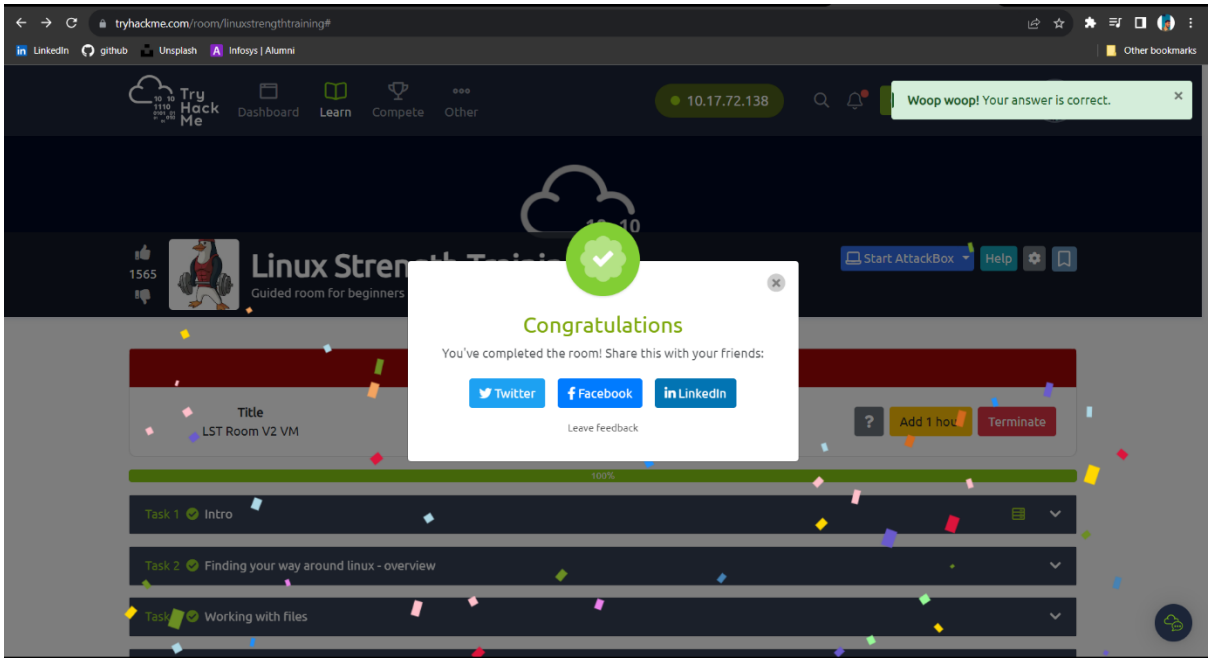
Q5.SSH as james and change the user to root?

A5. No answer needed

Q6. What is the root flag?

A6. Flag{6$8$hyJSJ3KDJ3881}

```
[sudo] password for james:
root@james:/home/james# id
uid=0(root) gid=0(root) groups=0(root)
root@james:/home/james# cd /root
root@james:~# ls
root.txt
root@james:~# cat root.txt
Flag{6$8$hyJSJ3KDJ3881}
```



The Room is complete

-Sadiq Sonalkar