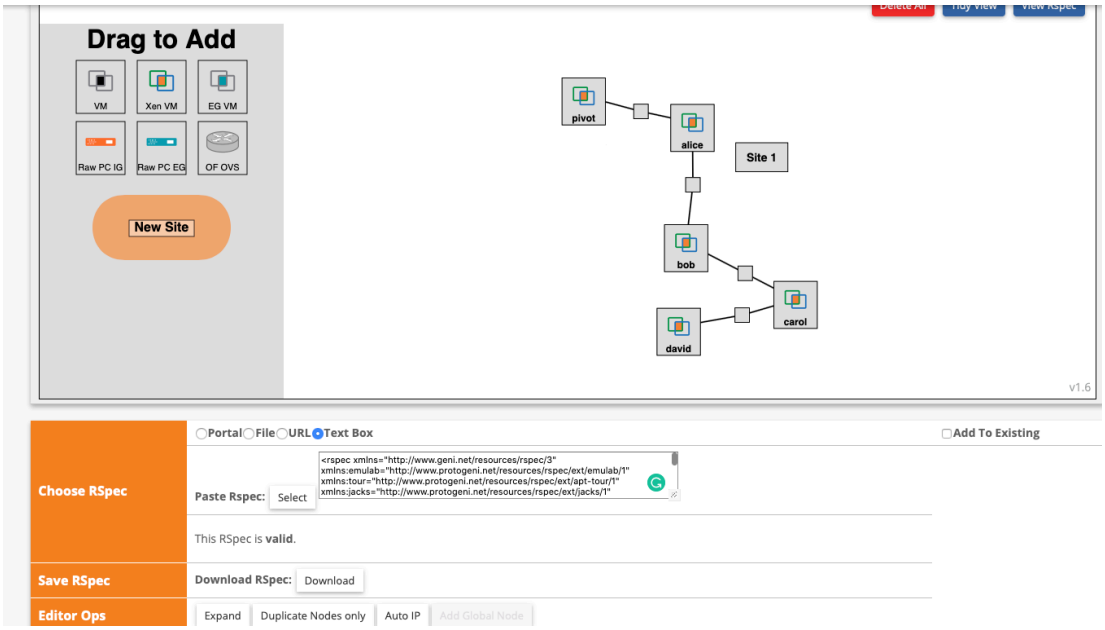
Cyberpaths

- CTF Password Lab -

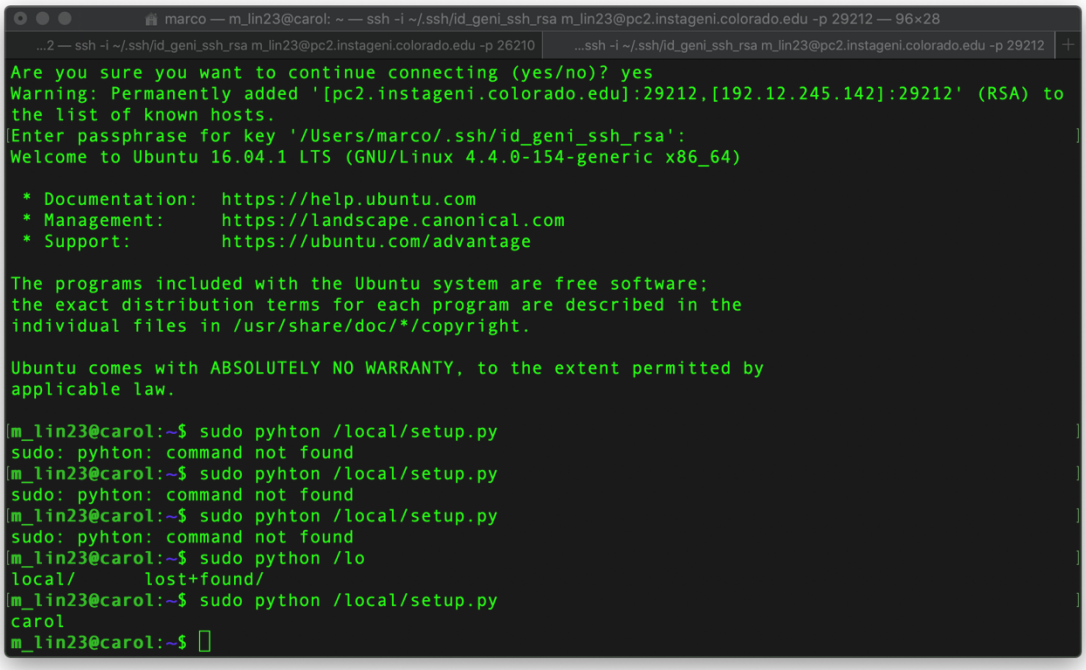
by Marco Lin

PART 1, SETTING UP THE TECHNOLOGY



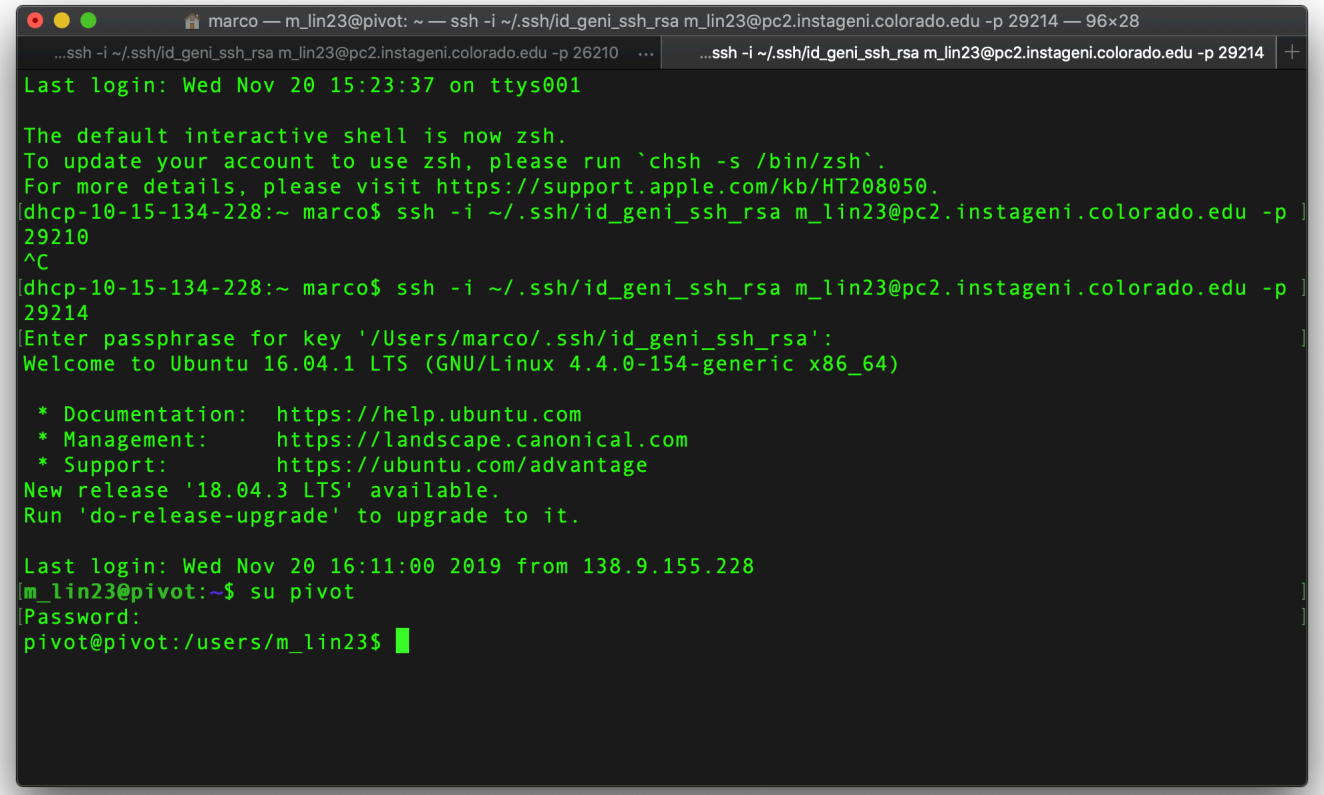
Run the following commands on each michine:

sudo python /local/setup.py

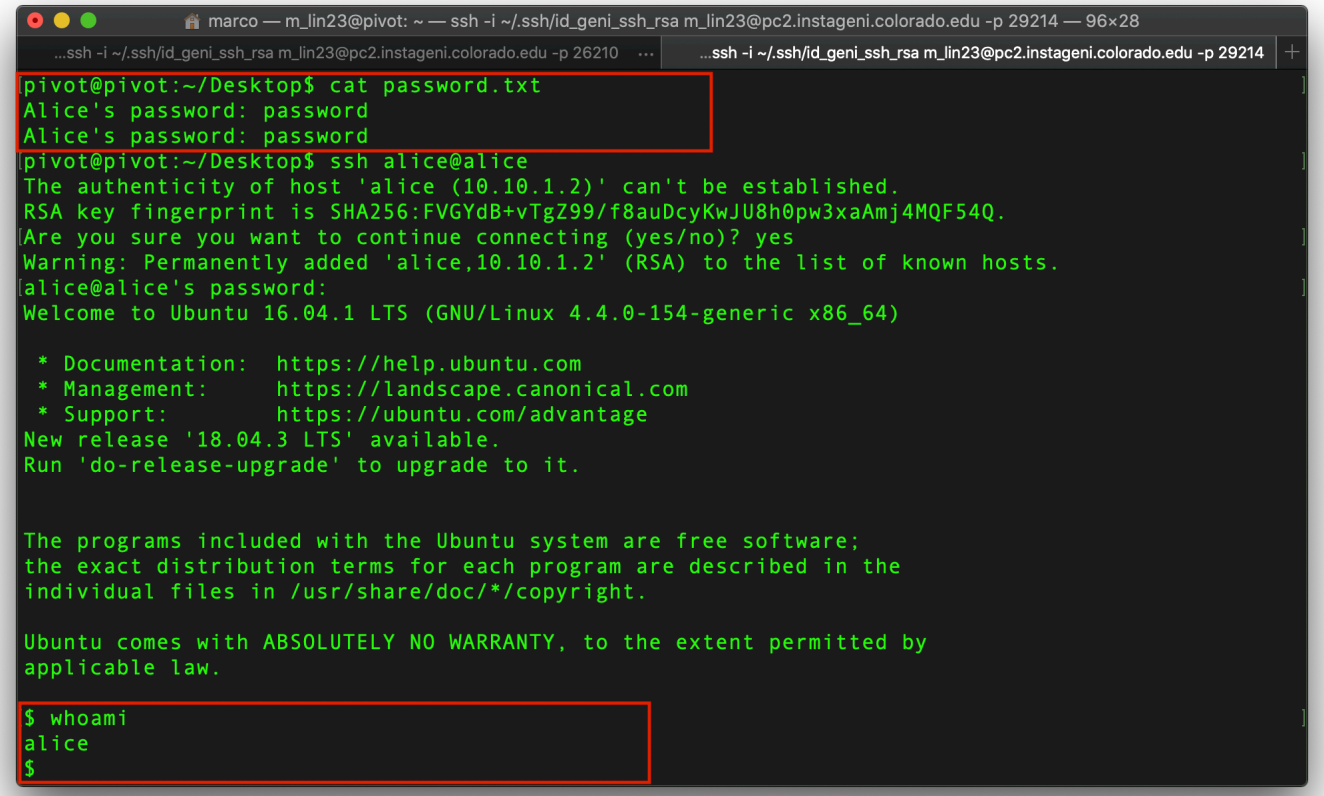


PART 2, THE MISSION

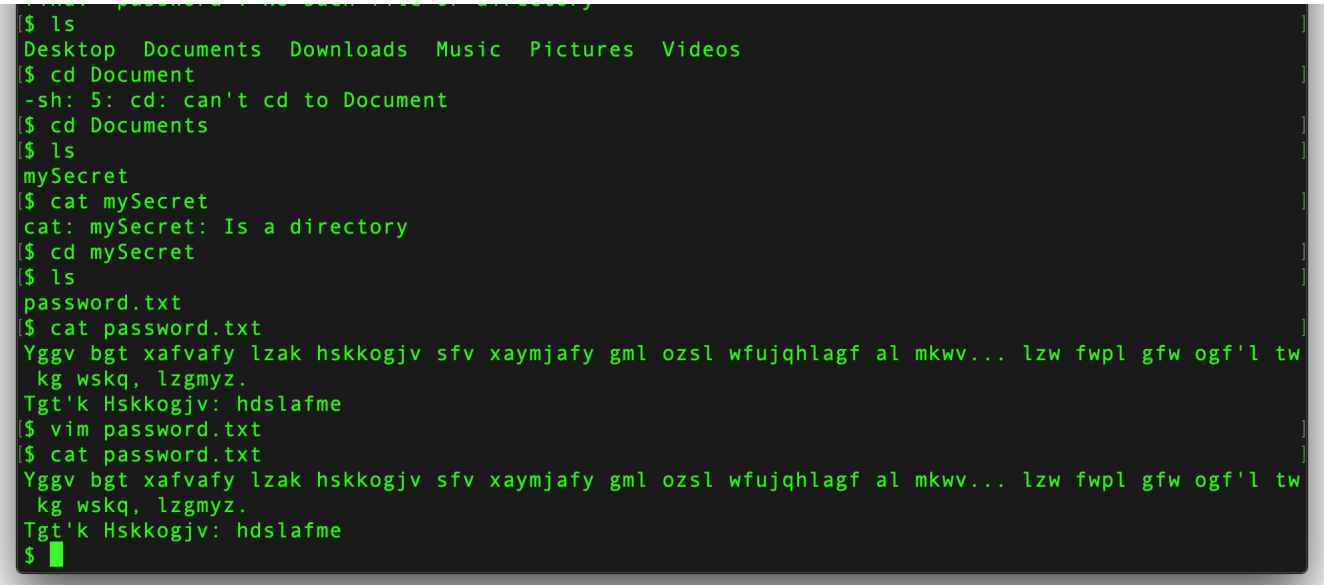
1. Using a pivot machine



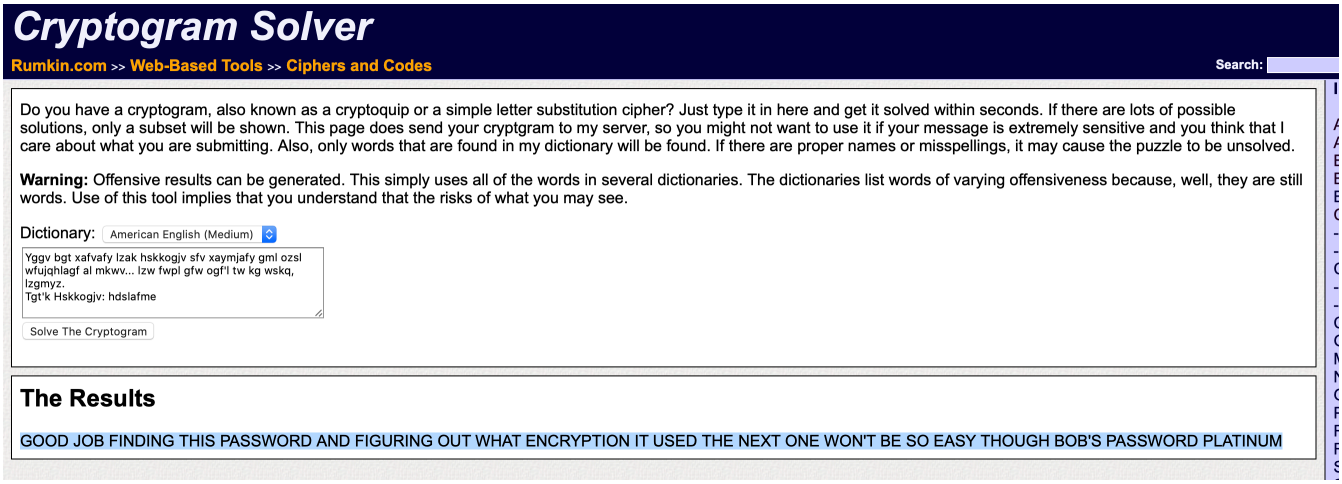
2. Find the password and login to Alice’s machine



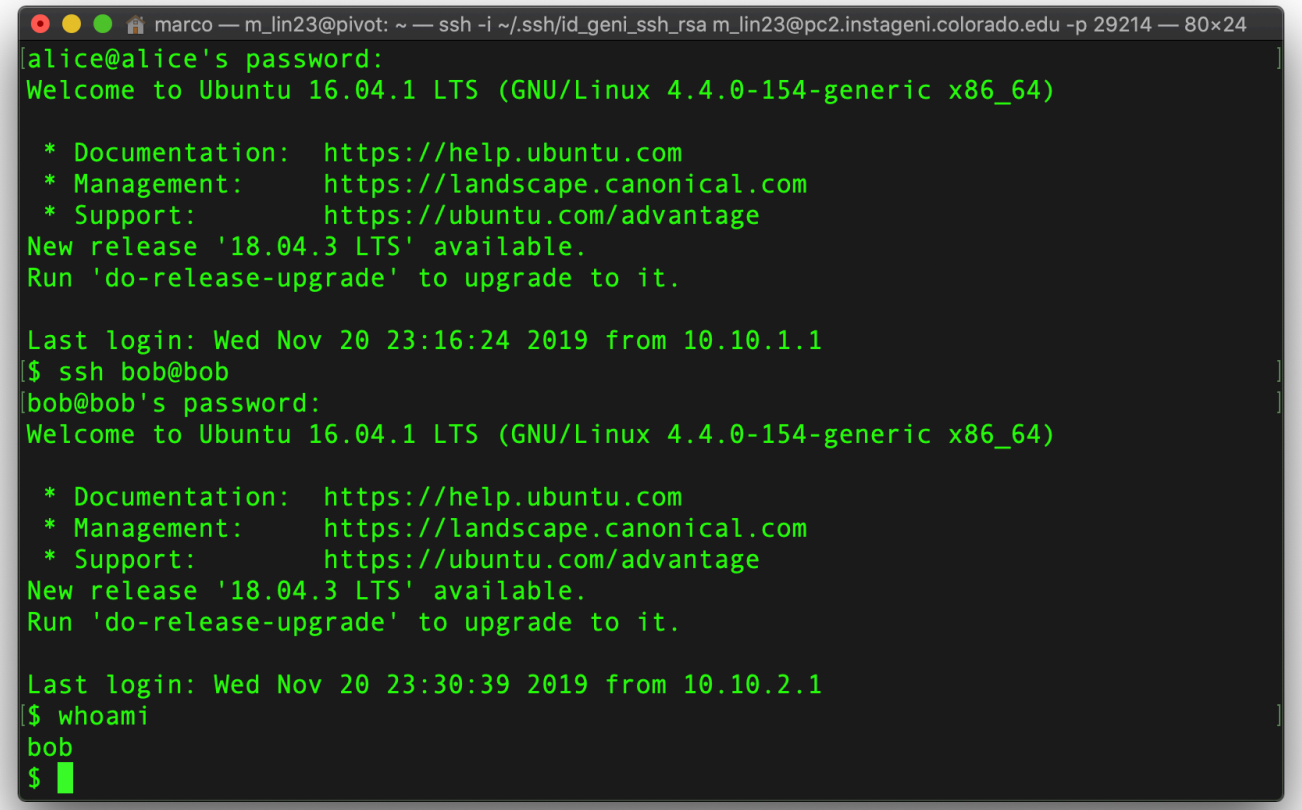
3. Find the bob's password



4. Crack bob's password by using the Ciphers and codes website.



5. Login bob's machine



6. Find the carol's password which is hidden file under Music folder.

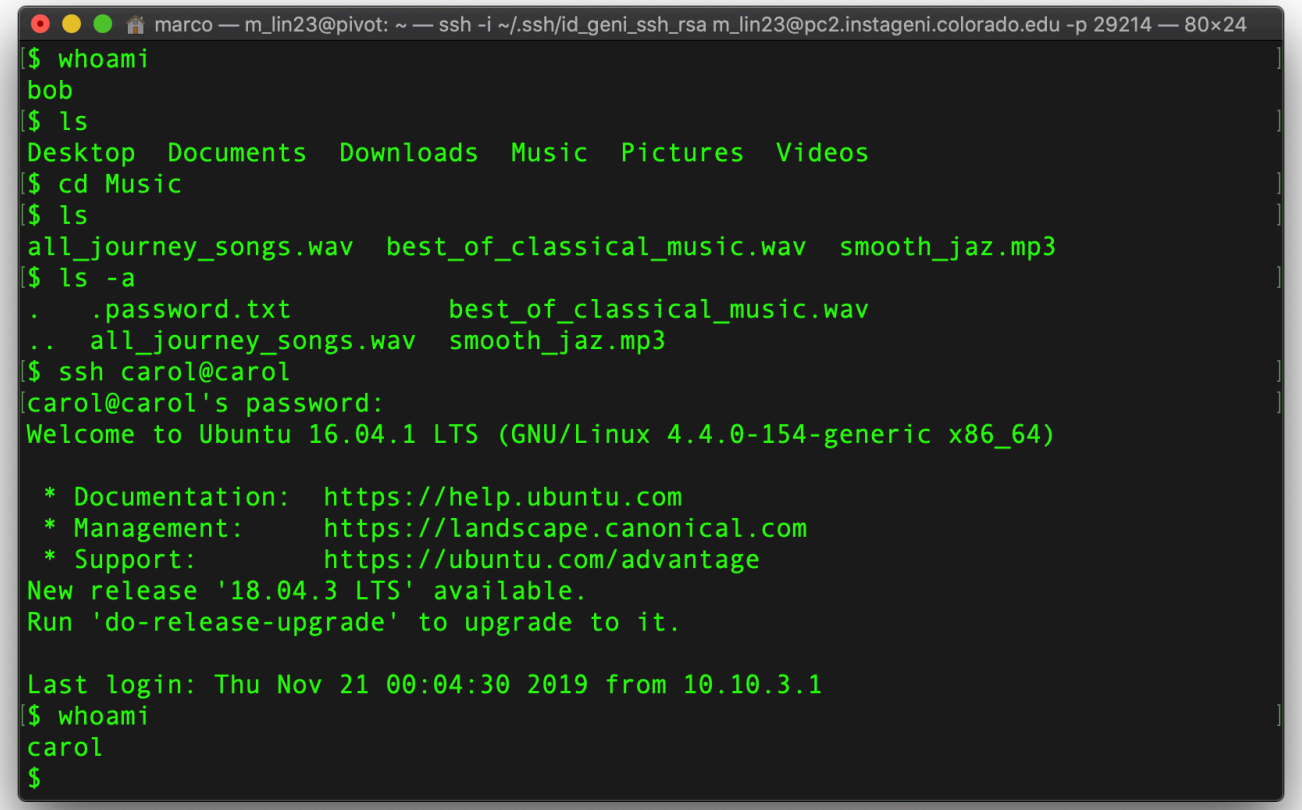
```
marco — m_lin23@pivot: ~ — ssh -i ~/.ssh/id_geni_ssh_rsa m_lin23@pc2.instageni.colorado.edu -p 29214 — 80×24

Last login: Wed Nov 20 23:16:24 2019 from 10.10.1.1
[$ ssh bob@bob
[bob@bob's password:
Welcome to Ubuntu 16.04.1 LTS (GNU/Linux 4.4.0-154-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
New release '18.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Wed Nov 20 23:30:39 2019 from 10.10.2.1
[$ whoami
bob
[$ ls
Desktop  Documents  Downloads  Music  Pictures  Videos
[$ cd Music
[$ ls
all_journey_songs.wav  best_of_classical_music.wav  smooth_jaz.mp3
[$ ls -a
.   .password.txt          best_of_classical_music.wav
..  all_journey_songs.wav  smooth_jaz.mp3
$
```

7. Get the password

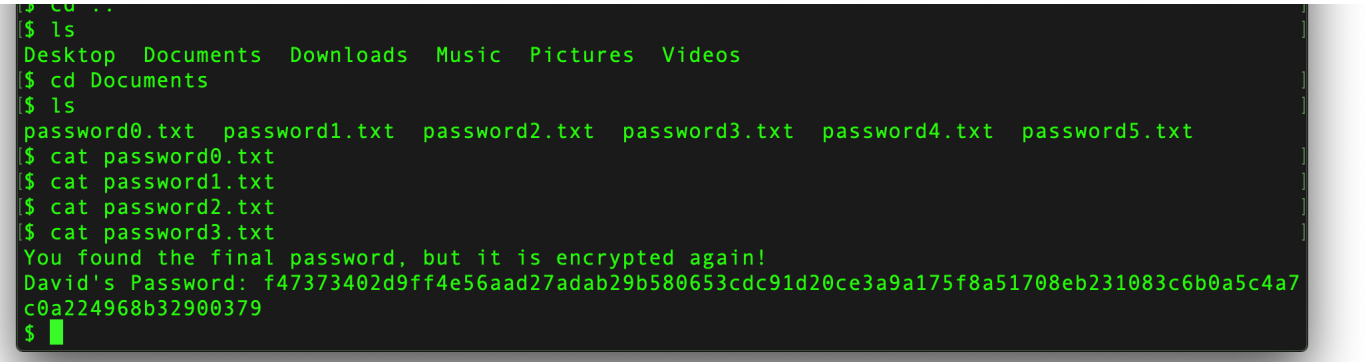
```
~ — m_lin23@client: ~ — -bash ... ~ — m_lin23@pivot: ~ — ssh -i ~/.ssh/id_geni_ssh_rsa m_lin23@pc2.instageni.colorado.edu -p 29214
Nice job finding the hidden file - here is Carol's password, but it is encrypted...
Carol's Password: 8601f6e1028a8e8a966f6c33fcd9aec4
~
~
```

8. Crack the password by using the website Crack Station.

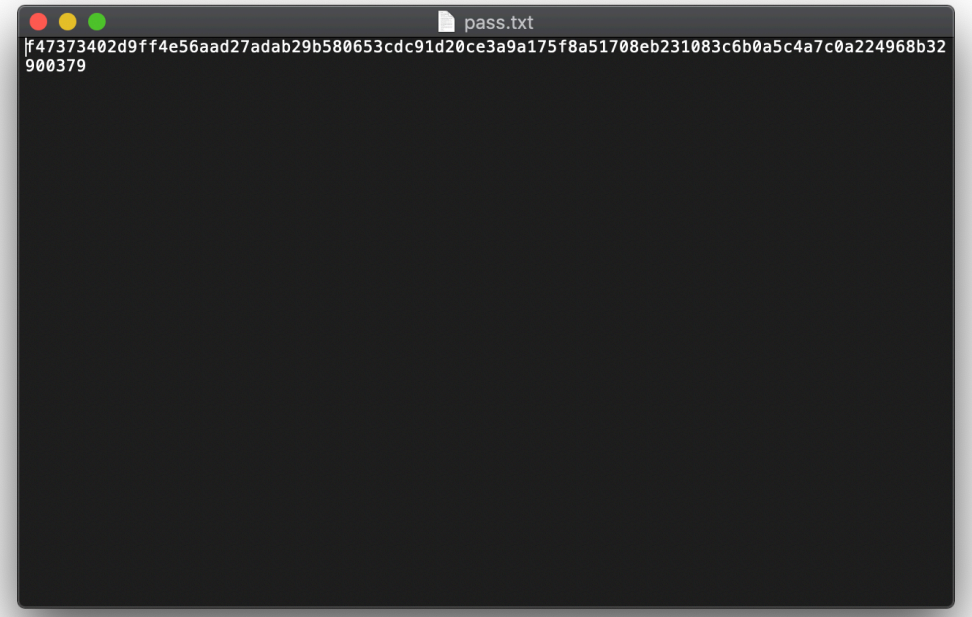
9. Login to carol's machine



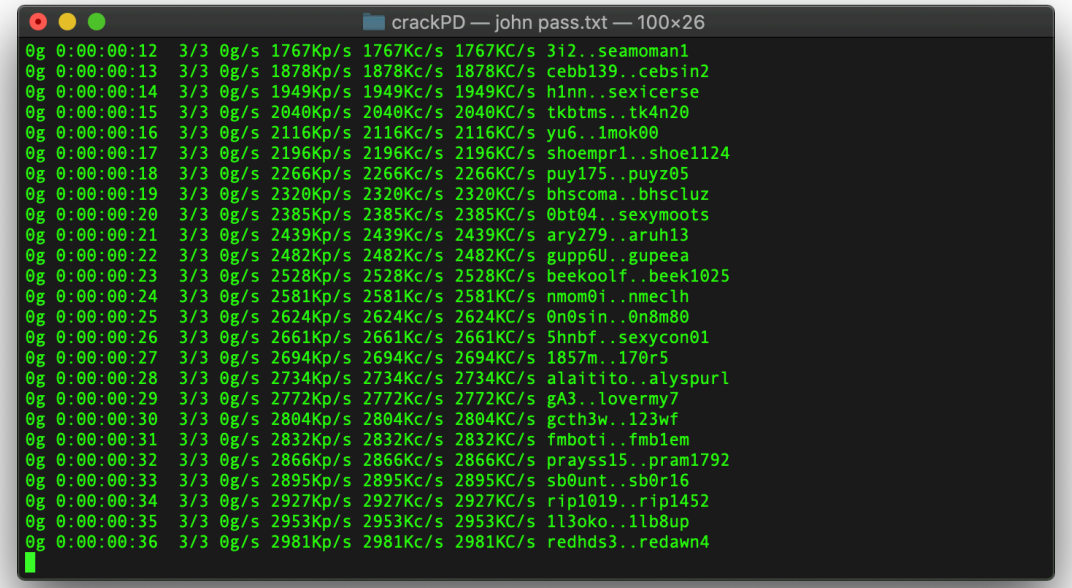
10. Looking for David's password which is under documents folder and the name of the file is password3.txt



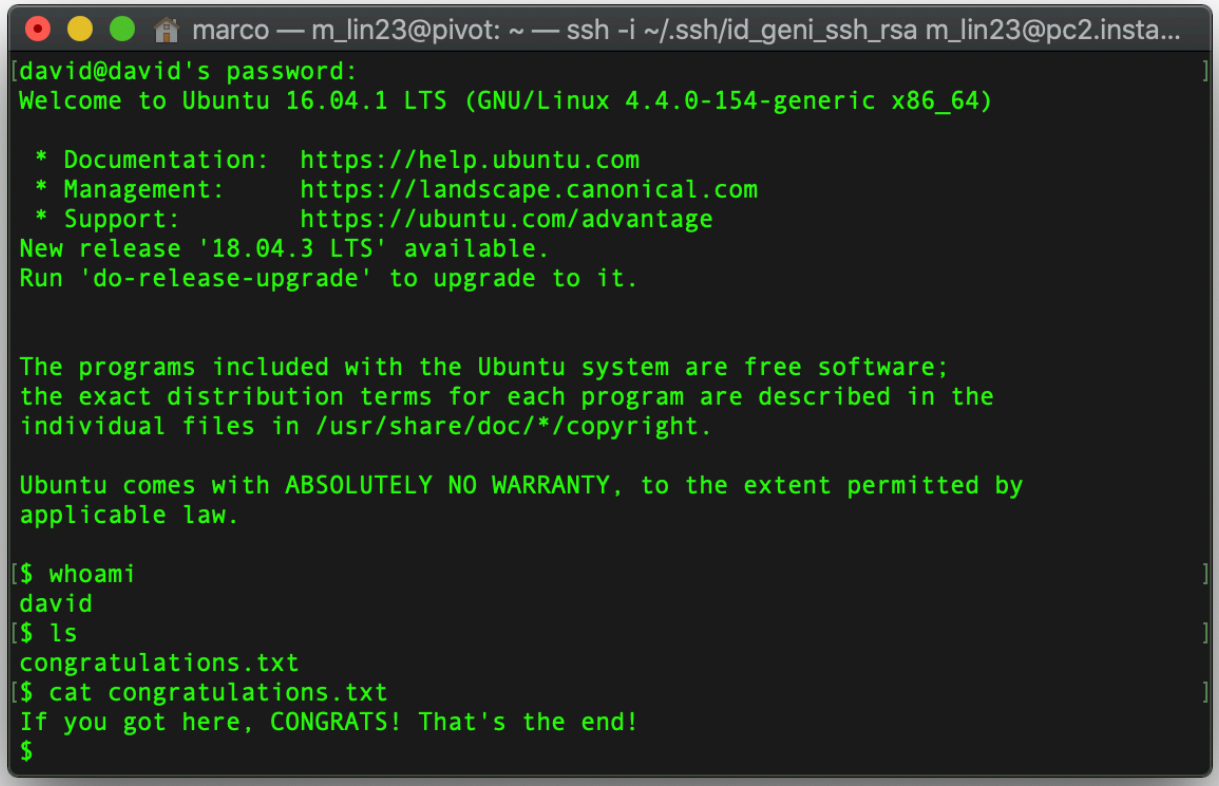
We can use the tool called john the ripper, we save the password in a text file like the following:



Run the john to crack the file and wait for around 30 min



Then we found the password is 55LqdcJM2b6Kw, and we can log into David's machine


marco — m_lin23@pivot: ~ — ssh -i ~/.ssh/id_geni_ssh_rsa m_lin23@pc2.insta...
david@david's password:
Welcome to Ubuntu 16.04.1 LTS (GNU/Linux 4.4.0-154-generic x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
New release '18.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
$ whoami
david
$ ls
congratulations.txt
$ cat congratulations.txt
If you got here, CONGRATS! That's the end!
$