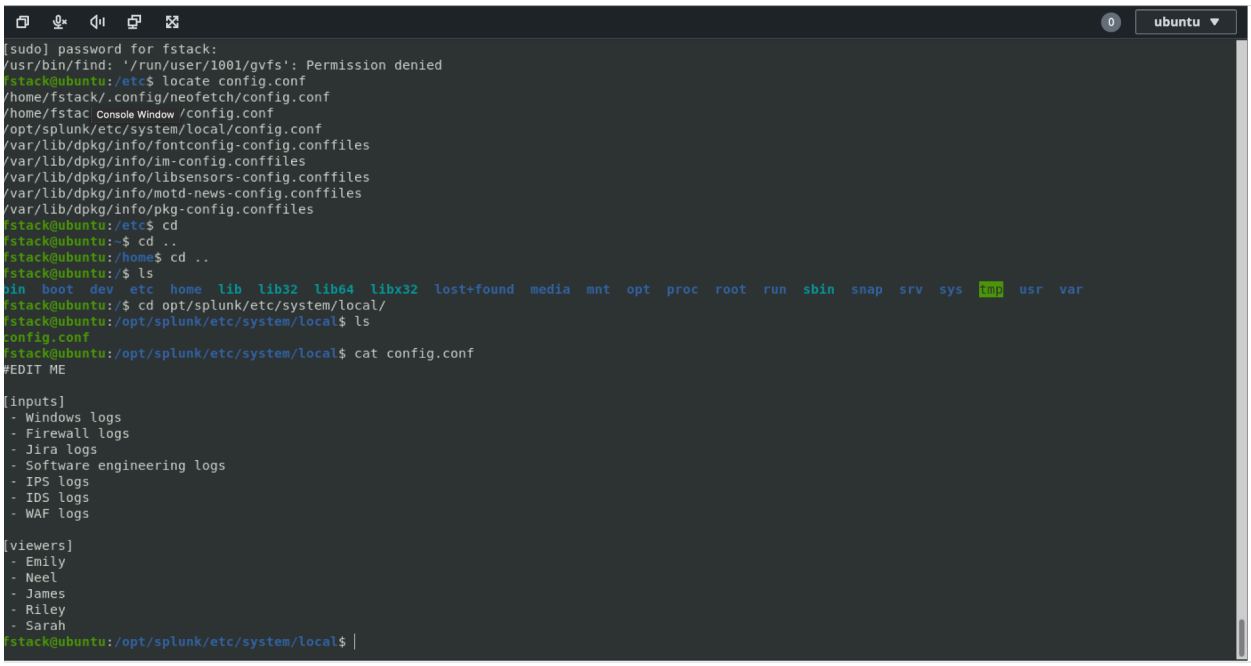
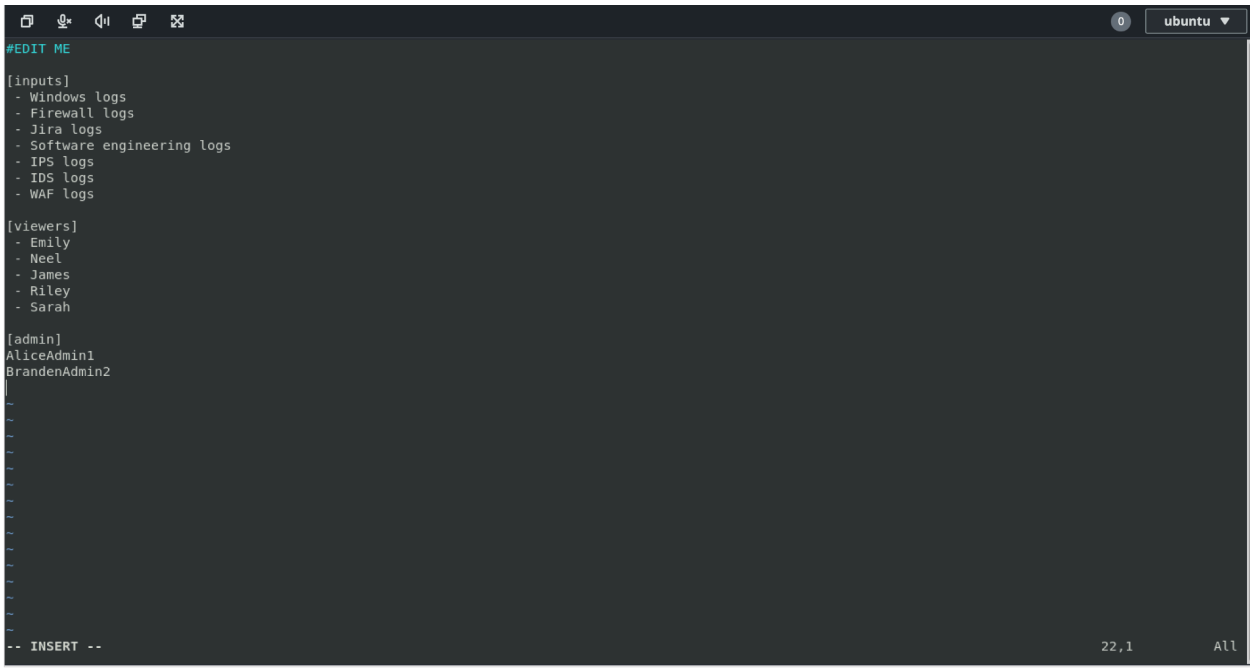
Career Simulation 1
Branden Pearl

1. To Locate the config.conf file, I used the command “sudo updatedb” just to ensure everything was up to date. I then used the “locate’ command to find the config.conf file in /opt/splunk/etc/system/local directory.



2. Check the file permissions of the `config.conf` file. What do you notice about its file permissions?
    - I noticed that everyone had rwx permission for the config.conf file. That is how the file was mistakenly edited by James.

3. Check the MD5 hash of the file.
    - The md5sum hash of config.conf file is listed in the above screenshot. The hash is c70754d9c7bab08a8c441f90c37f27eb
4. Edit the file by adding the following lines to the end. You can use vi or nano for this. Be sure to save the file after making the change.
    - I did save the file correctly by using the ":x" command.



5. Check the MD5 hash of the file one more time. How does it compare to the MD5 hash before you edited the file?
    - The MD5 hash is different because I edited the file. The hash is õ338c0f161ae5dfb86ae415c795bc576

```
fstack@ubuntu:/$ cd opt/splunk/etc/system/local/
fstack@ubuntu:/opt/splunk/etc/system/local$ ls
config.conf
fstack@ubuntu:/opt/splunk/etc/system/local$ cat config.conf
#EDIT ME

[inputs]
 - Windows logs
 - Firewall logs
 - Jira logs
 - Software engineering logs
 - IPS logs
 - IDS logs
 - WAF logs

[viewers]
 - Emily
 - Neel
 - James
 - Riley
 - Sarah
fstack@ubuntu:/opt/splunk/etc/system/local$ ls -l
total 4
-rwxrwxrwx 1 root root 185 Sep 29  2022 config.conf
fstack@ubuntu:/opt/splunk/etc/system/local$ md5sum config.conf
c70754d9c7bab08a8c441f90c37f27eb  config.conf
fstack@ubuntu:/opt/splunk/etc/system/local$ vim config.conf
fstack@ubuntu:/opt/splunk/etc/system/local$ dm5sum config.conf

Command 'dm5sum' not found, did you mean:

  command 'md5sum' from deb coreutils (8.30-3ubuntu2)

Try: sudo apt install <deb name>

fstack@ubuntu:/opt/splunk/etc/system/local$ md5sum config.conf
6338c0f161ae5dfb86ae415c795bc576  config.conf
fstack@ubuntu:/opt/splunk/etc/system/local$
```

Console Window

6. Create a backup of the file into your home directory by copying the file into the `/home/fstack` directory.
    - I used the “cp” command to copy the config.conf file into my home directory.

```
[inputs]
 - Windows logs
 - Firewall logs
 - Jira logs
 - Software engineering logs
 - IPS logs
 - IDS logs
 - WAF logs

[viewers]
 - Emily
 - Neel
 - James
 - Riley
 - Sarah
fstack@ubuntu:/opt/splunk/etc/system/local$ ls -l
total 4
-rwxrwxrwx 1 root root 185 Sep 29  2022 config.conf
fstack@ubuntu:/opt/splunk/etc/system/local$ md5sum config.conf
c70754d9c7bab08a8c441f90c37f27eb  config.conf
fstack@ubuntu:/opt/splunk/etc/system/local$ vim config.conf
fstack@ubuntu:/opt/splunk/etc/system/local$ dm5sum config.conf

Command 'dm5sum' not found, did you mean:

  command 'md5sum' from deb coreutils (8.30-3ubuntu2)

Try: sudo apt install <deb name>

fstack@ubuntu:/opt/splunk/etc/system/local$ md5sum config.conf
6338c0f161ae5dfb86ae415c795bc576  config.conf
fstack@ubuntu:/opt/splunk/etc/system/local$ cp config.conf /home/fstack/ copy_config.conf
cp: target 'copy_config.conf' is not a directory
fstack@ubuntu:/opt/splunk/etc/system/local$ cp config.conf /home/fstack/
fstack@ubuntu:/opt/splunk/etc/system/local$ ls /home/fstack/
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos  config.conf  demo1  demo2  practice  sample.sh  ubuntu
fstack@ubuntu:/opt/splunk/etc/system/local$
```

Console Window

Conclusion

The problem was James accidentally edited the incorrect config.conf file. I solved the problem by locating the file under opt/splunk/etc/system/local directory. Once I located the file I checked the hash of the original file by using the dm5sum command and the original hash was c70754d9c7bab08a8c441f90c37f27eb. I used the vim command to add Alice and myself as admins so that we could properly view the file that was mistakenly erased by James. After I edited the file in vim, I saved the file with :x command to save and quit, followed by me checking the hash of the config.conf file. I then made a copy of the file and put it in my home directory.

The main problem of the file is that everyone has read, write, and executable permissions on the file. I found out by using the command ls -l. My recommendation to Stack Full Software is to change the permission of the file to read only for others and give their admin or group along with the owner of the file read, write, and executable permissions. You can do so by creating a group for admin and then adding the correct users to the group. After that you can use the command chmod 774 config.conf to change the permission of the file, so that this doesn't happen again.