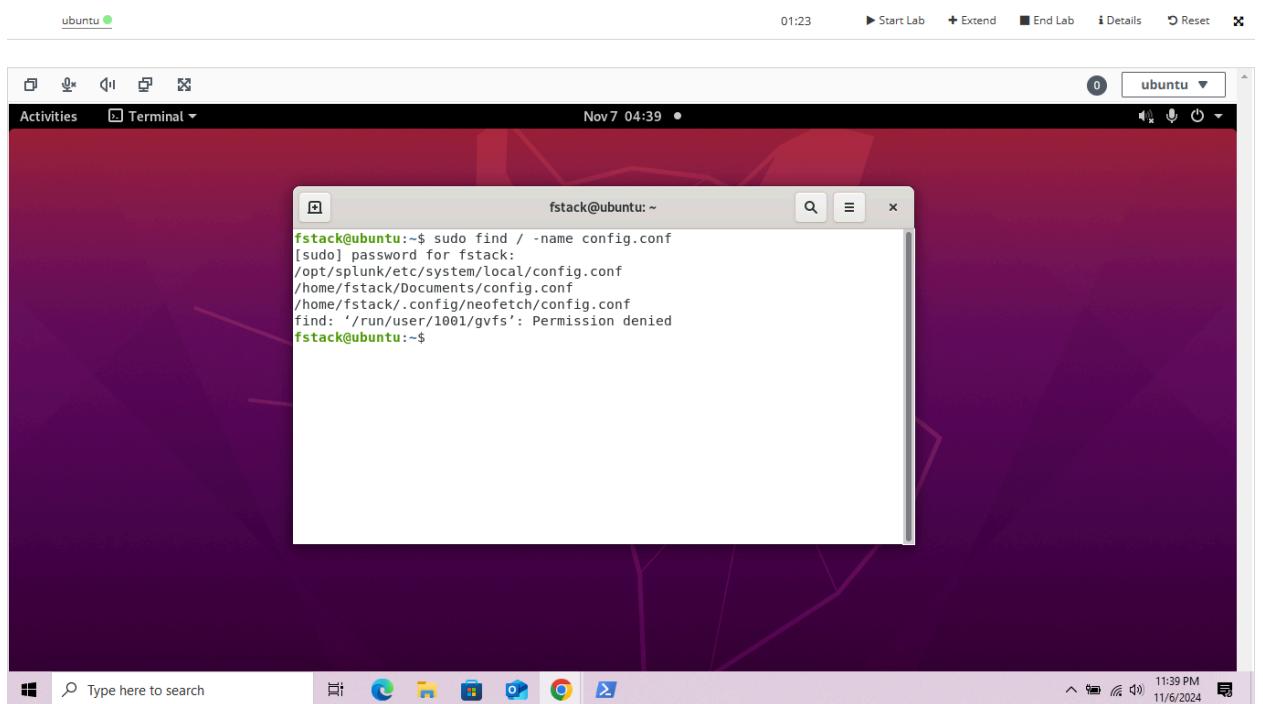


Permissions Report

I was assigned to check out the log files on Splunk, however I ran into an issue. I was unable to check the files because another worker accidentally changed the configuration file "config.conf". In which I had to change the permissions in order to view the log files.

I had to locate exactly where the file was and find what directory I needed to change to. I did this by entering "sudo find / -name config.conf". This showed that I was denied access.



A screenshot of a Linux desktop environment, likely Ubuntu, showing a terminal window. The terminal window title is "fstack@ubuntu: ~". The command entered is "sudo find / -name config.conf". The output shows the command asking for a password, listing several paths including "/opt/splunk/etc/system/local/config.conf" and "/home/fstack/.config/neofetch/config.conf", and then failing with "find: '/run/user/1001/gvfs': Permission denied". The desktop background is a purple gradient, and the taskbar at the bottom shows various application icons.

```
fstack@ubuntu:~$ sudo find / -name config.conf
[sudo] password for fstack:
/opt/splunk/etc/system/local/config.conf
/home/fstack/Documents/config.conf
/home/fstack/.config/neofetch/config.conf
find: '/run/user/1001/gvfs': Permission denied
fstack@ubuntu:~$
```

I needed to change into "opt/splunk/etc/system/local" in order to access this file.

A screenshot of a Linux desktop environment, likely Ubuntu, showing a terminal window titled "fstack@ubuntu: /opt/splunk/etc/system/local". The terminal displays the following command and its output:

```
fstack@ubuntu:~$ sudo find / -name config.conf
[sudo] password for fstack:
/opt/splunk/etc/system/local/config.conf
/home/fstack/Documents/config.conf
/home/fstack/.config/neofetch/config.conf
find: '/run/user/1001/gvfs': Permission denied
fstack@ubuntu:~$ cd /opt/splunk/etc/system/local
fstack@ubuntu:/opt/splunk/etc/system/local$
```

Once I entered the directory. Once I looked in the contents of the file “ls -l” I noticed “-rwxrwxrwx”. That indicates the Owner, the Group, and anyone else had full access to the file.

A screenshot of a Linux desktop environment, likely Ubuntu, showing a terminal window titled "fstack@ubuntu: /opt/splunk/etc/system/local". The terminal displays the following command and its output:

```
fstack@ubuntu:~$ sudo find / -name config.conf
[sudo] password for fstack:
/opt/splunk/etc/system/local/config.conf
/home/fstack/Documents/config.conf
/home/fstack/.config/neofetch/config.conf
find: '/run/user/1001/gvfs': Permission denied
fstack@ubuntu:~$ cd /opt/splunk/etc/system/local
fstack@ubuntu:/opt/splunk/etc/system/local$ ls -l
total 4
-rwxrwxrwx 1 root root 187 Nov  7 03:14 config.conf
fstack@ubuntu:/opt/splunk/etc/system/local$
```

To fix that I first needed to check the “MD5 Hash” and see the specific fingerprint of the current file by entering “md5sum config.conf” this showed me the current state of the file.

A screenshot of an Ubuntu desktop environment. At the top, there's a header bar with icons for Start Lab, Extend, End Lab, Details, Reset, and a close button. The main area shows a terminal window titled "ubuntu" with the command "fstack@ubuntu:~\$ sudo find / -name config.conf" being run. The terminal output shows the search results for the config.conf file, including its location in /opt/splunk/etc/system/local and its md5sum hash. The desktop background is a purple abstract design.

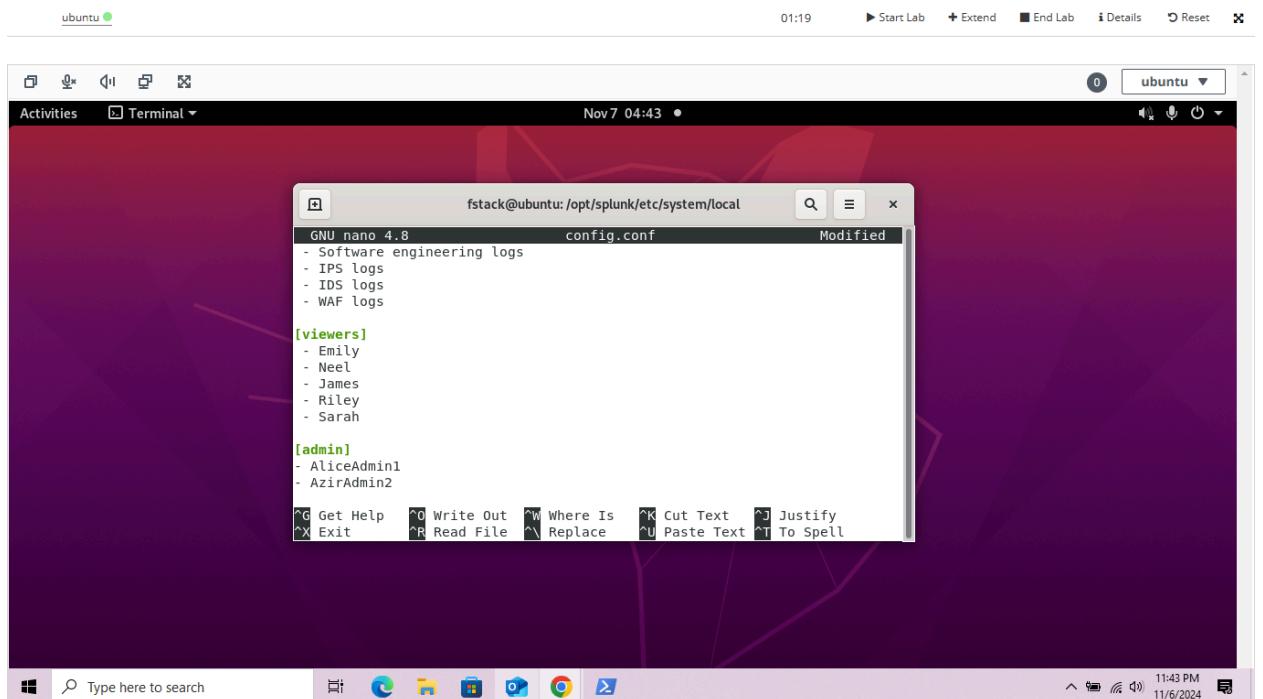
```
fstack@ubuntu:~$ sudo find / -name config.conf
[sudo] password for fstack:
/opt/splunk/etc/system/local/config.conf
/home/fstack/Documents/config.conf
/home/fstack/.config/neofetch/config.conf
find: '/run/user/1001/gvfs': Permission denied
fstack@ubuntu:~$ cd /opt/splunk/etc/system/local
fstack@ubuntu:/opt/splunk/etc/system/local$ ls -l
total 4
-rwxrwxrwx 1 root root 187 Nov  7 03:14 config.conf
fstack@ubuntu:/opt/splunk/etc/system/local$ md5sum config.conf
428d2b746569b0a9018ca3535f0ccc4e config.conf
fstack@ubuntu:/opt/splunk/etc/system/local$
```

Next I needed to change the file so only the owner and the group can view it, preventing anyone else access to the file and potentially being a threat to the file. I did this by using Nano (text editor) to write a script to indicate that Alice and I are the proper admins and owners of the file. I simply put “nano config.conf”

A screenshot of an Ubuntu desktop environment, similar to the one above. It shows a terminal window titled "ubuntu" with the command "fstack@ubuntu:~\$ sudo find / -name config.conf" being run. The terminal output is identical to the previous screenshot, showing the config.conf file and its md5sum hash. The desktop background is a purple abstract design.

```
fstack@ubuntu:~$ sudo find / -name config.conf
[sudo] password for fstack:
/opt/splunk/etc/system/local/config.conf
/home/fstack/Documents/config.conf
/home/fstack/.config/neofetch/config.conf
find: '/run/user/1001/gvfs': Permission denied
fstack@ubuntu:~$ cd /opt/splunk/etc/system/local
fstack@ubuntu:/opt/splunk/etc/system/local$ ls -l
total 4
-rwxrwxrwx 1 root root 187 Nov  7 03:14 config.conf
fstack@ubuntu:/opt/splunk/etc/system/local$ md5sum config.conf
428d2b746569b0a9018ca3535f0ccc4e config.conf
fstack@ubuntu:/opt/splunk/etc/system/local$ nano config.conf
```

Then I typed “[admin]” and under that put “AliceAdmin1” and “AzirAdmin2”. I also made sure to save the file.



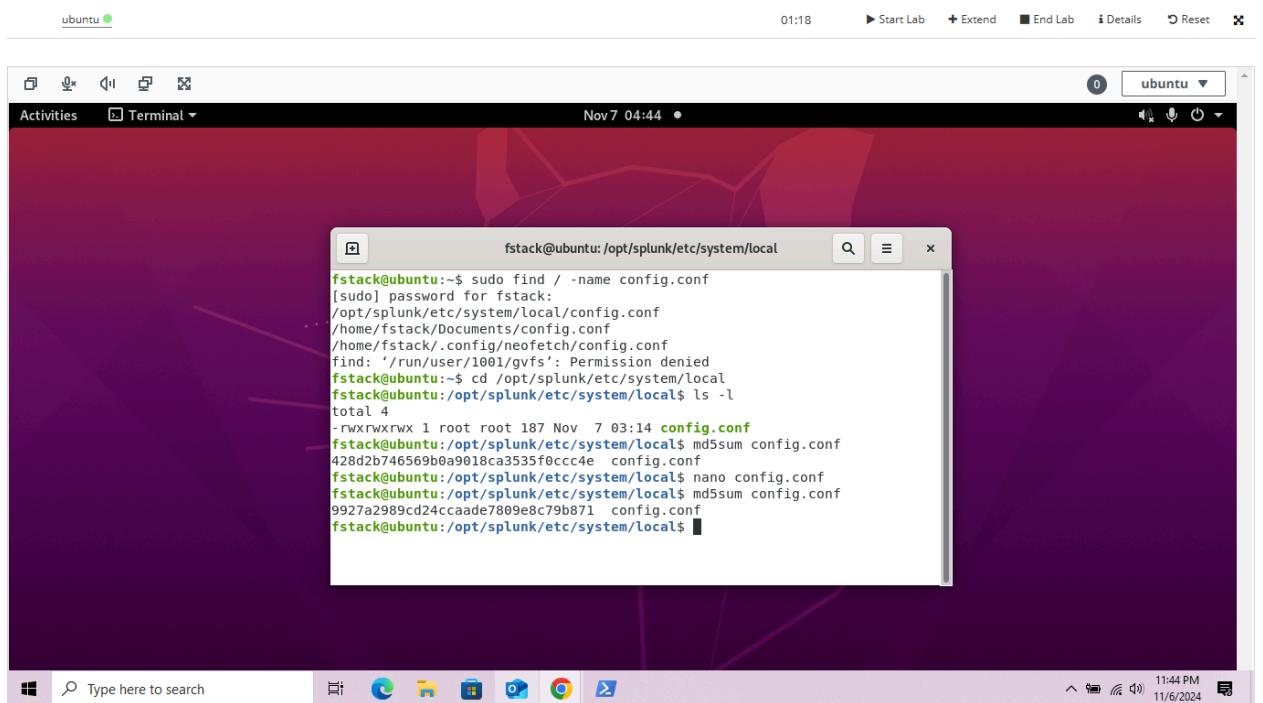
```
GNU nano 4.8 config.conf Modified
- Software engineering logs
- IPS logs
- IDS logs
- WAF logs

[viewers]
- Emily
- Neel
- James
- Riley
- Sarah

[admin]
- AliceAdmin1
- AzirAdmin2

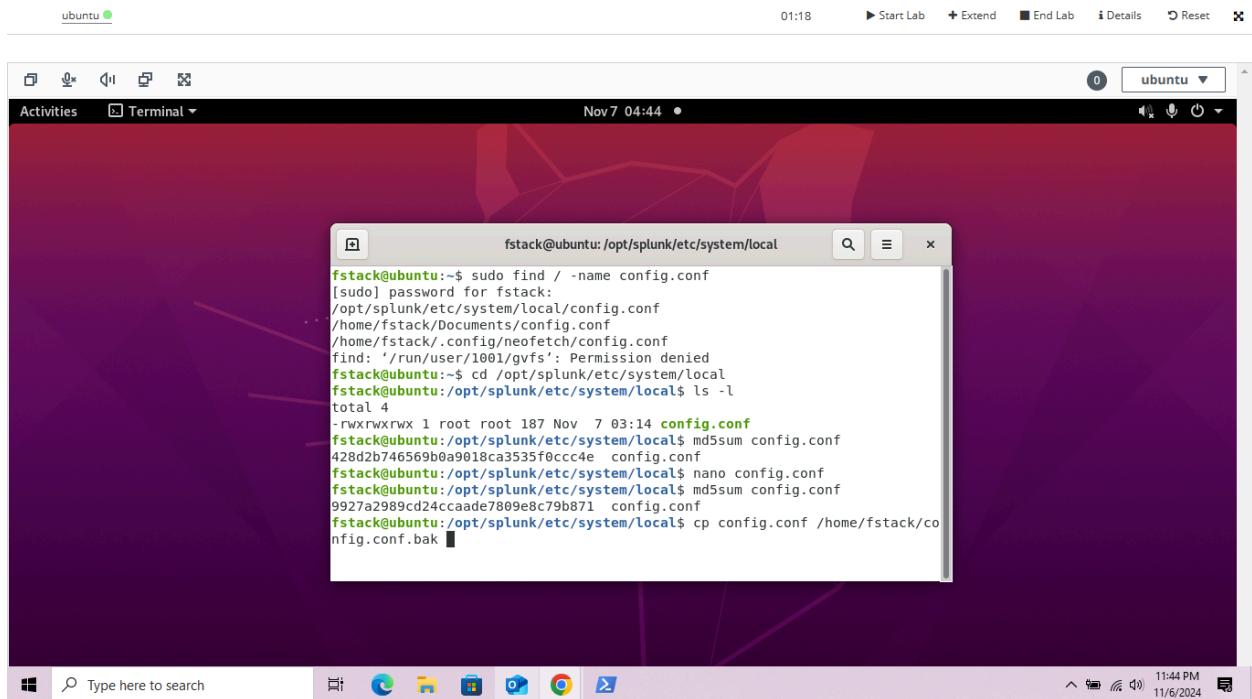
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify
^X Exit ^R Read File ^\ Replace ^U Paste Text ^T To Spell
```

I checked the MD5 hash of the file again (md5sum config.conf) to see if the fingerprint of the file changed. It did!



```
fstack@ubuntu:~$ sudo find / -name config.conf
[sudo] password for fstack:
/opt/splunk/etc/system/local/config.conf
/home/fstack/Documents/config.conf
/home/fstack/.config/neofetch/config.conf
find: '/run/user/1001/gvfs': Permission denied
fstack@ubuntu:~$ cd /opt/splunk/etc/system/local
fstack@ubuntu:/opt/splunk/etc/system/local$ ls -l
total 4
-rwxrwxrwx 1 root root 187 Nov  7 03:14 config.conf
fstack@ubuntu:/opt/splunk/etc/system/local$ md5sum config.conf
428d2b746569b0a9018ca3535f0cc4c config.conf
fstack@ubuntu:/opt/splunk/etc/system/local$ nano config.conf
fstack@ubuntu:/opt/splunk/etc/system/local$ md5sum config.conf
9927a2989cd24ccaade7809e8c79b871 config.conf
fstack@ubuntu:/opt/splunk/etc/system/local$
```

After completing the steps to change the file's permissions I went ahead and copied a file to the /home/fstack directory. I did this by entering “cp config.conf /home/fstack/config.conf.bak”. I specifically copied it to the config.conf.bak file to indicate that it is a backup file, just in case another incident like this occurs.



A screenshot of a Linux desktop environment, likely Ubuntu, showing a terminal window. The terminal window title is "fstack@ubuntu:/opt/splunk/etc/system/local". The terminal shows the following command history:

```
fstack@ubuntu:~$ sudo find / -name config.conf
[sudo] password for fstack:
/opt/splunk/etc/system/local/config.conf
/home/fstack/Documents/config.conf
/home/fstack/.config/neofetch/config.conf
find: '/run/user/1001/gvfs': Permission denied
fstack@ubuntu:~$ cd /opt/splunk/etc/system/local
fstack@ubuntu:/opt/splunk/etc/system/local$ ls -l
total 4
-rwxrwxrwx 1 root root 187 Nov  7 03:14 config.conf
fstack@ubuntu:/opt/splunk/etc/system/local$ md5sum config.conf
428d2b746569b0a9018ca3535f0cc4e config.conf
fstack@ubuntu:/opt/splunk/etc/system/local$ nano config.conf
fstack@ubuntu:/opt/splunk/etc/system/local$ md5sum config.conf
9927a2989cd24ccaade7809e8c79b871 config.conf
fstack@ubuntu:/opt/splunk/etc/system/local$ cp config.conf /home/fstack/co
nfig.conf.bak
```

Once that was done I made sure to change into the /home/fstack directory “cd /home/fstack”.

A screenshot of a Linux desktop environment, likely Ubuntu, showing a terminal window titled "fstack@ubuntu: ~". The terminal displays a command-line session where the user is attempting to modify configuration files. The session starts with a password prompt, followed by commands to change directory, copy files, and edit configuration files. The terminal window has a standard title bar with icons for search, minimize, maximize, and close.

```
[sudo] password for fstack:  
/opt/splunk/etc/system/local/config.conf  
/home/fstack/Documents/config.conf  
/home/fstack/.config/neofetch/config.conf  
find: '/run/user/1001/gvfs': Permission denied  
fstack@ubuntu:~$ cd /opt/splunk/etc/system/local  
fstack@ubuntu:/opt/splunk/etc/system/local$ ls -l  
total 4  
-rwxrwxrwx 1 root root 187 Nov 7 03:14 config.conf  
fstack@ubuntu:/opt/splunk/etc/system/local$ md5sum config.conf  
428d2b746569b0a9018ca3535f0cc4e config.conf  
fstack@ubuntu:/opt/splunk/etc/system/local$ nano config.conf  
fstack@ubuntu:/opt/splunk/etc/system/local$ md5sum config.conf  

```

to look into the “config.conf.bak” file to view the permissions, “ls -l config.conf.bak”.

A screenshot of a Linux desktop environment, likely Ubuntu, showing a terminal window titled "fstack@ubuntu: ~". The terminal displays a command-line session where the user runs "ls -l config.conf.bak" to view the file's permissions. The output shows the file is owned by "fstack" and has permissions "-rw-rw-r--". The terminal window has a standard title bar with icons for search, minimize, maximize, and close.

```
fstack@ubuntu:~$ ls -l config.conf.bak  
-rw-rw-r-- 1 fstack fstack 221 Nov 7 04:45 config.conf.bak
```

I noticed that the only people who can have majority access were the owners and the group. I knew this because it read “-rw-rw-r–” letting me know that anyone that isn't the owner or group couldn't write on this file.

To help protect sensitive files, StackFull Software can strengthen security by changing the ownership of important files. This can be done easily using the “chown” command in the terminal. For example, running “sudo chown azir config.conf” will make me the owner of the config.conf file. If the file needs to be owned by both a user and a group, the command “sudo chown azir:admin logs” can be used to make azir the owner and assign the admin group as the group owner of the logs directory.

Changing the owner of a file is a good way to ensure that only authorized users or groups have access to sensitive information, preventing unauthorized modifications.

Another useful tool for keeping track of file integrity is the MD5 hash. An MD5 hash is essentially a unique "fingerprint" for a file. It allows you to check whether a file has been altered by comparing the current hash to the original one. If the hash changes unexpectedly, it could indicate that the file has been modified, which might be a sign of tampering or some other security issue. This makes MD5 hashes an important tool for verifying the integrity of critical files and detecting any unauthorized changes.