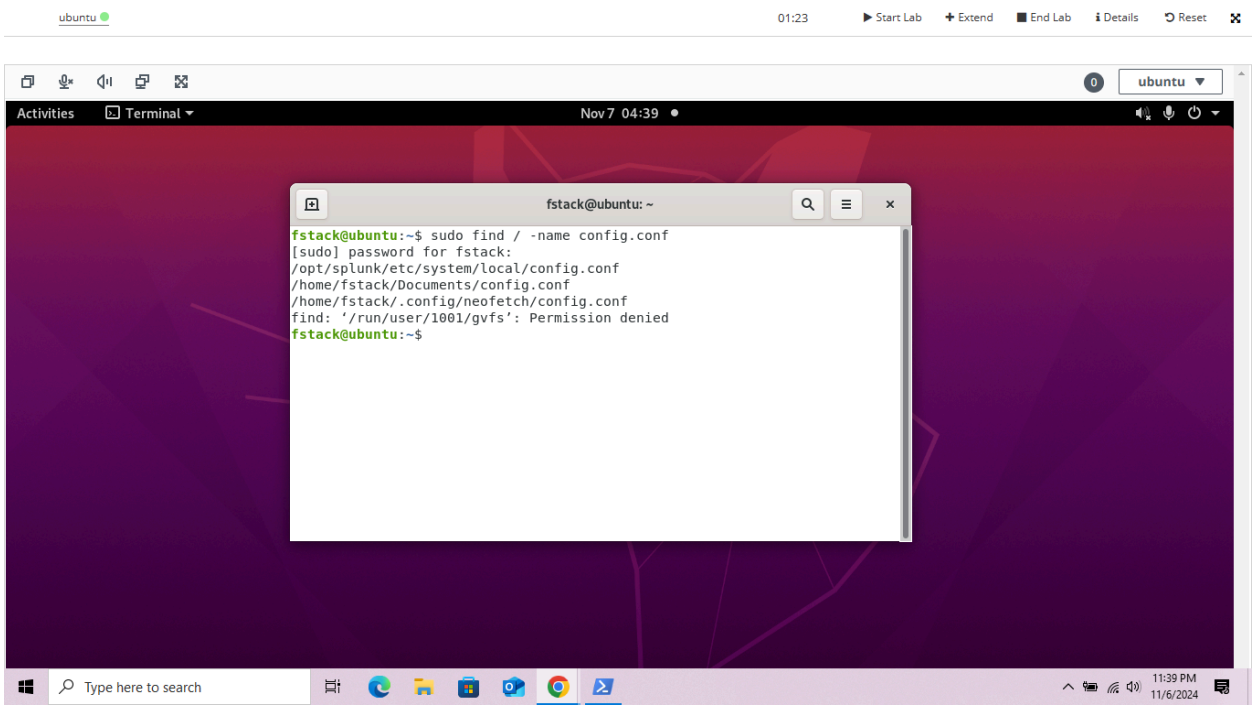
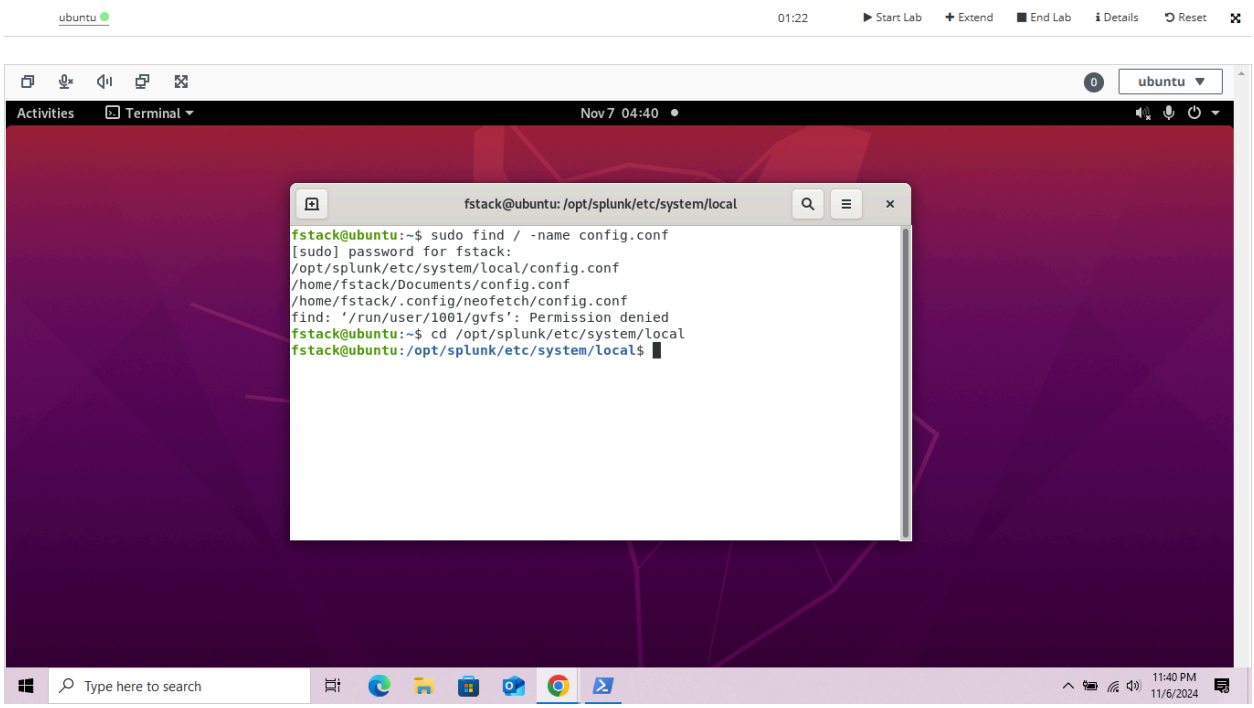
Permissions Report

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.

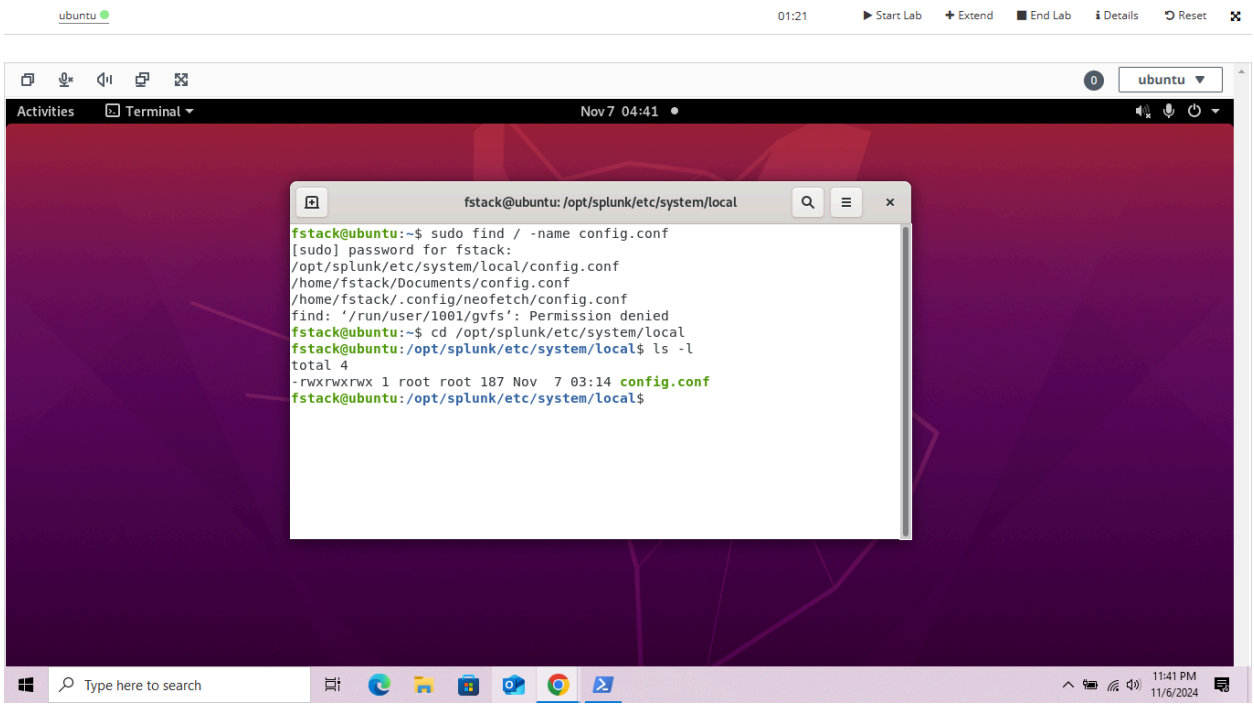
I had to locate exactly where the file was and find what directory I needed to change to. I did this by entering “sudo find / -name config.conf. This showed that I was denied access.



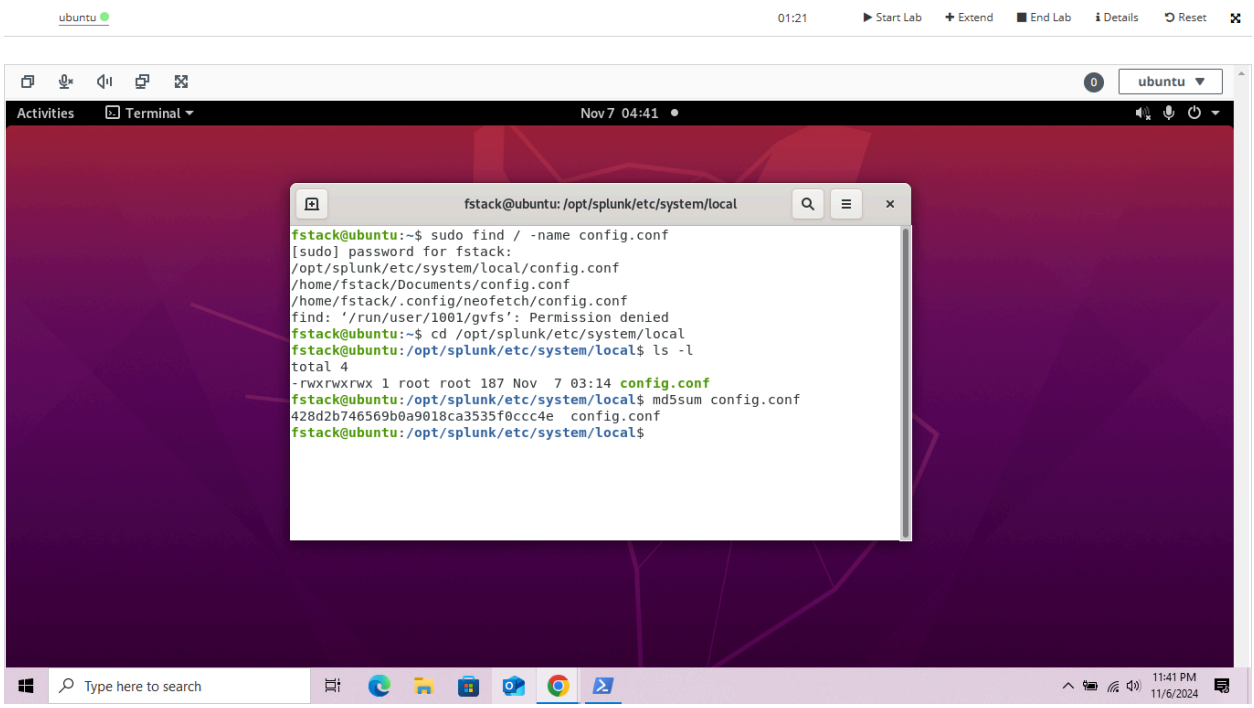
I needed to change into “opt/splunk/etc/system/local” in order to access this file.



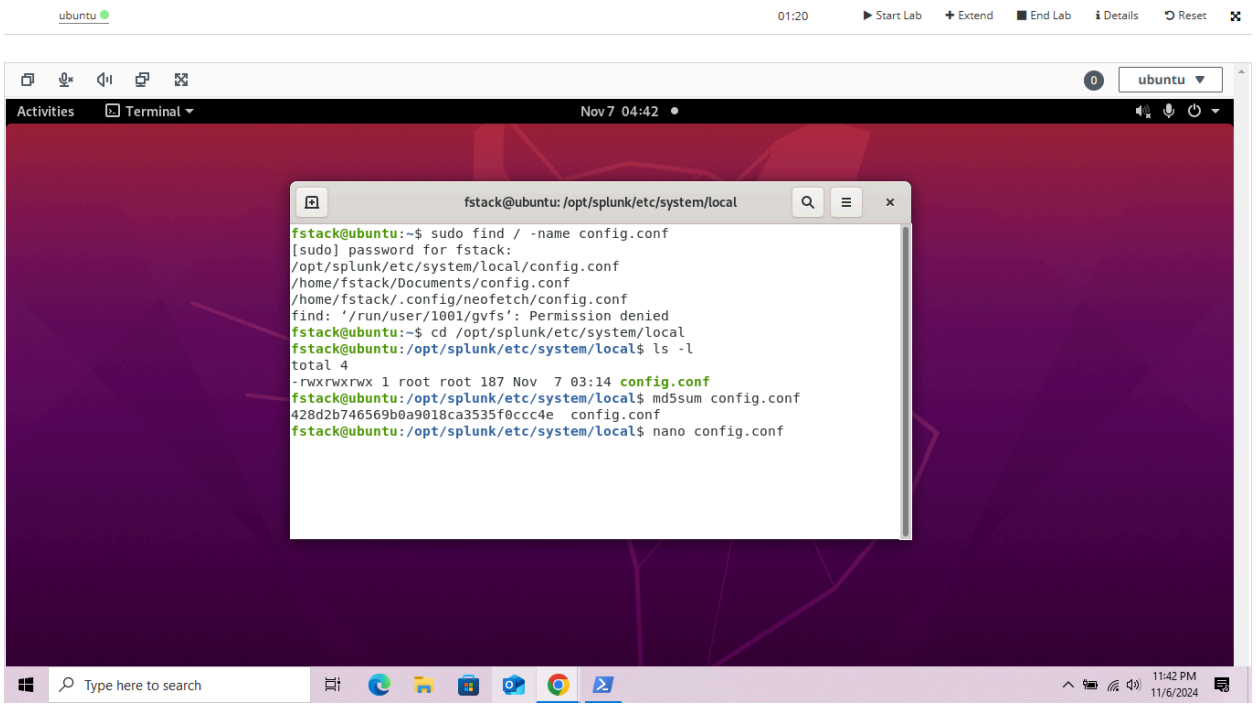
Once I entered the directory. Once I looked in the contents of the file “ls -l” I noticed“-rwxrwxrwx”. That indicates the Owner, the Group, and anyone else had full access to the file.



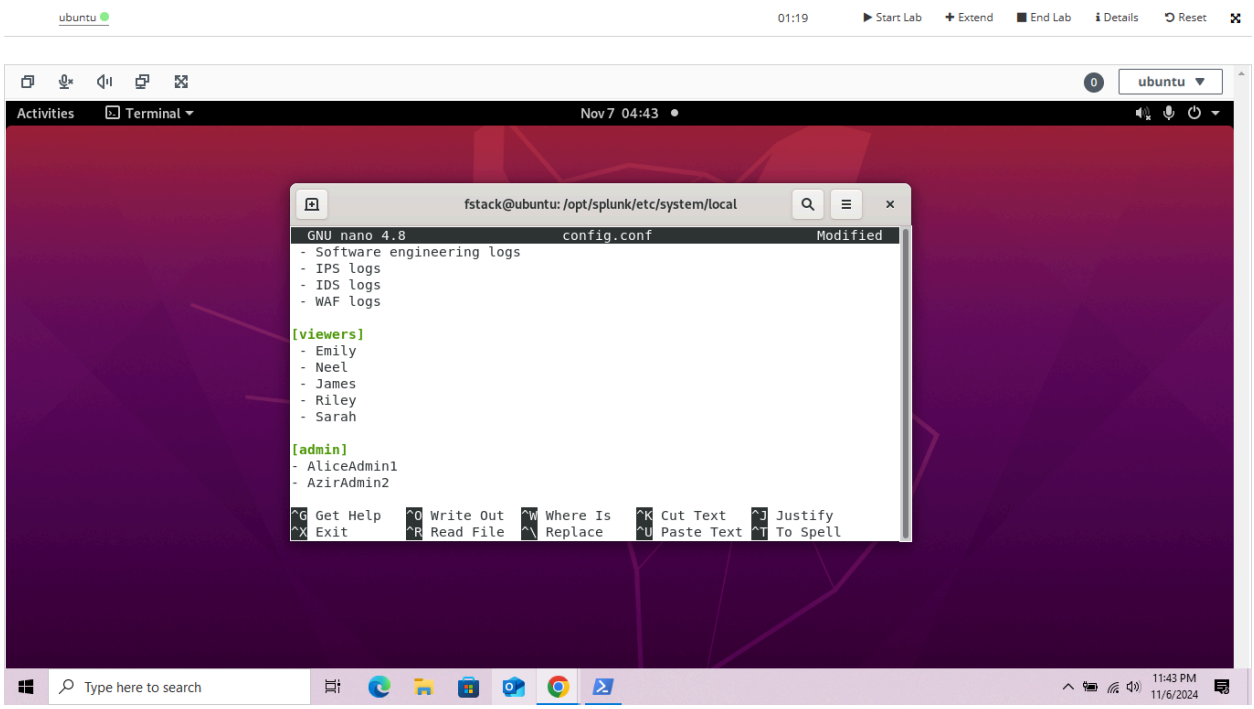
To fix that I first needed to check the “MD5 Hash” and see the specific fingerprint of the current file by entering “md5sum config.conf” this showed me the current state of the file.



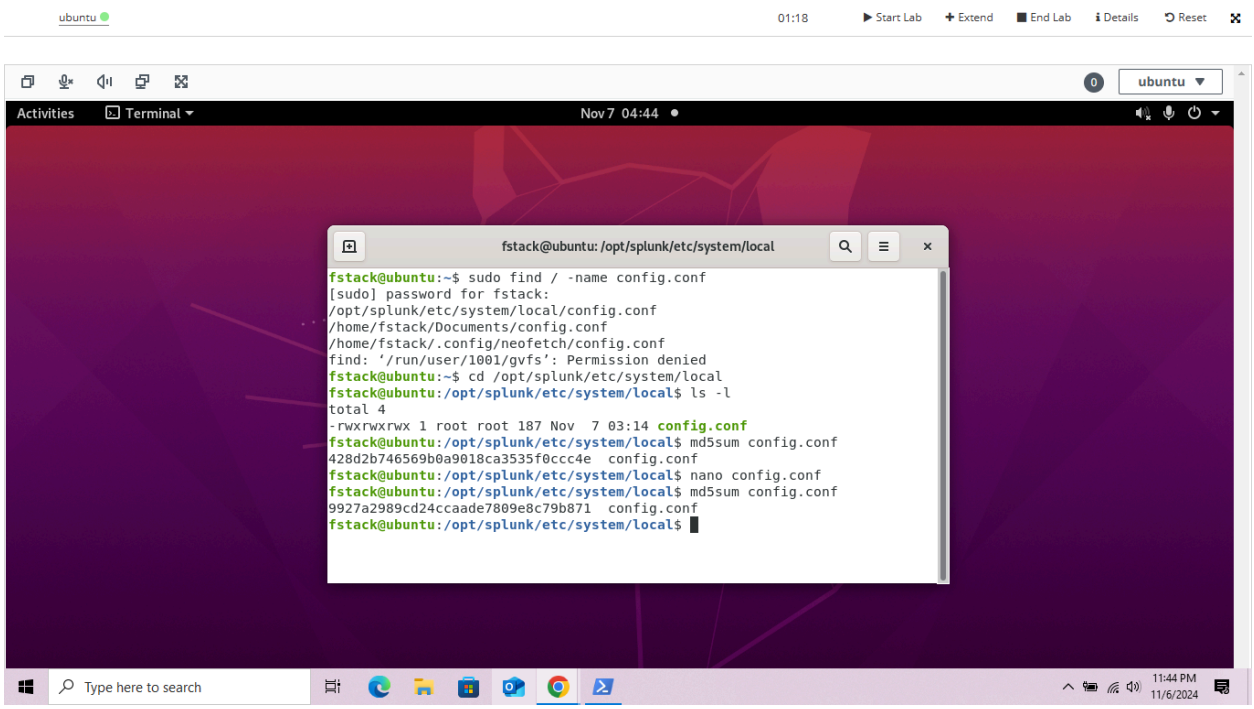
Next I needed to change the file so only the owner and the group can view it, preventing anyone else access to the file and potentially being a threat to the file. I did this by using Nano (text editor) to write a script to indicate that Alice and I are the proper admins and owners of the file. I simply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



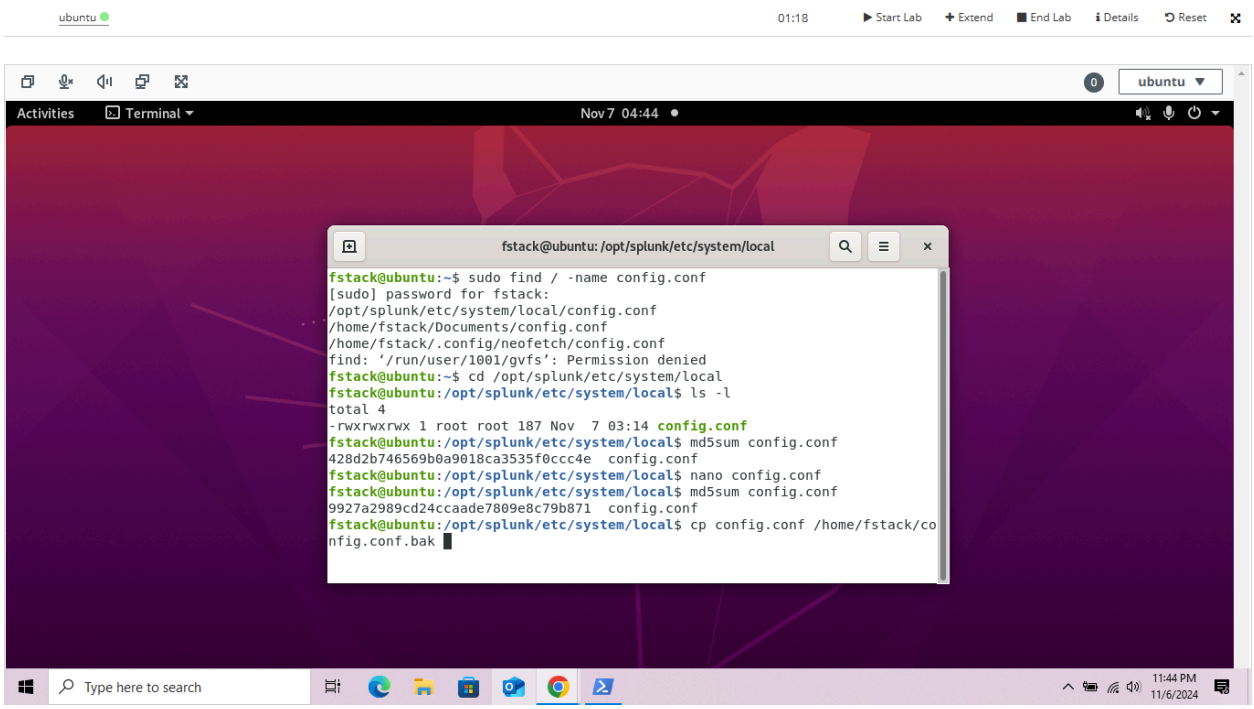
Then I typed “[admin]” and under that put “AliceAdmin1” and “AzirAdmin2”. I also made sure to save the file.



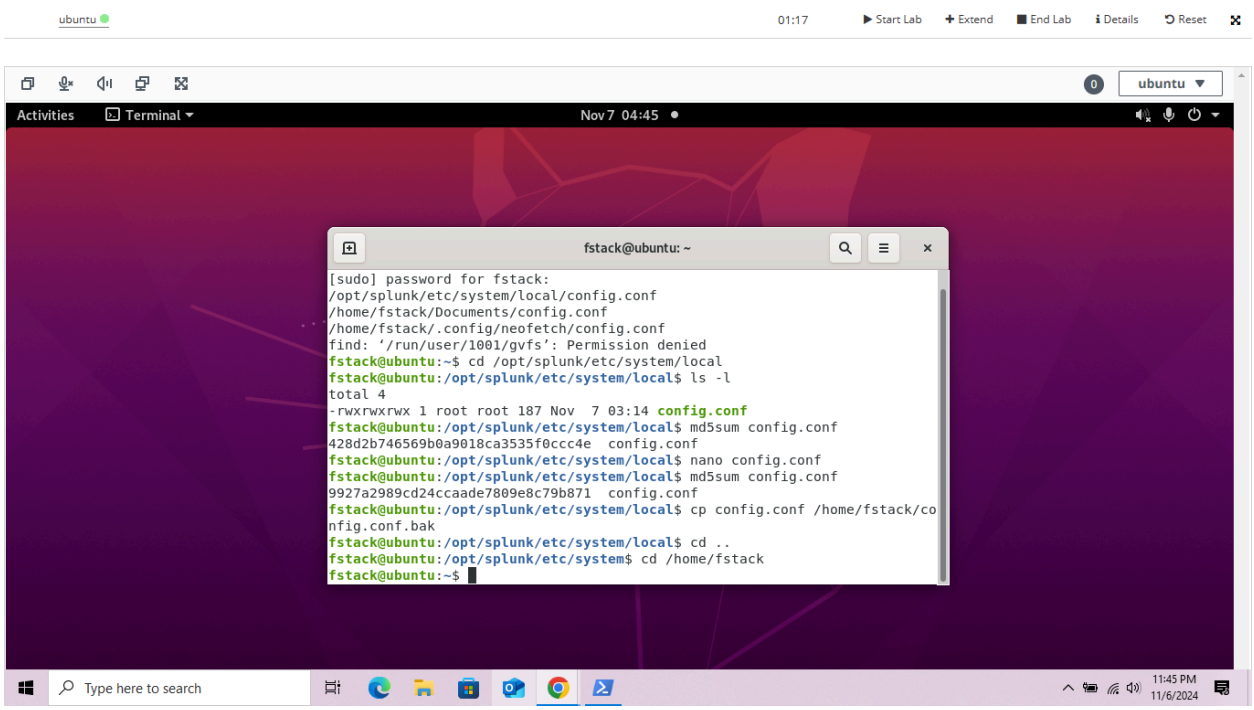
I checked the MD5 hash of the file again (md5sum config.conf) to see if the fingerprint of the file changed. It did!



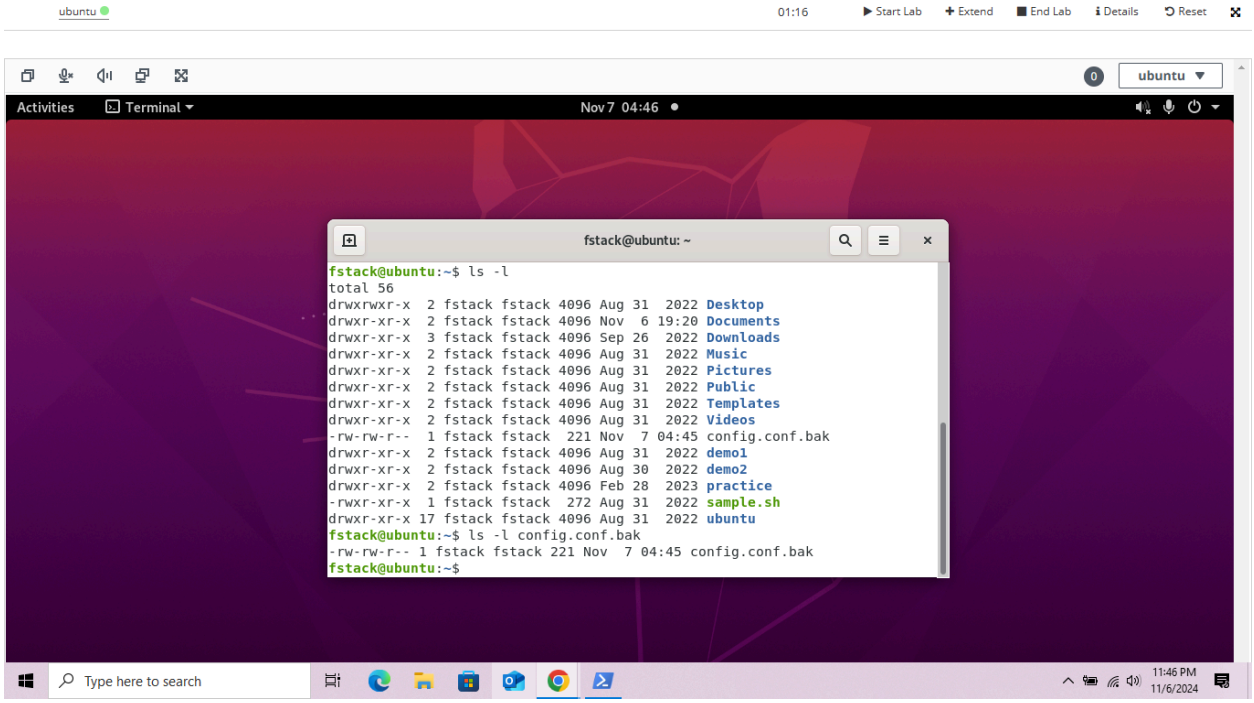
After completing the steps to change the file's permissions I went ahead and copied a file to the /home/fstack directory. I did this by entering “cp config.conf /home/fstack/config.conf.bak”. I specifically copied it to the config.conf.bak file to indicate that it is a backup file, just in case another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



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



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