Alice Full Stack Software Level 2 SOC

Executive Summary: Having access to config.conf file by locating it and looking at the hash to check integrity. Edited the file so I can have access to Splunk and placed a backup file on my fstack drive.

Introduction: I am trying to have access to splunk but did not have permissions. James changed the configuration file name of config.conf that is preventing me from accessing the logs.

Body: First I had to locate the file config.conf by using the locate command after which I change directories to that file. I checked the permissions by using the ls -l command and found out that everyone have access to that file. I then check the hash of the file using the md5sum hash after which I used the vim command to edit the file. Changed the file to:

[admin]

─ AliceAdmin1  
  ─ [YourName]Admin2

c70754d9c7bab08a8c441f90c37f27eb original file

21f0e7ac9ba04elaed957ab05241b5b changed file

After which I checked the hash one last time to check the integrity see above to store integrity. Finally I made a copy of the file to my fstack directory by using the cp command.

Conclusion: This is for record keeping for people who needs access to the file. In conclusion,

I located the file, verified the hash, edit the file and then I made a backup copy to my directory.

A screenshot of a computer

Description automatically generated

Locate /opt/splunk/etc/system/local/config.conf

A screen shot of a computer

Description automatically generated

Cd into the local

A screen shot of a computer

Description automatically generated

Look at the permission file



The hash of the file

A screenshot of a computer

Description automatically generated’

Vim the file and paste the output.

A screenshot of a computer

Description automatically generated

Get a different Hash on the file