Career Simulation 1: The Permissions Problem Report

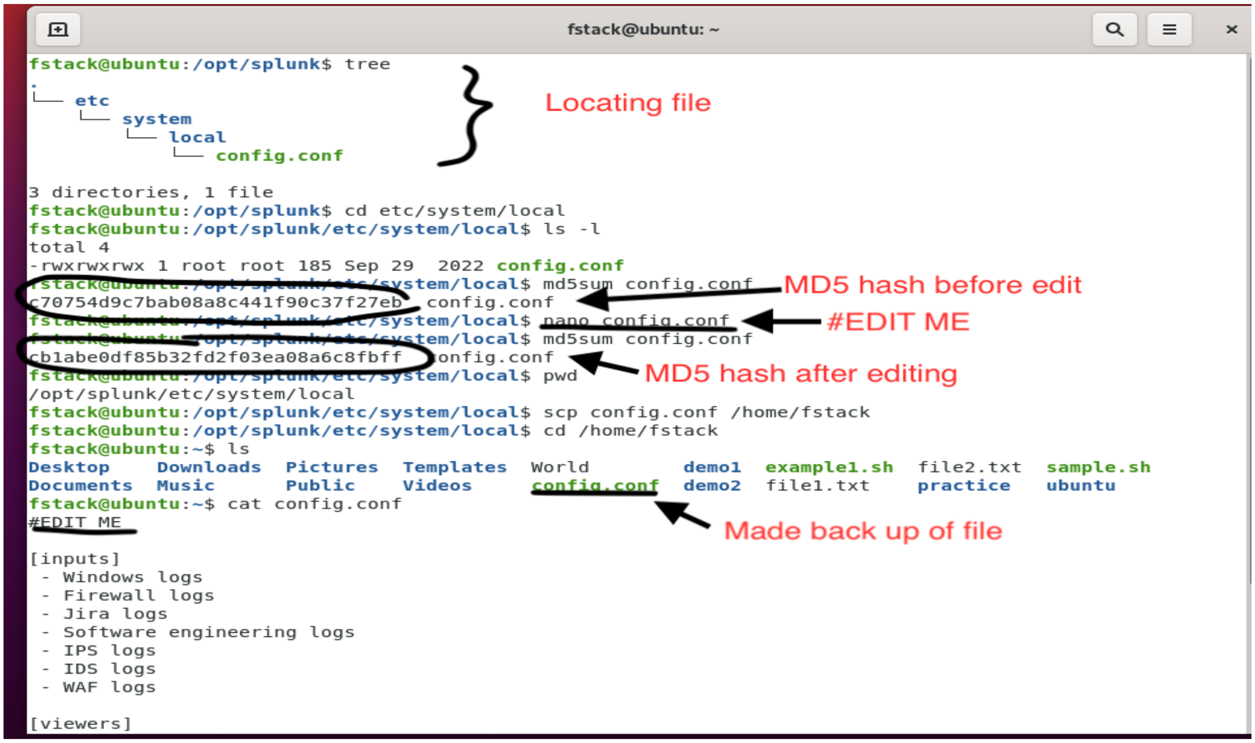
The Problem: a configuration file was not operating within defined parameters.
The Solution: Lvl1 SOCA located file, modified file, made a backup in home directory, and verified solution.
Recommendations: edit/correct file to reflect appropriate user permissions, implement and utilize Principle of Least Privilege for all files and systems, and, as dictated by security protocols, create a copy/backup in another directory.
Further Guidelines: use programs to monitor file integrity, update and enact technical policies and security measures.

The configuration[1] of a particular file was found to inhibit the ability to view logs[2] within a directory. A Level 1 SOC Analyst, under supervision of a Level 2 SOC Analyst, remedied the issue and offered recommendations for improved security measures. This report outlines the steps taken to correct the problem, visual explanations of procedures and jargon, and guidance to ensure proper authorizations are in place, as well as, how to mitigate similar recurrences.

The attached screen captures outline steps taken by the Lvl1 SOCA:

1. Located the file.
2. Checked the MD5 hash to establish a “before” checksum.
3. Accessed the file to make corrections.
4. Rechecked the MD5 hash for “after” checksum.
5. Created a backup/copy in a higher level directory.
6. Modifications to the file.
7. Verifying file status and date stamps.

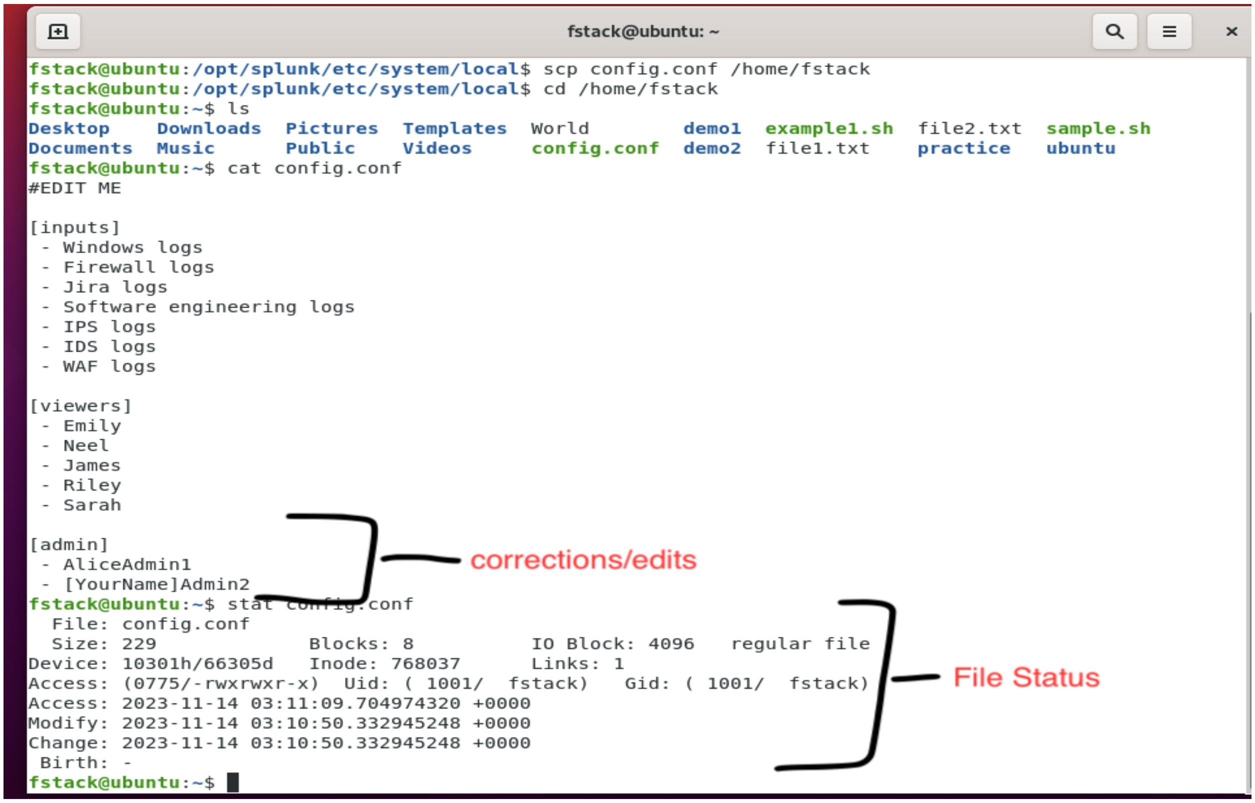
Slide 1



```
fstack@ubuntu:/opt/splunk$ tree
.
└── etc
    └── system
        └── local
            └── config.conf

3 directories, 1 file
fstack@ubuntu:/opt/splunk$ cd etc/system/local
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$ nano config.conf
fstack@ubuntu:/opt/splunk/etc/system/local$ md5sum config.conf
cb1abe0df85b32fd2f03ea08a6c8fbff  config.conf
fstack@ubuntu:/opt/splunk/etc/system/local$ pwd
/opt/splunk/etc/system/local
fstack@ubuntu:/opt/splunk/etc/system/local$ scp config.conf /home/fstack
fstack@ubuntu:/opt/splunk/etc/system/local$ cd /home/fstack
fstack@ubuntu:~$ ls
Desktop    Downloads  Pictures  Templates  World        demo1  example1.sh  file2.txt  sample.sh
Documents  Music      Public    Videos     config.conf  demo2  file1.txt    practice   ubuntu
fstack@ubuntu:~$ cat config.conf
#EDIT ME

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

[viewers]
```

Career Simulation 1: The Permissions Problem Report

Slide 2



```
fstack@ubuntu:/opt/splunk/etc/system/local$ scp config.conf /home/fstack
fstack@ubuntu:/opt/splunk/etc/system/local$ cd /home/fstack
fstack@ubuntu:~$ ls
Desktop    Downloads  Pictures  Templates  World        demo1  example1.sh  file2.txt  sample.sh
Documents  Music      Public    Videos     config.conf  demo2  file1.txt    practice   ubuntu
fstack@ubuntu:~$ 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

[admin]
 - AliceAdmin1
 - [YourName]Admin2
fstack@ubuntu:~$ stat config.conf
  File: config.conf
  Size: 229             Blocks: 8          IO Block: 4096   regular file
Device: 10301h/66305d   Inode: 768037      Links: 1
Access: (0775/-rwxrwxr-x)  Uid: ( 1001/  fstack)   Gid: ( 1001/  fstack)
Access: 2023-11-14 03:11:09.704974320 +0000
Modify: 2023-11-14 03:10:50.332945248 +0000
Change: 2023-11-14 03:10:50.332945248 +0000
 Birth: -
fstack@ubuntu:~$
```

The program, md5sum, calculates and verifies file integrity of 128 bit MD5 hashes, using Message-Digest Algorithm 5, in situations that are not security related. For security related reasons, use one of six hash functions, that computes checksums of various lengths (224, 256, 384, or 512 bits), in the SHA-2 hashes family. At a later date (TBD), a Lvl2 SOCA will conduct a brief pertaining to the utilization and management of those six functions.

Summary

A file configuration issue was found within the Splunk directory. A Level 2 SOC Analyst established a Secure Shell (SSH) connection to Splunk server for Lvl 1 SOCA to investigate, remedy the issue, and verify correction. File was edited to add the correct permissions. Future issues can be avoided by establishing appropriate permission levels, backups for sensitive files, updating security policies, and monitoring files.

[1] A configuration file, often shortened to config file, defines the parameters, options, settings and preferences applied to operating systems, infrastructure devices, and applications.

[2] Linux logs (named after ships logs) live in /var/log and are a record of events that happen on the computer, exactly what events depend on the log file.