

The Permissions Problem

1. Executive Summary

This report outlines the problem and resolution of a configuration issue within StackFull Software's Splunk SIEM. The problem stemmed from an unauthorized edit to the `config.conf` file, which stopped new users from searching anything within the Splunk SIEM.

To resolve this issue, we first located the `config.conf` file within the `/opt/splunk` directory. We then changed the directory to the location of the file and checked the file permission using `ls -l config.conf`, getting back `rw-rw-rw-`. This shows that anyone with access to the file was able to edit the file without authorization.

Using the `md5sum` command, we verified the integrity of the file after executing any necessary edits using the nano file editor, creating a hash before and after editing. The final step taken was to create a backup file and save it in the `/home/fstack` directory to ensure quick recovery if any unauthorized changes or corruption of the file occurs.

2. Introduction

My name is Eric Liu from the cybersecurity department. As a new employee at StackFull Software, I was recently given access to Splunk and all relevant log files of the company. When trying to search anything, I was unable to search anything due to some odd configuration issues within Splunk. James, a Level 1 SOC Analyst had inadvertently changed a configuration file named `config.conf`, which is preventing me from looking at logs. I am given the task of finding the `config.conf` and modifying the configuration file so that the department can properly view logs with Splunk.

1. Body

3.1

The first step was to find the configuration file. To do that, I used the `find` command and entered in the command line; `find /opt/splunk/ -name "config.conf"`. The reason why I used `find` was because I was given the fact that all Splunk stores all of its files within the `/opt/splunk` directory, so it helps narrow down the search. After entering that command line, I was given the location of `config.conf`, with the direct path being `/opt/splunk/etc/system/local/config.conf`.

```
fstack@ubuntu:~$ find /opt/splunk -name "config.conf"
/opt/splunk/etc/system/local/config.conf
fstack@ubuntu:~$
```

(Figure 1)

3.2

After using the `cd` command line; `cd /opt/splunk/etc/system/local`, I checked the file permissions of `config.conf` using the `ls -l` command line; `ls -l config.conf`. When looking at the file permissions, it shows that users, groups, and others all have read, write, and execute permission, so that crosses out file permission as being the problem. This explains the unauthorized edit of the file.

```
fstack@ubuntu:~$ find /opt/splunk -name "config.conf"
/opt/splunk/etc/system/local/config.conf
fstack@ubuntu:~$ cd /opt/splunk/etc/system/local/
fstack@ubuntu:/opt/splunk/etc/system/local$ ls -l config.conf
-rwxrwxrwx 1 root root 185 Sep 29 2022 config.conf
fstack@ubuntu:/opt/splunk/etc/system/local$
```

(Figure 2)

3.3

I used the `md5sum` command line; `md5sum config.conf`, so that we can compare later, producing a hash of `c70754d9c7bab08a8c441f90c37f27eb`. We will reference this hash later.

```
fstack@ubuntu:~$ find /opt/splunk -name "config.conf"
/opt/splunk/etc/system/local/config.conf
fstack@ubuntu:~$ cd /opt/splunk/etc/system/local/
fstack@ubuntu:/opt/splunk/etc/system/local$ ls -l config.conf
-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$
```

(Figure 3)

3.4

I used the `nano config.conf` command line to see what the file contained and it was missing the admin section of the file. So I edited the file and added an Admin section and included Alice as well as myself in the list.

```
GNU nano 4.8 config.conf
[inputs]
- Windows logs
- Firewall logs
- Jira logs
- Software engineering logs
- IPS logs
- IDS logs
- WAF logs

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

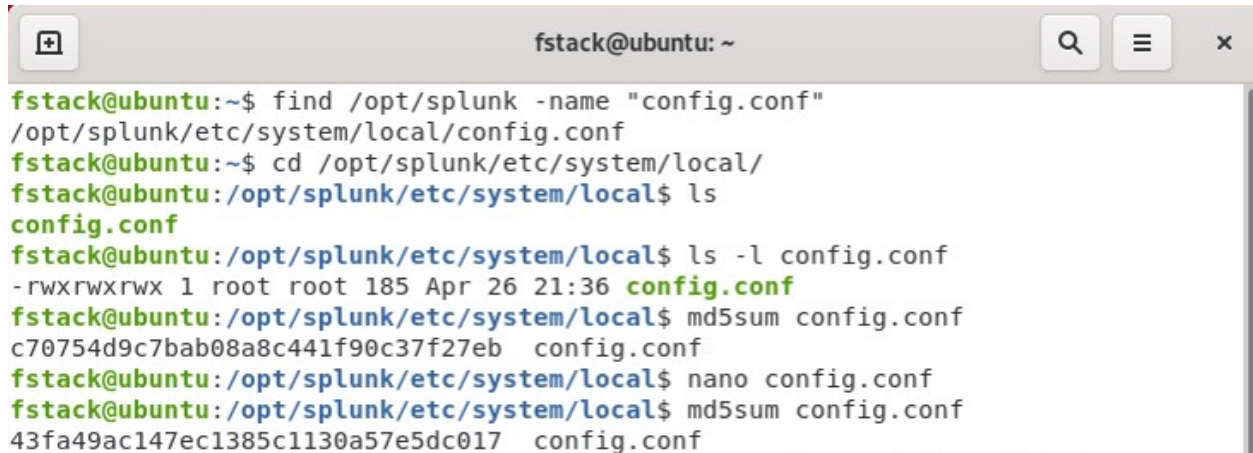
[admin]
- AliceAdmin1
- EricAdmin2
```

(Figure 4)

3.5

After I saved and exited the file, I used the `md5sum` command line again and received a new hash of `43fa49ac147ec1385c1130a57e5dc017`. The reason I made sure to execute a `md5sum config.conf` before and after editing the file is because I wanted to make sure

that the edit actually happened. I got the original hash before the edit so I know exactly what the file looked at that moment. Getting a new hash after editing helps confirm that the file is different and verifies the integrity of the file.

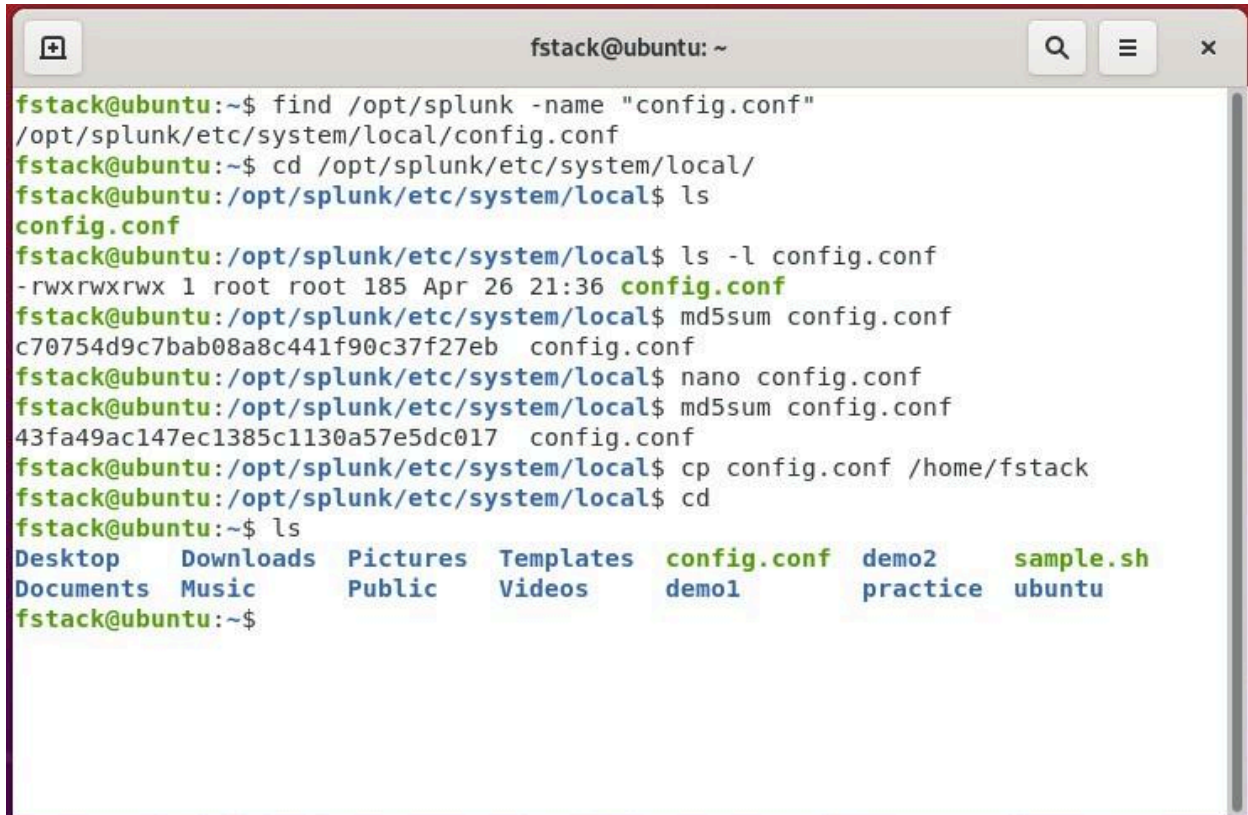


```
fstack@ubuntu: ~  
fstack@ubuntu:~$ find /opt/splunk -name "config.conf"  
/opt/splunk/etc/system/local/config.conf  
fstack@ubuntu:~$ cd /opt/splunk/etc/system/local/  
fstack@ubuntu:/opt/splunk/etc/system/local$ ls  
config.conf  
fstack@ubuntu:/opt/splunk/etc/system/local$ ls -l config.conf  
-rwxrwxrwx 1 root root 185 Apr 26 21:36 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  
43fa49ac147ec1385c1130a57e5dc017 config.conf
```

(Figure 5)

3.6

The last step taken was to make a backup of config.conf so I copied the file and copied it to the /home/fstack directory with the command line `cp config.conf /home/fstack`. This helps ensure that if the file gets corrupted, or an edit causes any problem, we have a clean copy to go back to. Attached below is a complete breakdown of every command performed and where the new backup is located.

A terminal window titled 'fstack@ubuntu: ~' showing a series of commands and their outputs. The user finds the 'config.conf' file in '/opt/splunk/etc/system/local/'. They then check its permissions (-rwxrwxrwx), calculate its MD5sum (c70754d9c7bab08a8c441f90c37f27eb), and use 'nano' to edit it. After another MD5sum check (43fa49ac147ec1385c1130a57e5dc017), they copy the file to '/home/fstack' and return to the home directory. A final 'ls' command shows the file in the home directory alongside other files like 'demo1', 'demo2', 'practice', and 'sample.sh'.

```
fstack@ubuntu:~$ find /opt/splunk -name "config.conf"
/opt/splunk/etc/system/local/config.conf
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$ ls -l config.conf
-rwxrwxrwx 1 root root 185 Apr 26 21:36 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
43fa49ac147ec1385c1130a57e5dc017 config.conf
fstack@ubuntu:/opt/splunk/etc/system/local$ cp config.conf /home/fstack
fstack@ubuntu:/opt/splunk/etc/system/local$ cd
fstack@ubuntu:~$ ls
Desktop  Downloads  Pictures  Templates  config.conf  demo2      sample.sh
Documents Music      Public    Videos    demo1        practice   ubuntu
fstack@ubuntu:~$
```

(Figure 6)

4. Conclusion

The config.conf file is fixed and access to logs and searching anything in Splunk is restored. A backup is securely copied over to **/home/fstack**, ensuring quick recovery if needed. In order to avoid any future mishaps, I suggest a few actions that should be taken. First, have other users test access to Splunk to confirm the usability. Second, monitor the /opt/splunk directory for any unauthorized changes. And third, when looking at the file permissions, I saw that everyone had access to read, write, and execute anything regarding config.conf. Measures should be taken to change permission access to edit the file to only authorized users, and everyone else access to only read the file.