Tyler Danner
Career Prep #1 Report

Stackfull Software Report

At Stackfull Software various business units store their log files into the Splunk SIEM. *(Firewall logs, Windows Event logs, Jira logs, software engineering logs, etc.)* This allows SOC analysts to view anything and everything that may be important when a cyber incident occurs. Proper logging is crucial for handling any cyber incidents.

Problem: _____

When joining Stackfull Software, I was granted access to splunk to view all of the various logs mentioned before. However, I was unable to search anything due to some odd configuration issue within Splunk. After an SSH connection to the Splunk server, it was noticed that another level 1 SOC analyst had inadvertently changed a configuration file that is preventing me from viewing logs. I was tasked with finding and modifying the configuration file to allow myself to properly view the log files within Splunk.

Solution: _____

To resolve this issue I had to first find the configuration file that was causing the problem. After understanding the exact file name I was looking for, I used the 'find' command to search the Splunk directory for *'config.conf'.* After receiving the direct path to the configuration file, I moved into the directory it was located in. I proceeded to list the permission of this file which were: read, write and execute for everyone. This was the first vulnerability I came across during this exercise. These permissions would allow anyone to access and make changes to the configuration file. To ensure I made the corrections, I ran the MD5 hash command and was given a unique key to compare with another after making the changes. After receiving the hash I was prepared to edit the configuration file. I added myself and my mentor, Alice to the [admin] section, and saved the configuration file. After making those changes I ran another MD5 hash and received a totally new, unique key assuring the changes were made to the file. I then made a backup of the configuration file in my home directory.

Improvements: _____

The Stackfull Software team can improve the security of files by checking their permissions, and seeing who has access to certain files. During this investigation, the configuration file that was producing the issue was able to be read and modified by everyone. As stated before these log files are crucial to the SOC analysts for any future cyber incidents, and the ability to modify these files could cause serious issues in the future. To ensure these files are not modified in any way, they should be assigned MD5 hashes to provide clarity if there are ever changes within the file. This would provide another layer of security as well as changing the permissions. With both of these adjustments, the Splunk log files would be much more secure and have a much smaller chance of inadvertent changes being made to disrupt workflow.