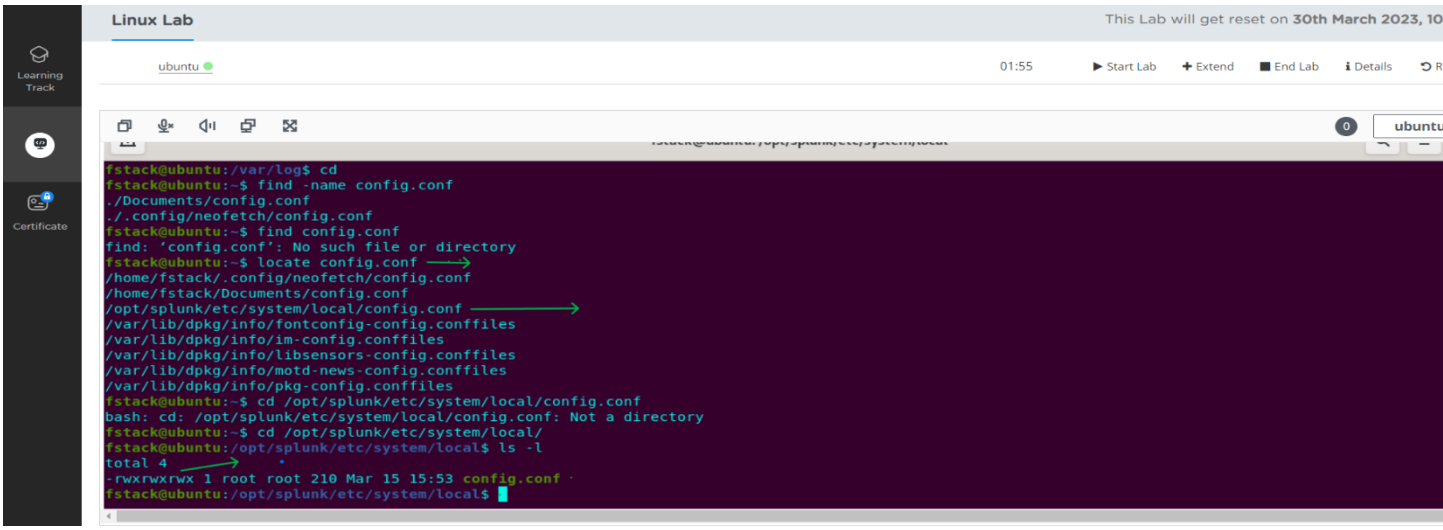
File investigation Report: Splunk

Report:

Subject: Investigation of Company Log Files

As a cybersecurity analyst at StackFull Software, it is incumbent upon my team and me to uphold the principles of confidentiality, integrity, and availability. These principles serve as the foundation of our daily operations and are critical to the security and functionality of our systems. Any failure to maintain these principles can lead to severe consequences.

A pertinent instance of this occurred following a decision made by my monitor, Alice, who holds the position of Level 2 in the Security Operations Center (SOC). Alice authorized me to investigate the company's log files. During my review of these logs, I identified several issues that merit immediate attention:



Findings and Recommendations Report

Investigation of System Security and File Management

Findings:

1. **Confidentiality Breach:**

- Issue: The config.conf file was accessible to all users, not restricted to administrators as intended. This unrestricted access compromises the confidentiality of sensitive information.
- Recommendation: Restrict access to the config.conf file to administrators only.

2. **Integrity Compromise:**

- Issue: The file permissions were incorrectly set to RWX-RWX-RWX for all users, allowing anyone to modify the file. Additionally, there was no hash algorithm implemented to verify the file's integrity.
- Recommendation: Modify file permissions to ensure only authorized modifications are possible and implement a hashing mechanism to monitor file integrity.

3. **Availability Issue:**

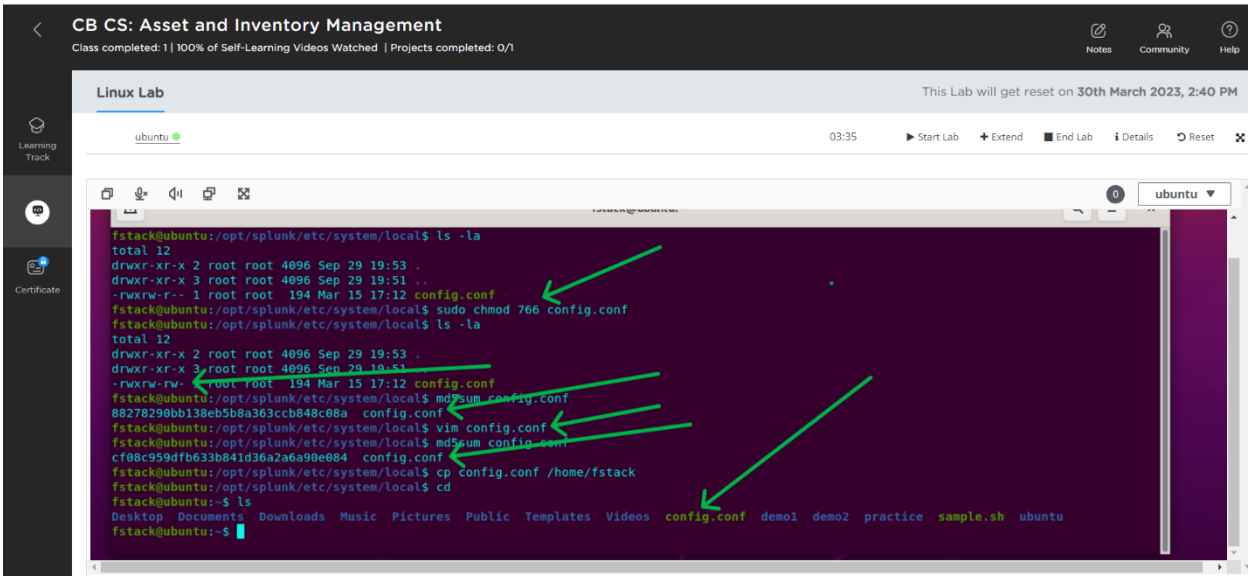
- Issue: The config.conf file was not readily available in the expected home directory, leading to inefficiencies and excessive time spent locating the file.
- Recommendation: Ensure critical configuration files are easily accessible to authorized users without compromising security.
-

3.Solutions Implemented:

a) Located the config.conf file within the local system folder to address the immediate availability concern.
b) Changed the file permissions to 764, ensuring that the owner has full permissions, the group can read and write, and others can only read.
c) Modified the file using VIM to add the current date and information for two administrators, enhancing file management and accountability.
d) Employed 'Hash5sum' to test the integrity of the configuration.conf file, establishing a baseline for future integrity verifications.
e) Created a backup of the config.conf file in the home directory, safeguarding against data loss and facilitating easier access.

Visual Documentation:

The steps taken to address these issues were documented using screenshots from a VM running Ubuntu in the Linux operating system. These images provide a clear, step-by-step illustration of the corrective actions implemented.



Executive Summary:

In our commitment to uphold the principles of the CIA Triad—Confidentiality, Integrity, and Availability—as the guiding framework for our information security practices, my team and I have undertaken several critical steps to reinforce our system's security posture.

1. **File Location and Access Control:** We successfully located the config.conf file and adjusted its access permissions to ensure that group members and other users are restricted to Read and Write operations only. This measure prevents unauthorized alterations while allowing necessary operational functionality.

2. **User Account Security**: We have established secure user accounts, namely AliceAdmin1 and AbdelAdmin2, to enforce role-based access controls. These accounts are designed to offer administrative privileges to authorized personnel, further securing our system's management.

3. **Integrity Verification:** A hashing algorithm has been implemented to maintain the integrity of the config.conf file. This critical step ensures that any unauthorized modifications are promptly detected, preserving the file's authenticity.

4. **Data Resilience:** To enhance our preparedness for any future security incidents, we have created a backup of the config.conf file in our home directory. This backup serves as an essential recovery point, ensuring that our system can be restored to a known, secure state in the event of a compromise.

These measures collectively strengthen our information security framework, ensuring that the principles of the CIA Triad are thoroughly applied within our environment.

For any questions or further concerns, please feel free to reach out.