■ Project Title: Linux Directory Navigation and File Exploration for Security Operations

This lab introduced foundational Linux command-line operations crucial for cybersecurity professionals. As a security analyst, being able to efficiently navigate file systems, locate logs, and read file contents is essential for investigating incidents and verifying system configurations. During this lab, I worked in a Linux environment using basic but powerful terminal commands such as pwd, ls, cd, and cat. These commands allowed me to navigate directories, examine log files, and extract key information from security-related files. The lab strengthened my confidence in command-line operations, improved my ability to trace data paths, and reinforced best practices for log review, directory structuring, and system analysis.

Task 1: Get the Current Directory Information

- Used pwd to identify the current working directory.
- Executed ls to list files and subdirectories present in /home/analyst.
- Practiced identifying directory structures — an important skill for locating evidence.

Task 2: Change Directory and List Subdirectories

- Navigated from /home/analyst to /home/analyst/reports using cd.
- Listed subdirectories and confirmed “projects” existed.
- Developed familiarity with Linux directory organization.

Task 3: Locate and Read File Contents

- Accessed /home/analyst/reports/users directory.
- Read Q1_added_users.txt using cat.
- Identified user aezra’s department (Sales) and mreed’s ID (1177, IT department).

Task 4: Navigate and Examine Log Files

- Navigated to /home/analyst/logs and located server_logs.txt.
- Used head to view the first 10 lines and found two warning messages.
- Demonstrated ability to review logs and detect potential issues.

Key Linux Commands Practiced

- pwd — Displays current working directory
- ls — Lists directory contents
- cd — Changes directories
- cat — Displays contents of a file
- head — Displays the first lines of a file

Key Takeaways

- Strengthened Linux navigation and file management skills essential for SOC roles. - Learned how to efficiently locate and interpret data within directories and logs. - Practiced retrieving information relevant to user and system management.
- Built a foundation for log investigation, privilege checks, and file integrity analysis.

Conclusion

This lab provided practical experience using Linux terminal commands to navigate directories, locate data, and review system logs—core capabilities for analysts investigating incidents or verifying system activity. By mastering these commands, I built operational fluency in Linux environments—an indispensable skill for cybersecurity operations, digital forensics, and incident response.