Capstone Project Report

Secure File Storage and Access Management on Linux

Report Date: 20th Dec 2025

Report Time: 12:49 PM

Reported By: Harsh Mohile

Machine: Kali-Linux, Oracle VirtualBox

Real-time scenario:

Globex Financial faced a security breach where an unauthorized user accessed confidential financial reports, exposing weak access controls and monitoring gaps. To enhance security, the company is implementing a secure access management system with strict permissions and real-time monitoring. The system will enforce user-specific access controls, allowing only file owners to modify or delete files, while others have read-only access. It will also track command history for auditing and log unauthorized access attempts for IT review. A secure web dashboard will enable real-time security monitoring, and all configurations will persist across reboots to ensure continuous protection and compliance.

1. Introduction

In modern IT environments, secure file storage and controlled access to sensitive data are critical to ensure confidentiality, integrity, and accountability. Linux provides robust mechanisms such as user and group permissions, Access Control Lists (ACLs), auditing, and logging to implement strong access control and monitoring.

2. Objective

The objectives of this project are:

• Create a secure file storage directory on Linux

• Implement role-based access using users and groups

• Enforce explicit permissions and ACLs

• Monitor command execution history

• Log and audit access events

• Provide console and web-based audit reporting

3. Tools and Technologies Used

• Kali Linux

• User & Group Management (useradd, groupadd, usermod)

• File Permissions (chmod, chown)

• ACL (setfacl, getfacl)

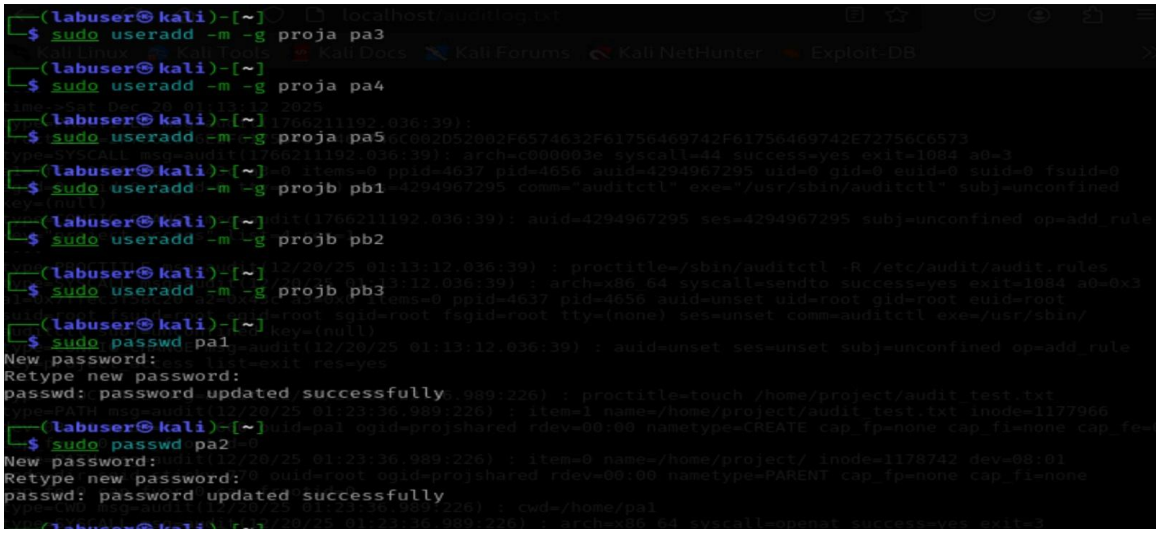
• auditd

• Apache2

• cron

4. User and Group Management

Multiple users and groups were created to simulate project-based access. Users were assigned to respective groups, and a shared group was used for controlled collaboration.



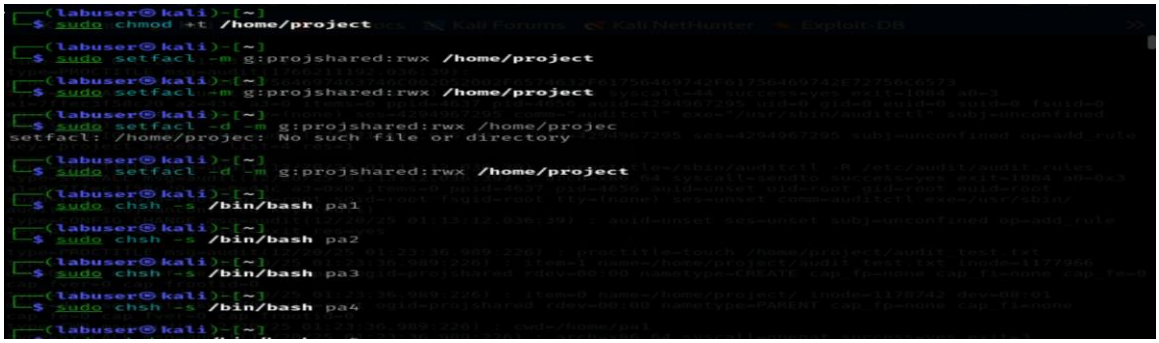
Instead of granting individual users direct ownership or exclusive access to the project directory, a **shared folder access model** was implemented. A dedicated shared group (projshared) was created, and authorized users from different project teams were added to this group. The project directory (/home/project) was assigned group ownership to this shared group, ensuring controlled collaboration while maintaining security.

This approach avoids user-specific dependency, simplifies access management, and follows **best practices of role-based access control (RBAC)**. Additionally, the use of **setgid** ensures that all newly created files inherit the shared group ownership, while the **sticky bit**

prevents unauthorized deletion of files by other users. This design enhances scalability, security, and accountability in multi-user environments.

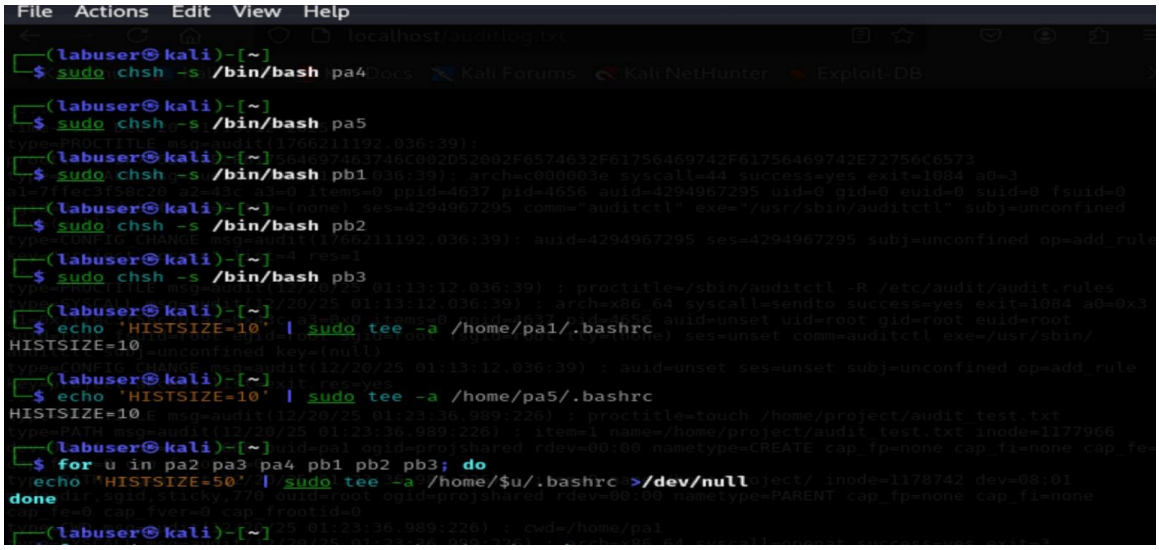
5. Secure Project Directory Configuration

A secure directory (/home/project) was created with restricted permissions, setgid and sticky bit enabled, and ACLs applied to ensure fine-grained access control.



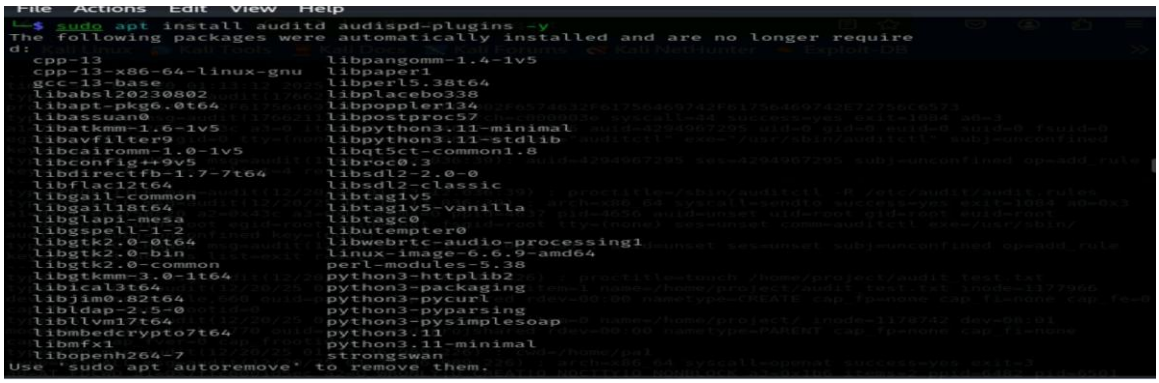
6. Command History Monitoring

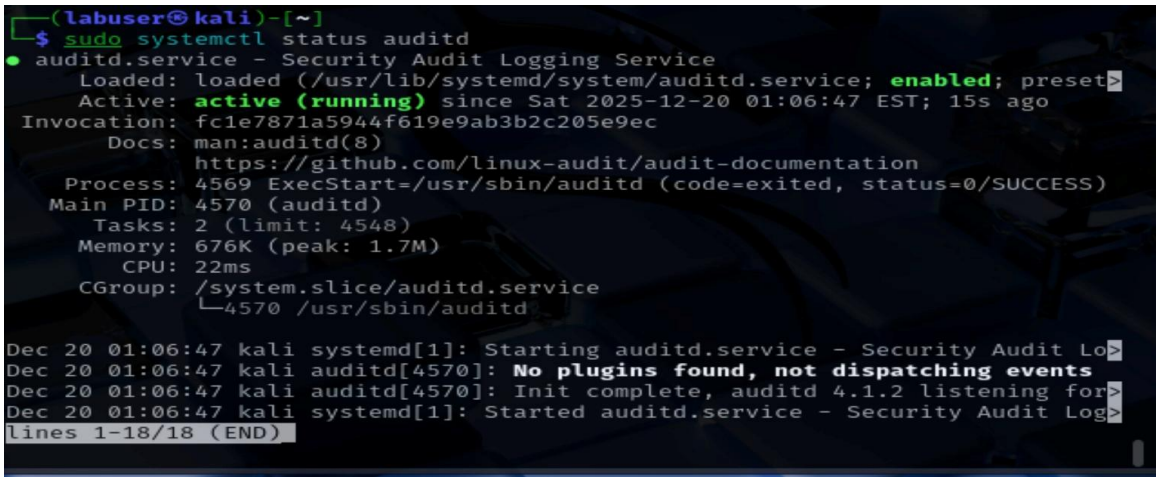
Command history limits were applied for selected users using HISTSIZE configuration to monitor recent activities.



7. Auditing and Logging

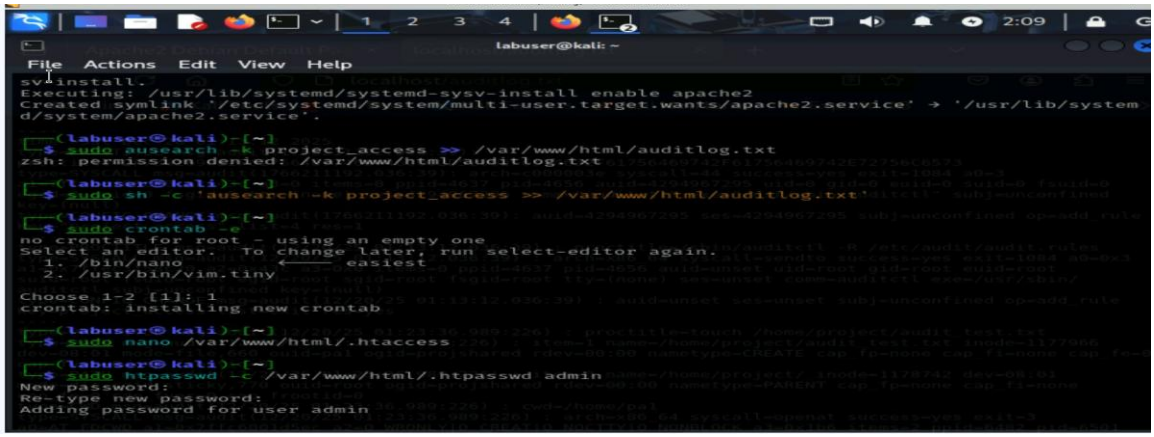
auditd was enabled and configured to monitor read, write, execute, and delete operations on the project directory.





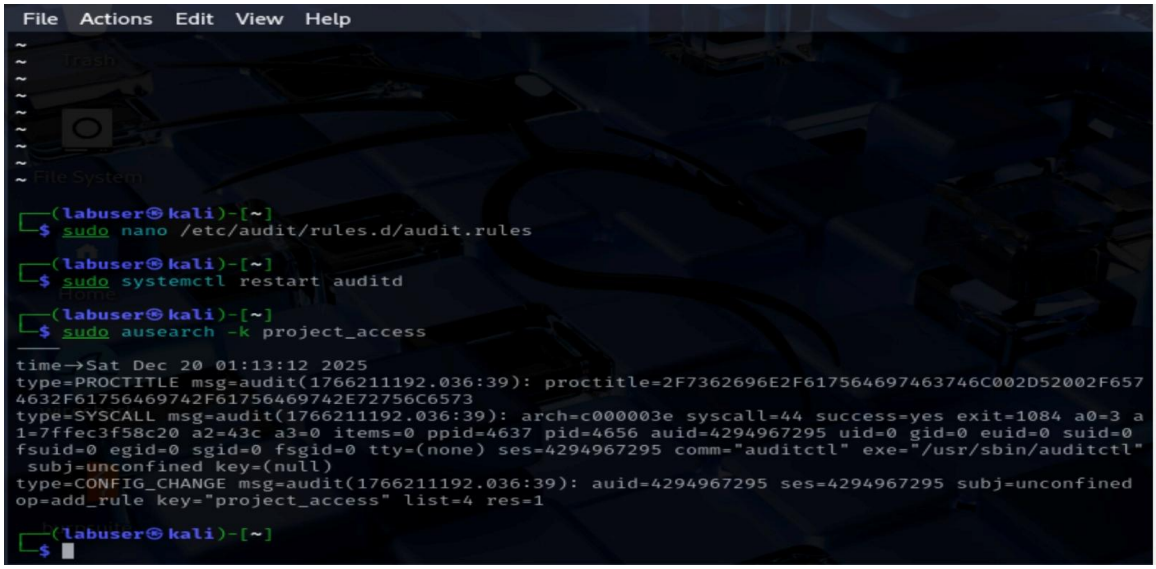
8. Access Monitoring

All file operations such as create, read, modify, and delete were successfully logged with user attribution.

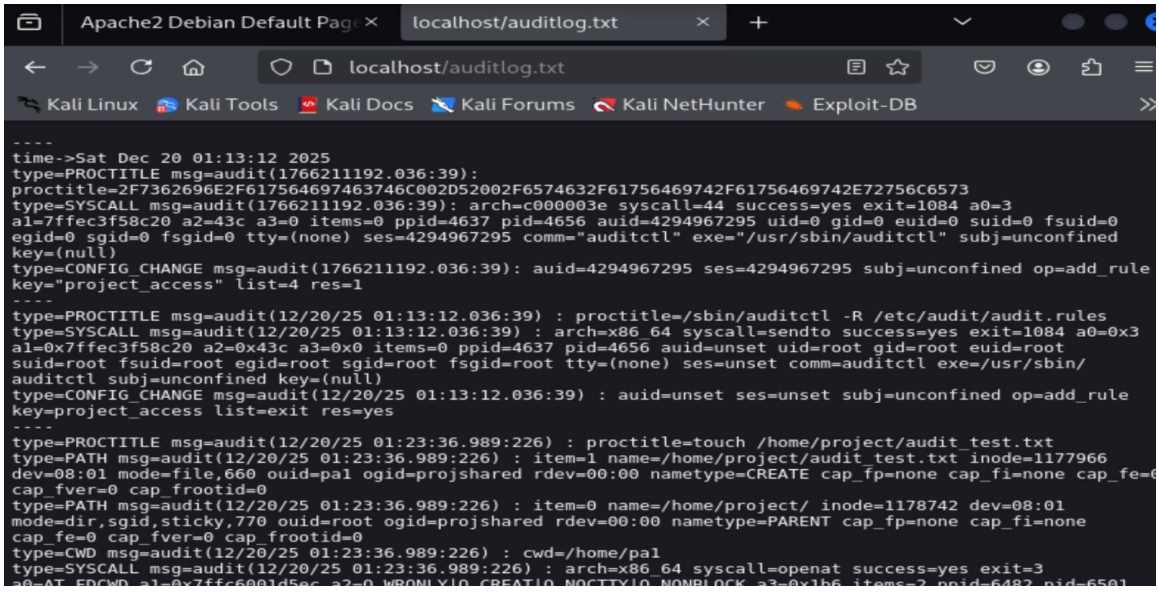


9. Console-Based Audit Reporting

Audit logs were extracted using ausearch and stored in a centralized log file.



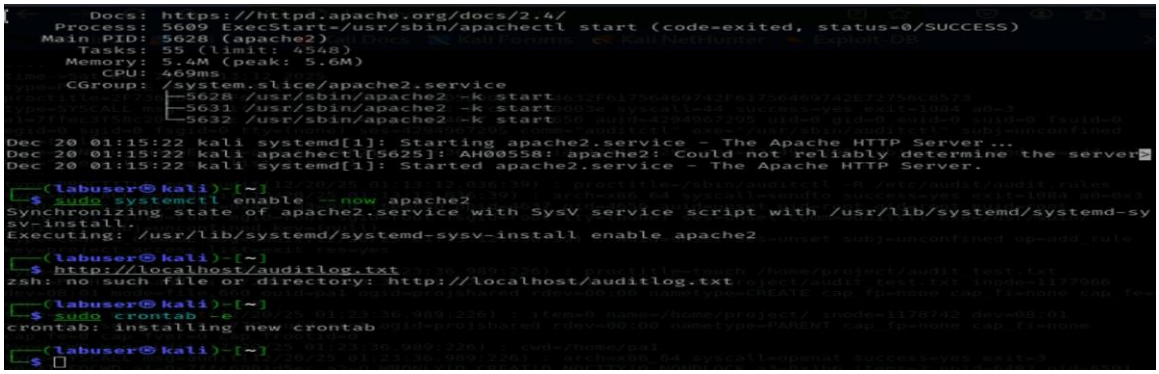
10. Web-Based Audit Reporting



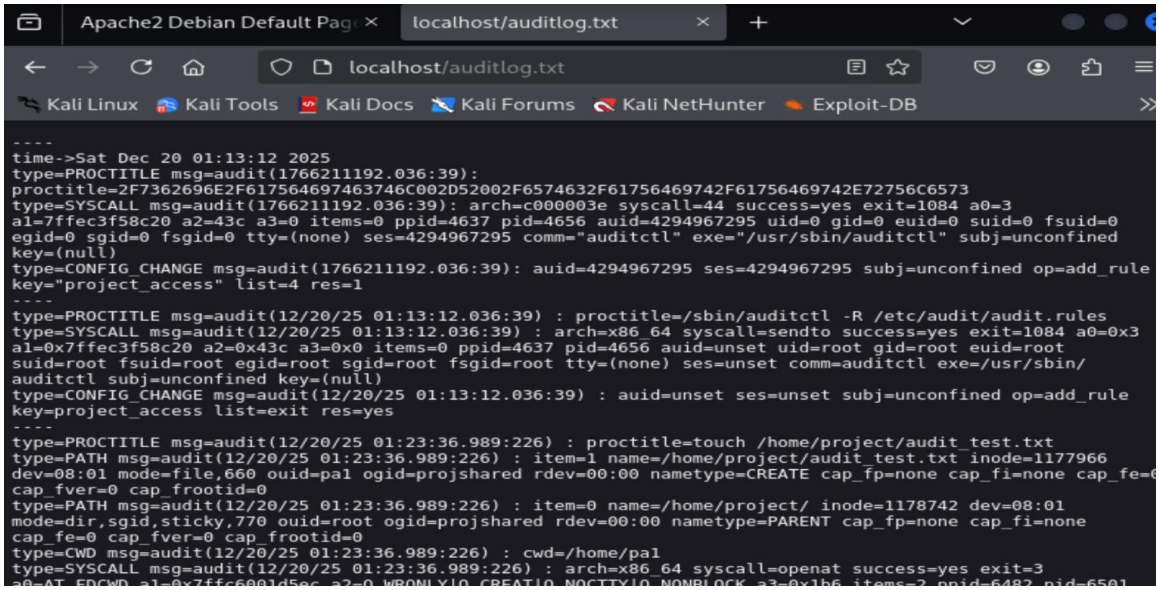
Apache2 was used to serve audit logs via browser access at http://localhost/auditlog.txt.

11. Automation

A cron job was configured to periodically update audit logs automatically.



Final Output



12. Conclusion

This project demonstrates a secure and auditable Linux file storage system suitable for enterprise environments.