

## Capstone Project Report

### Secure File Storage and Access Management on Linux

**Report Date:** 20<sup>th</sup> 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.

```
(labuser@kali)-[~]
$ sudo useradd -m -g proj_a pa3
$ sudo useradd -m -g proj_a pa4
$ sudo useradd -m -g proj_a pa5
$ sudo useradd -m -g proj_b pb1
$ sudo useradd -m -g proj_b pb2
$ sudo useradd -m -g proj_b pb3
$ sudo passwd pa1
$ sudo passwd pa2
```

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.

```
(labuser@kali)-[~]
$ sudo chmod +t /home/project
$ sudo setfacl -m g:projshared:rwX /home/project
$ sudo setfacl -m g:projshared:rwX /home/project
$ sudo setfacl -d -m g:projshared:rwX /home/project
setfacl: /home/project: No such file or directory
$ sudo setfacl -d -m g:projshared:rwX /home/project
$ sudo chsh -s /bin/bash pa1
$ sudo chsh -s /bin/bash pa2
$ sudo chsh -s /bin/bash pa3
$ sudo chsh -s /bin/bash pa4
(labuser@kali)-[~]
```

## 6. Command History Monitoring

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

```
File Actions Edit View Help
(labuser@kali)-[~]
$ sudo chsh -s /bin/bash pa4
$ sudo chsh -s /bin/bash pa5
(labuser@kali)-[~]
$ sudo chsh -s /bin/bash pb1
$ sudo chsh -s /bin/bash pb2
$ sudo chsh -s /bin/bash pb3
(labuser@kali)-[~]
$ echo 'HISTSIZE=10' | sudo tee -a /home/pa1/.bashrc
HISTSIZE=10
(labuser@kali)-[~]
$ echo 'HISTSIZE=10' | sudo tee -a /home/pa5/.bashrc
HISTSIZE=10
(labuser@kali)-[~]
$ for u in pa2 pa3 pa4 pb1 pb2 pb3; do
  echo 'HISTSIZE=50' | sudo tee -a /home/$u/.bashrc >/dev/null
done
(labuser@kali)-[~]
```

## 7. Auditing and Logging

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

```
File Actions Edit View Help
$ sudo apt install auditd auditd-plugins -y
The following packages were automatically installed and are no longer required:
d:
  cpp-13      libpangomm-1.4-1v5
  cpp-13-x86-64-linux-gnu  libpaper1
  gcc-13-base  libperl5.38t64
  libabsl20230802  libplacebo338
  libapt-pkg6.0t64  libpoppler134
  libassuan0      libpostproc57
  libatkmm-1.6-1v5  libpython3.11-minimal
  libavfilter9     libpython3.11-stdlib
  libcairo-mm-1.0-1v5  libqt5ct-common1.8
  libconfig+9v5     libqt5ct-qt5
  libdirectfb-1.7-7t64  libSDL2-2.0-0
  libflac12t64      libSDL2-classic
  libgail-common  libtag1v5
  libgail18t64      libtag1v5-vanilla
  libglapi-mesa     libtagC0
  libgspell-1-2     libutempter0
  libgtk2.0-0t64    libwebRTC-audio-processing1
  libgtk2.0-bin      linux-image-6.6.9-amd64
  libgtk2.0-common  perl-modules-5.38
  libgtkmm-3.0-1t64  python3-hitlib2
  libical3t64        python3-packaging
  libjam0.82t64      python3-pycurl
  libldap-2.5-0      python3-pyparsing
  libllvml17t64      python3-pysimplesoap
  libmbcrypted07t64  python3.11
  libmfx1             python3.11-minimal
  libopenh264-7      strongswan
Use 'sudo apt autoremove' to remove them.
```

```
(labuser@kali)-[~]
$ sudo systemctl status auditd
● auditd.service - Security Audit Logging Service
   Loaded: loaded (/usr/lib/systemd/system/auditd.service; enabled; preset=
   Active: active (running) since Sat 2025-12-20 01:06:47 EST; 15s ago
   Invocation: fc1e7871a5944f619e9ab3b2c205e9ec
     Docs: man:auditd(8)
           https://github.com/linux-audit/audit-documentation
   Process: 4569 ExecStart=/usr/sbin/auditd (code=exited, status=0/SUCCESS)
   Main PID: 4570 (auditd)
     Tasks: 2 (limit: 4548)
    Memory: 676K (peak: 1.7M)
       CPU: 22ms
   CGroup: /system.slice/auditd.service
           └─4570 /usr/sbin/auditd

Dec 20 01:06:47 kali systemd[1]: Starting auditd.service - Security Audit Log
Dec 20 01:06:47 kali auditd[4570]: No plugins found, not dispatching events
Dec 20 01:06:47 kali auditd[4570]: Init complete, auditd 4.1.2 listening for
Dec 20 01:06:47 kali systemd[1]: Started auditd.service - Security Audit Log
lines 1-18/18 (END)
```

## 8. Access Monitoring

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

```
File Actions Edit View Help
$ sudo systemctl status auditd
$ sudo ausearch -k project_access >> /var/www/html/auditlog.txt
$ sudo sh -c 'ausearch -k project_access >> /var/www/html/auditlog.txt'
$ sudo crontab -e
no crontab for root - using an empty one
Select an editor. To change later, run select-editor again.
1. /bin/nano
2. /usr/bin/vim.tiny
Choose 1-2 [1]: 1
crontab: installing new crontab
$ sudo nano /var/www/html/.htaccess
$ sudo htpasswd -c /var/www/html/.htpasswd admin
Adding password for user admin
```

## 9. Console-Based Audit Reporting

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





## 11. Automation

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

```
Docs: https://httpd.apache.org/docs/2.4/
Process: 5609 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
Main PID: 5628 (apache2)
Tasks: 55 (limit: 4548)
Memory: 5.4M (peak: 5.6M)
CPU: 469ms
CGroup: /system.slice/apache2.service
└─5628 /usr/sbin/apache2 -k start
   └─5631 /usr/sbin/apache2 -k start
      └─5632 /usr/sbin/apache2 -k start
Dec 20 01:15:22 kali systemd[1]: Starting apache2.service - The Apache HTTP Server...
Dec 20 01:15:22 kali apachectl[5625]: AH00558: apache2: Could not reliably determine the server's
Dec 20 01:15:22 kali systemd[1]: Started apache2.service - The Apache HTTP Server.

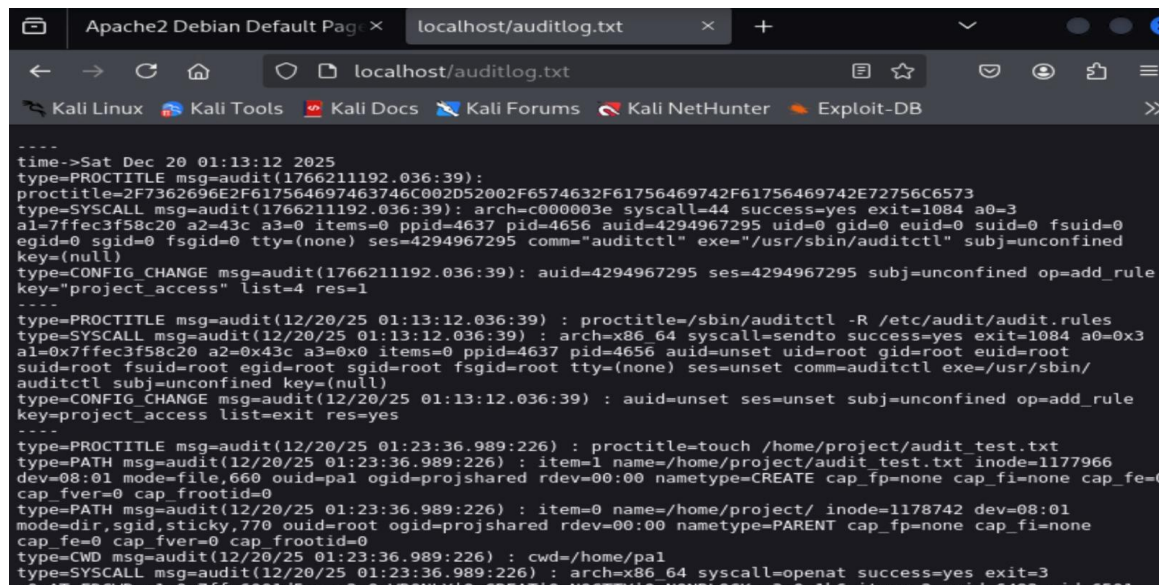
(labuser@kali)~$ sudo systemctl enable --now apache2
Synchronizing state of apache2.service with SysV service script with /usr/lib/systemd/systemd-sy
sv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable apache2

(labuser@kali)~$ http://localhost/auditlog.txt
zsh: no such file or directory: http://localhost/auditlog.txt

(labuser@kali)~$ sudo crontab -e
crontab: installing new crontab

(labuser@kali)~$
```

## Final Output



```
----
time->Sat Dec 20 01:13:12 2025
type=PROCTITLE msg=audit(1766211192.036:39):
proctitle=2F7362696E2F617564697463746C00D052002F6574632F61756469742F61756469742E72756C6573
type=SYSCALL msg=audit(1766211192.036:39): arch=c000003e syscall=44 success=yes exit=1084 a0=3
a1=7ffec3f58c20 a2=43c a3=0 items=0 ppid=4637 pid=4656 auid=4294967295 uid=0 gid=0 euid=0 fsuid=0
egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="auditctl" exe="/usr/sbin/auditctl" subj=unconfined
key=(null)
type=CONFIG_CHANGE msg=audit(1766211192.036:39): auid=4294967295 ses=4294967295 subj=unconfined op=add_rule
key="project_access" list=4 res=1
----
type=PROCTITLE msg=audit(12/20/25 01:13:12.036:39) : proctitle=/sbin/auditctl -R /etc/audit/audit.rules
type=SYSCALL msg=audit(12/20/25 01:13:12.036:39) : arch=x86_64 syscall=sendto success=yes exit=1084 a0=0x3
a1=0x7ffec3f58c20 a2=0x43c a3=0x0 items=0 ppid=4637 pid=4656 auid=unset uid=root gid=root euid=root
suid=root fsuid=root egid=root sgid=root fsgid=root tty=(none) ses=unset comm=auditctl exe=/usr/sbin/
auditctl subj=unconfined key=(null)
type=CONFIG_CHANGE msg=audit(12/20/25 01:13:12.036:39) : auid=unset ses=unset subj=unconfined op=add_rule
key=project_access list=exit res=yes
----
type=PROCTITLE msg=audit(12/20/25 01:23:36.989:226) : proctitle=touch /home/project/audit test.txt
type=PATH msg=audit(12/20/25 01:23:36.989:226) : item=1 name=/home/project/audit test.txt inode=1177966
dev=08:01 mode=file,660 ouid=pal ogid=projshared rdev=00:00 nametype=CREATE cap_fp=none cap-fi=none cap-fe=6
cap_fver=0 cap_frootid=0
type=PATH msg=audit(12/20/25 01:23:36.989:226) : item=0 name=/home/project/ inode=1178742 dev=08:01
mode=dir,sgid,sticky,770 ouid=root ogid=projshared rdev=00:00 nametype=PARENT cap_fp=none cap-fi=none
cap-fe=0 cap_fver=0 cap_frootid=0
type=CWD msg=audit(12/20/25 01:23:36.989:226) : cwd=/home/pal
type=SYSCALL msg=audit(12/20/25 01:23:36.989:226) : arch=x86_64 syscall=openat success=yes exit=3
a0=AT_FDCWD a1=0x7ffec6001d5ec a2=0 WRONLY O_CREAT O_NOCTTY O_NONBLOCK a3=0x1b6 items=2 ppid=6482 pid=6501
```

## 12. Conclusion

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