

Project Topic: Secure File Storage and Access Management for Project Teams

Commands and Scripts Documentation Used

Implementation Steps:

Step 1: User & Group Configuration with ACLs

Created user accounts for **Project-A** and **Project-B**, configuring **ACLs** to restrict file access to owners only.

- **Created project groups:**

```
sudo groupadd projectA  
sudo groupadd projectB
```

- **Created users and assigned groups:**

Used the following command to create user accounts for **projectA** and assigned them to groups.

```
sudo adduser -m -g projA pA1  
sudo adduser -m -g projA pA2  
sudo adduser -m -g projA pA3  
sudo adduser -m -g projA pA4  
sudo adduser -m -g projA pA5
```

Used the following command to create user accounts for projectB and assigned them to groups.

```
sudo adduser -m -g projA pB1  
sudo adduser -m -g projA pB2  
sudo adduser -m -g projA pB3
```

- **Set passwords for users:**

Used the following command to set password for users in the ProjectA

```
sudo passwd PA1  
sudo passwd PA2  
sudo passwd PA3  
sudo passwd PA4  
sudo passwd PA5
```

Used the following command to set password for users in the ProjectB

```
sudo passwd PA1  
sudo passwd PA2  
sudo passwd PA3
```

- **Created and secured project directories:**

Used the following command to create and secure the project directory

```
sudo mkdir /home/project
```

Assigned group ownership to to the groups in the directory and set directory permissions using the following commands;

```
sudo chown :projectA /home/project
```

```
sudo chown :projectB /home/project
```

```
sudo chmod 770 /home/project
```

- **Applied ACLs:**

Configured ACLs and restricted modifications using the following commands;

```
sudo setfacl -m u:PA1:rwX /home/project
```

```
sudo setfacl -m u:PA2:rwX /home/project
```

```
sudo setfacl -m u:PA3:rwX /home/project
```

```
sudo setfacl -m u:PA4:rwX /home/project
```

```
sudo setfacl -m u:PA5:rwX /home/project
```

```
sudo setfacl -m u:PB1:rwX /home/project
```

```
sudo setfacl -m u:PB2:rwX /home/project
```

```
sudo setfacl -m u:PB3:rwX /home/project
```

Used the following command to restrict others from deleting or modifying the files;

```
sudo setfacl -m g::r-x /home/project
```

Used the command below to apply default ACLs:

```
sudo setfacl -d -m u::rwX /home/project
```

```
sudo setfacl -d -m o::--- /home/project
```

Used the command below to stick the sticky bit;

```
sudo chmod +t /home/project
```

Step 2: Apply directory and file permissions

Used the following commands to change the default shell of the users;

```
sudo chsh -s /bin/bash PA1
```

```
sudo chsh -s /bin/bash PA2
```

```
sudo chsh -s /bin/bash PA3
```

```
sudo chsh -s /bin/bash PA4
```

```
sudo chsh -s /bin/bash PA5
```

```
sudo chsh -s /bin/bash PB1
```

```
sudo chsh -s /bin/bash PB2
sudo chsh -s /bin/bash PB3
```

- **Command History Retention**

Set the history limit for senior analysts (PA1 and PA5) using the command below;

```
echo "HISTSIZE=10" | sudo tee -a /home/PA1/.bashrc
echo "HISTSIZE=10" | sudo tee -a/home/PA5/.bashrc
```

Used the command below to set the limit history for other users;

```
echo "HISTSIZE=50" | sudo tee -a /home/PA2/.bashrc
echo "HISTSIZE=50" | sudo tee -a/home/PA3/.bashrc
echo "HISTSIZE=50" | sudo tee -a/home/PA4/.bashrc
echo "HISTSIZE=50" | sudo tee -a/home/PB1/.bashrc
echo "HISTSIZE=50" | sudo tee -a/home/PB2/.bashrc
echo "HISTSIZE=50" | sudo tee -a/home/PB3/.bashrc
```

Step 3: Syslog Unauthorized Access Logging: Enable access logging. (Auditd Monitoring)

Used Syslog/Syslog to log unauthorized access attempts, ensuring secure storage for IT review.

Used the command below to install and configure linux audit daemon:

- **Installed auditd:**

```
sudo apt-get install auditd -y
sudo apt install rsyslog
sudo nano /etc/rsyslog.d/security.conf
```

Used the following command to create audit rules and log access towards the project directory: **sudo auditctl -w /home/project -p rwx -k project_access**

Used the command below to start and enable **auditd** service and verify status:

```
sudo systemctl start auditd
sudo systemctl enable auditd
sudo systemctl status auditd
```

- **Created audit rule:**

Used the command below to create and verify the audit rules:

```
sudo nano /etc/audit/rules.d/audit.rules and typed the following command;
-w /home/project -p rwx -k project_access and pressed ctrl+s to save and ctrl+x to exit.
```

Used this command to restart the **auditd** service;

```
sudo systemctl restart auditd
```

- **Viewed logs:**

Tested the configuration using the command below;

sudo ausearch -k project_access

Step 4: Web Dashboard Setup: Developed a web-based reporting interface

Developed a web dashboard for IT teams to monitor and analyze security violations.

- **Installed Apache2:** Used the following command to install Apache2:

sudo apt-get install apache2

Transferred logs using the following commands: **ausearch -k project_access >> /var/www/html/auditlog.txt** and **crontab** for automation: **crontab -e**

Typed the following command within the crontab file, saved and exited:

***/5 * * * * ausearch -k project_access >> /var/www/html/auditlog.txt**

Used the following command to edit apache2 configuration; **sudo nano /etc/apache2/sites-available/000-default.conf**

Typed the following command in the GNU nano 7.2 to add or modify, then pressed Ctrl S to save and Ctrl X to exit.

<VirtualHost>

<Directory /var/www/html>

AllowOverride All

</Directory>

Used the following command to secure access: **sudo nano /var/www/html/.htaccess**

Typed this in the nano text editor GNU 7.2;

AuthType Basic

AuthName "Restricted Access"

AuthUserFile /var/www/html/.htpasswd

Require valid-user

Used the following command to add password as admin; **sudo htpasswd**

-c/var/www/html/.htpasswd admin

Used the following command to start and enable apache2

systemctl start apache2

systemctl enable apache2

Step 5: Verify and Validate configurations:

Ensured security settings persist after reboots to maintain continuous protection and compliance

Logged in as PA1 and created a text file;

su - PA1

touch /home/project/testfile.txt

Logged in as PA2 and removed the file created by user PA1, got an error and then logged out; **su - PA2 and rm -f /home/project/testfile.txt**

Logged in as senior analyst (PA1) and viewed the command history;

su - PA1

History

Used the following command to test audit logging of unauthorised access attempts; **sudo ausearch -k project_access**

Used the following link on the web browser to generate a web-based report;

<http://localhost/auditlog.txt>

Conclusion:

This project successfully implemented access control, command tracking, unauthorized access logging and a monitoring Dashboard.

These measures enhance security, accountability, visibility and audit readiness for sensitive financial data.

Prepared by: Janefrances Nwachukwu

Date: 08/14/2025