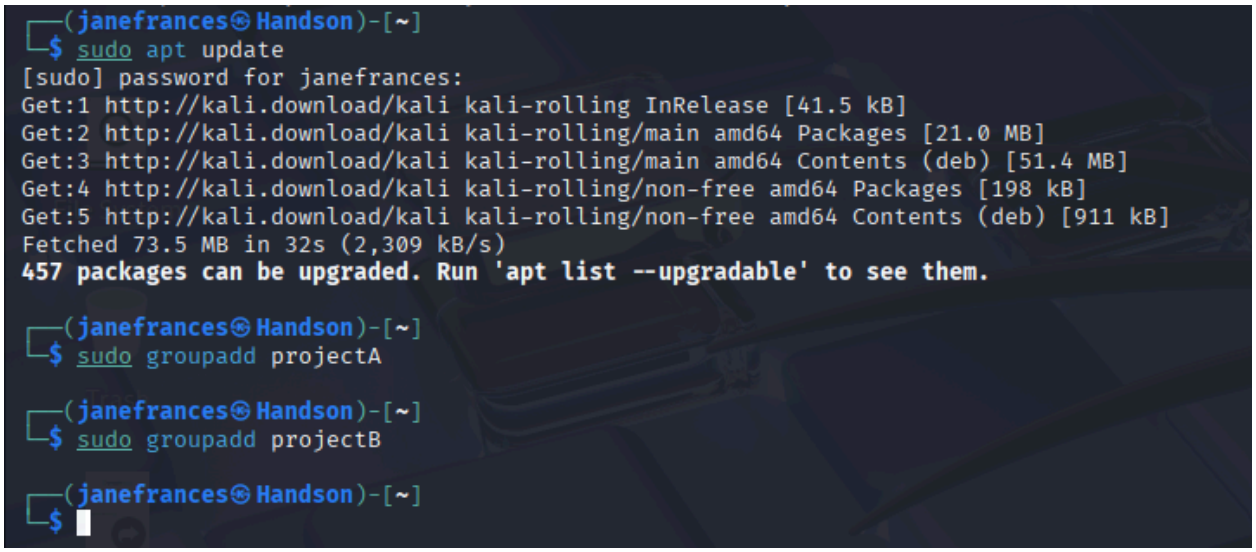
Project Topic: Secure File Storage and Access Management for Project Teams

Output Screenshots

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.

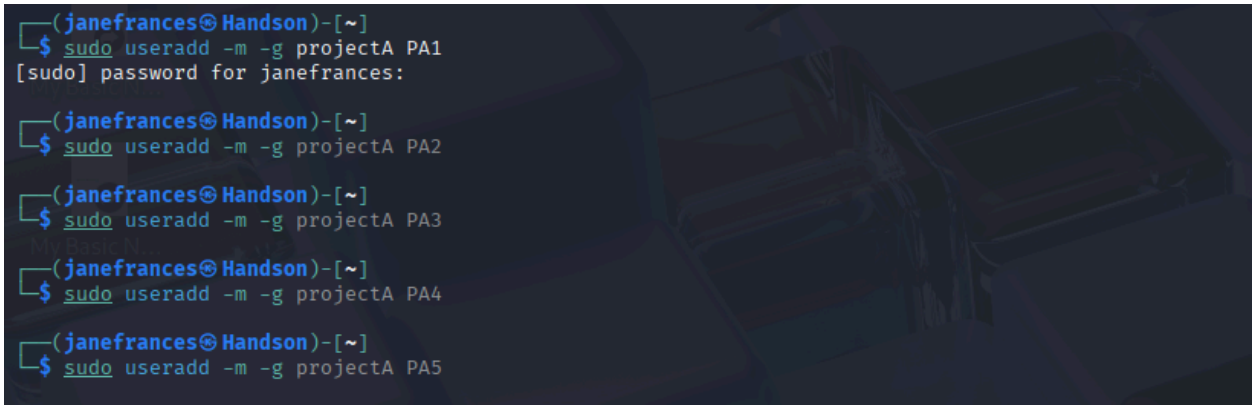
sudo groupadd projectA

sudo groupadd projectB

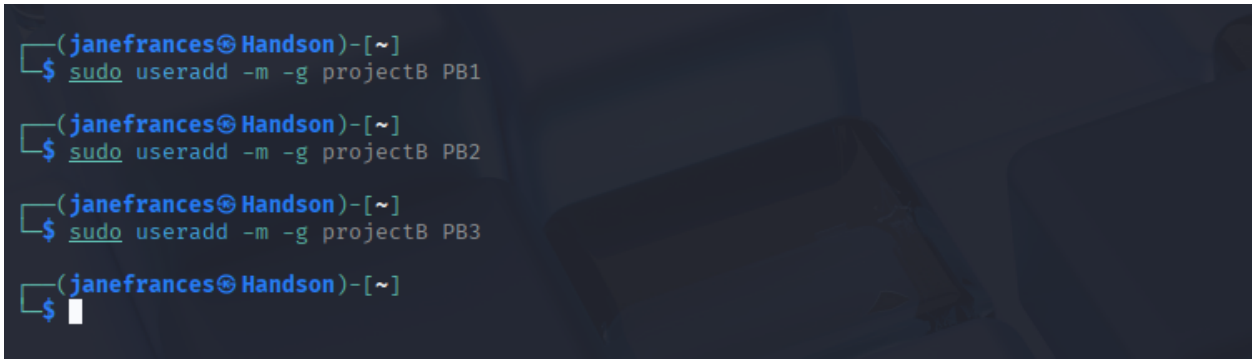


Used the following command to create user accounts for projectA and assigned them to groups.

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



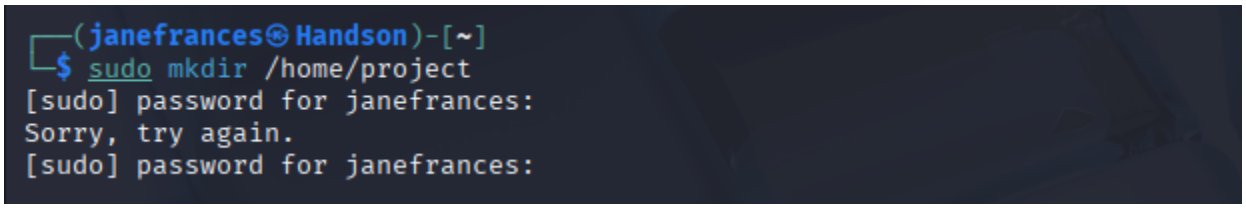
Used the following command to set password for users in the ProjectA

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

Used the following command to create and secure the project directory
sudo mkdir /home/project

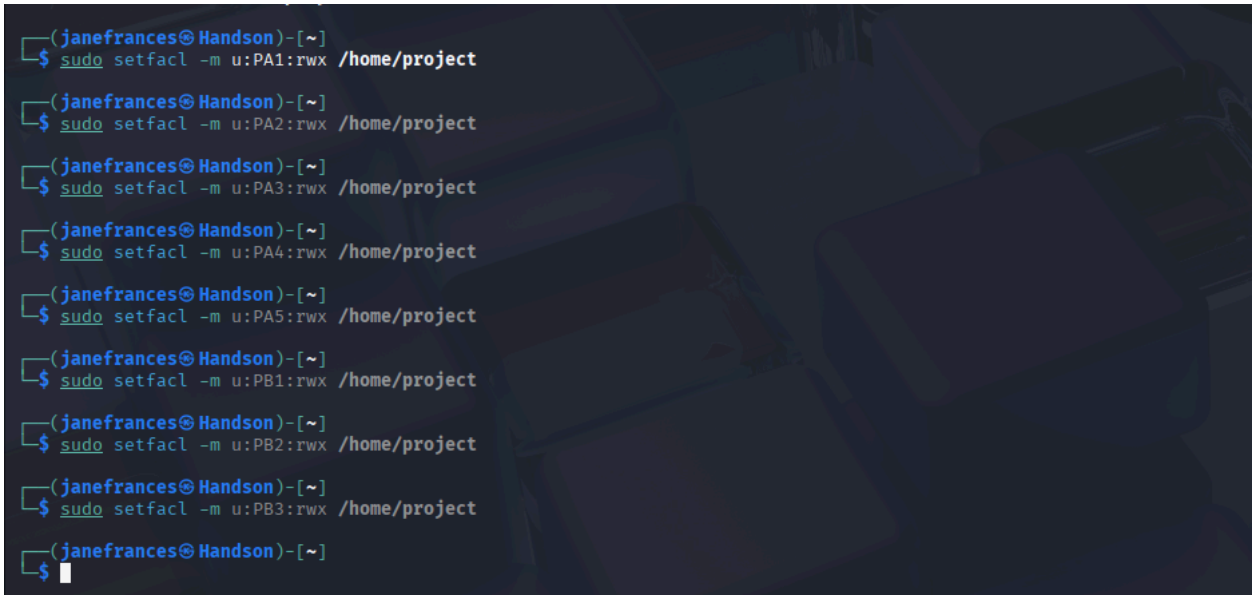


Assigned group ownership to to the groups in the directory and set directory permissions using the following commands;

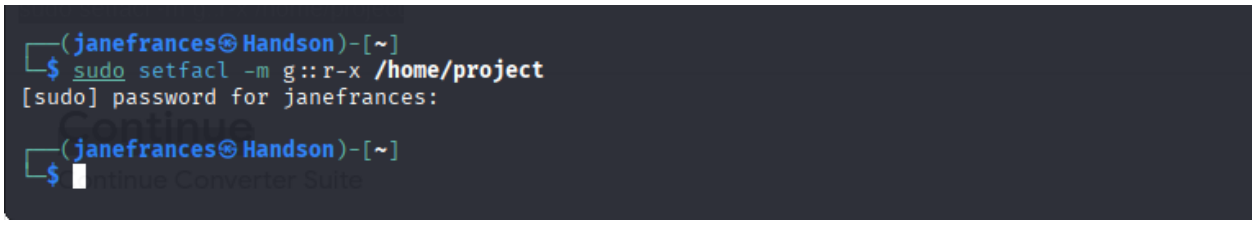
sudo chown :projectA /home/project
sudo chown :projectB /home/project
sudo chmod 770 /home/project

Configured ACLs and restricted modifications using the following commands;

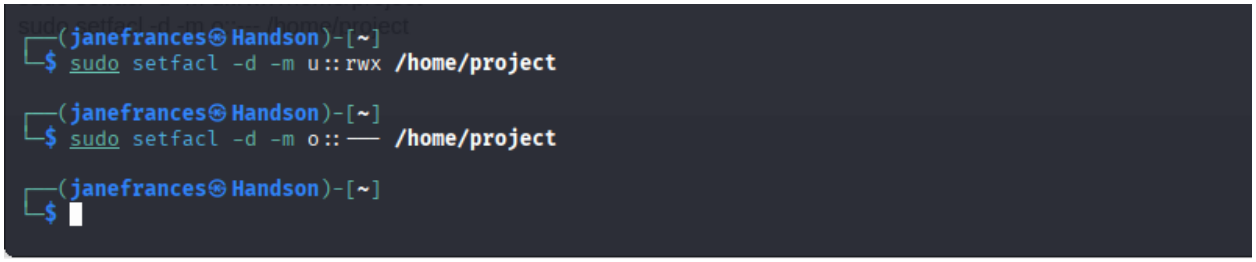
sudo setfacl -m u:PA1:rwx /home/project
sudo setfacl -m u:PA2:rwx /home/project
sudo setfacl -m u:PA3:rwx /home/project
sudo setfacl -m u:PA4:rwx /home/project
sudo setfacl -m u:PA5:rwx /home/project
sudo setfacl -m u:PB1:rwx /home/project
sudo setfacl -m u:PB2:rwx /home/project
sudo setfacl -m u:PB3:rwx /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

```
┌──(janefrances㉿Handson)-[~]
└─$ sudo chmod +t /home/project

┌──(janefrances㉿Handson)-[~]
└─$
```

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

```
┌──(janefrances㉿Handson)-[~]
└─$ sudo chsh -s /bin/bash PA1
┌──(janefrances㉿Handson)-[~]
└─$ sudo chsh -s /bin/bash PA2

┌──(janefrances㉿Handson)-[~]
└─$ sudo chsh -s /bin/bash PA3

┌──(janefrances㉿Handson)-[~]
└─$ sudo chsh -s /bin/bash PA4
┌──(janefrances㉿Handson)-[~]
└─$ sudo chsh -s /bin/bash PA5

┌──(janefrances㉿Handson)-[~]
└─$ sudo chsh -s /bin/bash PB1

┌──(janefrances㉿Handson)-[~]
└─$ sudo chsh -s /bin/bash PB2
┌──(janefrances㉿Handson)-[~]
└─$ sudo chsh -s /bin/bash PB3

┌──(janefrances㉿Handson)-[~]
└─$
```

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

```
┌──(janefrances㉿Handson)-[~]
└─$ echo “HISTSIZE=10” | sudo tee -a /home/PA1/.bashrc
[sudo] password for janefrances:
“HISTSIZE=10”

┌──(janefrances㉿Handson)-[~]
└─$ echo “HISTSIZE=10” | sudo tee -a /home/PA5/.bashrc
“HISTSIZE=10”

┌──(janefrances㉿Handson)-[~]
└─$ echo “HISTSIZE=50” | sudo tee -a /home/PA2/.bashrc
“HISTSIZE=50”

┌──(janefrances㉿Handson)-[~]
└─$ echo “HISTSIZE=50” | sudo tee -a /home/PA3/.bashrc
“HISTSIZE=50”

┌──(janefrances㉿Handson)-[~]
└─$ echo “HISTSIZE=50” | sudo tee -a /home/PA4/.bashrc
“HISTSIZE=50”

┌──(janefrances㉿Handson)-[~]
└─$ echo “HISTSIZE=50” | sudo tee -a /home/PB1/.bashrc
“HISTSIZE=50”

┌──(janefrances㉿Handson)-[~]
└─$ echo “HISTSIZE=50” | sudo tee -a /home/PB2/.bashrc
“HISTSIZE=50”

┌──(janefrances㉿Handson)-[~]
└─$ echo “HISTSIZE=50” | sudo tee -a /home/PB3/.bashrc
“HISTSIZE=50”

┌──(janefrances㉿Handson)-[~]
└─$
```

Step 3: Enable access logging. 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:
sudo apt-get install auditd -y

```
┌──(janefrances㉿Handson)-[~]
└─$ sudo apt update
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [21.0 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [51.4 MB]
Fetched 72.4 MB in 36s (2,004 kB/s)
457 packages can be upgraded. Run 'apt list --upgradable' to see them.

┌──(janefrances㉿Handson)-[~]
└─$ sudo apt-get install auditd -y
[sudo] password for janefrances:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following additional packages will be installed:
  libauparse0t64
Suggested packages:
  audispd-plugins
The following NEW packages will be installed:
  auditd libauparse0t64
0 upgraded, 2 newly installed, 0 to remove and 457 not upgraded.
Need to get 286 kB of archives.
After this operation, 954 kB of additional disk space will be used.
Get:1 http://http.kali.org/kali kali-rolling/main amd64 libauparse0t64 amd64 1:4.0.2-2+b2 [68.6 kB]
Get:2 http://http.kali.org/kali kali-rolling/main amd64 auditd amd64 1:4.0.2-2+b2 [217 kB]
Fetched 286 kB in 16s (17.3 kB/s)
Selecting previously unselected package libauparse0t64:amd64.
(Reading database ... 434780 files and directories currently installed.)
Preparing to unpack .../libauparse0t64_1%3a4.0.2-2+b2_amd64.deb ...
Adding 'diversion of /lib/x86_64-linux-gnu/libauparse.so.0 to /lib/x86_64-linux-gnu/libauparse.so.0.usr-is-merged by libauparse0t64'
Adding 'diversion of /lib/x86_64-linux-gnu/libauparse.so.0.0.0 to /lib/x86_64-linux-gnu/libauparse.so.0.0.0.usr-is-merged by libauparse0t64'
Unpacking libauparse0t64:amd64 (1:4.0.2-2+b2) ...
Selecting previously unselected package auditd.
Preparing to unpack .../auditd_1%3a4.0.2-2+b2_amd64.deb ...
Unpacking auditd (1:4.0.2-2+b2) ...
Setting up libauparse0t64:amd64 (1:4.0.2-2+b2) ...
Setting up auditd (1:4.0.2-2+b2) ...
update-rc.d: We have no instructions for the auditd init script.
update-rc.d: It looks like a non-network service, we enable it.
audit-rules.service is a disabled or a static unit, not starting it.
auditd.service is a disabled or a static unit, not starting it.
Processing triggers for man-db (2.13.1-1) ...
Processing triggers for kali-menu (2025.2.7) ...
Processing triggers for libc-bin (2.41-6) ...

┌──(janefrances㉿Handson)-[~]
└─$
```

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

```
┌──(janefrances㉿Handson)-[~]
└─$ sudo auditctl -w /home/project -p rwxa -k project_access
Old style watch rules are slower
```

Used the command below to start and enable **auditd** service and very status:
sudo systemctl start auditd
sudo systemctl enable auditd
sudo systemctl status auditd

```
┌──(janefrances㉿Handson)-[~]
└─$ sudo systemctl start auditd

┌──(janefrances㉿Handson)-[~]
└─$ sudo systemctl enable auditd
Synchronizing state of auditd.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable auditd
Created symlink '/etc/systemd/system/multi-user.target.wants/auditd.service' → '/usr/lib/systemd/system/auditd.service'.

┌──(janefrances㉿Handson)-[~]
└─$
```

```
┌──(janefrances㉿Handson)-[~]
└─$ sudo systemctl start auditd

┌──(janefrances㉿Handson)-[~]
└─$ sudo systemctl enable auditd
Synchronizing state of auditd.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable auditd
Created symlink '/etc/systemd/system/multi-user.target.wants/auditd.service' → '/usr/lib/systemd/system/auditd.service'.

┌──(janefrances㉿Handson)-[~]
└─$ sudo systemctl status auditd
● auditd.service - Security Audit Logging Service
     Loaded: loaded (/usr/lib/systemd/system/auditd.service; enabled; preset: disabled)
     Active: active (running) since Wed 2025-08-13 00:19:26 EDT; 4min 50s ago
 Invocation: a228f5f741604f719935e10540283973
       Docs: man:auditd(8)
             https://github.com/linux-audit/audit-documentation
   Main PID: 224346 (auditd)
      Tasks: 2 (limit: 4546)
     Memory: 672K (peak: 1.8M)
        CPU: 36ms
     CGroup: /system.slice/auditd.service
             └─224346 /usr/sbin/auditd

Aug 13 00:19:26 Handson systemd[1]: Starting auditd.service - Security Audit Logging Service...
Aug 13 00:19:26 Handson auditd[224346]: No plugins found, not dispatching events
Aug 13 00:19:26 Handson auditd[224346]: Init complete, auditd 4.0.2 listening for events (startup state enable)
Aug 13 00:19:26 Handson systemd[1]: Started auditd.service - Security Audit Logging Service.

┌──(janefrances㉿Handson)-[~]
└─$
```

Used the command below to create and verify the audit rules: **sudo nano /etc/audit/rules.d/audit.rules** and typed the following command and pressed **ctrl+s to save** and **ctrl+x to exit; -w /home/project -p rwxa -k project_access**

Used this command to restart the auditd service;

sudo systemctl restart auditd

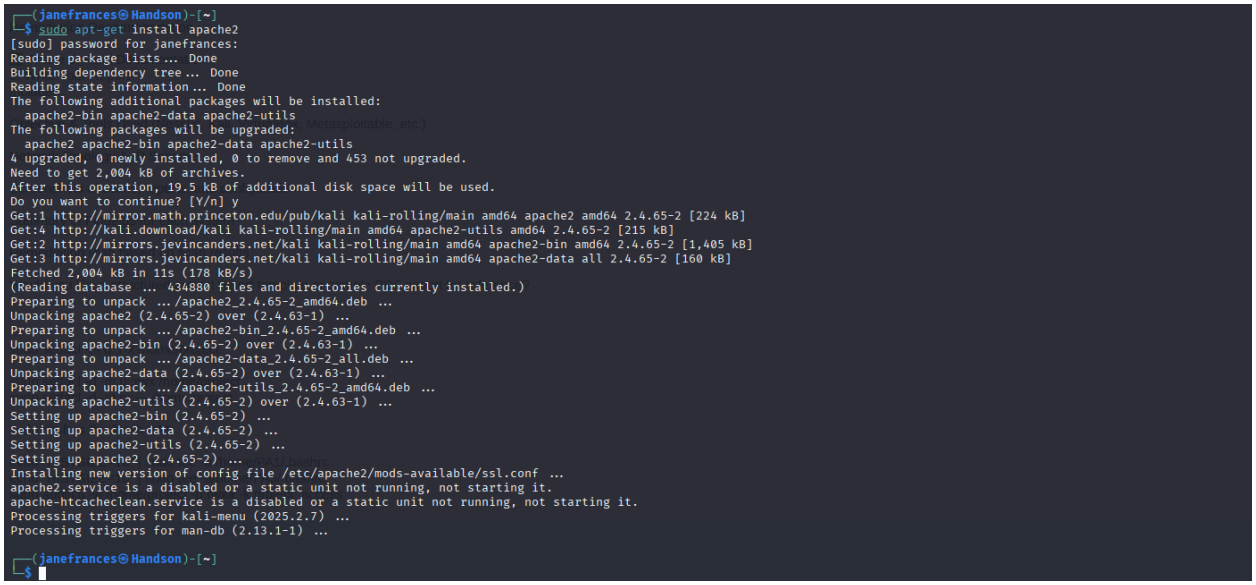
Tested the configuration using the command below;

sudo ausearch -k project_access

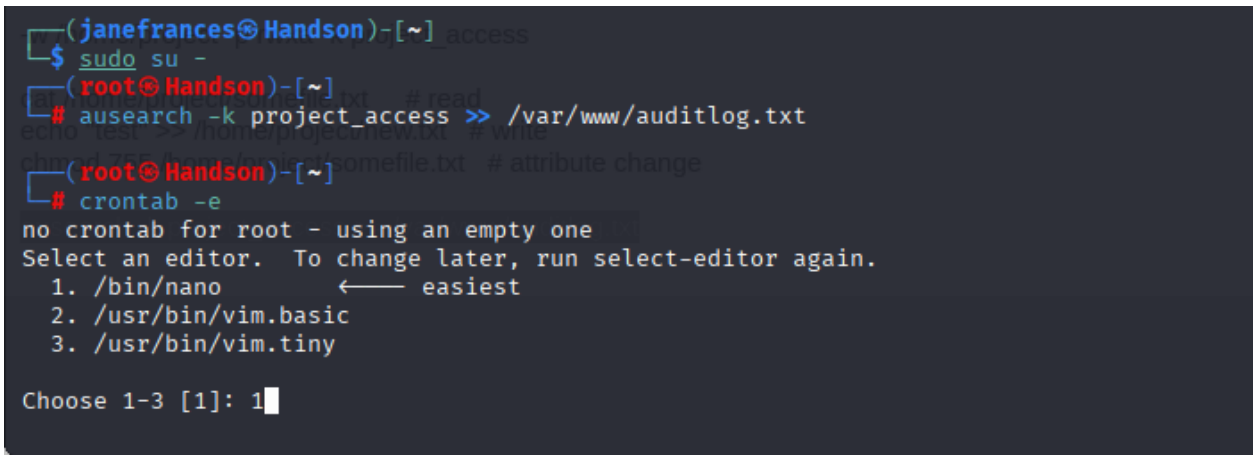
(janefrances㉿Handson)-[~]
$ sudo ausearch -k project_access
time->Wed Aug 13 13:59:06 2025
type=PROCTITLE msg=audit(1755107946.545:528): proctitle=617564697463746C002D77002F686F6D652F70726F6A656374002D700072777861002D
type=SOCKADDR msg=audit(1755107946.545:528): saddr=100000000000000000000000
type=SYSCALL msg=audit(1755107946.545:528): arch=c000003e syscall=44 success=yes exit=1084 a0=4 a1=7ffe63fb7a90 a2=43c a3=0 it
comm="auditctl" exe="/usr/sbin/auditctl" subj=unconfined key=(null)
type=CONFIG_CHANGE msg=audit(1755107946.545:528): auid=1000 ses=2 subj=unconfined op=add_rule key="project_access" list=4 res=
time->Wed Aug 13 14:01:49 2025
type=PROCTITLE msg=audit(1755108109.639:535): proctitle=2F7362696E2F617564697463746C002D52002F6574632F61756469742F61756469742E
type=SOCKADDR msg=audit(1755108109.639:535): saddr=100000000000000000000000
type=SYSCALL msg=audit(1755108109.639:535): arch=c000003e syscall=44 success=yes exit=1084 a0=3 a1=7ffed9234a10 a2=43c a3=0 it
) ses=4294967295 comm="auditctl" exe="/usr/sbin/auditctl" subj=unconfined key=(null)
type=CONFIG_CHANGE msg=audit(1755108109.639:535): auid=4294967295 ses=4294967295 subj=unconfined op=remove_rule key="project_a
time->Wed Aug 13 14:01:49 2025
type=PROCTITLE msg=audit(1755108109.643:539): proctitle=2F7362696E2F617564697463746C002D52002F6574632F61756469742F61756469742E
type=SYSCALL msg=audit(1755108109.643:539): arch=c000003e syscall=44 success=yes exit=1084 a0=3 a1=7ffed9236ea0 a2=43c a3=0 it
) ses=4294967295 comm="auditctl" exe="/usr/sbin/auditctl" subj=unconfined key=(null)
type=CONFIG_CHANGE msg=audit(1755108109.643:539): auid=4294967295 ses=4294967295 subj=unconfined op=add_rule key="project_acce
(janefrances㉿Handson)-[~]
$

Step 4: Develop a web-based reporting interface. Developed a web dashboard for IT teams to monitor and analyze security violations.

4.1 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**

```
┌──(janefrances㉿Handson)-[~]
└─$ sudo su -
┌──(root㉿Handson)-[~]
└─# ausearch -k project_access >> /var/www/auditlog.txt

┌──(root㉿Handson)-[~]
└─# crontab -e
no crontab for root - using an empty one
Select an editor.  To change later, run select-editor again.
  1. /bin/nano        <---- easiest
  2. /usr/bin/vim.basic
  3. /usr/bin/vim.tiny

Choose 1-3 [1]: 1
crontab: installing new crontab

┌──(root㉿Handson)-[~]
└─#
```

Used the following command to edit apache2 configuration; **sudo nano /etc/apache2/sites-availbale/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>

```
┌──(root㉿Handson)-[~]
└─# sudo nano /etc/apache2/sites-available/000-default.conf

┌──(root㉿Handson)-[~]
└─#
```

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**

```
┌──(root㉿Handson)-[~]
└─# sudo htpasswd -c /var/www/html/.htpasswd admin
New password:
Re-type new password:
Adding password for user admin

┌──(root㉿Handson)-[~]
└─#
```

Used the following command to start and enable apache2

systemctl start apache2

systemctl enable apache2

```
┌──(root㉿Handson)-[~]
└─# systemctl start apache2

┌──(root㉿Handson)-[~]
└─# systemctl enable apache2
Synchronizing state of apache2.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable apache2
Created symlink '/etc/systemd/system/multi-user.target.wants/apache2.service' → '/usr/lib/systemd/system/apache2.service'.

┌──(root㉿Handson)-[~]
└─#
```

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

```
┌──(root㉿Handson)-[~]
└─# su - PA1
“HISTSIZE=10”: command not found
┌──(PA1㉿Handson)-[~]
└─$ touch /home/project/testfile.txt

┌──(PA1㉿Handson)-[~]
└─$
```

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**

```
┌──(PA2㉿Handson)-[~]
└─$ rm -f /home/project/testfile.txt
rm: cannot remove '/home/project/testfile.txt': Operation not permitted

┌──(PA2㉿Handson)-[~]
└─$
```

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

su - PA1

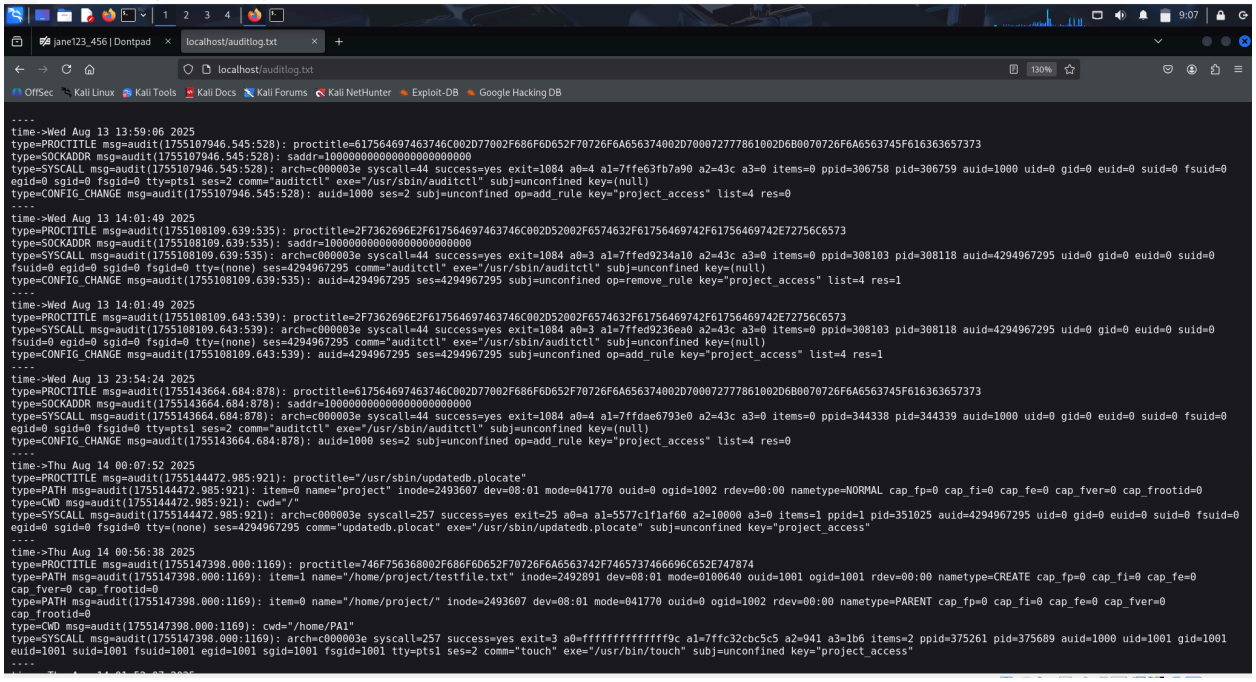
History

```
┌──(root㉿Handson)-[~]
└─# su - PA1
“HISTSIZE=10”: command not found
┌──(PA1㉿Handson)-[~]
└─$ history
    1  exit
    2  touch /home/project/testfile.txt
    3  exit
    4  history

┌──(PA1㉿Handson)-[~]
└─$
```

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

```
┌──(janefrances㉿Handson)-[~]
└─$ sudo ausearch -k project_access

[sudo] password for janefrances:
/var/log/audit/audit.log is not owned by root
NOTE - using built-in end_of_event_timeout: 2
NOTE - using built-in logs: /var/log/audit/audit.log
----
time->Wed Aug 13 13:59:06 2025
type=PROCTITLE msg=audit(1755107946.545:528): proctitle=617564697463746C002D77002F686F6D652F70726F6A656374002D70007
2777861002D6B0070726F6A6563745F616363657373
type=SOCKADDR msg=audit(1755107946.545:528): saddr=100000000000000000000000
type=SYSCALL msg=audit(1755107946.545:528): arch=c000003e syscall=44 success=yes exit=1084 a0=4 a1=7ffe63fb7a90 a2=
43c a3=0 items=0 ppid=306758 pid=306759 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts1
ses=2 comm="auditctl" exe="/usr/sbin/auditctl" subj=unconfined key=(null)
type=CONFIG_CHANGE msg=audit(1755107946.545:528): auid=1000 ses=2 subj=unconfined op=add_rule key="project_access"
list=4 res=0
----
time->Wed Aug 13 14:01:49 2025
type=PROCTITLE msg=audit(1755108109.639:535): proctitle=2F7362696E2F617564697463746C002D52002F6574632F61756469742F6
1756469742E72756C6573
type=SOCKADDR msg=audit(1755108109.639:535): saddr=100000000000000000000000
type=SYSCALL msg=audit(1755108109.639:535): arch=c000003e syscall=44 success=yes exit=1084 a0=3 a1=7ffed9234a10 a2=
43c a3=0 items=0 ppid=308103 pid=308118 auid=4294967295 uid=0 gid=0 euid=0 suid=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(1755108109.639:535): auid=4294967295 ses=4294967295 subj=unconfined op=remove_rule key
="project_access" list=4 res=1
----
time->Wed Aug 13 14:01:49 2025
type=PROCTITLE msg=audit(1755108109.643:539): proctitle=2F7362696E2F617564697463746C002D52002F6574632F61756469742F6
1756469742E72756C6573
type=SYSCALL msg=audit(1755108109.643:539): arch=c000003e syscall=44 success=yes exit=1084 a0=3 a1=7ffed9236ea0 a2=
43c a3=0 items=0 ppid=308103 pid=308118 auid=4294967295 uid=0 gid=0 euid=0 suid=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(1755108109.643:539): auid=4294967295 ses=4294967295 subj=unconfined op=add_rule key="p
roject_access" list=4 res=1
----
time->Wed Aug 13 23:54:24 2025
type=PROCTITLE msg=audit(1755143664.684:878): proctitle=617564697463746C002D77002F686F6D652F70726F6A656374002D70007
2777861002D6B0070726F6A6563745F616363657373
type=SOCKADDR msg=audit(1755143664.684:878): saddr=100000000000000000000000
type=SYSCALL msg=audit(1755143664.684:878): arch=c000003e syscall=44 success=yes exit=1084 a0=4 a1=7ffdae6793e0 a2=
43c a3=0 items=0 ppid=344338 pid=344339 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts1
ses=2 comm="auditctl" exe="/usr/sbin/auditctl" subj=unconfined key=(null)
type=CONFIG_CHANGE msg=audit(1755143664.684:878): auid=1000 ses=2 subj=unconfined op=add_rule key="project_access"
list=4 res=0
----
time->Thu Aug 14 00:07:52 2025
type=PROCTITLE msg=audit(1755144472.985:921): proctitle="/usr/sbin/updatedb.plocate"
type=PATH msg=audit(1755144472.985:921): item=0 name="project" inode=2493607 dev=08:01 mode=041770 ouid=0 ogid=1002
 rdev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=CWD msg=audit(1755144472.985:921): cwd="/"
type=SYSCALL msg=audit(1755144472.985:921): arch=c000003e syscall=257 success=yes exit=25 a0=a a1=5577c1f1af60 a2=1
0000 a3=0 items=1 ppid=1 pid=351025 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(no
```

Used the following link on the web browser to generate a web-based report;
http://localhost/auditlog.txt



Prepared by: Janefrances Nwachukwu
Date: 08/14/2025