

## Step 1: Setup File Access Policies (Confidentiality)

### 1. Create a Confidential File:

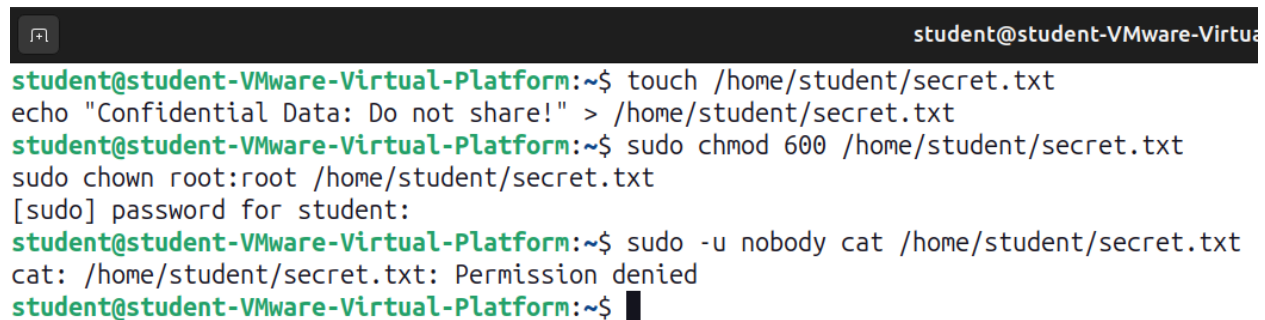
```
touch /home/student/secret.txt
echo "Confidential Data: Do not share!" > /home/student/secret.txt
```

### 2. Apply Strict File Permissions (DAC)

```
sudo chmod 600 "/home/student/secret.txt"
sudo chown root:root "/home/student/secret.txt"
```

### 3. Test Unauthorized Access

```
sudo -u nobody cat /home/student/secret.txt
Expected Outcome: Permission denied
```

A terminal window with a dark background. The title bar shows a window icon and the text 'student@student-VMware-Virtua'. The terminal output shows the following commands and their results:

```
student@student-VMware-Virtual-Platform:~$ touch /home/student/secret.txt
echo "Confidential Data: Do not share!" > /home/student/secret.txt
student@student-VMware-Virtual-Platform:~$ sudo chmod 600 /home/student/secret.txt
sudo chown root:root /home/student/secret.txt
[sudo] password for student:
student@student-VMware-Virtual-Platform:~$ sudo -u nobody cat /home/student/secret.txt
cat: /home/student/secret.txt: Permission denied
student@student-VMware-Virtual-Platform:~$ █
```

## Step 2: Enforce Integrity Policies Using Immutability

### 1. Enable File Immutability (Biba Model)

```
sudo chattr +i /home/student/secret.txt
```

### 2. Test Integrity Policy

```
sudo echo "Unauthorized Change" >> /home/student/secret.txt
```

Expected Outcome: Operation not permitted

### 3. Remove Immutability (Only When Required)

```
sudo chattr -i /home/student/secret.txt
```

```
student@student-VMware-Virtual-Platform:~$ sudo chattr +i /home/student/secret.txt
student@student-VMware-Virtual-Platform:~$ sudo echo "Unauthorized Change" >> /home/student/secret.txt
bash: /home/student/secret.txt: Operation not permitted
student@student-VMware-Virtual-Platform:~$ sudo chattr -i /home/student/secret.txt
student@student-VMware-Virtual-Platform:~$
```

## Step 3: Implement Mandatory Access Control (MAC) using SELinux/AppArmor

### 1. Check SELinux/AppArmor Status

```
sestatus # For SELinux
sudo aa-status # For AppArmor
```

If disabled, enable SELinux:

```
sudo setenforce 1
```

## 2. Apply SELinux Labeling (MAC)

```
sudo semanage fcontext -a -t httpd_sys_content_t "/home/student/secret.txt"
sudo restorecon -v /home/student/secret.txt
```

Expected Outcome:

- The file can only be accessed by HTTP services (if allowed).
- Prevents unauthorized processes from reading/modifying it.

```
student@student-VMware-Virtual-Platform:~/my_secure_dir$ sudo setenforce 1
setenforce: SELinux is disabled
student@student-VMware-Virtual-Platform:~/my_secure_dir$ pwd
/home/student/my_secure_dir
student@student-VMware-Virtual-Platform:~/my_secure_dir$ sudo semanage fcontext -a -t httpd_sys_content_t "/home/student/secret.txt"
libsemanage.semanage_read_policydb: Could not open kernel policy /var/lib/selinux/default/active/policy.kern for reading. (No such file or directory).
FileNotFoundError: No such file or directory
student@student-VMware-Virtual-Platform:~/my_secure_dir$ sudo restorecon -v /home/student/secret.txt
student@student-VMware-Virtual-Platform:~/my_secure_dir$
```

## Step 4: Monitor Policy Violations Using Auditd

### 1. Install & Enable Auditd

```
sudo apt install auditd -y
sudo systemctl start auditd
sudo systemctl enable auditd
```

### 2. Add Audit Rule for Unauthorized Access

```
sudo auditctl -w /home/student/secret.txt -p war -k confidential_access
```

### 3. Check Audit Logs

```
sudo ausearch -k confidential_access --start today
```

```

student@student-VMware-Virtual-Platform:~/my_secure_dir$ sudo apt install auditd -y
sudo systemctl start auditd
sudo systemctl enable auditd
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libhashkit2t64 libhiredis1.1.0 libmemcached1t64 libmemcachedutil2t64 libpcrc2-posix3 proftpd-doc
Use 'sudo apt autoremove' to remove them.
Suggested packages:
  audispd-plugins
The following NEW packages will be installed:
  auditd
0 upgraded, 1 newly installed, 0 to remove and 10 not upgraded.
Need to get 215 kB of archives.
After this operation, 726 kB of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu noble-updates/main amd64 auditd amd64 1:3.1.2-2.1build1.1 [215 kB]
Fetched 215 kB in 1s (230 kB/s)
Selecting previously unselected package auditd.
(Reading database ... 196291 files and directories currently installed.)
Preparing to unpack .../auditd_1%3a3.1.2-2.1build1.1_amd64.deb ...
Unpacking auditd (1:3.1.2-2.1build1.1) ...
Setting up auditd (1:3.1.2-2.1build1.1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/auditd.service → /usr/lib/systemd/system/auditd.service.
Processing triggers for man-db (2.12.0-4build2) ...
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
student@student-VMware-Virtual-Platform:~/my_secure_dir$

```

---

```

student@student-VMware-Virtual-Platform:~/my_secure_dir$ sudo auditctl -w /home/student/secret.txt -p war -k confidential_access
student@student-VMware-Virtual-Platform:~/my_secure_dir$ sudo ausearch -k confidential_access --start today
-----
time->Thu Mar 27 16:58:42 2025
type=PROCTITLE msg=audit(1743074922.289:143): proctitle=617564697463746C002D7F002F686F6D652F73747564656E742F7365637265742E747874002D7000776172002D6800636F6E66
6964656E7469616C5F616363657373
type=SYSCALL msg=audit(1743074922.289:143): arch=c000003e syscall=44 success=yes exit=1100 a0=4 a1=7fffd782860 a2=44c a3=0 items=0 ppid=11180 pid=11181 auid=
1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts1 ses=4 comm="auditctl" exe="/usr/sbin/auditctl" key=(null)
type=CONFIG_CHANGE msg=audit(1743074922.289:143): auid=1000 ses=4 op=add_rule key="confidential_access" list=4 res=1
student@student-VMware-Virtual-Platform:~/my_secure_dir$ █

```