Title: Unauthorized Access Investigation using auditd in Linux

---

Scenario: A sensitive payroll file (`/secure/payroll.txt`) was accessed without permission by a user named `legal_admin`. As a cybersecurity analyst, you were tasked to monitor the file and investigate unauthorized access using `auditd`.

Objectives:

- Monitor access to a sensitive file using Linux audit tools.
- Identify unauthorized access attempts.
- Analyze audit logs for user activity.
- Recommend improvements to access control policies.

Setup Commands:

```
# 1. Create folder and file
sudo mkdir /secure
sudo touch /secure/payroll.txt
```

```
# 2. Create users
sudo useradd finance_user
sudo useradd legal_admin
```

```
# 3. Assign ownership and restrict file permissions
sudo chown finance_user:finance_user /secure/payroll.txt
sudo chmod 600 /secure/payroll.txt
```

```
# 4. Temporarily allow read access to legal_admin (simulated misconfiguration)
sudo setfacl -m u:legal_admin:r-- /secure/payroll.txt
```

Enable auditd and Monitor the File:

```
# 5. Start auditd service
sudo systemctl start auditd
```

```
# 6. Add audit watch on the file
sudo auditctl -w /secure/payroll.txt -p r -k payroll_read
```

Simulate Unauthorized Access:

```
# 7. Simulate access by legal_admin
sudo -u legal_admin cat /secure/payroll.txt
```

Review Logs:

```
# 8. Search for audit logs by key
sudo ausearch -k payroll_read
```

Sample Output Snippet:

```
type=PATH msg=audit(...) name="/secure/payroll.txt" ...
type=SYSCALL msg=audit(...) comm="cat" exe="/usr/bin/cat" key="payroll_read"
```

Access Control Worksheet Summary:

- **Note(s):**
  - File accessed on 2025-08-07 at 05:19:24 by user `legal_admin`.
  - Command used: `cat`, recorded by auditd.
  - Action logged with key: `payroll_read`.
- **Issue(s):**
  - Unauthorized user had read access to a sensitive file.
  - ACLs allowed access that violated least privilege.
  - No real-time alert was triggered.
- **Recommendation(s):**
  - Revoke unnecessary ACLs.
  - Enforce Role-Based Access Control (RBAC).
  - Enable persistent logging and regular log audits.
  - Require multi-step approval for sensitive data access.

Screenshots to Add:

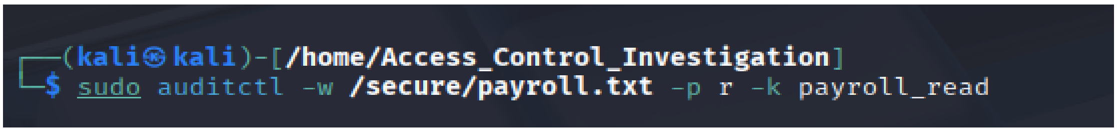
- Terminal output from `auditctl`, `cat`, and `ausearch`.
- Access Control Worksheet filled in.

Conclusion: This exercise demonstrates how Linux systems can detect unauthorized file access using auditd, and how proper configuration of permissions and logging can enhance data security. This example is ideal for including in a cybersecurity portfolio.

Screenshots :

◆ `auditctl` Watch Rule Added

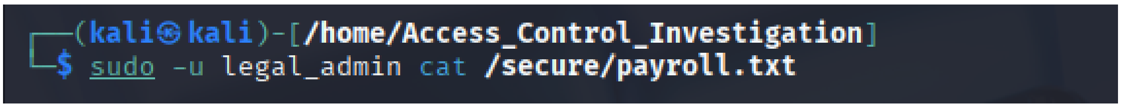
This shows the command to monitor `/secure/payroll.txt` for read access using auditd.



```
┌──(kali㉿kali)-[/home/Access_Control_Investigation]
└─$ sudo auditctl -w /secure/payroll.txt -p r -k payroll_read
```

◆ Unauthorized access using `cat`

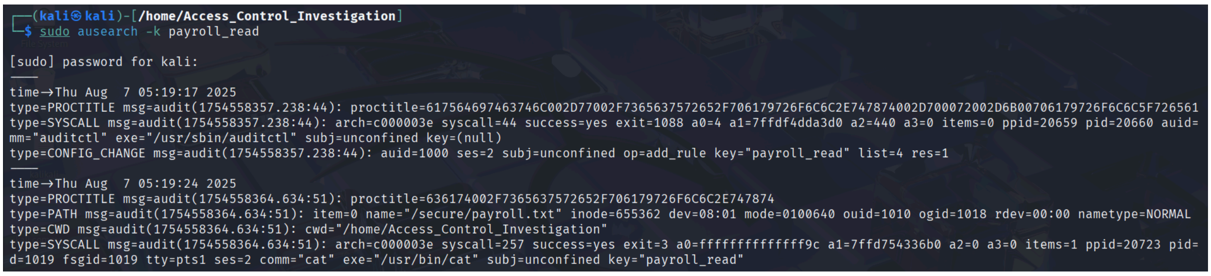
Simulated access by user `legal_admin`.



```
┌──(kali㉿kali)-[/home/Access_Control_Investigation]
└─$ sudo -u legal_admin cat /secure/payroll.txt
```

◆ ausearch output

Auditd successfully logged the unauthorized access.



```
┌──(kali㉿kali)-[/home/Access_Control_Investigation]
└─$ sudo ausearch -k payroll_read

[sudo] password for kali:
----
time→Thu Aug  7 05:19:17 2025
type=PROCTITLE msg=audit(1754558357.238:44): proctitle=617564697463746C002D77002F7365637572652F706179726F6C6C2E747874002D700072002D6B00706179726F6C6C5F726561
type=SYSCALL msg=audit(1754558357.238:44): arch=c000003e syscall=44 success=yes exit=1088 a0=4 a1=7ffdf4dda3d0 a2=440 a3=0 items=0 ppid=20659 pid=20660 auid=
mm="auditctl" exe="/usr/sbin/auditctl" subj=unconfined key=(null)
type=CONFIG_CHANGE msg=audit(1754558357.238:44): auid=1000 ses=2 subj=unconfined op=add_rule key="payroll_read" list=4 res=1
----
time→Thu Aug  7 05:19:24 2025
type=PROCTITLE msg=audit(1754558364.634:51): proctitle=636174002F7365637572652F706179726F6C6C2E747874
type=PATH msg=audit(1754558364.634:51): item=0 name="/secure/payroll.txt" inode=655362 dev=08:01 mode=0100640 ouid=1010 ogid=1018 rdev=00:00 nametype=NORMAL
type=CWD msg=audit(1754558364.634:51): cwd="/home/Access_Control_Investigation"
type=SYSCALL msg=audit(1754558364.634:51): arch=c000003e syscall=257 success=yes exit=3 a0=ffffffffffffff9c a1=7ffd754336b0 a2=0 a3=0 items=1 ppid=20723 pid=
d=1019 fsgid=1019 tty=pts1 ses=2 comm="cat" exe="/usr/bin/cat" subj=unconfined key="payroll_read"
```

Access controls worksheet:

	Note(s)	Issue(s)	Recommendation(s)
Authorization /authentication	• The user `legal_admin` accessed the sensitive payroll file `/secure/payroll.txt`. • The incident occurred on **August 7, 2025 at 05:19:24**. • Access was executed via `cat` command on a Linux terminal using UID 1011.	• The user had **read-level access** to a sensitive file outside their job scope. • This account likely **should not have active access** to payroll files. • ACL permissions were misconfigured, violating the principle of least privilege.	• Revoke unnecessary ACL permissions from non-finance users. • Implement **Role-Based Access Control (RBAC)** to limit access by department. • Enable **auditd** logging persistently and review logs weekly. • Add **multi-user approval policies** for payroll file access