

## Opgave 28 - Audit af et directory

### □ Formålet med øvelsen

Formålet med denne øvelse er at **demonstrere, hvordan auditd kan overvåge et directory**. Auditd kan ikke kun overvåge ændringer i individuelle filer, men også aktiviteter i hele directories. Dette gør det muligt at overvåge, hvem der tilgår, ændrer eller forsøger at eksekvere filer i et bestemt directory.

---

### □ Information

Directories kan overvåges med **auditd** på samme måde som filer.

De rettigheder, der kan overvåges, er:

- **Read (r)** → Når en fil eller directory bliver læst
- **Write (w)** → Når en fil eller directory bliver ændret
- **Attribute (a)** → Når filmetadata ændres
- **Execute (x)** → Når en fil eksekveres, eller nogen forsøger at tilgå directoryet (fx `cd /etc/`)

Hvis `execute (x)`-rettigheden overvåges, vil et forsøg på at skifte sti ind i directoryet (fx `cd /etc/`) udløse en auditlog.

---

### □ Instruktioner

1. **Opret et nyt directory** ved at køre:

```
mkdir /tmp/audit_directory
```

2. **Opret en auditregel**, der overvåger directoryet, med kommandoen:

```
auditctl -w /tmp/audit_directory -k directory_watch_rule
```

*Bemærk, at permissions bevidst er undladt.*

3. **Bekræft reglen** ved at udskrive audit-reglerne med:

```
auditctl -l
```

4. Notér, hvilke rettigheder der overvåges. Da `-p` ikke blev angivet, vil standardrettigheder blive anvendt.
5. **Ændr ejerskabet af directoryet** til `root`, og begræns adgang for andre brugere:

```
chown root:root /tmp/audit_directory
chmod 700 /tmp/audit_directory
```

6. **Test adgangsbegrænsning:**
7. Log ind med en bruger, der **ikke** er root.
8. Prøv at køre:

```
ls /tmp/audit_directory
```

9. Dette burde resultere i en **Permission Denied**-fejl.

10. **Analyser loggen** for directoryet med:

```
ausearch -i -k directory_watch_rule
```

*Dette vil returnere en log, der ligner nedenstående:*

```
type=PROCTITLE msg=audit(03/28/2023 20:29:14.761:407) : proctitle=ls --color=auto tmp
type=PATH msg=audit(03/28/2023 20:29:14.761:407) : item=0 name=tmp inode=269341 dev=fd:00 mode=dir,700 ouid=root ogid=root rdev=00:00 nametype=NORMAL cap_fp=none cap_fi=none cap_fe=0 cap_fver=0 cap_fr
ootid=0
type=CWD msg=audit(03/28/2023 20:29:14.761:407) : cwd=/home
type=SYSCALL msg=audit(03/28/2023 20:29:14.761:407) : arch=x86_64 syscall=openat success=no exit=EAC
CES(Permission denied) a0=AT_FDCWD a1=0x5620f46ad4a0 a2=0_RDONLY|0_NONBLOCK|0_DIRECTORY|0_CLOEXEC a3
=0x0 items=1 ppid=2194 pid=2471 auid=martin uid=martin gid=martin euid=martin suid=martin fsuid=mart
in egid=martin sgid=martin fsgid=martin tty=tty1 ses=1 comm=ls exe=/usr/bin/ls subj=unconfined key=d
irectory_watch
```

## □ Analyse af logs

`ausearch` viser detaljerede logs over audit-hændelser, men kan være mindre overskueligt end `aureport`. Bemærk, at `aureport` **ikke fungerer** for directory-regler. Hvis du leder efter noget specifikt i en stor auditlog, kan du filtrere output med `grep`:

```
aureport -k | grep directory_watch_rule
```

## □ Links

□ [Ausearch-manualside](#)

🕒 2025-04-03 05:55:59