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:

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