Øvelse 28 – Audit af et directory i Linux

Information

Formålet med denne øvelse er at demonstrere, hvordan **auditd** kan anvendes til at overvåge aktiviteter i et helt directory.
I modsætning til overvågning af enkeltfiler giver directory-overvågning mulighed for at registrere adgangsforsøg, ændringer og eksekvering i en samlet struktur.

Dette er særligt relevant for:

- Overvågning af følsomme mapper
- Detektering af uautoriserede adgangsforsøg
- Compliance og sporbarhed (accountability)

Auditd kan overvåge følgende rettigheder på et directory:

- **Read (r)** – læsning af indhold
- **Write (w)** – ændringer i directoryet
- **Attribute (a)** – ændring af metadata
- **Execute (x)** – forsøg på at tilgå directoryet (fx cd)

Hvis execute-rettigheden overvåges, vil et forsøg på at skifte ind i directoryet udløse en audit-hændelse.

Instruktioner

Husk at notere dine observationer i dit cheat sheet.

I denne øvelse arbejder du med at overvåge et helt directory og analysere, hvordan systemet registrerer adgangsforsøg og ændringer.

Formålet er at undersøge:

- hvordan auditd registrerer adgang til beskyttede områder
- hvordan mislykkede adgangsforsøg logges
- hvordan man kan identificere hvem der forsøger at tilgå et directory

Du skal derfor ikke kun udføre kommandoerne, men også være opmærksom på:

- hvad der sker i systemet
- hvilke hændelser der bliver registreret
- hvordan disse kan bruges i en sikkerhedskontekst

1 Opret et directory til audit

1. Opret et nyt directory: `mkdir /tmp/audit_directory`

---

2 Opret auditregel for directoryet

1. Opret en auditregel, der overvåger directoryet: `auditctl -w /tmp/audit_directory -k directory_watch_rule` **Bemærk:**
   - Der er bevidst ikke angivet permissions (-p)
   - Auditd anvender derfor standardovervågning
2. Verificér reglen: `auditctl -l`
3. Notér hvilke rettigheder der overvåges.

 Hvilke handlinger bliver registreret, når der ikke er angivet `-p`?

---

3 Begræns adgang til directoryet

1. Ændr ejerskab til root: `chown root:root /tmp/audit_directory`
2. Fjern adgang for andre brugere: `chmod 700 /tmp/audit_directory`

---

4 Test adgangsbegrænsning

1. Log ind som en bruger, der ikke er root.
2. Forsøg at tilgå directoryet: `ls /tmp/audit_directory`
3. Notér fejlen (Permission denied).

---

5 Analyser audit-logs

1. Udskriv audit-hændelser relateret til directoryet: `ausearch -i -k directory_watch_rule`
2. Undersøg:
   - Hvem (uid / bruger) forsøgte at tilgå directoryet

- Hvilken handling blev forsøgt? Kan du identificere hvilken kommando brugeren anvendte?
- Kig efter "success=no" eller exit-værdier i loggen Kan du skelne mellem et legitimt og et uautoriseret adgangsforsøg? Her skal log linjerne studeres

---

Refleksion

- Hvorfor er directory-overvågning vigtigere end kun fil-overvågning?
- Hvilke directories bør overvåges på en produktionsserver?
- Hvordan kan disse audit-logs anvendes i et SIEM-system som Wazuh?

Links

- ausearch man page
- Auditctl man page

Last update: 2026-03-20 13:58:28