Øvelse 26 – Installation og introduktion til auditd

Information

Formålet med denne øvelse er at introducere **auditd** og lave den indledende opsætning af auditd i Linux.
Auditd er et centralt værktøj til logning og overvågning af sikkerhedsrelevante systemhændelser og anvendes ofte i forbindelse med systemadministration, compliance og incident response.

I denne øvelse arbejdes der med auditd på **Ubuntu Server**.

Audit daemon (auditd) fungerer ved hjælp af **audit-regler**, som definerer hvilke hændelser der skal overvåges. Når en regel trigges, registreres hændelsen i audit-loggen.

Auditd-logs findes som udgangspunkt i følgende fil: `/var/log/audit/audit.log`

Vigtigt:
Auditd registrerer ikke selve indholdet af ændringer, men giver detaljer om:

- hvem der udførte handlingen
- hvornår det skete
- hvilken type handling der blev udført

Baggrund

Auditd kan anvendes til at overvåge blandt andet:

- Ændringer i filer og mapper
- Adgang til systemressourcer
- Systemkald og procesoprettelse
- Fejl og mislykkede handlinger

Auditd anvendes ofte som datakilde for:

- SIEM-systemer (fx Wazuh, Splunk, Elastic SIEM)
- Compliance-krav om revision(fx ISO 27001, GDPR)

Mange sikkerhedsværktøjer bygger ovenpå auditd eller kan analysere audit-loggen direkte.

Instruktioner

Husk at notere observationer og resultater i dit Linux cheat sheet.

---

1 Installation og status på auditD

1. Installer auditd (hvis den ikke allerede er installeret): `sudo apt install auditd`
2. Verificér at auditd kører: `systemctl status auditd`
   *Output bør vise, at servicen er **active (running)**.*
3. Udskriv de nuværende audit-regler: `auditctl -l`

Som udgangspunkt bør der ikke være nogen regler.

---

2 Gennemgang af audit-loggen

1. Udskriv audit-logfilen: `cat /var/log/audit/audit.log`
2. Gennemse outputtet:
   - Er loggen let eller svær at læse?
   - Hvilke informationer kan du identificere (tid, bruger, handling)?

---

3 Analyseværktøjer (overblik)

Audit-loggen kan hurtigt blive uoverskuelig. Derfor anvendes typisk følgende værktøjer:

- **ausearch** – bruges til at søge efter specifikke hændelser
- **aureport** – bruges til at generere overskuelige rapporter

Disse værktøjer gennemgås i de kommende øvelser.

Hvorfor er dette vigtigt?

At arbejde direkte med auditd giver en grundlæggende forståelse for, hvordan systemhændelser kan overvåges på Linux.

- Auditd anvendes ofte til compliance og sikkerhedsovervågning
- Mange SIEM-systemer kan analysere auditd-logs direkte
- Auditd udgør fundamentet for mere avanceret detektion og overvågning

---

Sammenligning: auditd og Sysmon

Auditd og Sysmon bygger på samme grundlæggende idé:

- at registrere systemhændelser
- skabe sporbarhed i systemet
- understøtte sikkerhedsovervågning og efterforskning

Hvor Sysmon leverer mange hændelser som standard, kræver auditd, at du selv definerer hvilke aktiviteter der skal overvåges.

Auditd kan derfor ses som en Linux-ækvivalent til Sysmon – men med større fleksibilitet og behov for manuel konfiguration.

Funktion	auditd (Linux)	Sysmon (Windows)
Platform	Linux	Windows
Filovervågning	Ja	Ja
Procesovervågning	Ja	Ja
Netværksovervågning	Begrænset	Ja
Logdestination	/var/log/audit/audit.log	Windows Event Log
SIEM-integration	Ja	Ja

Auditd anvendes i praksis ofte på samme måde som Sysmon – nemlig som en datakilde til overvågning og detektion af systemhændelser.

Klar til næste øvelse

Sørg for at auditd er installeret og aktiv, da næste øvelse bygger videre på analyse og filtrering af auditd-logs.

 I denne øvelse har du set auditd's opsætning og logformat.
I næste øvelse arbejder du med at definere regler og generere konkrete hændelser.

Links

- https://linux.die.net/man/8/auditd
- https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

---

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