Øvelse 29 – Overvågning af privilegerede kommandoer (sudo)

Information

Formålet med denne øvelse er at demonstrere, hvordan **auditd** kan anvendes til at overvåge brugen af privilegerede kommandoer.
Ved at logge anvendelsen af `sudo` kan man identificere:

- hvem der forsøger at opnå administrative rettigheder
- hvilke kommandoer der bliver udført med forhøjede privilegier
- potentielt misbrug af systemet

Dette er centralt i:

- Sikkerhedsovervågning (privilege escalation)
- Incident response
- Compliance og sporbarhed (accountability)

Instruktioner

Husk at notere dine observationer i dit cheat sheet.

I denne øvelse arbejder du med at overvåge brugen af `sudo` og analysere, hvordan systemet registrerer privilegerede handlinger.

Formålet er at undersøge:

- hvordan auditd registrerer brug af administrative rettigheder
- hvordan man kan se hvilken kommando der blev udført
- hvordan man kan identificere brugeren bag handlingen

---

1 Opret auditregel for sudo

1. Tilføj en auditregel, der overvåger `sudo`: `sudo auditctl -w /usr/bin/sudo -p x -k sudo_usage`

> **Forklaring:**
>
> - `-w` → overvåg en fil
> - `/usr/bin/sudo` → programmet der overvåges
> - `-p x` → registrér eksekvering
> - `-k sudo_usage` → nøgle til filtrering

---

2 Udfør sudo-kommandoer

1. Kør en simpel kommando med sudo: `sudo ls /root`
2. Prøv evt. også: `sudo cat /etc/shadow`

---

3 Analyser audit-logs

1. Søg efter hændelser: `sudo ausearch -i -k sudo_usage`
2. Undersøg:
   - Hvilken bruger udførte kommandoen (auid / uid)
   - Hvilken kommando blev kørt (proctitle)
   - Hvilket program blev eksekveret (exe)
   - Tidspunkt for hændelsen

---

4 Lav en rapport

```
sudo aureport -i -k | grep sudo_usage
```

Yderligere analyse

Undersøg følgende i loggen:

- `auid` → den oprindelige bruger (meget vigtig i sikkerhed)
- `uid` → hvilken bruger processen kører som (ofte root)
- `exe` → hvilket program der blev kørt
- `comm` → procesnavn

Refleksion

- Hvorfor er overvågning af `sudo` vigtig i en sikkerhedskontekst?
- Hvordan kan man opdage misbrug af administrative rettigheder?
- Hvordan kunne disse logs anvendes i et SIEM-system som Wazuh?

Links

- https://man7.org/linux/man-pages/man8/ausearch.8.html
- https://man7.org/linux/man-pages/man8/auditctl.8.html

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