Opgave 26 - Installer auditd

Formålet med øvelsen

Formålet med denne øvelse er at **introducere auditd** og at lave den **indledende opsætning** af auditd i Linux.
Auditd er et kraftfuldt værktøj til logning og overvågning af systemhændelser, hvilket gør det til en vigtig del af systemadministration og sikkerhed.

I denne øvelse vil du:

- Installere og aktivere auditd
- Bekræfte, at det kører korrekt
- Udforske auditd's regler og logfiler
- Forberede dig på senere analyser af logs

Introduktion

Når det kommer til sikkerhed og overvågning i Linux, er **auditd** et af de vigtigste værktøjer. Det hjælper administratorer med at overvåge kritiske ændringer i systemet, såsom adgang til filer, ændringer i systemindstillinger og mistænkelige handlinger.

Audit daemon (`auditd`) fungerer som et logningssystem for **foruddefinerede begivenheder**, kaldet *audit-regler*. Hver gang en regel aktiveres, registreres en hændelse i en *audit-log* – en slags "alarm", der kan bruges til sikkerhedsanalyse eller fejlretning.

Som udgangspunkt findes alle `auditd`-logs i:

```
/var/log/audit/audit.log
```

Hvad kan auditd overvåge?

- **Ændringer i filer og mapper** (fx adgang, sletning, ændringer)
- **Hvem der tilgår systemressourcer**
- **Systemkald og procesændringer**
- **Fejl og mislykkede adgangsforsøg**

Vigtigt!
`auditd` er **ikke** et versionsstyringssystem og holder derfor ikke styr på *hvad* der blev ændret

– kun *hvem* der foretog ændringen.

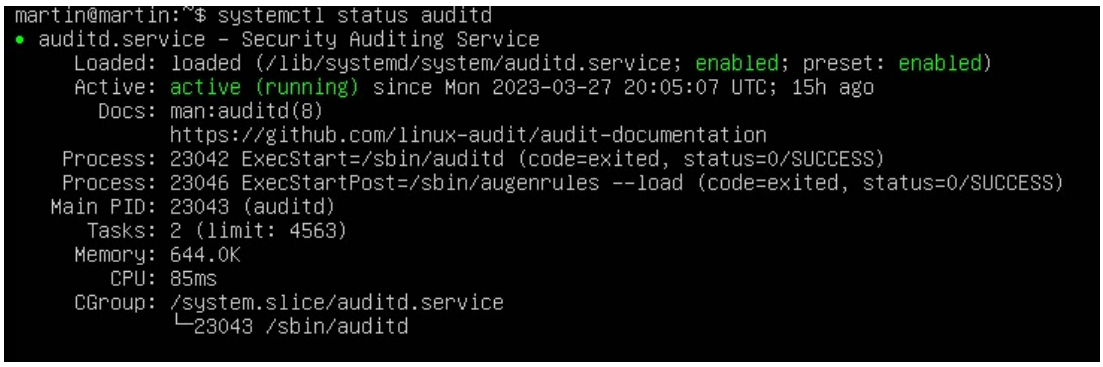
Instruktioner

1. **Installer audit daemon** (hvis den ikke allerede er installeret):

```
sudo apt install auditd
```

2. **Verificér, at `auditd` kører**:

```
systemctl status auditd
```



3. **Udskriv nuværende audit-regler** med kommandoen:

```
auditctl -l
```

4. **Udskriv logfilen** for at se registrerede begivenheder:

```
cat /var/log/audit/audit.log
```

```
type=CRED_DISP msg=audit(1680005204.441:534): pid=26765 uid=1000 auid=1000 ses=135 subj=unconfined m
sg='op=PAM:setcred grantors=pam_permit acct="root" exe="/usr/bin/sudo" hostname=martin addr=? termin
al=/dev/tty1 res=success'UID="martin" AUID="martin"
type=USER_ACCT msg=audit(1680005211.753:535): pid=26782 uid=1000 auid=1000 ses=135 subj=unconfined m
sg='op=PAM:accounting grantors=pam_permit acct="martin" exe="/usr/bin/sudo" hostname=martin addr=? t
erminal=/dev/tty1 res=success'UID="martin" AUID="martin"
type=USER_CMD msg=audit(1680005211.753:536): pid=26782 uid=1000 auid=1000 ses=135 subj=unconfined ms
g='cwd="/home/martin" cmd=617564697463746C202D6C exe="/usr/bin/sudo" terminal=tty1 res=success'UID="
martin" AUID="martin"
type=CRED_REFR msg=audit(1680005211.753:537): pid=26782 uid=1000 auid=1000 ses=135 subj=unconfined m
sg='op=PAM:setcred grantors=pam_permit,pam_cap acct="root" exe="/usr/bin/sudo" hostname=martin addr=
? terminal=/dev/tty1 res=success'UID="martin" AUID="martin"
type=USER_START msg=audit(1680005211.753:538): pid=26782 uid=1000 auid=1000 ses=135 subj=unconfined
msg='op=PAM:session_open grantors=pam_limits,pam_env,pam_env,pam_permit,pam_umask,pam_unix acct="roo
t" exe="/usr/bin/sudo" hostname=martin addr=? terminal=/dev/tty1 res=success'UID="martin" AUID="mart
in"
type=USER_END msg=audit(1680005211.757:539): pid=26782 uid=1000 auid=1000 ses=135 subj=unconfined ms
g='op=PAM:session_close grantors=pam_limits,pam_env,pam_env,pam_permit,pam_umask,pam_unix acct="root
" exe="/usr/bin/sudo" hostname=martin addr=? terminal=/dev/tty1 res=success'UID="martin" AUID="marti
n"
type=CRED_DISP msg=audit(1680005211.757:540): pid=26782 uid=1000 auid=1000 ses=135 subj=unconfined m
sg='op=PAM:setcred grantors=pam_permit acct="root" exe="/usr/bin/sudo" hostname=martin addr=? termin
al=/dev/tty1 res=success'UID="martin" AUID="martin"
```

Analyse af logs

Hvis loggen virker uoverskuelig, er du ikke alene! Mange finder den svær at læse. Derfor bruger man typisk to værktøjer til analyse af specifikke begivenheder:

- `ausearch` → Bruges til at søge efter specifikke hændelser
- `aureport` → Giver en overskuelig rapport over logs

Begge værktøjer bliver gennemgået i de kommende øvelser.

Hvorfor er dette vigtigt?

At arbejde direkte med `auditd` kan virke teknisk, men det giver en **grundlæggende forståelse** for, hvordan audit-logning fungerer i Linux.
Mange større og mere intuitive auditsystemer (f.eks. **SIEM-systemer**) benytter **auditd** eller kan læse `auditd`-loggen.
Auditd bruges ofte til **compliance-formål** (f.eks. GDPR, ISO 27001).

Auditd vs. Sysmon

Hvis du har arbejdet med sikkerhedslogning på **Windows**, kender du måske **Sysmon**. Det er et lignende værktøj, men til Microsoft-systemer.

Funktion	Auditd (Linux)	Sysmon (Windows)

Funktion	Auditd (Linux)	Sysmon (Windows)
Platform	Linux	Windows
Overvåger filer?	Ja, filændringer og adgang	Ja, filændringer
Overvåger processer?	Ja, systemkald og processkabelse	Ja, detaljeret procesovervågning
Overvåger netværk?	Begrænset, kræver ekstra moduler	Ja, registrerer netværksforbindelser
Logdestination	`/var/log/audit/audit.log`	Windows Event Log
SIEM-integration	Ja (ELK, Splunk, Wazuh)	Ja (Splunk, ELK, Defender ATP)

- **Auditd er Sysmon for Linux**, men kræver lidt mere konfiguration.
- **Sysmon er lettere at bruge**, især for sikkerhedsanalyse på Windows.
- **Begge bruges i SIEM-systemer** til trusselsdetektion og hændelseslogning.

Hvis du arbejder med både **Linux og Windows**, er det en fordel at kende **begge værktøjer**. Vi vil i senere øvelser se på, hvordan du kan bruge auditd til mere avanceret overvågning.

Hvad nu?

I de næste øvelse vil vi dykke dybere ned i, hvordan du analyserer *auditd*-logs effektivt. Sørg for, at *auditd* er installeret og aktivt, så du er klar til næste skridt!

Links

- auditd man-side
- Sysmon for Windows

2025-04-03 05:55:59