Øvelse 31 – Auditd og CIS Benchmark (detektion i praksis)

Information

Formålet med denne øvelse er at arbejde med **CIS Benchmark for Ubuntu Server** og anvende anbefalinger til at definere relevante auditd-regler.

I praksis anvendes standarder som CIS til at:

- identificere hvilke systemhændelser der bør overvåges
- etablere et sikkerhedsbaseline
- understøtte compliance og revision

I denne øvelse skal du selv finde en relevant anbefaling og omsætte den til en auditd-regel.

Tanken bag øvelsen er, at du nu anvender din viden og færdigheder med auditd i en realistisk sikkerhedskontekst, og kobler det til CIS kontroller og benchmarks.

Baggrund

CIS Benchmarks indeholder anbefalinger til, hvordan systemer bør konfigureres sikkert.

For auditd indeholder benchmarket blandt andet:

- hvilke filer der bør overvåges
- hvilke systemkald der er relevante
- hvordan logning bør konfigureres

Disse anbefalinger bruges ofte som udgangspunkt for:

- hardening
- SIEM-detektion
- sikkerhedsovervågning

Fra compliance til implementering (auditd)

Når man arbejder med sikkerhed i praksis, starter man ofte med et **compliance-krav**, som derefter omsættes til konkrete tekniske løsninger.

Processen kan beskrives sådan:

```
+------------------------+        +------------------------------+        +---
------------------------------+
| Compliance / Kontrol   | -----> | CIS Benchmark                | -----> |
Implementering (auditd)          |
+------------------------+        +------------------------------+        +---
------------------------------+
| Hvad kræves?           |        | Hvad anbefales?              |        |
Hvordan gør vi det i praksis?    |
+------------------------+        +------------------------------+        +---
------------------------------+
| Overvåg ændringer i    |        | CIS Ubuntu Server            |        |
auditctl -w /etc/passwd          |
| brugerdata             |        | 4.1.3.x anbefaler            |        | -p
wa -k identity                |
|                        |        | overvågning af /etc/passwd   |        |
|
+------------------------+        +------------------------------+        +---
------------------------------+
```

 Forklaring:

1. **Compliance / kontrol**
   Organisationen ønsker at kunne opdage ændringer i brugerdata
2. **CIS Benchmark**
   CIS Benchmark anbefaler en række overvågninger af kritiske filer som F.eks. `/etc/passwd`, `/etc/shadow` og `/etc/sudoers`
3. **Implementering (auditd)**
   Dette omsættes til en auditd-regel

Instruktioner

Husk at dokumentere dine valg og observationer.

I denne øvelse arbejder du som en sikkerhedsanalytiker.

Du skal:

- finde en relevant anbefaling i CIS Benchmark
- forstå hvad den forsøger at beskytte
- omsætte den til en auditd-regel
- teste om den virker

 Din løsning er korrekt når: - din auditregel genererer logs - du kan forklare hvad der bliver detekteret - du kan koble det til CIS og sikkerhed

> **Forudsætning:**
> auditd er konfigureret jf. CIS Benchmark (afsnit 4.1.1.1)

---

1 Find en relevant CIS-anbefaling

1. Find **CIS Benchmark for Ubuntu Server**
2. Gå til afsnit **4.1.3 Configure auditd rules**
3. Vælg én anbefaling du vil implementere

 Eksempler (valgfrit): - overvågning af `/etc/passwd` - overvågning af `/etc/sudoers` - overvågning af privileged commands

---

2 Forstå anbefalingen

Besvar:

- Hvad forsøger denne regel at beskytte?
- Hvilken type hændelse vil man opdage?
- Hvorfor er dette sikkerhedsrelevant?
- Hvilken CIS Control / Safeguard understøttes?

---

3 Implementér auditd-reglen

1. Opret en auditregel baseret på anbefalingen
2. Brug enten:
3. `auditctl` (midlertidig)
4. eller `/etc/audit/rules.d/` (persistent)

 Hint: CIS Benchmark anvender ofte shell-syntaks som `\` til at opdele lange kommandoer over flere linjer.

Eksempel:

```
awk '...' \
&& '...' \
&& '...'
```

Her betyder `\`, at kommandoen fortsætter på næste linje.

 Når du selv arbejder med kommandoen, kan du enten: - skrive den på én linje
- eller sikre korrekt linjeskift i terminalen

Vær opmærksom på, at dette er shell-syntaks og ikke en del af selve audit-reglen.

---

4 Valider implementeringen af reglen

I CIS Benchmark findes der et *Audit*-afsnit til hver anbefaling, som beskriver hvordan man verificerer en korrekt implementering.

Du skal nu validere din regel på samme måde.

1. Find *Audit*-afsnittet for din valgte CIS-anbefaling
2. Kør de relevante kontrolkommandoer fra benchmarken
3. Kontrollér at din regel fremgår korrekt:
4. i konfigurationsfiler (on disk)
5. i aktive regler (`auditctl -l`)
6. Verificér at din regel virker ved at trigge en hændelse og undersøge loggen:

   ausearch -i -k

 Matcher din implementering det, som CIS anbefaler?

---

5 Dokumentation

Dokumentér:

- hvilken CIS-regel du valgte
- din auditd-regel
- hvordan du testede den
- hvad du kunne se i loggen

Refleksion

- Hvorfor er det vigtigt at bruge standarder som CIS?
- Hvad er forskellen på en teknisk regel og en sikkerhedsdetection?
- Hvordan kunne denne regel anvendes i et SIEM-system som Wazuh?

Links

- https://man7.org/linux/man-pages/man8/auditctl.8.html
- https://man7.org/linux/man-pages/man8/ausearch.8.html
- https://www.cisecurity.org/cis-benchmarks

Last update: 2026-03-24 09:04:36