Opgave 29 - Overvågning af OS API'et for specifikke systemkald

Formålet med øvelsen

Formålet med denne øvelse er at **demonstrere, hvordan auditd kan overvåge systemkald til operativsystemets API**.
Ved at opsætte regler til at registrere specifikke systemkald kan administratorer identificere potentielt skadelige handlinger såsom uautoriserede processafslutninger, filændringer eller adgang til kritiske ressourcer. Dette bruges ofte til **sikkerhedsovervågning, fejlretning og compliance-formål**.

Information

Operativsystemer tilbyder et sæt **systemkald** (syscalls), som applikationer bruger til at kommunikere med kernens API. **Auditd** kan bruges til at registrere, hvilke processer der foretager bestemte systemkald, hvilket gør det muligt at spore handlinger såsom:

- Oprettelse eller afslutning af processer
- Ændringer i filsystemet
- Netværksforbindelser
- Systemændringer og administrative handlinger

I denne øvelse vil vi fokusere på **overvågning af processer, der bliver afsluttet**, ved at logge `kill`-systemkaldet.

Instruktioner

Overvågning af processer, der bliver afsluttet

1. **Tilføj en auditregel**, der registrerer `kill`-systemkaldet (som bruges til at afslutte processer), med kommandoen:

   ```
   auditctl -a always,exit -F arch=b64 -S kill -F key=kill_rule
   ```

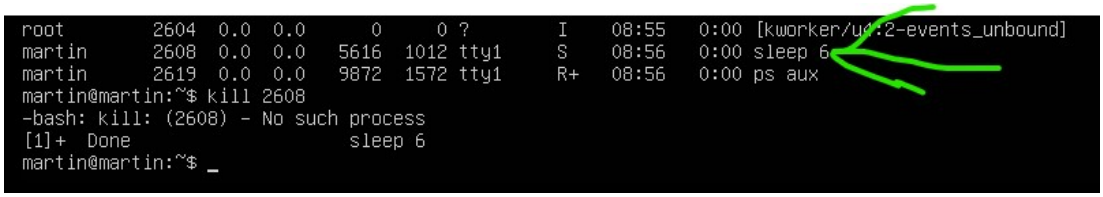
2. `-a always,exit` → Overvåg alle afslutninger af systemkald.

3. `-F arch=b64` → Specificerer systemarkitekturen (64-bit i dette tilfælde).
4. `-S kill` → Overvåg `kill`-systemkaldet.
5. `-F key=kill_rule` → Tilføjer en nøgle (*key*), så loggen kan filtreres senere.
6. **Start en baggrundsproces** med:

```
sleep 600 &
```

7. Dette starter en proces, der sover i 600 sekunder (10 minutter).
8. **Find proces-ID'et (PID)** for `sleep`-processen ved at køre:

```
ps aux | grep sleep
```



9. **Afslut processen** ved at køre:

```
kill <proces ID>
```

10. Udskift `<proces ID>` med det faktiske PID fra forrige trin.
11. **Verificér, at hændelsen blev logget** ved at køre:

```
aureport -i -k | grep kill_rule
```

12. Hvis reglen fungerer korrekt, bør du se en række nye logs.

 Bemærk: Der kan være flere rækker i loggen, da auditd ofte genererer flere relaterede hændelser.

Yderligere analyse

Hvis du vil se mere detaljerede oplysninger om, hvem der afsluttede processen, og hvordan systemkaldet blev udført, kan du bruge:

```
ausearch -i -k kill_rule
```

Dette vil vise: - Hvilken bruger der udførte systemkaldet. - Hvilken proces, der blev afsluttet. - Det præcise tidspunkt for hændelsen.

Links

- Ausearch-manualside
- Auditd-manualside

2025-04-03 05:55:59