Øvelse 16 – Nedlukning af logservice

Information

Formålet med denne øvelse er at demonstrere, hvordan logging kan deaktiveres på en Linux-maskine, og hvilke sikkerhedsmæssige konsekvenser dette kan have.

Logging er en central del af systemovervågning, fejlfinding og sikkerhedsanalyse. Hvis en angriber får privilegeret adgang og kan slukke for logging, kan det forhindre efterforskning af hændelser og skjule skadelig aktivitet.

Øvelsen introducerer også metoder til at opdage og afbøde deaktivering af logging, f.eks. ved brug af fjernlogging og host-baseret overvågning.

Baggrund

Log-daemons som **rsyslog** registrerer systemhændelser og gemmer dem i logfiler.

Disse services kan dog stoppes ligesom andre systemprocesser i Linux. Hvis logging stoppes, vil nye systemhændelser ikke længere blive registreret.

En angriber med **root-adgang** kan udnytte dette til at:

- skjule sin aktivitet
- undgå detektion
- vanskeliggøre incident response og digital forensics

Derfor er det vigtigt at forstå både **hvordan logging kan deaktiveres**, og **hvordan dette kan opdages**.

Instruktioner

1 Stop og maskér rsyslog

I dette trin skal du deaktivere rsyslog-servicen.

1. Forhindr rsyslog i at starte automatisk:

```
sudo systemctl mask rsyslog
```

Maskering betyder, at servicen ikke kan startes – heller ikke manuelt – før maskeringen fjernes.

2. Stop logservicen:

```
sudo systemctl stop rsyslog
```

Når rsyslog stoppes, vil systemet ikke længere skrive nye logbeskeder til syslog-filer.

---

2 Test om logging er stoppet

I dette trin skal du kontrollere, om logningen faktisk er stoppet.

1. Log en testbesked:

```
logger "Test log entry"
```

2. Undersøg syslog:

```
tail -n 10 /var/log/syslog
```

Hvis beskeden **ikke vises**, betyder det, at rsyslog ikke længere registrerer logbeskeder.

---

3 Genaktiver logging

I dette trin skal logservicen aktiveres igen.

1. Fjern maskeringen af rsyslog:

```
sudo systemctl unmask rsyslog
```

2. Start logservicen igen:

```
sudo systemctl start rsyslog
```

3. Test at logging virker:

```
logger "Logging is working again"
```

```
tail -n 10 /var/log/syslog
```

Hvis beskeden vises i loggen, er logging blevet genaktiveret korrekt.

---

4 Sikkerhedsforanstaltninger mod logdeaktivering

Hvis en angriber kan deaktivere lokal logging, kan det gøre efterforskning vanskelig.

Derfor anvendes ofte **central logning**, hvor logs sendes til en ekstern logserver.

Dette betyder, at logdata stadig gemmes et andet sted, selv hvis den lokale logservice stoppes.

Dog garanterer dette ikke, at lokal logning stadig fungerer. Derfor er det vigtigt også at overvåge selve logservicen på værten.

Overvågning med Wazuh

Et eksempel på overvågningssoftware er **Wazuh**.

Wazuh fungerer både som:

- **SIEM** (Security Information and Event Management)
- **HIDS** (Host-based Intrusion Detection System)

En Wazuh-agent kan installeres på serveren og bruges til at:

- overvåge kritiske services som rsyslog
- registrere stop eller ændringer af logtjenester
- rapportere hændelser til en central Wazuh-server

Hvis en angriber forsøger at deaktivere rsyslog, kan Wazuh generere en sikkerhedshændelse.

Selv hvis en angriber stopper Wazuh-agenten, vil Wazuh-serveren kunne registrere, at forbindelsen til agenten er forsvundet.

Refleksion

Reflektér over følgende spørgsmål og notér dine svar:

- Hvorfor bør en server ikke tillade, at en lokal bruger kan slukke for logging?
- Hvordan kan man opdage, at en angriber har deaktiveret rsyslog?
- Hvilke andre metoder kan en angriber bruge til at skjule sin aktivitet?

- Hvordan kan kritiske logfiler beskyttes mod manipulation?

Links

Rsyslog Documentation

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