Opgave 16 - Nedlukning af logservice

Formål

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

Derudover vil øvelsen introducere måder at opdage og forhindre deaktivering af logging ved brug af fjernlogging og systemd-logning.

Information

Logging-daemons som Rsyslog kan stoppes ligesom andre systemprocesser i Linux. Dette kan dog have alvorlige konsekvenser, da det betyder, at ingen logs bliver registreret, hvilket gør det umuligt at spore hændelser på systemet.

En angriber med **root-adgang** kan udnytte dette til at slette sine spor og deaktivere overvågning. Derfor er det vigtigt at forstå, hvordan man kan opdage og forhindre logdeaktivering.

Instruktioner

1. Stop og start Rsyslog

For at stoppe logservicen og forhindre, at logs genereres, skal du bruge følgende kommandoer:

1. **Forhindre `rsyslog` i at starte automatisk**:

   ```
   sudo systemctl mask rsyslog
   ```

   - `mask` sikrer, at `rsyslog` ikke kan startes automatisk eller manuelt, før det bliver "unmasked".

2. **Stop logservicen**:

   ```
   sudo systemctl stop rsyslog
   ```

- Dette stopper `rsyslog`, så det ikke længere logger.

---

2. Test, om logging er stoppet

For at verificere, at logningen er stoppet, kan du køre følgende kommandoer:

1. **Log en testbesked:**

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

2. **Tjek, om beskeden er logget i syslog:**

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

- Hvis den nye logbesked **ikke vises**, betyder det, at logging er slået fra.

---

3. Genstart Rsyslog for at genoptage logging

Hvis du vil **genaktivere logningen**, skal du gøre følgende:

1. **Fjern maskeringen af `rsyslog`**:

```
sudo systemctl unmask rsyslog
```

2. **Genstart logservicen**:

```
sudo systemctl start rsyslog
```

3. **Test, om logging fungerer igen**:

```
logger "Logging is working again"
tail -n 10 /var/log/syslog
```

- Hvis beskeden vises, er logningen genaktiveret.

---

3. Sikkerhedsforanstaltninger for at forhindre logdeaktivering

For at sikre, at logfiler ikke bliver slettet eller ændret af en trusselsaktør, sendes de typisk til en *logserver*. Dette garanterer dog ikke, at logsystemet på selve værten stadig fungerer. For at sikre, at lokal logning faktisk sker, er det nødvendigt at overvåge logservicen på værten.

En måde at gøre dette på er ved at anvende et *Host-baseret Intrusion Detection System (HIDS)*. Et eksempel på et HIDS er OSSEC, som også anvendes af Wazuh.

HIDS kan overvåge aktiviteter på den enkelte host og sende data til et centralt system (f.eks. et SIEM-system som Wazuh). Wazuh-agenten kører på værten og overvåger systemændringer, processer og logfiler, hvilket gør det muligt at opdage forsøg på at deaktivere `rsyslog`.

Overvågning med Wazuh

Wazuh fungerer både som en **log-indsamler (SIEM)** og et **HIDS**, hvilket gør det muligt at registrere uautoriserede ændringer i systemlogning. Hvis en angriber forsøger at deaktivere `rsyslog`, kan Wazuh generere en hændelse.

- **Wazuh-agenten** kører lokalt på serveren og overvåger kritiske processer og services.
- Hvis en angriber slukker `rsyslog`, kan Wazuh udløse en hændelse.
- Wazuh-serveren overvåger også forbindelsen til agenterne. Hvis en agent stopper med at sende logs, kan det indikere et angreb.

En potentiel bekymring er, om en angriber, der kan slukke `rsyslog`, også kan deaktivere Wazuh-agenten. Dette ville være muligt, men Wazuh-serveren overvåger også, om den stadig har forbindelse til agenterne. Hvis en agent Wazuh serveren ikke længere kan opnå forbindelse til en agent, genereres der en hændelse, som kan indikere en kompromittering af systemet.

Refleksion

Refleksionsopgaver:

- Hvorfor bør en server ikke tillade, at en lokal bruger slukker for logging?
- Hvordan kunne du opdage, at en angriber har deaktiveret Rsyslog?
- Hvilke andre metoder kunne en angriber bruge for at skjule sin aktivitet?
- Hvordan kan man beskytte kritiske logfiler mod manipulation?

Links

- Rsyslog Documentation

2025-04-03 05:55:59