Øvelse 39 – Installation af ClamAV og Maldet

Formål

Formålet med denne øvelse er at at installere to open source antivirusværktøjer til Linux: **ClamAV** og **Linux Malware Detect (Maldet)**.
Du lærer at:

- Installere antivirusmotorer til Linux
- Aktivere ClamAVs baggrundsdaemon `clamd`
- Forberede integration mellem Maldet og ClamAV
- Forstå hvordan værktøjerne bruges som supplement til SIEM-baseret detektion

---

Baggrund

Maldet (Linux Malware Detect) er et antivirussystem, som anvender signaturbaseret statisk analyse og automatisk opdatering af signaturdatabaser.
ClamAV er et andet open source antivirusprojekt, oprindeligt designet til e-mailscanning, men bruges også til almindelig filscanning og som motor i andre systemer.

Selvom Linux sjældent rammes af traditionel malware som Windows, er antivirussystemer relevante i fx:

- Delte udviklingsmiljøer
- Webservere og filservere
- Undersøgelse af mistænkelig aktivitet
- Analysemiljøer for reverse engineering

Maldet kan bruge ClamAV som ekstern motor via baggrundsservicen `clamd`, hvilket øger scanningshastigheden betydeligt. For at aktivere denne integration, skal `clamd` være startet korrekt.

Trin-for-trin installation

1. Installer nødvendige værktøjer

Installer ClamAV, baggrundsdaemonen `clamd` og hjælpeværktøjer:

```
sudo apt install clamav clamav-daemon wget inotify-tools ed -y
```

> `clamav-daemon` indeholder `clamd`, som giver hurtigere scanning i Maldet.
> `ed` er en klassisk teksteditor, som Maldet bruger internt.

---

2. Start ClamAV daemon

Start `clamd` som systemservice, så Maldet kan bruge den effektivt:

```
sudo systemctl start clamav-daemon
```

Bekræft, at den kører:

```
sudo systemctl status clamav-daemon
```

---

3. Download og installer Maldet manuelt

1. Skift til `root` for at undgå ejerskabsproblemer:

   ```
   sudo su -
   ```

2. Download den nyeste version af Maldet:

   ```
   wget https://www.rfxn.com/downloads/maldetect-current.tar.gz
   ```

3. Udpak installationsfilerne:

   ```
   tar xzvf maldetect-current.tar.gz
   ```

4. Skift til den udpakkede mappe:

   ```
   cd maldetect-1.6.*
   ```

5. Kør installationen:

   ```
   ./install.sh
   ```

6. Bekræft installationen:

   ```
   maldet --version
   ```

7. Skift tilbage til din almindelige bruger:

```
exit
```

> *Tip:* Når installationen er færdig, kan du teste med:
>
> ```
> echo "test" > test.txt
> sudo maldet -a test.txt
> ```
>
> *Det bekræfter, at Maldet er klar til scanning.*

Nyttige links

- Maldet – GitHub
- Inotify-tools
- ClamAV Daemon

Refleksionsspørgsmål

- Hvad er fordelen ved at kombinere Maldet og ClamAV i et Linux-baseret miljø?
- Hvordan kunne dette setup integreres med en SIEM-løsning som Wazuh?
- Hvorfor er det vigtigt, at antivirusværktøjer til Linux også understøtter automatisk opdatering?

Når installationen er på plads, fortsætter næste øvelse med at konfigurere **overvågning**, **notifikationer** og **automatisk karantæne**.

2025-04-29 07:28:03