Øvelse 41 – Malware-skanning med ClamAV og Maldet

Formål

I denne øvelse skal du teste Maldet og ClamAV ved at placere malware-simuleringsfiler i et overvåget directory. Du vil observere, hvordan systemet automatisk detekterer og fjerner filerne. Øvelsen giver dig praktisk erfaring med detektion, karantæne og analyse af malwarefund på en Linux-server.

Forudsætning

Denne øvelse forudsætter, at:

- `clamav-daemon` (clamd) er startet
- Maldet kører i monitor-mode og overvåger mappen `/home` via systemd

Du kan bekræfte opsætningen med:

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

Baggrund

Når Maldet er konfigureret korrekt (se Øvelse 40), overvåger den specifikke mapper og scanner filer for malware. Når en fil matcher en kendt signatur – fx fra ClamAV eller Maldets egne – vil den blive markeret som inficeret og som standard sat i karantæne.

Til test bruges **EICAR-filer** – sikre testfiler, der simulerer malware ved blot at matche kendte signaturer. De er harmløse og anerkendt som industristandard til test af antivirus.

Trin-for-trin test

1. Download testfiler

Download følgende EICAR-simuleringsfiler til den overvågede `/home`-mappe:

```
sudo wget https://secure.eicar.org/eicar.com -P /home
sudo wget https://secure.eicar.org/eicar.com.txt -P /home
sudo wget https://secure.eicar.org/eicar_com.zip -P /home
sudo wget https://secure.eicar.org/eicarcom2.zip -P /home
```

> Hvis `wget` fejler, kan du alternativt oprette en testfil manuelt:
>
> ```
> echo 'X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*'
> > /home/eicar.txt
> ```

---

2. Vent og kontroller

1. Vent ca. 10–20 sekunder på, at Maldet scanner filerne automatisk.
2. Bekræft, at filerne **ikke længere findes i `/home`** – de er flyttet i karantæne.
3. Åbn logfilen og tjek fund:

   ```
   sudo tail -n 20 /usr/local/maldetect/logs/event_log
   ```

Du bør se linjer som:

```
{hit} malware hit ... found for /home/eicar.com
{quar} malware quarantined from ...
```

Samspil med SIEM systemer

Når Maldet identificerer og fjerner filer, gemmes detaljerede hændelser i logfiler. Disse logfiler kan indgå i en større overvågningsarkitektur – fx ved at blive videresendt til et **SIEM-system** som **Wazuh**.

> Det betyder, at malwarefund fra én maskine kan visualiseres og analyseres centralt – på tværs af hele netværket. SIEM kan udsende alarmer, oprette dashboards og korrelere hændelser med fx loginforsøg eller netværkstrafik.

I et produktionsmiljø giver det mulighed for:

- Hurtig reaktion og overblik ved fund
- Automatisk incident detection og compliance-dokumentation
- Historiske analyser og mønstergenkendelse

Denne øvelse lægger dermed grund for videre logintegration og Blue Team-aktiviteter i fx Wazuh, Elastic eller Graylog.

Nyttige links

- EICAR testfiler
- Maldet – GitHub

Refleksionsspørgsmål

- Hvordan virker Maldets samarbejde med ClamAV i denne øvelse?
- Hvad er fordelene ved at bruge EICAR-filer til test?
- Hvordan kunne du overvåge for malwarefund i Wazuh – fx ved at analysere Maldets logs?
- Kunne du genbruge teknikker fra tidligere øvelser med logovervågning og egne regler?

CIS Controls – Kobling

CIS Control	Titel	Relevans
10 – Malware Defenses	Simuleret test af respons	Du validerer, at detektering og karantæne fungerer korrekt
08 – Audit Log Management	Fund logges	Du analyserer logfiler, som også kan bruges i SIEM-overvågning
06 – Access Control Management	Karantænebegrænsning	Malware fjernes straks, så brugere ikke interagerer med skadelig kode

---

Du har nu testet hele kæden fra installation over konfiguration til aktiv detektion – og kan gå videre til at analysere hændelser centralt eller tilpasse Maldets regler og integration yderligere.

2025-04-11 10:32:41