Øvelse 40 – Konfiguration af Maldet til overvågning og respons

Formål

Formålet med øvelsen er at lære at konfigurere **Linux Malware Detect (Maldet)** til at:

- Overvåge specifikke mapper i realtime
- Udsende e-mailnotifikationer ved fund
- Automatisk sætte inficerede filer i karantæne

Du opnår forståelse for, hvordan Maldet tilpasses et konkret miljø, og hvordan det kan indgå som en del af en automatiseret malwaredetekteringsstrategi.

Baggrund

Maldet gemmer sine indstillinger i konfigurationsfilen `/usr/local/maldetect/conf.maldet`. Her definerer man:

- Hvilke mapper der skal overvåges
- Hvad der skal ske ved fund (logning, notifikation, karantæne)
- Hvem der skal modtage alarmer

I denne øvelse opretter du en separat fil, der indeholder de overvågede stier, og tilknytter den via Maldets konfiguration. Når Maldet kombineres med en aktiv **clamd**-daemon fra ClamAV, opnår du hurtig scanning og automatiseret respons.

> *Hvorfor ekstern sti-fil?*
> Det gør det lettere at ændre eller tilføje mapper uden at redigere hele konfigurationsfilen. Det er især nyttigt i automatiserede eller versionstyrede opsætninger.
>
> Automatiseret detektion og karantæne reducerer behovet for manuel reaktion og øger systemets modstandskraft – især i miljøer med mange brugere eller automatisk filhåndtering.
> Når fund logges og alarmer udsendes, kan output integreres i en SIEM-løsning som **Wazuh** og indgå i en samlet sikkerhedsstrategi.

Forudsætninger

- Du har gennemført installationen i Øvelse 39
- Maldet er installeret og tilgængelig som kommando
- `clamd` fra ClamAV kører som systemservice
- Du arbejder i et testmiljø med root-adgang

Trin-for-trin konfiguration

1. Redigér konfigurationsfilen

1. Åbn Maldets konfigurationsfil:

```
sudo nano /usr/local/maldetect/conf.maldet
```

> *Tip:* Du kan søge efter bestemte felter i `nano` ved at trykke `Ctrl + W` og derefter skrive navnet på variablen, fx `email_alert`.

1. Tilpas overvågning af mapper via ekstern sti-fil:

```
default_monitor_mode="/usr/local/maldetect/monitor_paths"
monitor_paths="/usr/local/maldetect/monitor_paths"
```

2. Aktiver e-mailnotifikationer (tilpas din lokale adresse):

```
email_alert="1"
email_addr="myusername@localhost"
```

3. Aktiver automatisk karantæne ved fund:

```
quarantine_hits="1"
```

---

2. Definér overvågede mapper

1. Opret filen, der definerer mapper til overvågning:

```
sudo nano /usr/local/maldetect/monitor_paths
```

2. Tilføj f.eks. følgende mappe:

```
/home
```

> Du kan tilføje flere linjer, én per mappe, fx `/var/www` til webservere.

---

3. Genstart Maldet

Genstart Maldet for at indlæse den nye konfiguration:

```
sudo systemctl restart maldet
```

Sørg samtidig for, at ClamAVs `clamd` stadig er aktiv:

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

> *Tip:* Maldet scanner automatisk nye filer i overvågede mapper. Du kan tjekke fund i logfilen:
>
> ```
> sudo tail -n 20 /usr/local/maldetect/logs/event_log
> ```

Nyttige links

- Maldet – GitHub

Refleksionsspørgsmål

- Hvilke fordele og ulemper er der ved at aktivere automatisk karantæne?
- Hvordan kan e-mailnotifikationer anvendes i et større sikkerhedssetup?
- Hvilke typer mapper ville det give mening at overvåge i en produktionsserver?
- Hvad sker der, hvis du overvåger en mappe med mange daglige ændringer – og hvilke problemer kan det give?

CIS Controls – Kobling

CIS Control	Titel	Relevans
10 – Malware Defenses	Automatiseret respons	Maldet detekterer og reagerer automatisk på malwarefund i definerede områder
08 – Audit Log Management	Hændelser logges	Fund og hændelser gemmes i Maldets logfiler og kan videresendes til SIEM
16 – Application Software Security	Hærdning via konfiguration	Tilpasning af Maldet sikrer aktiv forsvar af systemområder og applikationsmapper

---

 I næste øvelse tester du opsætningen ved at placere simuleret malware i overvågede mapper og observere Maldets automatiske reaktion.

2025-04-29 07:28:03