Øvelse – Analyse af Windows Event Logs

Information

Windows operativsystemer registrerer løbende hændelser i et centralt logsystem kaldet **Windows Event Log**.

Disse logs anvendes blandt andet til:

- fejlsøgning af systemproblemer
- overvågning af systemets tilstand
- sikkerhedsovervågning
- analyse af sikkerhedshændelser

Logs organiseres i forskellige **logkanaler**, hvor de mest almindelige er:

Log	Formål
Application	Events fra applikationer
System	Events fra Windows systemkomponenter
Security	Login, adgangskontrol og sikkerhedshændelser

Sammenligning med Linux

I tidligere øvelser har du arbejdet med logsystemer i Linux.
Selvom Linux og Windows er forskellige operativsystemer, findes mange af de samme logningsprincipper i begge systemer.

I Linux anvendes typisk to forskellige typer logsystemer:

Linux	Beskrivelse
rsyslog	Traditionelt logsystem der gemmer logs som **tekstfiler** i `/var/log`
systemd journal	Moderne logsystem der gemmer logs i et **struktureret binært format**

Eksempler på klassiske Linux-logfiler:

```
/var/log/syslog
/var/log/auth.log
```

Disse logs kan læses direkte som tekst og analyseres med værktøjer som:

```
grep
tail
cat
```

Windows anvender i stedet et **centralt og struktureret logsystem** kaldet **Windows Event Log**, hvor alle hændelser gemmes som **events** i binære `.evtx` filer.

Disse logs kan blandt andet analyseres via:

- **Event Viewer**
- **PowerShell (Get-WinEvent)**

En vigtig forskel er derfor:

System	Logtype
rsyslog	tekstbaserede logs
systemd journal	strukturerede logs
Windows Event Log	strukturerede events

Denne øvelse introducerer derfor, hvordan Windows organiserer og analyserer logs ved hjælp af **Event IDs**, PowerShell og Windows Event Logs.

Instruktioner

1 Undersøg hvilke logs der findes

Åbn **PowerShell som administrator**.

Kør følgende kommando:

```
Get-WinEvent -ListLog *
```

Denne kommando viser alle event logs på systemet.

Spørgsmål

1. Hvor mange logs findes der på systemet?
2. Hvilke logs virker relevante i forhold til sikkerhed?
3. Er der flere logs end du forventede sammenlignet med Linux?

---

2 Find de logs der er aktive

Ikke alle logs er nødvendigvis aktiveret.

Kør:

```
Get-WinEvent -ListLog * | Where-Object {$_.IsEnabled} | Select LogName,
RecordCount
```

Spørgsmål

1. Hvor mange logs er aktiveret?
2. Hvorfor tror du, at nogle logs er deaktiverede?

---

3 Undersøg System-loggen

Vis de seneste events i **System-loggen**:

```
Get-WinEvent -LogName System -MaxEvents 20
```

Vis udvalgte felter:

```
Get-WinEvent -LogName System -MaxEvents 20 |
Select TimeCreated, Id, LevelDisplayName, Message
```

Spørgsmål

1. Hvilke typer events optræder hyppigst?
2. Find et event med niveau **Warning** eller **Error**.

4️⃣ Undersøg Security-loggen

Security-loggen indeholder information om:

- loginforsøg
- logoff
- adgangskontrol
- ændringer i sikkerhedspolitikker

Kør:

```
Get-WinEvent -LogName Security -MaxEvents 20
```

Vis eventene i et mere læsbart format:

```
Get-WinEvent -LogName Security -MaxEvents 10 |
Format-List TimeCreated, Id, LevelDisplayName, Message
```

Spørgsmål

1. Hvilke Event IDs ser du?
2. Hvilke aktiviteter repræsenterer disse events?

5️⃣ Undersøg login events

Inden du går videre, skal du sørge for at der findes relevante hændelser i loggen.

Lav derfor følgende aktiviteter på systemet:

- log af og på mindst én gang
- lav eventuelt ét loginforsøg med forkert kodeord

Windows registrerer loginhændelser med specifikke **Event IDs**.

Event ID	Betydning
4624	Successful login
4625	Failed login
4634	Logoff

Kør følgende kommando:

```
Get-WinEvent -FilterHashtable @{
    LogName='Security'
    Id=4624,4625,4634
} -MaxEvents 20
```

Vis eventene mere detaljeret:

```
Get-WinEvent -FilterHashtable @{
    LogName='Security'
    Id=4624,4625,4634
} -MaxEvents 10 |
Format-List TimeCreated, Id, Message
```

Spørgsmål

1. Finder du både succesfulde og fejlede loginforsøg?
2. Hvilke brugernavne optræder i loggen?
3. Kan du se forskel på et succesfuldt og et fejlet login i event-beskrivelsen?

---

6 Vurder en sikkerhedshændelse

Find et event med **Event ID 4625** hvis det findes i loggen.

Spørgsmål

1. Hvad fortæller eventet om den fejlede loginhændelse?
2. Hvilke oplysninger i eventet kunne være relevante i en sikkerhedsundersøgelse?
3. Hvilke spor kan hjælpe dig med at vurdere, hvad der er sket?

---

7 Find hvor logs gemmes på systemet

Windows gemmer event logs som **.evtx-filer**.

Navigér til følgende mappe:

```
C:\Windows\System32\winevt\Logs\
```

Spørgsmål

1. Hvor mange logfiler ligger i denne mappe?
2. Hvilke filer svarer til:
   - Security log
   - System log
   - Application log

Refleksionsspørgsmål

1. Hvilke forskelle oplever du mellem loganalyse i Linux og Windows?
2. Hvorfor er logs vigtige i forbindelse med **sikkerhedshændelser**?
3. Hvilke begrænsninger kan der være ved kun at analysere Windows logs?
4. Hvorfor tror du, at man skal være **administrator** for at læse Security-loggen?
5. Hvornår vil PowerShell være særligt nyttigt i forbindelse med loganalyse?

Ekstra opgave (valgfri)

Undersøg en af følgende logs:

- Microsoft-Windows-PowerShell/Operational
- Microsoft-Windows-TerminalServices-LocalSessionManager/Operational
- Microsoft-Windows-Windows Defender/Operational

Eksempel:

```
Get-WinEvent -LogName "Microsoft-Windows-PowerShell/Operational" -MaxEvents
20
```

Spørgsmål

1. Hvilken type aktivitet registrerer denne log?
2. Hvordan kunne denne log være nyttig i en sikkerhedsundersøgelse?
3. Hvilke hændelser i denne log ville du finde særligt interessante, hvis du skulle undersøge mistænkelig aktivitet?

Links

Windows Event Log overview

Get-WinEvent PowerShell documentation

Windows Security auditing and Event IDs

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