Øvelse 25.2 – Opsætning af Wazuh-agent (Gruppeøvelse på Proxmox)

Information

Formålet med denne øvelse er at opnå en grundlæggende forståelse af, hvordan **Wazuh-agenter** fungerer, samt hvordan et **SIEM-system** anvender logfiler til at overvåge og detektere sikkerhedshændelser.

Wazuh er et SIEM-system, der analyserer logdata for potentielle sikkerhedstrusler og hændelser. Når mistænkelige aktiviteter opdages, kan systemet generere sikkerhedshændelser og alarmer.

Ved at opsætte en Wazuh-agent på en Ubuntu-maskine får I indsigt i, hvordan logs indsamles, sendes og analyseres centralt.

I denne øvelse skal I:

- installere en Wazuh-agent på **Target host**
- verificere forbindelsen til en tidligere opsat **Wazuh-server**
- udløse en sikkerhedshændelse ved at oprette en ny bruger

Wazuh arbejdes der videre med senere på semesteret.

Hvis du ønsker et overblik allerede nu, kan du se denne video:

https://www.youtube.com/watch?v=v_6VWB-_wtw

Baggrund

Wazuh overvåger et system ved at analysere loglinjer fra logfiler på den enkelte host.

For at Wazuh kan modtage logdata fra et system, skal der installeres en **Wazuh-agent** på den overvågede maskine.

Agenten:

- indsamler logdata fra systemet
- sender data til Wazuh-serveren
- gør det muligt for serveren at analysere hændelser centralt

Logfiler skaber i sig selv ikke værdi eller øger sikkerheden, medmindre de bliver analyseret og overvåget.
SIEM-systemer som Wazuh automatiserer denne analyse og kan generere hændelser ved mistænkelige mønstre eller handlinger i logdata.

Instruktioner

Øvelsen udføres som gruppearbejde og løses selvstændigt uden for undervisningen.

---

1 Opsætning og afprøvning af Wazuh-agent

I dette trin installerer I en Wazuh-agent på den maskine, der skal overvåges.

1. Installer Wazuh-agenten på **Target host**
   (Ubuntu-maskinen i jeres tidligere opsatte miljø – ikke selve Wazuh-serveren).

Følg opsætningsguiden i Wazuh webinterfacet:

```
Agents management → Summary → Deploy new agent
```

Hvis I ikke kan finde installationsguiden i GUI'en, kan følgende dokumentation bruges: https://documentation.wazuh.com/current/installation-guide/wazuh-agent/wazuh-agent-package-linux.html 2. Verificér at Wazuh-agenten kører korrekt:-

```
sudo systemctl status wazuh-agent
```

Hvis output viser **active (running)**, er agenten startet korrekt.

---

1. Bekræft at Wazuh-agenten har forbindelse til Wazuh-serveren.

Følg guiden her:

https://documentation.wazuh.com/current/user-manual/agents/agent-connection.html#checking-connection-with-the-wazuh-manager

Nu burde agenten være registreret i Wazuh-dashboardet.

---

2 Test af sikkerhedshændelse

I dette trin skal I udløse en sikkerhedshændelse, som Wazuh kan registrere.

1. På den overvågede Ubuntu-maskine (**Target host**) opret en ny bruger:

```
sudo adduser darth
```

1. Log ind på **Wazuh-dashboardet**.
2. Navigér til:

```
Threat hunting → Events
```

1. Verificér at Wazuh har registreret hændelsen for oprettelse af en ny bruger.
2. Udvid hændelsen ved at klikke på pilen til venstre og identificér:
   - hvilken logfil Wazuh-agenten læste fra (feltet **location**)
   - hvilken **MITRE ATT&CK-teknik** der er registreret (T1136 – Create Account)
3. Undersøg hvor mange detaljer om den nyoprettede bruger, der fremgår af hændelsen.

Nu burde I kunne se, hvordan Wazuh analyserer logdata og genererer sikkerhedshændelser.

---

3 Sikkerhedsrefleksion

Diskutér i gruppen:

- Hvorfor er det vigtigt at overvåge ændringer i brugeradministration?
- Hvordan kan en angriber misbruge en nyoprettet bruger?
- Hvordan kan en systemadministrator reagere på en sådan hændelse?
- Hvilke andre hændelser kunne Wazuh anvendes til at overvåge?
- Hvordan kan loganalyse hjælpe med at opdage **indre trusler (insider-angreb)**?

Links

Setting up a Wazuh agent
https://documentation.wazuh.com/current/installation-guide/wazuh-agent/wazuh-agent-package-linux.html

---

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