Opgave 25.2(Gruppe øvelse på proxmox) - Opsætning af Wazuh agent

Formål

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 logs for potentielle sikkerhedstrusler og hændelser, når mistænkelige aktiviteter opdages. Ved at opsætte en Wazuh-agent på en Ubuntu-maskine, kan vi få indsigt i, hvordan logs bliver indsamlet og analyseret.

I denne øvelse skal du installere og konfigurere en Wazuh-agent på Promox **Target host**, validere forbindelsen til en tidligere opsat Wazuh-server, og udløse en hændelse ved at oprette en ny bruger på systemet.

Vi arbejde med Wazuh senere på semesteret. Men hvis du vil havde et overblik kan du se denne youtub video.

Information

Wazuh overvåger et system ved at analysere linjer fra logfiler på det enkelte system. For at Wazuh kan modtage loglinjer fra et system, skal der være en applikation på det overvågede system, som sender disse loglinjer til Wazuh. Denne type applikation kaldes i Wazuh-domænet en **agent**.

Logfiler i sig selv skaber ikke værdi eller øger sikkerheden, medmindre de bliver analyseret og overvåget. SIEM-systemer som Wazuh kan automatisere loganalyse og sende hændelse ved mistænkelige mønstre eller hændelser i en logfil.

Instruktioner

1. Opsætning og afprøvning af Wazuh-agent

1. Lav opsætningen af Wazuh-agenten på **Target host** ved at følge opsætnings guiden i *Wazuh web interfacet* under *Agents management -> summary _ og under summary klik på _Deploy new agent*
   Guiden nederst på denne side viser hvordan du finder opsætnings guiden i web interfacet
2. Efter installationen Verificer, at Wazuh-agenten kører korrekt:

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

3. Hvis output viser "**active (running)**", er agenten startet korrekt.
4. Bekræft, at Wazuh-agenten har forbindelse til Wazuh-serveren ved at følge guiden i afsnittet Using the Wazuh dashboard.

2. Test af sikkerhedshændelse

1. På den overvågede Ubuntu-maskine **Target host**, opret en ny bruger med navnet `darth`:

```
sudo useradd darth
```

2. Log ind på **Wazuh-dashboardet**, og navigér til *Threat hunting*.
3. I *Threat hunting* under *events*, valider at Wazuh har detekteret en hændelse med oprettelse af en ny bruger.
4. Udvid informationen om hændelsen ved at klikke på pilen til venstre for hændelsens linje, og identificér, hvilken logfil Wazuh-agenten læste fra (feltet hedder *location*) samt at **MITRE ATT&CK teknikken T1136**. er den anvendte teknik.
5. Undersøg, hvor mange detaljer om den nye bruger, der fremgår af hændelsen.

3. Sikkerhedsrefleksion

- 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 bruges til at overvåge?
- Hvordan kan loganalyse hjælpe med at opdage **indre trusler** (insider-angreb)?

Bonus opgave

Hvis du er tidligt færdig, kan du vælge en **Proof of concept** gennemgange til wazuh. Wazuh har en guide til dem som kan findes her. Udvælg en af POC'erne og implementer den.
VI vender tilbage til disse POC'er senere

Links

- Setting up a Wazuh agent

2025-04-03 05:55:59