Øvelse 25.1 – Eftermiddag

Opsætning af Wazuh-server på Promox(Selvstændig gruppeøvelse)

Information

Formålet med denne øvelse, er at introducer *Wazuh* som er et *SIEM/XDR* system, der skal anvendes senere på semesteret.
Herudover er formålet at gruppen begynder at selvstændigt arbejde på større projekter, for at skabe rutinering, og opsamling på det tidligere arbejde med *CLI* kommandoer.

I denne øvelse skal gruppen sætte sin første applikation i drift på Proxmox. Senere i dette semester skal vi arbejde med detektering ved hjælp af et SIEM/XDR-system. Til dette bruger vi det open source SIEM/XDR-system, Wazuh. Wazuh er egentlig en distribueret serverapplikation (dvs. den består af flere forskellige komponenter, der kommunikerer over netværket). Men for at gøre arbejdet med Wazuh nemmere skal I blot deploye Wazuh som et såkaldt "single node", hvor alle applikationer eksekveres på en enkelt server.

En Wazuh-server som en single node er meget ressourcekrævende, så brug derfor Ubuntu-serveren med 8 GB RAM og 4 CPU-kerner, som I tidligere har opstillet. (I Proxmox kan I se ressourceforbruget.)

Når Wazuh-serveren er opstillet og afprøvet, skal I skabe et overblik (ikke implementerer) over hvilke porte firewallen bør tillade trafik på, samt hvilke brugerkonti (Linux login) der anvendes til eksekvering af Wazuh server.

Instruktioner

1. Følg quick-start installationsguiden for Wazuh-serveren: Wazuh server quick start
2. Hvis I vil ændre det automatisk genererede password, kan I finde hjælp her: Wazuh - change default password
3. Test at Wazuh-serveren virker ved at tilgå dashboardet fra f.eks. jeres Kali-instans (skridt 2 i guiden).
4. Skab overblik over, hvilke porte Wazuh server anvender: Wazuh architecthure

Vær opmærksom på, at når I eksekverer som single node, anvendes både Wazuh-serveren, Wazuh-indexeren og Wazuh-dashboardet

I skal ikke implementere firewallregler endnu. Vi venter, indtil I har sat agentapplikationer op, som kommunikerer med Wazuh. Så bliver det nemmere for jer at fejlfinde.

1. Anvend kommandoen: `ps aux | grep wazuh` for at se, hvilke processer der eksekveres i forbindelse med Wazuh, og hvilken bruger de eksekveres med.
2. Overvej om alle brugerne, der anvendes, er hensigtsmæssige.

I skal ikke forsøge at ændre brugeren, der anvendes – blot observer.

1. Lav dokumentation for jeres nuværende opsætning af hosts på Proxmox.

Et tænkt eksempel kunne være:

Host	Beskrivelse	Services	IP Adresse	Hostname	CPU Core
Wazuh server	Host der kører Wazuh SIEM/XDR systemet	Wazuh SIEM, XDR	192.168.1.10	wazuh-server	4
Target host	Host der overvåges af Wazuh	OpenSSH, Wazuh Agent	192.168.1.11	target-host	2
Kali	Kali Linux til penetration testing	Kali Tools, OpenSSH	192.168.1.12	kali-server	2
Proxmox	Host der kører Proxmox Virtualization	Proxmox VE, Web Interface	192.168.1.13	proxmox-server	8
OpnSense VM	OpnSense router/firewall	OpnSense Firewall, Router	192.168.1.1	opnsense-vm	2

Eksemplet viser en dokumentation, som fungerer som et **supplement til jeres netværksdiagram** og giver et klart overblik over opsætningen.

Tabellen **skal løbende opdateres**, da systemkomponenterne kan ændre sig i takt med, at nye tjenester installeres eller eksisterende konfigurationer opdateres.

Denne type dokumentation understøtter **Asset Management**, og er afgørende for:

- fejlfinding
- systemopdateringer
- sikkerhedsgennemgange
- onboarding af nye teammedlemmer

Links

- Wazuh documentation

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