Eftermiddags opgave uge 09 - Opsætning at Ubuntu server på Proxmox (Gruppe opgave)

Information

Senere på semesteret skal vi arbejde med SIEM/XDR-systemet Wazuh, som er meget ressourcekrævende. Et SIEM/XDR-system kan bruges til at overvåge hændelser og reagere på dem. Wazuh er baseret på et såkaldt Host-based Intrusion Detection System (HIDS), men det er meget modulært og kan derfor integreres med netværksbaserede indtrængningsdetekteringssystemer såsom Suricata, som OpenSense anvender.

Wazuh kræver betydelige ressourcer, hvilket de fleste bærbare computere ikke kan håndtere. Derfor skal gruppen opsætte en konfiguration med Wazuh på Proxmox-platformen. I dag skal gruppen opsætte 2 Ubuntu-servere på Proxmox: én til at hoste Wazuh og én Ubuntu-server, som Wazuh skal overvåge. I dag skal der kun opsættes Ubuntu.

Ubuntu-server-VM'erne, der skal opsættes på Proxmox, skal have følgende specifikationer:

Host	Description	CPU Cores	HDD	RAM
Wazuh server	Host running Wazuh SIEM/XDR system	4	80GB	8GB
Target host	Host being monitored by Wazuh	2	30GB	4GB

Med undtagelse af oprettelsen af VM maskinen på Promox, så er processen for installation ubuntu server den samme som i tidligere har prøvet. I kan finde en guide til opsætning af Ubuntu på Proxmox her

Husk at VM'ernes netværk adapter skal være på vmbr10 bridge. Altså samme netværk som opensense. I skal blot anvende DHCP

I faget systemsikkerhed, dækkes netværks opsætning(Det gør det i netværk og kommunikations sikkerhed). Dette betyder at den segmentering i placer jeres server i, er noget i selv tager stilling til

Instruktioner

1. Opret begge Ubuntu server VM'er på Proxmox, jvf overstående specifikationer.
2. Opret en bruger til hvert gruppe medlem på VM'erne.
3. Giv hvert gruppemedlems bruger `sudo` rettigheder, ved at tilføje dem til sudo gruppen.
   Du kan finde vejledning her
   Vær opmærmsom på at tutorialen ikke sætter netværk interfacet til det interface i skal bruge

Det er god praksis ikke at tillade `root` login på sin VM, og gruppen bør derfor også sikre at der ikke længere kan logges ind som root. På Ubuntu server kan dette gøres med kommandoen `sudo passwd -l root`.

2025-04-03 05:55:59