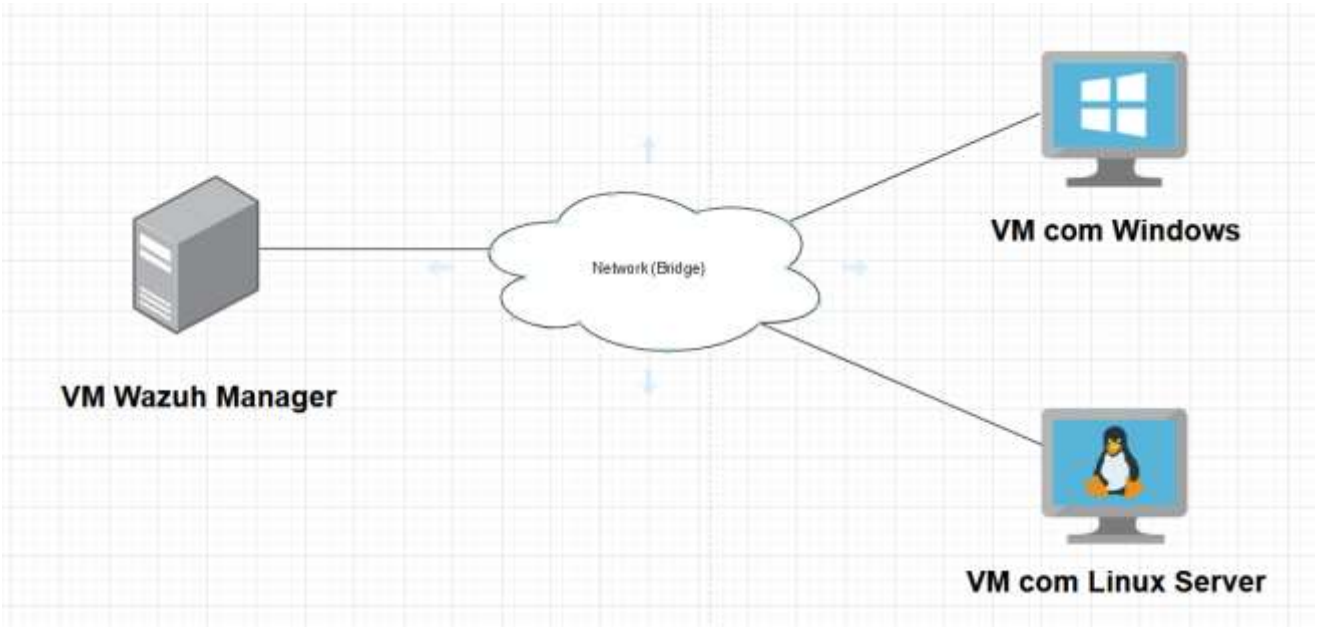
TRABALHO DE AVALIAÇÃO

Trabalho de avaliação de Cibe Segurança Ativa.

O trabalho deve ser realizado em grupos de 2 elementos e se necessário um grupo de 3 elementos.

O trabalho consiste em montar um esquema semelhante ao abaixo com recurso a máquinas virtuais, usando o virtual box por exemplo.



O trabalho consiste em proceder à instalação de um servidor com o Wazuh e duas máquinas (Windows e Linux) com os agentes do Wazuh para serem monitorizadas. Na máquina Linux instale o servidor apache2.

O Wazuh é um software de segurança *open-source* projetado para monitorizar e analisar a segurança de sistemas e redes de computadores. Foi desenvolvido para ajudar as organizações a detetar e responder a ameaças de segurança cibernéticas em tempo real, bem como para fornecer informações sobre a postura de segurança geral de suas infraestruturas.

Principais recursos do Wazuh:

1. Deteção de Intrusões: O Wazuh é conhecido por sua capacidade de deteção de intrusões, identificando atividades suspeitas ou potencialmente maliciosas em sistemas e redes, como tentativas de login fracassadas, reconhecimentos de portas, atividades anômalas de utilizadores, entre outras.

2. Monitorização de Logs: Coleta, analisa e normaliza *logs* de várias fontes, como *logs* de sistemas operativos, aplicativos, firewalls e dispositivos de rede, para ajudar na deteção de ameaças.
3. Correlação de Eventos: O Wazuh utiliza regras predefinidas e personalizáveis para correlacionar eventos de log e identificar padrões de atividade maliciosa ou suspeita.
4. Alertas em Tempo Real: Quando uma ameaça é detetada, o Wazuh gera alertas em tempo real, permitindo que as equipas de cibe segurança respondam rapidamente às ameaças.
5. Integração com outras Ferramentas: Ele pode ser integrado com outras ferramentas de segurança, como SIEM (Security Information and Event Management) e IDS/IPS (Intrusion Detection System/Intrusion Prevention System), para uma visão abrangente da postura de segurança.
6. Gestão de Vulnerabilidades: O Wazuh também pode ser usado para identificar vulnerabilidades em sistemas, ajudando a priorizar as correções.
7. Personalização: Os utilizadores podem criar regras personalizadas para se adequar às necessidades específicas de segurança de sua organização.

O Wazuh é uma ferramenta poderosa para ajudar as organizações a manterem a segurança de seus sistemas e redes, oferecendo uma maneira eficaz de monitorizar, detetar e responder a ameaças informáticas. É uma opção popular para empresas e organizações que buscam melhorar sua postura de segurança e garantir a conformidade com regulamentações de segurança cibernética

Sugestão:

- Usar o Ubuntu para a instalação da máquina que vai ter o (Wazuh como servidor);
- Utilizar o método de instalação QuickStart;
- Colocas todas as placas de rede das VM em modo bridge para facilitar as configurações de rede.

O resultado final do trabalho consiste em apresentar um relatório em que descrevem os vários passos pedidos:

- Descrever e documentar a instalação das 3 VM
- Listar as diversas vulnerabilidades detetadas
- Corrigir 15 vulnerabilidades em cada máquina com o agente Wazuh
- Na máquina Linux dar prioridade a falhas que possam existir relacionadas com o apache2
- Como conclusão identificar as vantagens e desvantagens deste tipo de software

O trabalho deve ser submetido no TEAMS até ao próximo dia 18/09/2023 até às 23h30.

Bom trabalho! ☺