Insper

Roteiro 2

Plataforma de Segurança - Wazuh

Objetivo

Objetivo é que o aluno possa instalar e configurar um sistema para gestão de ameaças e compliance.

Faça a instalação do Wazuh por meio de sua documentação:

https://documentation.wazuh.com/current/installation-guide/index.html

Requisitos mínimos para instalação:

- Ubuntu 12 ou superior.
- 4 GB de RAM
- 2 cores CPU

Este roteiro tem como objetivo permitir ao aluno conhecer de forma prática algumas ferramentas para o monitoramento de ameaças tecnológicas. O Wazuh é uma ferramenta open source para a detecção de ameaças, monitoramento de segurança, resposta a incidentes e conformidade regulatória. Ele pode ser usado para monitorar terminais, serviços em nuvem e contêineres e para agregar e analisar dados de fontes externas.

Lembrando que neste ambiente deverão estar a aplicação e o jump server ou outro similar.

Insper

Perguntas iniciais

1) O que é e quais são as características de um SIEM?

2)Em que situações o grupo instalaria um SIEM?

3) Qual a diferença de um SIEM para um Gerenciador de LOG (SYSLOG)?

Tarefa

- Configure o Wazuh para atender as suas necessidades de análise de vulnerabilidades.
- colocar elastic IP no servidor Wazuh e configurar um subdomínio com o nome "monitoramento" para este servidor.
- Configure o Wazuh para detectar tentativas de brute force ssh nos servidores.
- Configure os alertas necessários para atender as suas necessidades de projeto.
- Insira o servidor de aplicação em um grupo com regras WEB.
- Faça uma trilha de auditoria indicando quais regras estão aplicadas em cada servidor.
    - Configuração de envio de alertas por e-mail.
    - Logs do cloudwatch encaminhados e tratados pelo Wazuh.

Perguntas

4) O que é o OSSEC?

5) Qual a função do Kibana no Wazuh?