📄 RELATÓRIO TÉCNICO

IMPLEMENTAÇÃO DO WAZUH (SIEM / XDR)

1️⃣ Instalação e Montagem do Ubuntu Server

1.1 Objetivo

Implementar um servidor Linux dedicado para atuar como **plataforma central de monitoramento de segurança**, utilizando o Wazuh.

1.2 Ambiente Utilizado

- **Sistema Operacional:** Ubuntu Server LTS
- **Versão:** 22.04 LTS
- **Arquitetura:** x86_64
- **Ambiente:** Laboratório / VM
- **Função:** Servidor Wazuh (Manager + Indexer + Dashboard

]

1.3 Procedimentos Realizados

- Instalação do Ubuntu Server via ISO oficial
- Configuração de:
    - Hostname
    - Endereço IP estático
    - DNS
- Atualização do sistema:

```
sudo apt update && sudo apt upgrade -y
```

1.4 Justificativa Técnica

O Ubuntu Server foi escolhido por ser:

- Estável
- Amplamente utilizado em ambientes corporativos

- Totalmente compatível com o Wazuh

---

2 Instalação do Wazuh Server

2.1 Objetivo

Instalar e configurar o **Wazuh Server** para atuar como:

- SIEM (Security Information and Event Management)
- HIDS/XDR (Host Intrusion Detection & Response)

2.2 Componentes Instalados

- **Wazuh Manager** – correlação e análise de eventos
- **Wazuh Indexer (OpenSearch)** – armazenamento e indexação
- **Wazuh Dashboard** – visualização e análise gráfica

2.3 Método de Instalação

Instalação utilizando o script oficial do Wazuh:

```
curl -sO https://packages.wazuh.com/4.12/wazuh-install.sh
sudo bash wazuh-install.sh -a
```

2.4 Verificações Pós-instalação

- Validação dos serviços:

```
systemctl status wazuh-manager
systemctl status wazuh-indexer
systemctl status wazuh-dashboard
```

- Acesso ao Dashboard via navegador:

```
https://<IP_DO_SERVIDOR>
```

2.5 Resultado

Servidor Wazuh instalado e operando corretamente, com acesso ao painel de gerenciamento e visualização de eventos.

---

3 Servidor no Ar

3.1 Estado do Serviço

- Todos os serviços ativos e funcionando
- Comunicação entre Manager, Indexer e Dashboard validada

3.2 Funcionalidades Ativas

- Detecção de vulnerabilidades
- Threat Hunting
- File Integrity Monitoring (FIM)
- Compliance (CIS Benchmarks)
- Mapeamento MITRE ATT&CK

3.3 Benefícios

- Monitoramento centralizado
- Visibilidade de segurança em tempo real
- Base para resposta a incidentes

---

4 Configuração do Agent

4.1 Objetivo

Integrar endpoints ao Wazuh Server para coleta de:

- Logs
- Eventos de segurança
- Alterações de arquivos
- Dados de inventário

4.2 Ambiente do Agent

- **Sistema:** Windows 10 Home
- **Versão:** 10.0.19045
- **Função:** Endpoint monitorado

4.3 Instalação do Agent

- Download do agente Wazuh para Windows
- Instalação do serviço
- Registro do agente no servidor Wazuh utilizando chave de autenticação

4.4 Validação

- Agent com status **Active**
- Comunicação confirmada com o servidor
- Recebimento de eventos no Dashboard

4.5 Funcionalidades Monitoradas

- Vulnerability Detection
- FIM (File Integrity Monitoring)
- MITRE ATT&CK mapping
- Logs de segurança do Windows

🎯 Conclusão

A implementação do Wazuh permitiu a criação de um **ambiente de monitoramento de segurança completo**, simulando um **SOC real**, com capacidade de:

- Detecção preventiva de vulnerabilidades
- Identificação de comportamentos maliciosos
- Auditoria de conformidade
- Monitoramento contínuo de endpoints

Este projeto demonstra conhecimentos práticos em:

- Linux Server
- Segurança da Informação
- SIEM / XDR
- Monitoramento e resposta a incidentes