Projeto Integrador IV

Sistema de Detecção de Intrusão

ARTHUR DA ROCHA PANETTO BLANDINO

ALEJANDRO CRISTH MENDONÇA MAGALHÃES

DANIEL JOSÉ HOLZ

LUCAS MIRANDA NEVES

Estrutura do Projeto

1. **Treinamento e Detecção Anômala (Isolation Forest com CICIDS2017)**
    - **Justificativa:** O CICIDS2017 é um dataset muito utilizado para avaliar intrusões em rede, contendo tráfegos normais e maliciosos simulados. O **Isolation Forest** é eficaz na detecção de anomalias por não necessitar de dados rotulados e pode ser treinado para identificar tráfegos suspeitos.
    - **Processamento de Dados:**
        - Carregar e processar o dataset CICIDS2017 (features como IP, portas, protocolos, etc.).
        - Treinar o modelo com **Isolation Forest** para classificar tráfegos normais vs suspeitos.
2. **Integração com a API do Shodan**
    - **Objetivo:** Enriquecer a detecção de intrusões com informações adicionais fornecidas pelo Shodan, como:
        - **IP Geolocalização:** Verificar a origem do IP e localização geográfica (continente, país, cidade).
        - **Portas Abertas e Serviços Expostos:** Quais serviços estão expostos pelo IP (SSH, HTTP, etc.).
        - **Histórico de Vulnerabilidades:** Se o IP está associado a alguma vulnerabilidade conhecida.

- **Sugestão de Parâmetros para o Shodan:**
    - Endereço IP do suspeito (obrigatório).
    - País ou região para entender se o tráfego está vindo de uma região suspeita.
    - Serviços/portas abertas que podem indicar tentativas de intrusão.
    - Qualquer possível vulnerabilidade (CVE) associada ao IP.
- **Relatório Gerado:**
    - Detalhar os resultados da busca no Shodan, como:
        - Informações sobre o IP.
        - Serviços em execução.
        - Vulnerabilidades encontradas.
        - Geolocalização (se relevante).

3. **Geração de Relatório**
    - **Conteúdo do Relatório:**
        - **Resumo da Detecção:** Relatar a data e hora do tráfego detectado, endereço IP suspeito e protocolo utilizado.
        - **Análise do Shodan:** Apresentar as informações coletadas pela API do Shodan, como vulnerabilidades e serviços.
        - **Recomendações:** Com base nos dados, sugerir medidas de mitigação ao cliente (por exemplo, bloquear o IP ou verificar possíveis vulnerabilidades nos sistemas internos).

Plano de Trabalho (para a Entrega 1)

1. Justificativa do Projeto

- O aumento nas ameaças cibernéticas, com ataques como DDoS, malware, e exploits, requer que empresas e organizações possuam um sistema robusto de detecção e resposta a intrusões.
- **Detecção de Intrusões** com **ML** é uma das formas mais eficientes de lidar com a crescente sofisticação desses ataques, enquanto APIs como a **Shodan** ajudam a contextualizar as ameaças.

2. Escopo do Projeto

- O sistema será capaz de:
    1. Detectar tráfegos anômalos utilizando o **Isolation Forest**.
    2. Consultar a **API do Shodan** para enriquecer os dados do tráfego anômalo.
    3. Gerar um **relatório detalhado**, explicando a ameaça detectada e possíveis mitigações.
- **Não está no escopo:**
    - A resposta automatizada (como bloqueios automáticos), apenas a detecção e geração de relatórios.

3. Plano de Trabalho

- **Semana 1-2:**
    - Exploração e limpeza do dataset **CICIDS2017**.
    - Treinamento inicial do modelo **Isolation Forest**.
- **Semana 3-4:**
    - Integração com a API do **Shodan**.
    - Testes com o tráfego detectado para validar o enriquecimento de dados.
- **Semana 5-6:**
    - Desenvolvimento do frontend para visualizar os relatórios.
- **Semana 7-10:**
    - Implementação final e ajustes no backend (incluindo a geração de relatórios automáticos).

- **Semana 11-12:**
    - Testes finais e preparação para a entrega.