Análise de Malware

Relatório TP2

Integração de Sistemas de Informação

Aluno: Adelino Daniel da Rocha Vilaça - a16939
Docente: Professor Luis Gonzaga Martins Ferreira

Licenciatura em Engenharia de Sistemas Informáticos (PL)

3º ano

Barcelos | Dezembro, 2024

Lista de Abreviaturas e Siglas

Índice de Figuras

Índice

1. Enquadramento / Tema

Este trabalho foi realizado no âmbito da Unidade Curricular de Integração de Sistemas de Informação, do curso de Engenharia de Sistemas Informáticos (Pós-Laboral). O objetivo deste segundo trabalho prático é o desenvolvimento de competências utilizando arquiteturas REST/SOAP, relativamente a este trabalho será REST, baseando-se no desenvolvimento de processos de interoperabilidade entre sistemas, assentes em serviços web.

O tema do projeto foca-se na Análise de Malware em ficheiros e URLs, utilizando a API do VirusTotal para detectar assinaturas de Malware. Este sistema permite que utilizadores façam upload de ficheiros e URLs para análise, com resultados detalhados sobre a presença de ameaças. A aplicação tem grande utilidade no contexto da Cibersegurança, auxiliando na identificação de ficheiros e websites maliciosos antes que possam comprometer sistemas ou dados sensíveis. Além disso, a análise de Malware automatizada contribui para a melhoria da segurança digital, oferecendo uma ferramenta prática e eficaz para a prevenção de ataques, podendo ser usada por qualquer pessoa mesmo sem conhecimentos técnicos na área.

Ao longo do projeto provavelmente irão ser feitas algumas alterações a nível estrutural para acrescentar/reduzir serviços para que não ponham em causa a finalização deste segundo trabalho e por consequentemente a cadeira de ISI.

2. Problema

O principal objetivo deste trabalho é demonstrar e resolver problemas relacionados com a análise de ficheiros e URLs para a deteção de Malware. O sistema visa permitir o envio de ficheiros e URLs por parte dos utilizadores, sendo analisados com a API do **VirusTotal**, que identifica assinaturas de Malware presentes. O desafio principal envolve a integração eficiente da API externa, a organização e análise dos resultados obtidos, bem como a gestão de dados sensíveis, garantindo a segurança e eficácia no processo de deteção.

3. Modelo de Entidade Relação (ER / Data Model)

O sistema permite analisar ficheiros e URLs submetidos por utilizadores para deteção de Malware, utilizando a API do VirusTotal. Cada utilizador pode enviar múltiplos ficheiros ou URLs (dentro do limite diário da API ou de acordo com o tipo de Role que o mesmo tem atribuído), que são analisados, com os resultados registados nas tabelas FileAnalysis e UrlAnalysis.

As "signatures" de Malware detetadas são associadas às análises através de tabelas intermediárias (FileAnalysisMalware e UrlAnalysisMalware). Assim o modelo de dados garantirá uma estrutura normalizada e eficiente para investigar as análises e as assinaturas de Malware relacionadas.

A tabela Role é utilizada para definir os diferentes papéis dos utilizadores, como Admin e User, permitindo que o sistema controle as permissões de acesso e as limitações de utilização da API.

Além disso, a tabela UserSession é utilizada para gerir as sessões dos utilizadores. Cada vez que um utilizador se autentica no sistema, uma nova entrada é criada na tabela UserSession, por sua vez registando o novo token de autenticação.

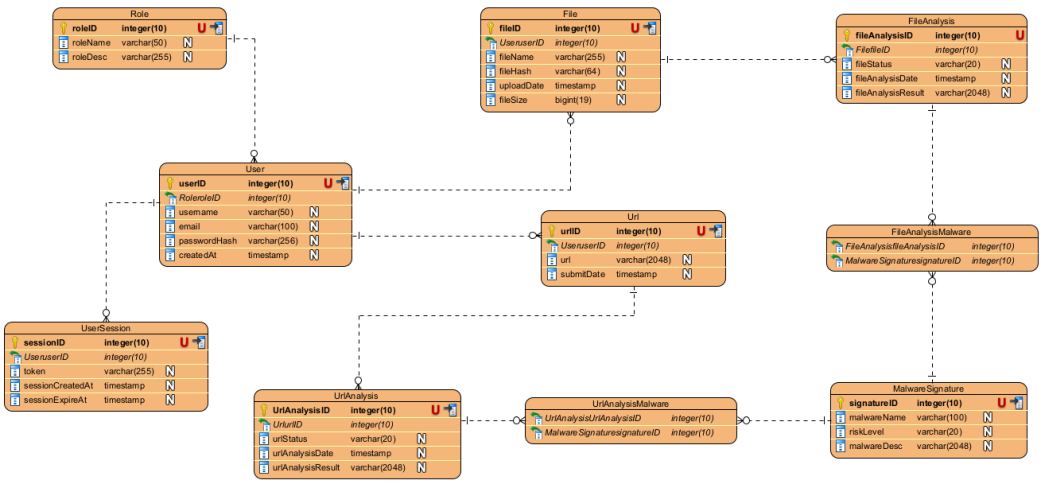

Figura 1 - Visualização do Modelo de Entidade Relação do Projeto

4. Arquitetura

4.1. Serviço de Submissão de Ficheiros para Análise

Objetivo: Permitir que os utilizadores façam upload de ficheiros para análise de Malware.

Descrição: O utilizador envia um ficheiro através do serviço, que será então enviado à API da VirusTotal para análise, retornando os resultados ao mesmo.

Possível Endpoint:

POST /files/upload

Input: Ficheiro a ser analisado (binário / base64).

Output: ID do ficheiro gerado pela VirusTotal para consultas futuras e a confirmação de que o ficheiro foi enviado para análise (Status).

API: Através do endpoint *file/scan* ou *file/upload* da API do VirusTotal, enviamos o ficheiro para ser analisado e para obter uma hash para monitorizar o status da mesma.

4.2. Serviço de Consulta de Resultados após Análise de Ficheiros

Objetivo: Permitir que os utilizadores consultem os resultados da análise de um ficheiro previamente submetido.

Descrição: O utilizador pode consultar os resultados da análise de um ficheiro com base no ID que foi retornado após o envio para a API do VirusTotal.

Endpoint sugerido:

GET /files/{fileId}/results

Input: ID do ficheiro (após upload).

Ouput: Normalização do JSON com Malware detectado (por exemplo, o nome do Malware, a Classificação da Ameaça, o Número de Antivírus que possivelmente detetaram o ficheiro malicioso, etc).

API: Através do endpoint *file/report* da API do VirusTotal, consultamos os resultados da análise de um ficheiro específico, incluindo detalhes sobre as assinaturas de Malware que foram identificadas (JSON)

4.3. Serviço de Análise de URLs com Malware

Objetivo: Permitir que os utilizadores verifiquem se um URL está associado a algum tipo de Malware ou atividades maliciosas.

Descrição: O serviço permitirá que os utilizadores forneçam um URL específico para análise e que retornem os resultados sobre a presença de algum tipo de Malware seja ele Phishing, Ransomware, Worms, etc, atividades maliciosas associadas a esse URL.

Endpoint sugerido:

POST /urls/analyze

Input: URL a ser analisado.

Saída: ID da análise e do Status de verificação.

API: Através do endpoint *url/scan* para submeter o URL e obter um ID de análise, depois, usaríamos o endpoint *url/report* para obter os resultados dessa mesma análise.

4.4. Serviço de Consulta de Assinaturas de Malware Conhecidas

Objetivo: Fornecer um serviço que permita a consulta por assinaturas de Malware específicas, verificando se o ficheiro analisado contém alguma assinatura conhecida.

Descrição: O utilizador pode consultar se um ficheiro (ou URL) corresponde a uma assinatura de Malware específica, ou verificar a lista de Malware conhecidos.

Endpoint sugerido:

GET /malware/signatures/{signatureId}

Input: ID da assinatura de Malware ou ID do ficheiro (dependendo da consulta).

Output: Detalhes sobre a assinatura, como o nome do Malware, Classificação de Risco e Histórico de Deteção.

API: O serviço pode ser baseado em informações extraídas dos relatórios de análise de ficheiros ou URLs e suas assinaturas associadas.

4.5. Serviço de Histórico de Análises (para um user específico) (Validar)

Objetivo: Manter um histórico das análises feitas pelo utilizador e permitir consultas sobre ficheiros ou URLs analisados anteriormente.

Descrição: O utilizador pode consultar um histórico de todos os arquivos ou URLs que foram submetidos para análise e verificar os resultados anteriores.

Endpoint sugerido:

GET /users/{userId}/history

Input: ID do utilizador.

Output: Lista de IDs dos ficheiros e URLs analisados, com detalhes de quando foram analisados e o status dessa análise.

API: A interação seria com a Base de Dados na Cloud (validar) que registaria os IDs dos ficheiros e URLs enviados à API do VirusTotal e os resultados associados.

4.6. Serviço de Pesquisa de Arquivos ou URLs por Hash (Validar)

Objetivo: Permitir que o utilizador faça uma pesquisa direta pela hash (MD5, SHA1, ou SHA256) de um ficheiro para verificar rapidamente se ele já foi analisado pelo VirusTotal.

Descrição: O serviço permite que o utilizador forneça uma hash e verifique se essa assinatura já foi analisada.

Endpoint sugerido:

GET /files/{hash}/status

Entrada: Hash do ficheiro (MD5, SHA1 ou SHA256).

Saída: Status da análise (se foi analisado anteriormente e, em caso afirmativo, apresenta os resultados).

API: Através do *endpoint file/report* ou *url/report* para consultar rapidamente o status de um ficheiro, caso ele já tenha sido analisado previamente.

5. Conclusão e Trabalhos Futuros (Concluir no Relatório Final)

6. Bibliografia

Não existem origens no documento atual.