Análise e identificação de Malwares através do tráfego de rede

Fernando A. R. Finardi
RA: 13165295

Introdução do Sistema

- Sistema Web para análise de malwares
- Analisa malwares de windows
- Análise dinâmica
- Faz uso de SandBox para a análise
- Para uso de especialistas

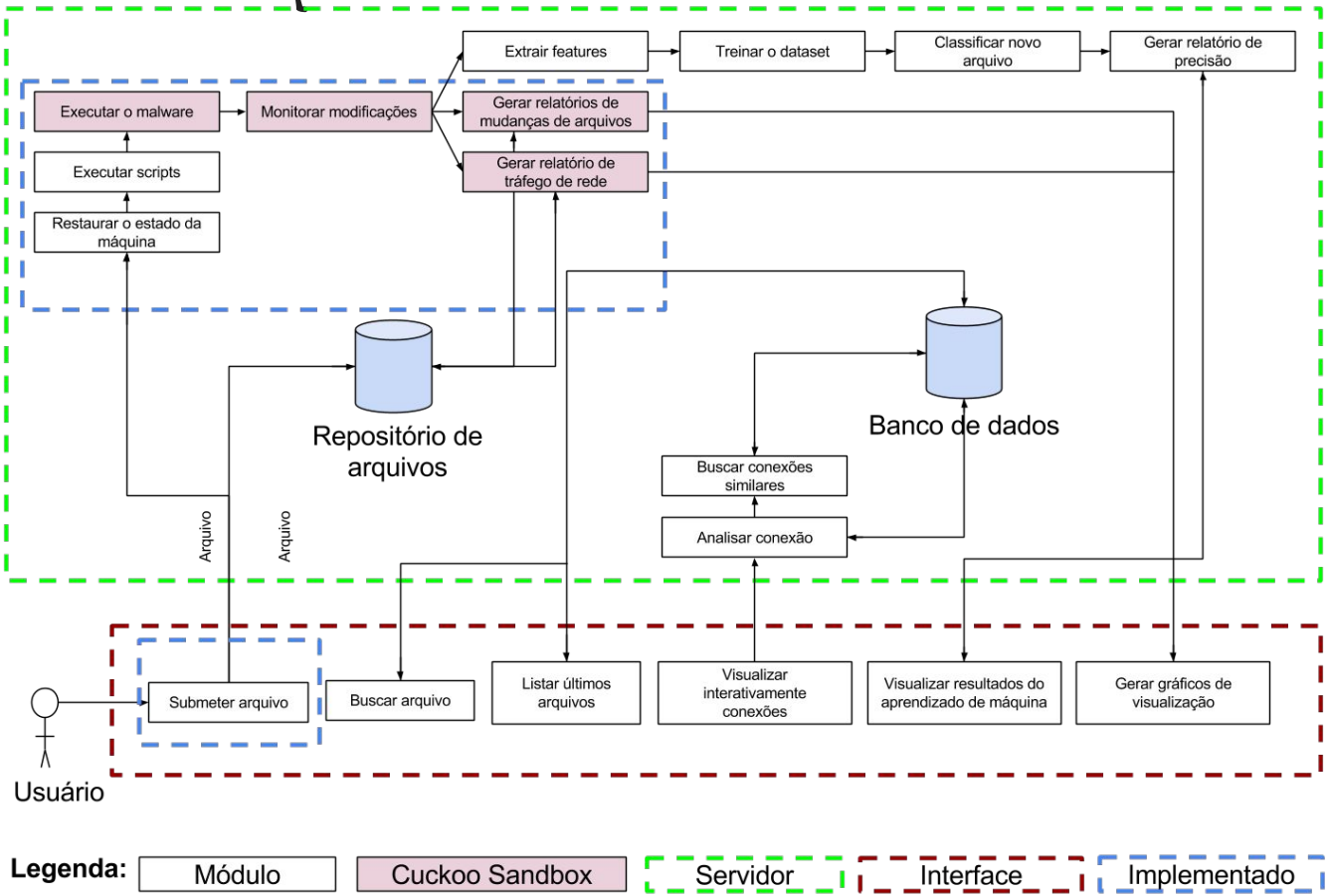
Objetivos

- Diminuição do tempo e trabalho no processo de análise, através da automação de processos
- Prover ao analista resultados relevantes sobre o malware
- Melhorar a qualidade da análise através de técnicas de visualização de dados e interatividade

Plano de Avaliação

- Comparação entre o tempo médio de análise obtido através do anterior processo de análise e o tempo médio de análise obtido através do novo artefato proposto
- Questionário ao analista de malware, o qual terá o objetivo de comparar a qualidade do artefato proposto com o processo anterior de análise

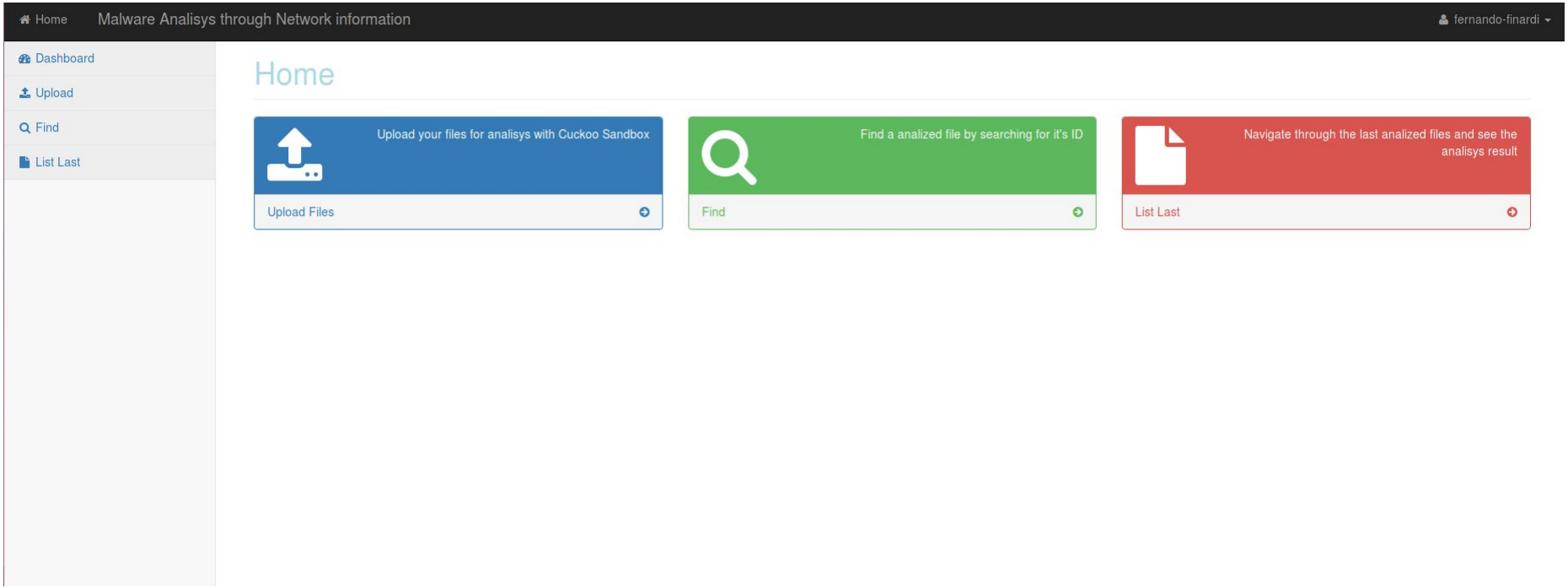
Diagrama de Arquitetura



Cronograma

	Cronograma do semestre	**Foi feito**	**Restante do trabalho**
Interface Web	-Submissão de arquivo -Listar os últimos últimos arquivos analisados -Buscar arquivo -Visualizar resultados em forma de texto	-Submissão de arquivo -Listar os últimos últimos arquivos analisados (incompleto) -Buscar arquivo (incompleto) -Visualizar resultados em forma de texto	-Visualizar resultados do aprendizado de máquina -Visualizar interativamente conexões -Visualizar resultados em forma de gráficos com relação de tempo -Gerar gráficos de visualização
Máquina Virtual	-Executar scripts -Restaurar o estado da máquina	-Executar scripts -Restaurar o estado da máquina	
Aprendizado de máquina			-Treinar o dataset -Classificar novo arquivo -Gerar relatório de precisão dos algoritmos
Análise dinâmica	-Executar o malware -Monitoramento das modificações -Geração de relatórios	-Executar o malware -Monitoramento das modificações -Geração de relatórios	
Análise de conexões			-Analisar conexões -Buscar conexões similares no banco de dados

DEMO


Home
Malware Analisys through Network information
fernando-finardi
Dashboard
Upload
Find
List Last
Home
Upload your files for analisys with Cuckoo Sandbox
Upload Files
Find a analized file by searching for it's ID
Find
Navigate through the last analized files and see the analisys result
List Last