webTEA: UMA FERRAMENTA PARA ANÁLISE E INTERPRETAÇÃO DE INCIDENTES DE SEGURANÇA

SBSEG – 2008

Eduardo de Oliveira

<eduardo@f1solucoes.com.br>

Leonardo Lemes Fagundes

<llemes@unisinos.br>

São Leopoldo, 03 de Setembro de 2008.

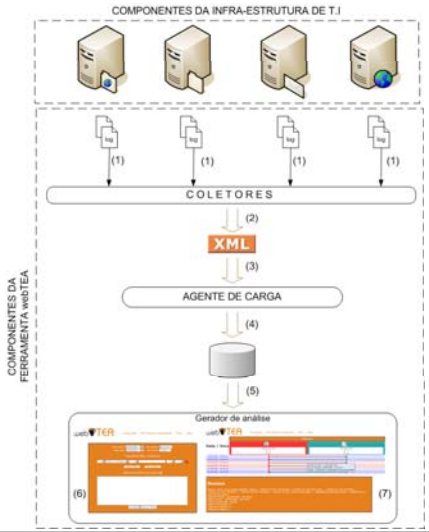
Introdução

- Objetivos
  - Desenvolvimento de uma ferramenta com as seguintes características:
    - Leitura e normalização de diferentes formatos de *logs*;
    - Armazenamento dos dados normalizados em um Banco de Dados;
    - Análise e interpretação dos dados por meio de um diagrama de seqüência (ordem cronológica dos eventos)#
    - Com livre distribuição (GPL).

"Um dos grandes problemas no domínio da ciência e outras áreas é a enorme quantidade de dados que são coletados ou gerados, e propõe-se que eles devam ser convertidos e apresentados por algum sistema de visualização capaz de facilitar a sua compreensão e interpretação"
[OWEN, 2007a].

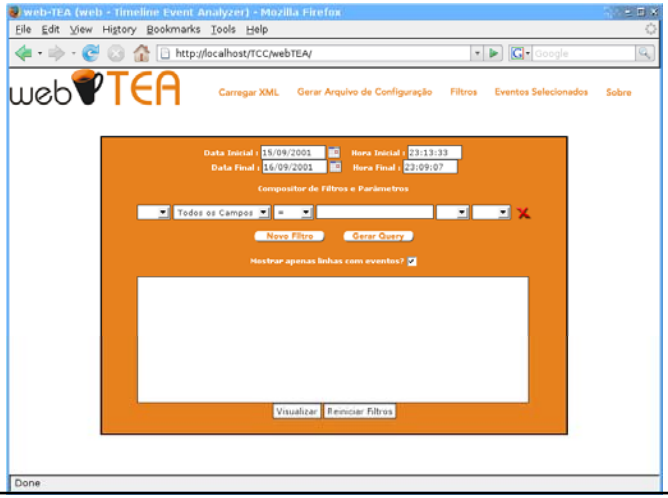
webTEA : web-based Timeline Event Analyzer

- Arquitetura



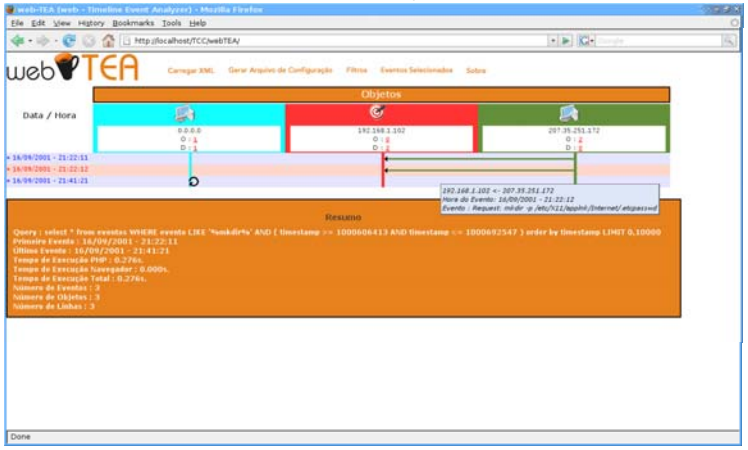
webTEA : web-based Timeline Event Analyzer

- Gerador de análise => Compositor de Filtros



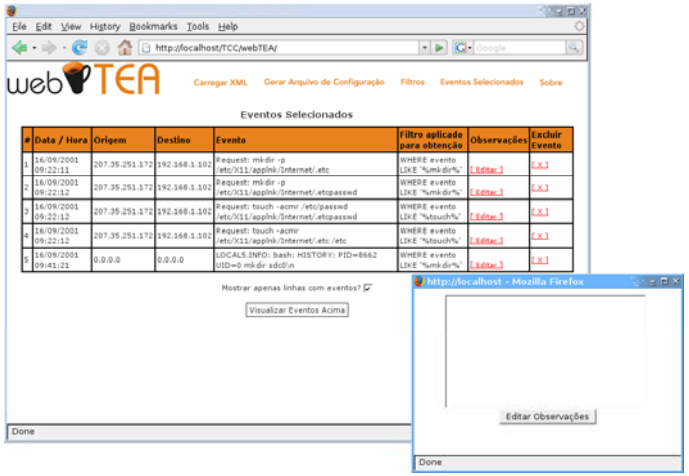
webTEA : web-based Timeline Event Analyzer

- Gerador de análise => Interface de visualização e análise



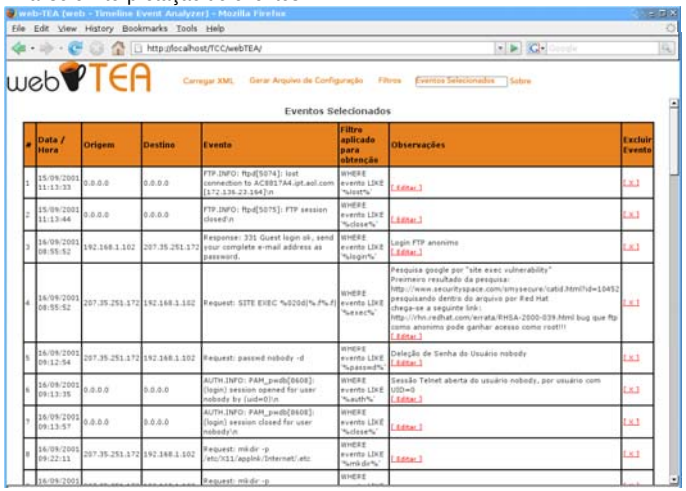
webTEA : web-based Timeline Event Analyzer

- Gerador de análise => Interface de eventos Selecionados



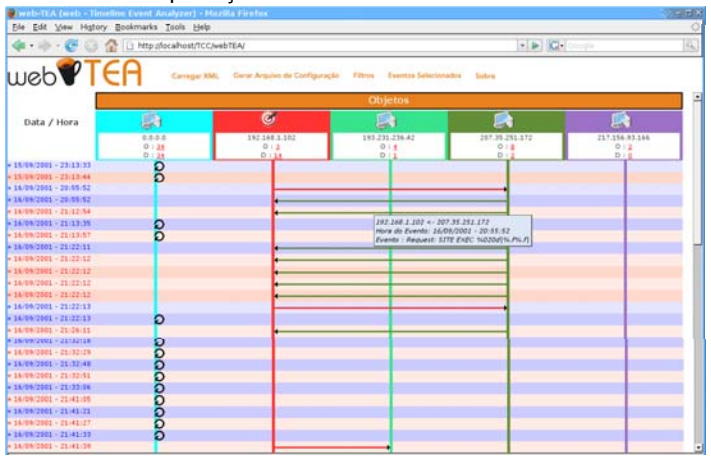
Avaliação Experimental

- Análise e interpretação de eventos



Avaliação Experimental

- Análise e interpretação de eventos



Conclusões

- Necessidade de novas ferramentas e aprimoramentos das técnicas de forense digital
- webTEA
  - Análise de dados de múltiplas fontes de registros
  - XML para configuração e normalização dos dados
  - Facilidade em estender a ferramenta (Coletores)#
  - Selecionar os eventos e reconstruir os passos do infrator através do diagrama
- Avaliação experimental (análise de eventos e desempenho)#
  - Resultados obtidos considerados satisfatórios
- Viabilidade de aplicação prática para peritos e administradores