

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

SBSEG – 2008

Eduardo de Oliveira

<eduardo@f1solucoes.com.br>

Leonardo Lemes Fagundes

<llemes@unisinoss.br>

São Leopoldo, 03 de Setembro de 2008.

Introdução

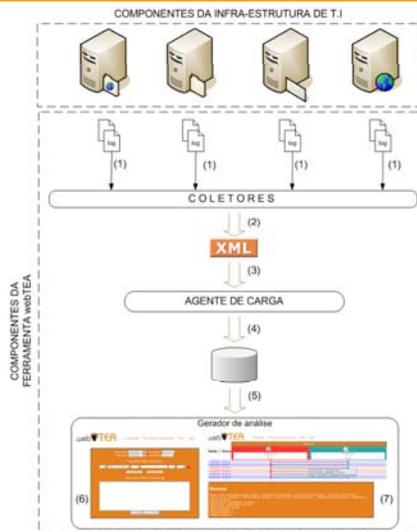
Objetivos

- 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

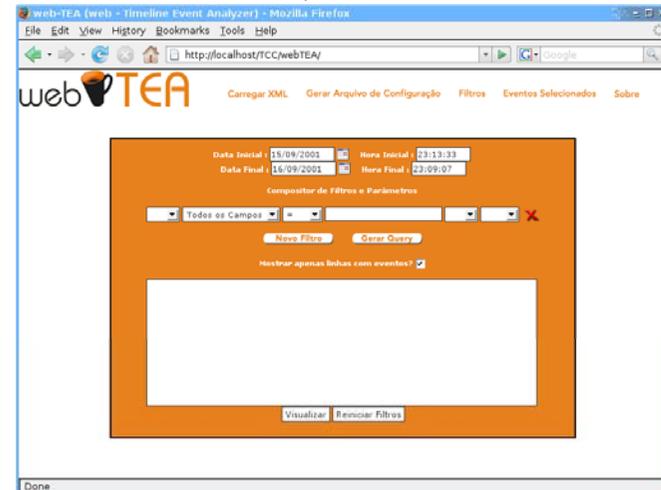
- Arquitetura



3

webTEA : web-based Timeline Event Analyzer

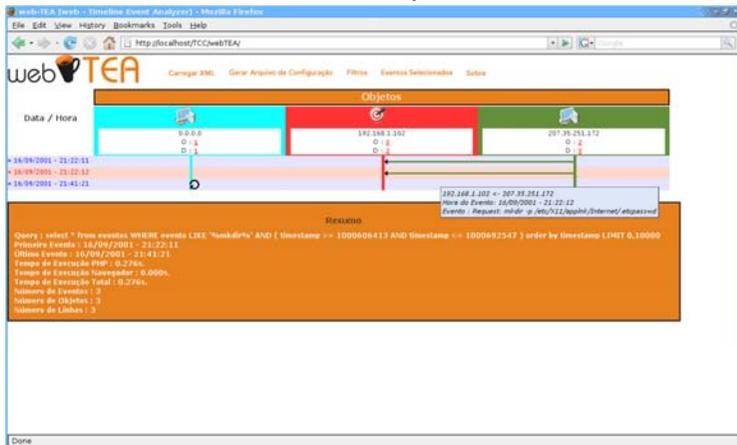
- Gerador de análise => Compositor de Filtros



4

webTEA : web-based Timeline Event Analyzer

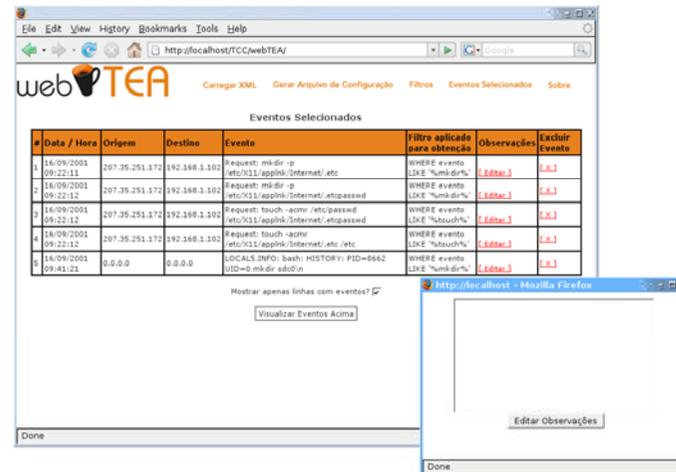
- Gerador de análise => Interface de visualização e análise



5

webTEA : web-based Timeline Event Analyzer

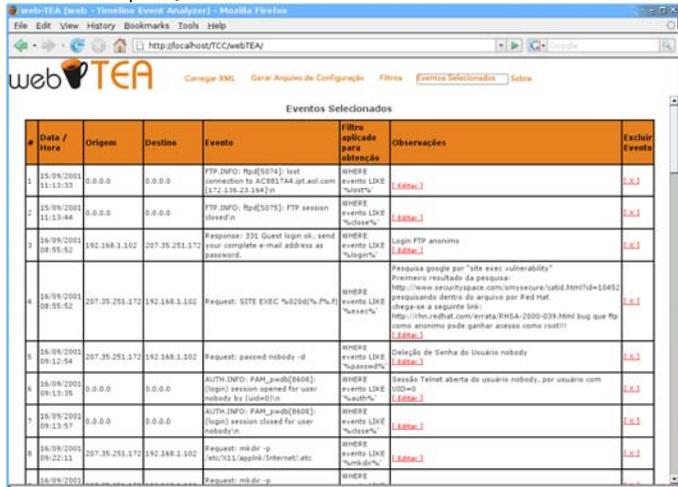
- Gerador de análise => Interface de eventos Seleccionados



6

Avaliação Experimental

- Análise e interpretação de eventos



webTEA (web - Timeline Event Analyzer) - Mozilla Firefox

Carregar XML, Gerar Arquivo de Configuração, Filtros, Eventos Selecionados, Sobre

Eventos Selecionados

#	Data / Hora	Origem	Destino	Evento	Filtro aplicado para seleção	Observações	Excluir Evento
1	15/09/2005 11:13:33	0.0.0.0	0.0.0.0	FTP INFO: Ftp([5174]: test connection to AC9317AA.upt.aol.com [172.138.23.244])	evento LINK %user%	[Link]	[X]
2	15/09/2005 11:13:44	0.0.0.0	0.0.0.0	FTP INFO: Ftp([5075]: FTP session closed)	evento LINK %user%	[Link]	[X]
3	16/09/2005 08:55:52	192.168.1.102	207.35.251.172	Response: 333 Guest login ok, send your complete e-mail address as password.	evento LINK %user%	Login FTP anônimo	[X]
4	16/09/2005 08:55:52	207.35.251.172	192.168.1.102	Request: SITE EXEC %0204%/%/	evento LINK %exec%	Pesquisa google por "site exec vulnerability" Primeiro resultado da pesquisa: http://www.securityspace.com/ym/secure/utid.html?id=10452 pesquisando dentro do arquivo por find.net (clique-se a seguinte link: http://www.nabifl.com/verata.html : 2000-039.html bug que Rp como anônimo pode ganhar acesso como root!!	[X]
5	16/09/2005 09:12:34	207.35.251.172	192.168.1.102	Request: passwd nobody:d	evento LINK %password%	Delegação de Senha de Usuário nobody	[X]
6	16/09/2005 09:13:35	0.0.0.0	0.0.0.0	AUTH INFO: PAM_pwdb[0408]: (login) session opened for user nobody by [uid=0]	evento LINK %uid%	Sessão Telnet aberta do usuário nobody, por usuário com UID=0	[X]
7	16/09/2005 09:13:37	0.0.0.0	0.0.0.0	AUTH INFO: PAM_pwdb[0408]: (login) session closed for user nobody by	evento LINK %user%	[Link]	[X]
8	16/09/2005 09:22:11	207.35.251.172	192.168.1.102	Request: mkdir -p /etc/ssl/certs/Internet*.etc.	evento LINK %uid%	[Link]	[X]
9	16/09/2005			Request: mkdir -p	evento LINK %uid%	[Link]	[X]

7

Avaliação Experimental

- Análise e interpretação de eventos



8

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