webTEA: Uma Ferramenta Para Análise de Incidentes de Segurança

Eduardo de Oliveira, Leonardo Lemes Fagundes

Universidade do Vale do Rio dos Sinos (UNISINOS)
Av. Unisinos, 950 – CEP 93.022-000 – São Leopoldo – RS – Brasil

eduardo@f1solucoes.com.br, llemes@unisinos.br

1. Introdução

O desenvolvimento de ferramentas que ofereçam suporte a etapa de análise e interpretação dos dados, conforme mencionado anteriormente, representa uma questão de pesquisa relevante e em aberto [Casey 2006]. Neste contexto este artigo apresenta uma ferramenta para visualização de eventos ordenados de maneira cronológica, o que resulta na reconstrução do cenário investigado.

2. Código de Prática Proposto

A Figura 1 ilustra uma visão geral da arquitetura proposta e as interações realizadas entre os seguintes componentes: serviços, coletores, agente de carga, repositório de dados e o gerador de análise.

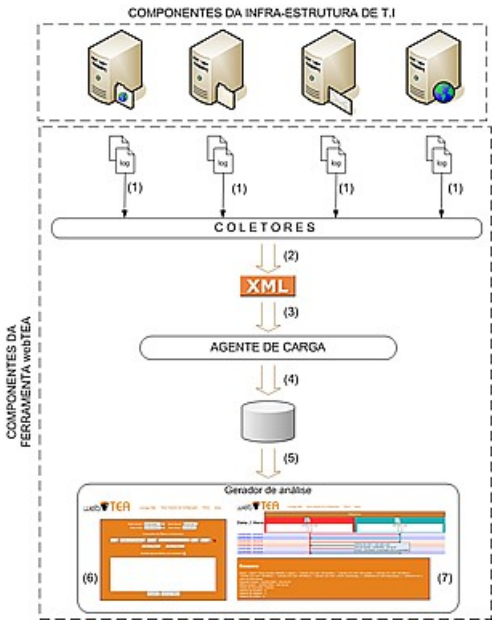

Figura 1: Visão geral da arquitetura do webTEA.

Os serviços representam o conjunto de registros selecionados pelo perito como possíveis fontes de informações sobre o incidente que se deseja analisar. Normalmente os serviços ativos na rede mantêm registros sobre o seu funcionamento e as atividades realizadas através de arquivos de log. Esses registros serão obtidos pelos coletores (1) e, em seguida, normalizados, ou seja, os registros dos diferentes tipos de serviços são interpretados e disponibilizados em um arquivo no formato XML (2). A utilização do formato XML se deve a sua simplicidade, extensibilidade, interoperabilidade e flexibilidade [Laurent 1998].

O agente de carga é o componente do webTEA que interpreta os arquivos XML (3) gerados pelos coletores e tem a função de armazenar as informações (4) neles contidas no repositório de dados. Uma vez que os arquivos XML gerados pelos coletores têm uma estrutura pré-definida e padronizada, o agente de carga faz a leitura dos dados contidos nesses arquivos e realiza a inserção dessas informações diretamente no repositório de dados.

O repositório de dados é um banco de dados, cuja principal função é armazenar as informações obtidas e normalizadas, que serão disponibilizadas ao gerador de análise (5) para a realização das consultas necessárias. O gerador de análise é o responsável pela seleção (6) e apresentação (7) dos dados. A seleção dos eventos é realizada através de filtros personalizados, já os registros que atendem aos critérios de cada filtro são visualizados através de um diagrama que exibe os eventos em ordem cronológica. Os filtros disponíveis pelo webTEA possibilitam ao perito realizar consultas pelos atributos de origem, destino, evento, intervalo de tempo e através de filtros específicos que permitem, por exemplo, identificar evidências de *worms*. Cada um dos atributos descritos acima pode ser comparado com um valor determinado pelo perito, utilizando-se de parâmetros de igualdade, similaridade e diferença. É possível, ainda, comparar os valores utilizando-se de expressões regulares. Além disso, a interface de filtros permite utilizar os operadores lógicos: "AND" e "OR" para concatenar diversos critérios de consulta.

Os dados obtidos pela aplicação dos filtros são apresentados através de um diagrama de seqüência (Figura 2) em que os elementos são dispostos em função da data e hora de ocorrência dos eventos. Esse diagrama representa as interações entre os diversos ativos (por exemplo, computadores, usuários, contas de e-mail, etc.) ao longo do tempo e permite identificar as eventos realizados. Esses eventos são apresentados na interface de análise por meio de setas que indicam o sentido do evento (objeto de origem para objeto de destino). Ao posicionar o mouse sobre a linha que representa o evento é possível obter todas as informações sobre o evento em análise.

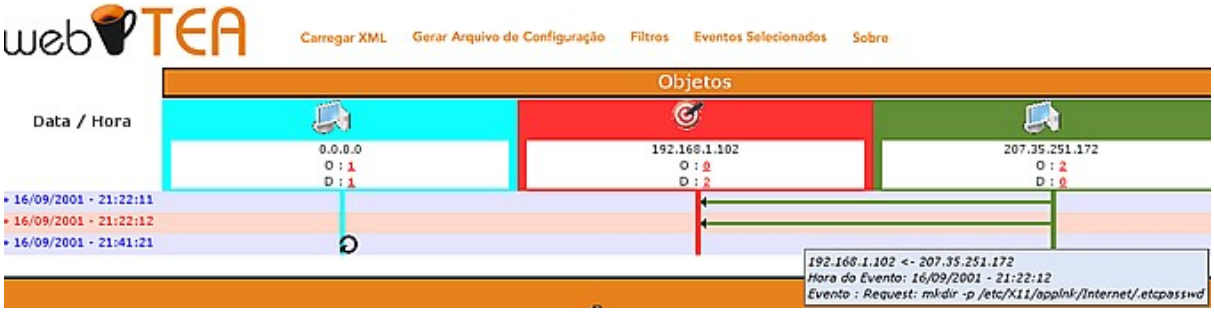

Figura 2: Visualização dos dados.

Outro recurso disponível na interface de visualização é a possibilidade de selecionar os eventos que se acredita estarem envolvidos com o incidente em análise. Para seleção do evento, basta que o perito clique sobre a linha e o evento é imediatamente selecionado. Através da interface de visualização dos eventos selecionados, o perito tem a possibilidade de registrar as suas observações para cada evento relevante, o que o auxilia no momento da elaboração do laudo técnico. Outra informação relevante exibida na interface de eventos selecionados é o filtro utilizado em cada consulta que retornou o respectivo evento.

3. Considerações Finais

Esse artigo propôs uma ferramenta web, distribuída sob licença GPL, denominada webTEA, cujo principal objetivo é auxiliar o perito forense durante as etapas de análise e interpretação de evidências. Essa ferramenta agiliza o processo de identificação e interpretação dos dados, o que resulta na obtenção de evidências que conduzem a respostas sobre os procedimentos realizados durante um incidente de segurança.

Referências

Casey, E. (2006) "Investigating Sophisticated: Security Beaches", em Communications of the ACM. [s.l.], v. 49, n. 2, p. 48-54, feb. 2006.

Laurent, S. (1998) "Why XML?", http://www.simonstl.com/articles/whyxml.htm. Outubro.