Uma Ferramenta de Monitoração Programável voltada à Detecção de Intrusão

Edgar Meneghetti, Luciano Gaspary, Liane Tarouco
Universidade Federal do Rio Grande do Sul, Instituto de Informática
Porto Alegre, Brasil, 91591-970
{edgar@cesup.ufrgs.br, paschoal@inf.ufrgs.br, liane@penta.ufrgs.br}

ABSTRACT

This paper proposes an intrusion detection system based on a Trace architecture, proposed in [4,5,6]. The main proposal of this architecture is for distributed management of high layer protocols and network services. The architecture provides a language called PTSL (Protocol Trace Specification Language), a graphical/textual language created to allow network managers to specify protocol traces to be monitored by an programmable agent. An efficient and easy tool for intrusion detection might be built through scenarios models, described by the language mentioned above. The proposal of a programmable tool that has the ability to receive a PTSL specification describing attacks and to observe the correspondent traces on the network, is the main contribution of this article.

Keywords: intrusion detection, network management, monitoring, Internet.

RESUMO

Este artigo propõe a utilização da arquitetura Trace proposta em [4,5,6] como um sistema para detecção de intrusão. Essa arquitetura destina-se ao gerenciamento distribuído de protocolos de alto nível. A arquitetura provê uma linguagem denominada PTSL (*Protocol Trace Specification Language*) que permite a especificação de traços de protocolos a serem monitorados por um agente programável. Uma ferramenta para detecção de intrusão eficiente e de fácil utilização pode ser definida através da modelagem de cenários de ataques usando a linguagem citada. A proposta de uma ferramenta de monitoração programável capaz de receber especificações PTSL referentes a ataques e observar os traços correspondentes é a principal contribuição deste artigo.

Palavras-chave: detecção de intrusão, gerenciamento de redes de computadores, monitoração, Internet.