Detecção de Intrusão utilizando Métodos de Inteligência Computacional

William Antonio da Rosa, Renato Bobsin Machado, Cristiano Antonio de Souza

Laboratório de Pesquisa em Segurança Computacional – LaPSeC,
Universidade Estadual do Oeste do Paraná – Campus Foz do Iguaçu

william.antonio@hotmail.com, {renatobobsin, cristianoantonio.souza10}@gmail.com

Objetivos

Neste trabalho objetiva-se definir e implementar um Sistema de Detecção de Intrusão (SDI), por meio da aplicação de métodos de inteligência computacional; e avaliar a solução proposta estatisticamente, considerando-se os índices verdadeiros positivo e negativo, e falsos positivo e negativo.

Métodos e Procedimentos

O SDI proposto (Figura 1) é baseado em rede, com arquitetura distribuída e detecção híbrida. O método foi definido conforme a padronização *Common Intrusion Detection Framework.* No módulo de captura de eventos, os pacotes serão extraídos da rede por meio da biblioteca TCPDUMP. No módulo de classificação serão aplicados métodos de inteligência computacional, especificamente Redes Neurais Artificiais (RNA) e K-Nearest Neighbors (KNN). Após a análise, os resultados do processamento serão armazenados em um arquivo de saída.
As assinaturas presentes na base do Snort 2.9.8.2 serão inseridas à base de exemplos do KNN e utilizadas, através de *crossover*, para treinamento da RNA *Multilayer Perceptron*.

Após a calibragem dos modelos, os mesmos serão submetidos a base de ataques pública KDDCup 99 e serão avaliados por meio de análises estatísticas.

Resultados

O principal resultado consiste na definição do modelo arquitetural (Figura 1) e experimental, a partir de um amplo estudo da literatura acerca

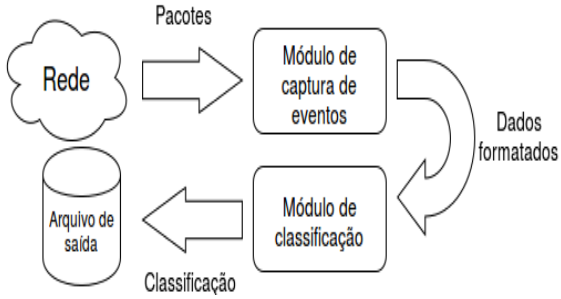

Figura 1 – Arquitetura do SDI

de soluções computacionais para detecção de intrusão. Em termos de implementação, foram testados e definidos os módulos de integração e interface envolvendo a captura de pacotes e a sua apresentação como entrada da RNA e na base de casos de exemplos do KNN.
Também destaca-se a configuração do ambiente experimental em laboratório, dando suporte a próxima etapa, que será a realização dos experimentos.

Conclusões

O presente trabalho possui contribuições na área de segurança computacional e na linha de pesquisa multi-institucional realizada entre a Universidade Estadual do Oeste do Paraná - Unioeste e a Universidade Federal de Santa Catarina - UFSC. Os resultados experimentais poderão subsidiar a criação de novos métodos de detecção de intrusão aplicando-se inteligência computacional.

Referências Bibliográficas

STANIFORD-CHEN, S. Common Intrusion Detection Framework (CIDF). 1998. Acessado em 07/08/2016. Disponível em: <http://gost.isi.edu/cidf/>