ANALISADOR DE ATIVIDADES HOSTIS NA PORTA 80 UTILIZANDO REDES NEURAIS

Autores

MAICON WENTZ MATSUBARA — *Aluno Graduação Unopar*
WAGNER DE PAULA RODRIGUES — *Docente Unopar*

Introdução

A segurança em redes, sem dúvidas, é um dos temas mais discutidos ao redor do mundo por se tratar de algo delicado, e para que se possa amenizar tal insegurança, novas ferramentas e métodos de detecções de invasão se dão por necessárias para ajudar um administrador de redes a conter essas ameaças.

As ferramentas IDS (Intrusion Detection System), tem por objetivo analisar o tráfego passante por uma determinada rede a procura de tentativas de invasões, desde uma varredura de serviços até um ataque efetivo sendo realizada na mesma, sendo que, caso seja detectado algo de suspeito, será gerado um alerta ao administrador de rede.

Redes Neurais Artificiais é uma estrutura de processamento de informações distribuídas paralelamente na forma de um grafo direcionado, onde cada nó represeta um Neurônio.

O modelo proposto para o trabalho é a implementação de um NIDS com análise baseada em Redes Neurais Artificiais utilizando o método por comportamento anômalo na porta 80.

Objetivo

O objetivo deste trabalho é a implementação de um NIDS para realizar análise de pacotes que trafegam na porta 80, afim de detectar hostilidades e comportamentos que fojem do padrão normal da rede.

Metodologia

O trabalho será desenvolvido basicamente em duas fases, a de estudo e a de implementação. Na fase de estudo será dividida em duas partes: embaseamento teórico e pesquisa de ferramentas para um desenvolvimento rápido e eficiente. A fase de desenvolvimento será divida em seqüencias, fases estas como: captura e análise dos pacotes, armazenamento em banco de dados, construção do sistema de Redes Neurais Artificiais e módulo de gerência de eventos. A fase de desenvolvimento poderá ocorrer algumas variações por depender muito da fase de estudos, pois poderão ser utilizadas algumas ferramentas prontas para a obtenção mais rápida de resultados.

Resultado

Os resultados com o desenvolvimento do IDS baseado em análise com Redes Neurais Artificiais, espera-se que com o treinamento e aprendizado da rede neural, baseados nos padrões dos pacotes de atividades normais, o mesmo seja capaz de distingüir o tráfego normal do tráfego hóstil dirigido aos serviços de porta 80, para que atinja um nível de desempenho em relação aos falsos positivos e negativos superiores aos IDS baseados em assinaturas de ataques, além de que, com o término do desenvolvimento do projeto, o nível de conhecimento adquirido com o mesmo seja o caminho para a continuação e dedicação na área de segurança em redes de computadores.

Conclusão

A partir dos estudos realizados, estima-se que o nível de desempenho de IDS com métodos de análise em anômalia utilizando redes neurais, seja bem superior aos que utilizam o método por abuso, onde se utiliza uma base de dados de assinatura.

Bibliografia

CANSIAN, Adriano Mauro. Desenvolvimento de um Sistema Adaptativo de Detecção de Intrusos em Redes de Computadores. São Carlos - SP, 1997.

DE LIMA, Igor Vinícius Mussoi, Uma Abordagem Simplificada de Detedção de Intrusão Baseada em Redes Neurais Artificiais. Florianópolis - SC, 2005.