Rodrigo Mendonça da Paixão
Lucas Teles Agostinho

Título Provisório da Monografia de Trabalho de Conclusão de Curso

São Paulo – Brasil

2015

Rodrigo Mendonça da Paixão
Lucas Teles Agostinho

Título Provisório da Monografia de Trabalho de Conclusão de Curso

Pré-monografia apresentada na disciplina Trabalho de Conclusão de Curso I, como parte dos requisitos para obtenção do título de Bacharel em Ciência da Computação.

Centro Universitário Senac

Bacharelado em Ciência da Computação

Orientador: Eduardo Heredia

São Paulo – Brasil

2015

Resumo

Palavras-chaves: IDS,Rede,Internet

Lista de ilustrações

Lista de tabelas

Lista de abreviaturas e siglas

IDS	Intrusion Detection System
IPS	Intrusion Prevention System
NIDS	Network Intrusion Detection System
IA	Inteligência Artificial
RNA	Rede Neural Artificial
IM	Inteligencia de maquina

Sumário

1 Introdução

1.1 Contexto

Nos dias atuais pessoas e empresas estão cada vez mais dependentes do uso da internet para realizar suas tarefas. Com o aumento da utilização também temos um aumento de casos de incidentes de quebra de segurança. Segundo o CERT (COMPUTER EMERGENCY RESPONSE TEAM,) tivemos um crescimento de 197% de incidentes no ano de 2014 relativo a 2013. A necessidade de se proteger contra estes ataques acabou despertando interesse por ferramentas automatizadas para detectar ataques e analisar formas de aprimorar as técnicas atuais para tal.

Chamamos as ferramentas de detecção de intrusão de IDS (Intrusion Detection System), seu trabalho é monitorar as atividades e analisar os eventos em um rede em busca de anomalias que sugiram uma invasão. Estes não costumam executar qualquer ação para impedir intrusões, sua principal função é alertar os administradores de sistemas que há uma possível violação de segurança, sendo assim uma ferramenta passiva. Temos as ferramentas de prevenção de intrusão, que são conhecidas como IPS (Intrusion Prevention System) estas são ferramentas que assim como IDS analisa o trafego e os eventos de uma rede, porem reage de forma a bloquear o acesso ou atividade maliciosa, senso assim uma ferramenta ativa .

Podemos classificar os IDS da seguinte forma.

Baseado em Host ou baseado em rede onde o primeiro faz uso de arquivos de log de cada computador individualmente e o segundo captura pacotes que trafegam na rede para analisar seu conteúdo.

Online ou Offline, onde um é capaz de detectar e marcar um intruso enquanto a esta sendo realizada a intrusão, e o outro analisa registros após o evento ocorrer e indica que houve uma violação de segurança tinha ocorrido desde a última verificação, respectivamente.

Baseado em abuso ou baseado em anomalia, onde por anomalia o sistema identifica comportamento fora do padrão, e por abuso compara as atividades na rede com comportamentos de ataques já conhecidos.

A maioria dos métodos utilizados para detecção são baseados em inteligencia artificial (IA), entre as varias técnicas conhecidas de IA, a que tem tido melhores resultados e consequente a mais usada é a de Redes Neurais Artificiais (RNA)[2][3].

As RNA são uma classe de algorítimos para aprendizado de maquina (AM),

usada para realizar classificação de dados. A rede neural é treinada de forma a dar mais importância para as principais características de uma determinada instancia de um problema, para ajudar a classificar os dados que ainda estão por vir. RNAs tem sido utilizadas com sucesso na detecção de intrusão [4][5][6], sela necessita de uma quantidade substancial de dados para realizar o treinamento, a partir desse treinamento que ela tera a capacidade de identificar os padrões para depois receber os dados novos para classificação.

1.2 Motivação

Esforços realizados para proporcionar segurança em ambientes computacionais, tem como motivação o fato de existirem riscos que podem comprometer a integridade, confiabilidade e disponibilidade da informação. Esses riscos são avaliados de acordo com as chances do mesmo ocorrer e com os custos envolvidos para tratá-lo. Técnicas de defesa vêm sendo aprimoradas, porém ainda existem diversas limitações que as impedem de estarem efetivamente preparadas para o qualquer tipo de ataque[7], sendo assim necessário soluções inovadoras para tratar os níveis de ameaças atuais e futuras. Este cenário é a principal motivação deste trabalho que consiste em propor, implementar e mensurar resultados de uma solução para treinamento de RNA para detecção e prevenção de intrusão.

1.3 Justificativa

Muitas tecnicas de IA tem sido utilizadas para IDS/IPS, a mais utilizada e a RNA[2], porem existem tipos de ataques que nao sao facilmente detectados, por ocorrerem com menor frequencia, tendo poucas entradas para o treino da RNA[7], resultando em mais erros, por esse motivo escolhemos trabalhar de forma a aprimorar seu resultados.

1.4 Objetivos

Temos como objetivo propor uma forma de aprimorar o sistema de aprendizado de redes neurais artificiais para detecção e prevenção de intrusão.

Para isso sera necessário utilizar uma base de testes com grande volume de dados de trafego em rede. Gerar uma base em um ambiente controlado para testes específicos. Implementar uma solução de IPS/IDS que utilize RNA para classificar os tipos de ataque. Comparar resultados com outras técnicas de treinamento para RNA.

1.5 Método de trabalho

Utilizaremos a base de dados de trafego em rede KDD Cup 99, por ser uma das bases mais completas e amplamente utilizada nos testes de IDS, sera essencial para se realizar uma comparação consistente de resultados.

Para gerar nossa base mais especifica iremos monitorar um ambiente de rede durante um período, no qual serão realizados alguns ataques controlados periodicamente, sera gerado um log que usaremos na nosso sistema.

Desenvolver uma solução para analise dos pacotes e eventos de uma rede, esta sera desenvolvida em Go, utilizara RNA para classificar as atividades na rede.

Realizar treinamento em ambas as bases de dados, serão formas diversificadas de treinamento, sera feito uma comparação de acertos/erros e tempo necessário para treino.

Faremos uma comparação de desempenho e efetividade de nossa solução e algumas que temos hoje.

1.6 Organização do trabalho

Este trabalho esta dividido em três partes. Na próxima seção, sera apresentado o estado da arte, onde sera revisado a literatura sobre detecção e prevenção de intrusão utilizando RNA.

Logo apos teremos a proposta de forma mais detalhada do que é pretendido realizar na próxima etapa do trabalho.

Por fim um cronograma de controle sobre como prosseguira a segunda etapa deste trabalho.

2 Revisão de Literatura

Em uma trabalho em conjunto do Departamento de Automacao e Sistemas da Universidade Federal de Santa Catarina (UFSC) (Paulo M. Mafra,Joni da Silva Fraga,Vinícius Moll,2008)[1] e com a Pontifícia Universidade Católica do Paraná (PUC-PR)(Altair Olivo Santin,2008) [1], foi desenvolvido um sistema multi-camadas chamado de POLVO-IIDS, utilizando redes neurais de Kohonen, que classifica os dados de forma genérica comportamentos considerados normais ou anômalo e para cada classe de ataque foi utilizada uma rede neural do tipo Support Vector Machine(SVM) especializada na detecção da classe correspondente e tendo como saída a indicação de trafego normal ou atividade maliciosa. A ideia de utilizar outra rede neural é utilizada para minimizar o numero de falsos positivos, pois com apenas um tipo de ataque para classifica, aumenta a precisão para identificar apenas duas categorias trafego normal ou anomalia.O valor de cada neurônio pode variar de 0 a 1, normalmente em redes neurais de Kohonen algum neurônio deve estar de 0,1 a 0,9, mas no POLVO-IIDS, foi utilizado de 0,2 a 0,8 para evitar erro de algum possível ataque. O trabalho indica de teve uma melhora nos resultados obtidos relacionados a outras literaturas,mostrando que o modelo POLVO-IIDS é um modelo eficiente.

Um trabalho feito na Pontifícia Universidade Católica do Rio de Janeiro(Renato Maia Silva,Marco Antonio Grivet M. Maia)[2], demostra um teste de desempenho para algumas diferentes entradas para o treinamento de Redes neurais artificiais, utilizando 4 redes, apenas uma utiliza as 41 categorias diferentes, as outras 3 utilizam apenas 9 categorias básicas do TCP-IP, usando um intervalo de -1 a 1. A primeira rede utilizando todas as 41 categorias e a segunda rede com apenas 9 categorias com apenas uma saída, identificando como 1 ataque ou -1 normal, a terceira com apenas uma saída e 9 categorias, indicando como -1 normal, 0 neptune ou 1 smurf e a ultima com 4 saídas e 9 categorias, indicando (-1 1 1 1) normal,(1 -1 1 1) neptune, (1 1 -1 1) back e (1 1 1 -1) smurf. As taxas de acertos foram acima de 90 por cento para todas as configurações testadas, a rede que teve um melhor resultado foi a terceira rede, tendo 97,5

Na Universidade Federal de Santa Maria(Bruno Lopes Dalmazo, Francisco Vogt, Tiago Perlin, Raul Ceretta Nunes ,2008)[3],utilizando serie temporal que eh um modelo matemático para apresentar amostragens periódicas que apresentam dependência entre as amostras, classificando os sistemas de detecção de intrusão em três componentes fundamentais: fonte de informação, analise e resposta.A fonte de informação representada por um coletor associado a um host, rede ou segmento de rede.Analise sendo parte da SDI que verifica eventos derivados da fonte de informação onde eh determinada a indicação que um evento eh uma intrusão que esta ocorrendo ou ja ocorreu.O detector de intrusões baseado em series temporais teve como resultado preliminar uma demostração que a utilização de

series temporais para a detecção de ataques, apresentam resultados satisfatórios para a detecção de um ataque e em pouco consumir de tempo de processamento.

3 Proposta do Trabalho (O que vai ser desenvolvido!)

4 Expectativas

5 Bibliografia

Referências

COMPUTER EMERGENCY RESPONSE TEAM. Disponível em: <http://www.cert.br/stats/incidentes>. Acesso em: 25/05/2015. Citado na página 7.