

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

Sumário

1 Introdução

Detecção de intrusão é uma forma de monitorar eventos em um sistema de computador ou uma rede de computadores, e analisar possíveis incidentes, utilizando de políticas ou uso prático.

1.1 Motivação

Eventos de intrusão estão ficando cada vez mais comuns, por que, empresas e pessoas dependem cada vez mais da infraestrutura computacional e estão cada vez mais conectados a internet para realizar suas tarefas, este crescimento é exponencial, existindo um risco de estar conectado a todo o tempo desta forma, a preocupação que vem crescendo juntamente a esta necessidade é relativo a segurança da informação. Mesmo existindo grande esforço para prover segurança neste ambiente, o número e complexidade de eventos relacionados a quebra de segurança continua crescendo. Pode ser visto pelos reportes feitos ao CERT (Computer Emergency Response Team) até o ano de 2014.

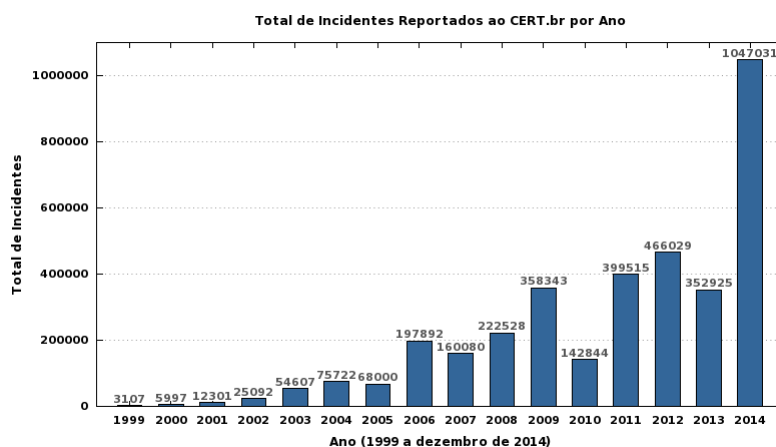


Figura 1 – Incidentes ano a ano. Fonte: (CERT/CC, 2015)

Com esses incidentes ficando cada vez mais comuns, é necessário investir em sistemas de detecção de intrusão e segurança computacional. O trabalho desses sistemas é monitorar as atividades e analisar os eventos em uma rede em busca de anomalias que sugiram uma invasão, para isso precisamos de sistemas suficientemente inteligentes para detecção, esses são classificados como Sistemas de Detecção de Intrusão (Intrusion Detection System - IDS), são soluções passivas para analisar os dados da rede e avisar se existe alguma atividade suspeita. Empresas como bancos por exemplo, precisam investir bastante em segurança pelo fato de ter um alto risco de perda financeira, como também a imagem da instituição, dificilmente seus clientes vão ficar tranquilos sabendo que a instituição que cuida de seu

dinheiro e retém várias dados pessoas foi invadida. Órgãos governamentais também se preocupam com o problemas de invasões, por medo de roubo de informações de outros países ou terroristas. Porém acontecer também roubo de novas tecnologias, estrangeiras e documentos importantes. Com tantas informações importantes fazem a segurança ser prioridade quando o assunto é tecnologia. Esta é a principal motivação para este trabalho, que irá propor, modelar, implementar e realizar experimentos de uma solução para IDS utilizando técnicas de inteligência artificial.

1.2 Objetivos

Temos como objetivo criar uma ferramenta que seja de fácil uso e possa ser usada por outros desenvolvedores em suas aplicações, onde irá detectar um ou mais tipos de ataques conhecidos e alguns semelhantes, dando um baixo número de erros.

1.3 Método de trabalho

Usando a linguagem de programações GO, será criada uma API multi-sistemas (Windows, MacOS e Linux) que monitora a rede usando um algoritmo de inteligência artificial, aprendendo como a rede se comporta em situações normais e conseguindo indentificar anomalias.

1.4 Organização do trabalho

2 Revisão de Literatura

2.1 Segurança e Detecção de intrusão

O IDS usa padrões já conhecidos de atividades ilegais para indentificar se o comportamento esta diferente do perfil tradicional, porém não é incomun ocorrer os chamados falsos negativos ou falsos positivos, isso ocorre por existir uma margem de erro nestas classificações. Após isso para negar o serviço ao intruso é necessario o uso de um Sistema de Prevenção de Intrusão (Intrusion Prevention System - IPS), este é uma solução ativa que provê políticas e regras para o tráfego de rede, quanto o IDS somente avisa a atividade suspeita, o IPS tenta parar essa atividade, porém também possui uma taxa de erro. Com a popularização de ferramentas e técnicas cada vez mais sofisticadas de intrusão é necessario criar ferramentas e tecnicas mais sofisticadas para IDS e IPS.

O objetivo é criar um sistema de detecção de intrusão que apresente um baixo indice de erros utilizando tecnicas de inteligencia artificial, onde o sistema vai aprender, quais são os comportamentos aceitos na rede de computadores.

Os principais objetivos da segurança computacional são:

Confidencialidade: a garantia de que a informação esteja disponível somente para aqueles que tem autorização para obtê-la.

Integridade: é a garantia de que a informação permanecerá inalterada mesmo sob situações críticas, como acidentes ou tentativas de manipulações hostis.

Disponibilidade: consiste na proteção dos recursos e serviços prestados pelo sistema de forma que eles não sejam degradados ou se tornem indisponíveis garantindo assim que a informação estará sempre acessível e pronta para o uso.

Qualquer atividade que possa comprometer qualquer um desses objetivos é considerada uma violação às políticas de segurança.

2.2 Ameaças à segurança

As falhas de segurança são contantes nos sistemas computacionais, essas os sujeitam a varios tipos de ameaças internas ou externas, que podem acabar desencadeando intrusoes que exploram as vulnerabilidades do sistema.

A motivação para exploração dessas vulnerabilidades podem ser de simples vandalismo até tecnicas de espionagem.

Segundo um relatório técnico gerado pelo Sandia National Laboratories (HOWARD; LONGSTAFF, 1998) é apresentado uma taxonomia que se baseia em ações para classificar ameaças à segurança em cima das informações que estão em transito.

As características destas são (podem ser visualizadas na figura 2):

Interrupção: As informações em trânsito são interrompidas, impossibilitando que as mesmas cheguem até seu destino e prejudicando a questão da disponibilidade dos recursos.

Interceptação: As informações são interceptadas durante a transmissão, comprometendo a confidencialidade da mensagem.

Modificação: As informações são interceptadas e alteradas durante a transmissão, afetando não só a confidencialidade como a integridade da mensagem.

Fabricação: Trata-se da inserção de informações em determinada comunicação, comprometendo a autenticidade das informações recebidas.

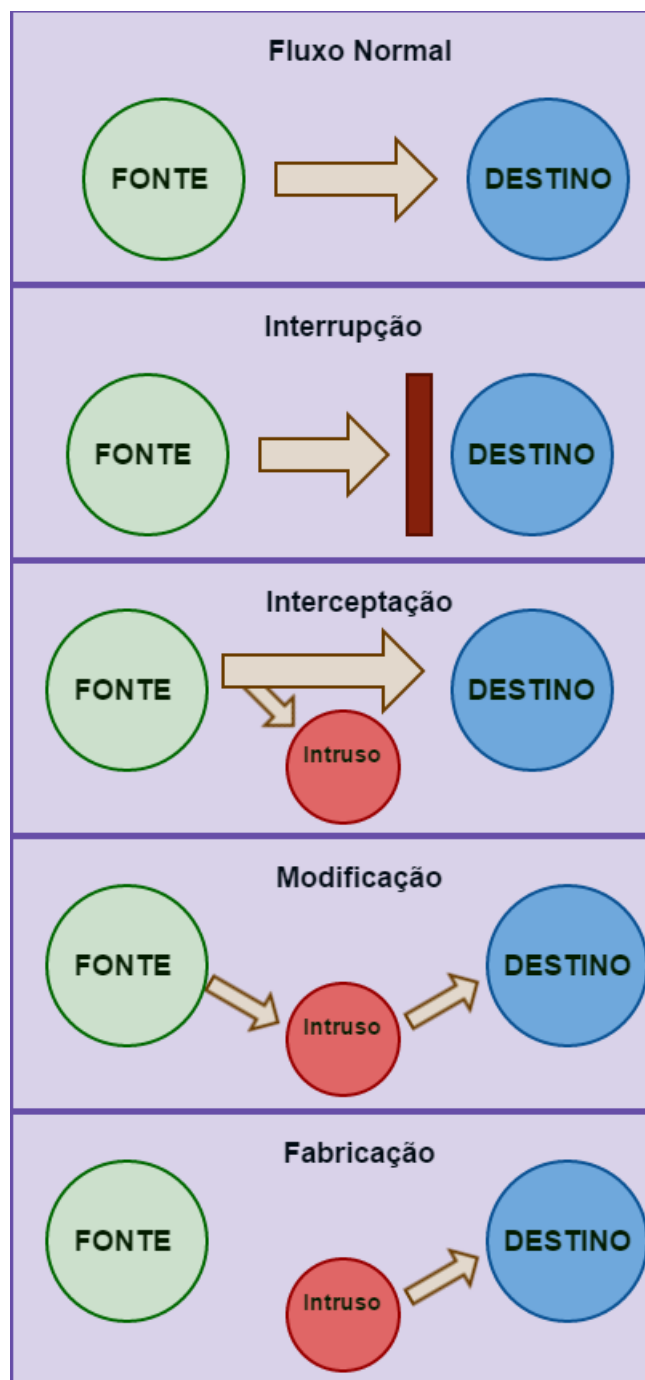


Figura 2 – Taxonomia baseada em ações

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

4 Expectativas

5 Bibliografia