

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

Figura 1 – Incidentes ano a ano	7
---	---

Lista de tabelas

Lista de abreviaturas e siglas

ABNT	Associação Brasileira de Normas Técnicas
abnTeX	ABsurdas Normas para TeX

Sumário

1	INTRODUÇÃO	7
1.1	Motivação	7
1.2	Objetivos	8
1.3	Método de trabalho	8
1.4	Organização do trabalho	8
2	REVISÃO DE LITERATURA	9
3	PROPOSTA DO TRABALHO	10
4	EXPECTATIVAS	11

1 Introdução

1.1 Motivação

Empresas e pessoas dependem cada vez mais da infra estrutura computacional e estarem conectados a internet para realizar suas tarefas, este crescimento é exponencial, e existe 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 numero e complexidade de eventos relacionados a quebra de segurança continua crescendo.

1.2 Objetivos

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. O IDS usa padrões já conhecidos de atividades ilegais para indentificar se o comportamento esta diferente do perfil tradicional. Porém não é incomum 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. Esta é a principal motivação para este trabalho, este irá propor, modelar, implementar e realizar experimentos de uma solução para IDS utilizando técnicas de inteligência artificial.

1.3 Método de trabalho

1.4 Organização do trabalho

2 Revisão de Literatura (Referencial Teórico + Trabalhos Relacionados)

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

4 Expectativas

Figura 1 - <http://www.cert.br/stats/incidentes>