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

ABNT	Associação Brasileira de Normas Técnicas
abnTeX	ABsurdas Normas para TeX

Sumário

1 Introdução

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 estante 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. Pode ser visto pelos reportes feitos ao CERT (Computer Emergency Response Team) até o ano de 2014.

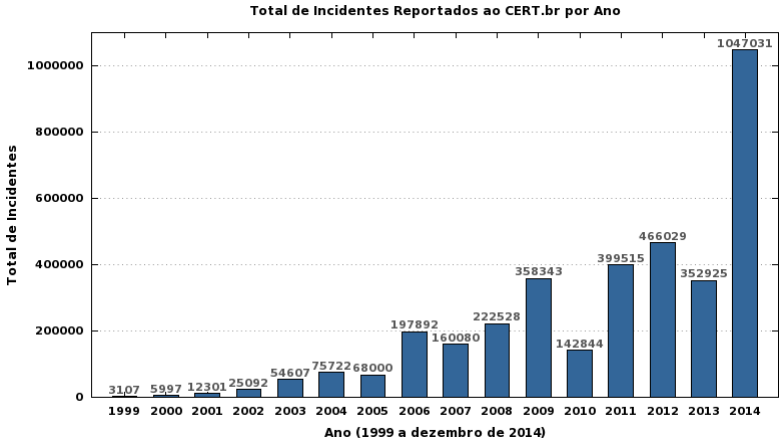

Figura 1: Incidentes ano a ano

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 um rede em busca de anomalias que sugiram uma invasão.

Os objetivos principais 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.

Autenticidade: associada à correta identificação de usuários ou computadores, visando proteger o sistema contra intrusos, normalmente garantida através de mecanismos de senhas e/ou assinatura digital

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 identificar 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 necessário 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 necessário criar ferramentas e técnicas 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.

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