1. Segurança da Informação

-O que é segurança da informação?

Está diretamente relacionada com proteção de um conjunto de informações, preservar seu valor para um indivíduo ou organização. Seus PILARES são manter a confidencialidade, integridade e disponibilidade. Seu conceito se aplica a todos os aspectos de proteção de informações e dados.

-Por que é importante?

A informação é algo de suma importância para uma organização e fundamental para os negócios. Por isso, é importante que seja adequadamente protegida. Com o crescimento da interconectividade entre ambientes de trabalho, a informação fica exposta a uma grande variedade de ameaças (uma circunstância que tem o potencial de causar danos ou perda). Daí a necessidade da segurança da informação, que é a proteção da informação contra os vários tipos de ameaças, minimizando os riscos de ataque

-O que é um ataque?

Um ataque ocorre quando uma ameaça é realizada, podem ocorrer por motivos diversos, desde apenas curiosidade até adquirir as informações para ganhos financeiros, extorsão ou espionagem, ou até mesmo ferir a imagem de alguma organização ou indivíduo. As principais classes de ataques são

--Principais Classes de Ataques

-DoS/DDOS ->

São negação de serviço. Forçar o sistema vítima a reinicializar ou consumir todos os recursos ou obstrui a mídia de comunicação entre os utilizadores.

-R2L ->

Ocorre quando um atacante tem a habilidade de enviar pacotes para uma máquina através da rede, mas não tem uma conta nessa máquina.

U2R ->

Atacante acessa o sistema como usuário normal e passa a explorar vulnerabilidades para ganhar acesso como root

-PROPER/Scan ->

Estes ataques são caracterizados pela tentativa de abertura de conexões em diversas portas de um mesmo destino, com o intuito de descobrir quais serviços e versões estão instaladas no host destino.

2. Problema

Os ataques reportados ao CERT aumentaram em 197% em 2014 relativo a 2013

É um problema atual, necessita de novas ferramentas e técnicas para lidar com o aumento de ataques e novos tipos de ataques

Obs.: O aumento do uso

3. Ferramenta IDS

-O que são?

->Ferramentas de análise.

-Como funciona:

Seu trabalho é monitorar as atividades e analisar os eventos em uma 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

->

4. Ferramenta IPS

-O que são?

->Ferramentas de prevenção

-Como funciona:

A princípio, o IPS era apenas um IDS que possibilitava alguma interação com o firewall para controlar o acesso. Em pouco tempo foi necessário desenvolver algo mais robusto, pois apenas comandar o firewall não bastava: ainda era possível que ao menos aquele pacote malicioso trafegasse na rede. A solução era implementar formas inteligentes de bloqueio dentro do IPS.

5. Técnicas de IDS/IPS

-Sistemas baseados em regras.

Usam técnicas que utilizam base de dados e verificam as assinaturas dos pacotes para verificar se são ataques,

-Sistemas adaptáveis (IA).

São sistemas que se adaptam, utilizam técnicas de IA para se adaptarem, das técnicas de IA a mais utilizada e que tido melhores resultados é a de Redes Neurais

6. Redes Neurais

-Como funcionam?

Aprendizado, Generalização e classificação.

Neurônios são considerados como as unidades básicas de processamento do cérebro. De modo análogo, modelos simplificados dos neurônios biológicos constituem as unidades básicas de processamento das RNAs o Perceptron.

A Função transferência soma todos os sinais de entrada ponderados pelos pesos das conexões

A função de ativação é geralmente utilizada com dois propósitos: limitar a saída do neurônio e introduzir não-linearidade no modelo

7. Redes Neurais

-Como funcionam?

Sua arquitetura normalmente de 3 camadas, uma de entrada, uma intermediaria e uma de saída, mas podem ter mais camadas intermediarias a saída de cada camada intermediária é utilizada como entrada para a próxima camada

8. POLVO-IIDS

-Como funciona?

POLVO é uma arquitetura baseada em multicamadas para a criação de um IDS, essa arquitetura consiste em duas camadas, um classificador que é uma Rede Neural de Kohonen e vários detectores de anomalias que são uma Support Vector Machine(SVM), para cada anomalia é criada uma SVM individual para cada tipo de ataque. Foi utilizada a base de dados KDD Cup 1999.

Extra:

Kohonen, 1988

É um tipo de rede neural não surprevisado

A escolha deste tipo de rede foi motivada pela característica das redes de kohonen em aprender padrões de forma automática (sem supervisão), pela facilidade em separar padrões conhecidos (treinados) e pela generalização na detecção de padrões (detecta variações de padrões conhecidos).

As SVMs suportam uma certa quantidade de ruído na entrada da rede (alguns ataques incluídos no trafego de treinamento) sem prejudicar o treinamento da mesma.

Worm: Esta classe corresponde a ataques gerados por worms, onde, geralmente, ha a abertura de milhares de conexões para diversos destinos em um curto período de tempo.

9. Clusterização Fuzzy

-Agregação Fuzzy

->

10. Motivação

Fato de existirem riscos que podem comprometer a segurança da informação. Esses riscos são avaliados de acordo com as chances de o 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, sendo assim necessário soluções inovadoras para tratar os níveis de ameaças atuais e futuras.

11. Objetivo

Implementar as abordagens do POLVO e Clusterização

Testar uma combinação das técnicas e comparar seus resultados