Universidade Federal do Pará
Faculdade de Computação
Bacharelado em Ciência da Computação

Avaliando Sistemas de Detecção de Intrusão em uma Rede Acadêmica

Glenon Mateus Barbosa Araújo

Trabalho de Conclusão de Curso

10 de julho de 2018

Sumário

Introdução

- Internet = conjuntos de redes heterogênea;
- maior a complexidade, maior numero de vulnerabilidades;
- CERT.br - 722205 incidentes reportados (Scan, Fraude, DoS, Worm);
- *Firewall* não é uma solução definitiva;
- Necessidade de outras ferramentas (flexibilidade, eficiência, desempenho, administração simplificada);

- Necessidade de implantação de um IDS;
- Uso gratuito;
- Ferramentas Snort e Suricata;

- **Geral:**
  - Avaliar e fazer um comparativo;
- **Secundário:**
  - Apresentar conceitos sobre segurança da informação;
  - Descrever problemas relacionados a ataques envolvendo redes de computadores;
  - Descrever as ferramentas, compreendendo requisitos, características, modos de atuação e funcionalidades;
  - Descrever o ambiente experimental;
  - Realizar experimentos e coltar dados.

- **Incidente de Segurança:** Qualquer evento oposto a segurança;
- **Ativo:** Qualquer coisa que tenha valor para a organização e para seus negócios;
- **Ameaça:** Qualquer evento que explore vulnerabilidades;
- **Vulnerabilidade:** Qualquer fraqueza que possa ser explorada;
- **Risco:** Probabilidade de uma ameaça se concretizar;
- **Ataque:** Qualquer ação que comprometa a segurança;
- **Impacto:** Consequências de um evento;

Segurança

Pilares da Segurança

- **Confidencialidade:** ligado à privacidade, acesso somente por pessoas ou grupos autorizados;
- **Integridade:** Informação ter valor correto, inviolabilidade da informação;
- **Disponibilidade:** relacionada ao acesso à informação;
- **Autenticidade:** garantia de que a informação foi elaborado ou distribuído pelo autor;
- **Legalidade:** garantia de que ações sejam realizadas em conformidade com os preceitos legais;
- **Não Repúdio:** emissor de uma mensagem não pode negar que a enviou;
- **Privacidade:** habilidade de uma pessoa controlar a exposição e a disponibilidade de informações acerca de si;

- ***Scanner:*** varrer a rede a procura de um alvo em potencial;
  - ***Portscanner*****:** verifica quais portas estão abertas no alvo;
  - **Vulnerabilidade:** verifica se o serviço está executando uma versão com alguma vulnerabilidades;
- **Negação de Serviço:** deixar um serviço ou recurso indisponível;

Sistema de Detecção de Intrusão

Definição

- **IDS:** Monitoramento de eventos que ocorrem em redes e sistemas computacionais, analisando sinais de possíveis ataques, alertando os administradores;
- **IPS:** todas as funcionalidades do IDS, porém é capaz de deter os incidentes;

Sistemas de Detecção de Intrusão

Tipos

- **HIDS:** sensor é instalado no *host*; verificação de informações relativas aos eventos e registros de *logs* e sistemas de arquivos;
- **NIDS:** sensor é instalado na rede; monitora e analisa o trafego do segmento de rede;
  - **Passivo:** monitora copias dos pacotes da rede (espelhamento)
  - **Ativo:** trafego passa através do sensor (atuação similar a de um *firewall*)
- **SDID:** envio de alertas para um servidor central (gerencia)
- **Forma de Detecção:**
  - **Assinaturas:** compara com uma base de assinaturas de ataques conhecidos;
  - **Anomalias:** determina um comportamento normal da rede, qualquer desvio desse comportamento gera alertas;

Sistemas de Detecção de Intrusão

Ferramentas

IDS em um Cenário Real

IDS em um Cenário Real

Testes Realizados

IDS em um Cenário Real

Resultados

IDS em um Cenário Real

Conclusão