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.

Segurança

Sistema de Detecção de Intrusão

Sistemas de Detecção de Intrusão

Tipos

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