

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

11 de julho de 2018

Agenda

- 1 Introdução
 - Motivação
 - Objetivos
- 2 Segurança
- 3 Sistemas de Detecção de Intrusão
 - Tipos
 - Ferramentas
- 4 IDS em um Cenário Real
 - Testes Realizados
 - Resultados
- 5 Considerações Finais

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);

Introdução

Motivação

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

Introdução

Objetivos

- **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

Definições

- **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

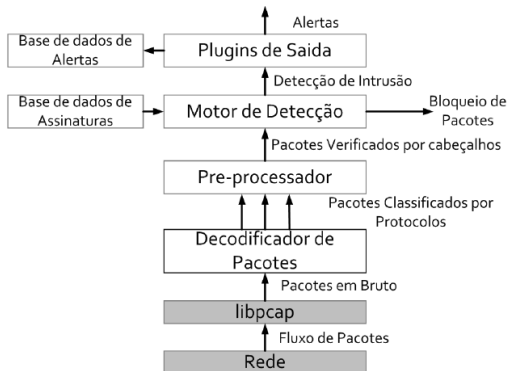
- **HIDS:** sensor é instalado no *host*; verificação de informações relativas aos eventos e registros de *logs* e sistemas de arquivos;
- **NIDS:** sensor é instalado na rede; monitora e analisa o tráfego do segmento de rede;
 - **Passivo:** monitora cópias dos pacotes da rede (espelhamento)
 - **Ativo:** tráfego 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

Snort

Linguagem C;
Lançamento em 1998;
Baseado em assinaturas e anomalias;
Sniffer; *Packet Logger*; NIDS;

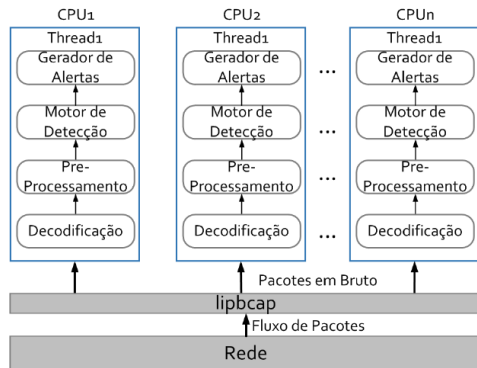


Sistemas de Detecção de Intrusão

Ferramentas

Suricata

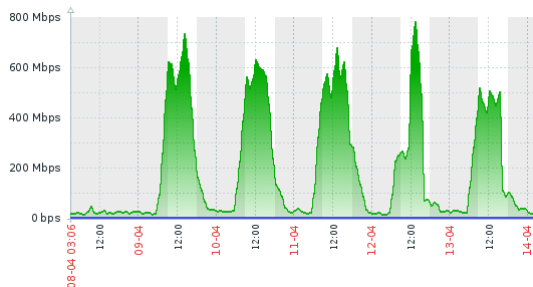
Lançamento em 2010;
Baseado em assinaturas e anomalias;
Arquitetura inspirada no Snort;
Multithread;
Sniffer; *Packet Logger*; NIDS; NSM;



IDS em um Cenário Real

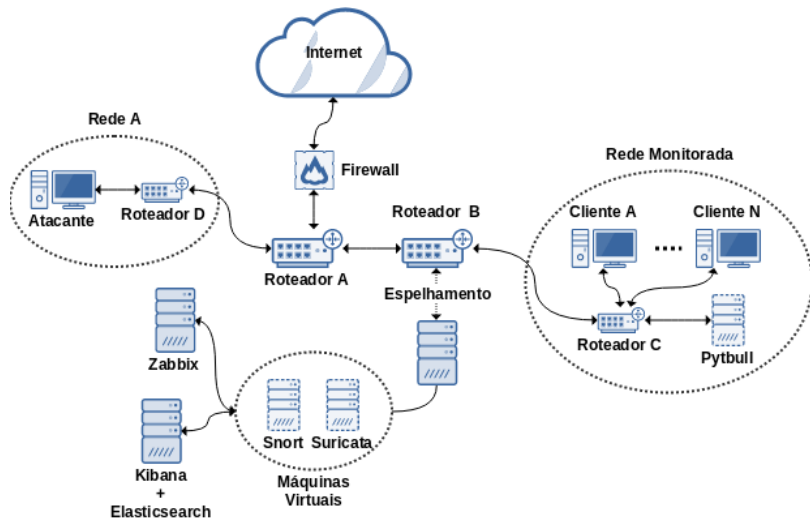
Cenário de Testes

Taxa de Transferência = 800 Mbps;
Quantidade de usuário indeterminado;



IDS em um Cenário Real

Infraestrutura



IDS em um Cenário Real

Teste Realizados

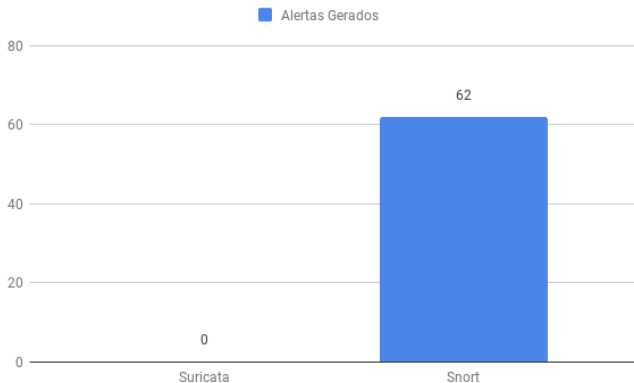
- **Portscanner**
 - nmap -F 200.239.72.19
 - nmap -A 200.239.72.19
 - execução dos comandos via *script*
- **Scan de Vulnerabilidade** (OpenVAS)
- **DoS** (Metasploit Framework)
 - use auxiliary/dos/tcp/synflood
- **Pytbull**

IDS em um Cenário Real

Resultados

nmap -F

Total = 62 alertas;
100% do Snort;

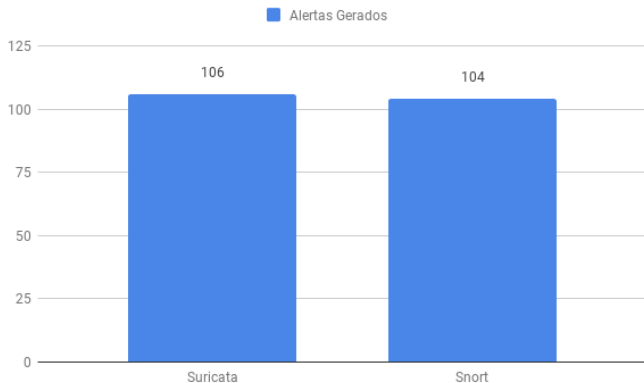


IDS em um Cenário Real

Resultados

nmap -A

Total = 210 alertas;
50.5% Suricata;
49.5% Snort;

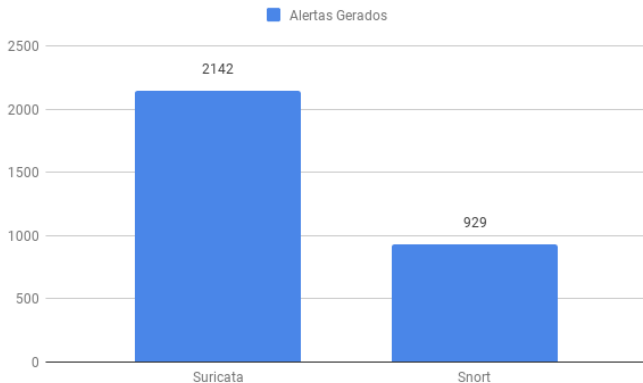


IDS em um Cenário Real

Resultados

OpenVAS

Total = 3071 alertas;
69.74% Suricata;
30.26% Snort;

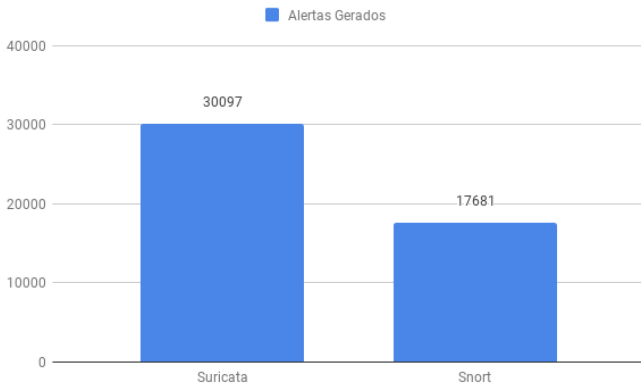


IDS em um Cenário Real

Resultados

Taxa de detecção

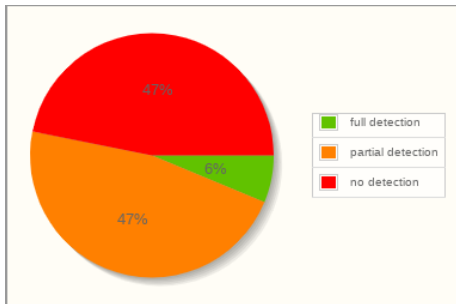
Total = 47778 alertas;
62.99% Suricata;
37.01% Snort;



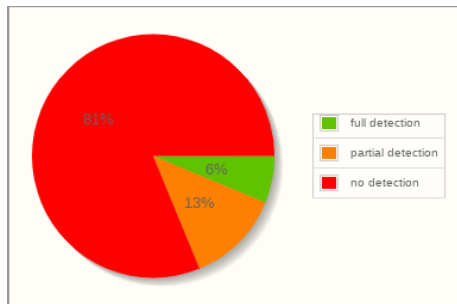
IDS em um Cenário Real

Resultados

Suricata







Snort




IDS em um Cenário Real

Resultados

Suricata

		último	mín	méd	máx
 Processor load (1 min average per core)	[méd]	0.0012	0	0.0326	0.545
 Processor load (5 min average per core)	[méd]	0.0006	0	0.0313	0.41
 Processor load (15 min average per core)	[méd]	0.0004	0	0.029	0.3375
 Used memory	[méd]	último 4.35 GB	mín 3.16 GB	méd 5.48 GB	máx 7.78 GB

Snort

		último	mín	méd	máx
 Processor load (1 min average per core)	[méd]	0.2558	0	0.1798	0.4625
 Processor load (5 min average per core)	[méd]	0.2561	0.0075	0.1788	0.3225
 Processor load (15 min average per core)	[méd]	0.2503	0.0125	0.1774	0.2825
 Used memory	[méd]	último 3.99 GB	mín 2.09 GB	méd 3.81 GB	máx 5.06 GB

Considerações Finais

- Documentação do Suricata;
- Implantação da infraestrutura de teste;
- Suricata teve um melhor desempenho porém não recomendado;
- Analisar as ferramentas tendo como foco a precisão (falsos positivos e falsos negativos);