Sistemas de Detecção de Intrusão

Roteiro

Sistemas de Detecção de Intrusão

Avaliação

Sistemas de Detecção de Intrusão

Sistemas de Detecção de Intrusão

- *IDS* é a sigla para *Intrusion Detection System*, ou Sistema de Detecção de Intrusão;

- Esses sistemas funcionam tentando identificar atividades anormais que possam vir a configurar invasões em computadores através da rede;

- Embora não sejam perfeitos e nem mostram todos os ataques possíveis, IDSs podem prover muita inteligência sobre o que está realmente acontecendo nos sistemas e redes => permitem reportes de atividades maliciosas/suspeitas em tempo-real.

O que vem a ser uma intrusão?

- Para os propósitos ligados a redes de computadores e sistemas, uma intrusão é simplesmente uma atividade não autorizada em um *host* ou rede.
  - Usuário legítimo tentando escalar privilégios;
  - Usuário remoto e não autenticado tentando comprometer um serviço em execução de modo a criar uma conta no sistema;
  - *Malware* presente em um *link* acessado por um usuário ingênuo.

IDS

- O funcionamento de um IDS depende do seu tipo e onde ele está localizado na rede.

- São classificados pela funcionalidade, agrupados nas seguintes categorias:

  - *Network-based Intrusion Detection Systems (NIDS)*

  - *Host-based Intrusion Detection Systems (HIDS)*

  - *Distributed Intrusion Detection Systems (DIDS)*

NIDS

- Monitora uma subrede (ou segmento de rede) inteira, aceitando todos os pacotes em tráfego e os encaminhando para as camadas de cima da pilha TCP/IP (modo promíscuo);

- O dispositivo de rede ao qual o NIDS está conectado deve enviar todos os pacotes para ele:
  - Se for um *hub*, não há configuração adicional;
  - Se for um *switch*, a porta deve ser colocada em modo de monitoração (*span port*).

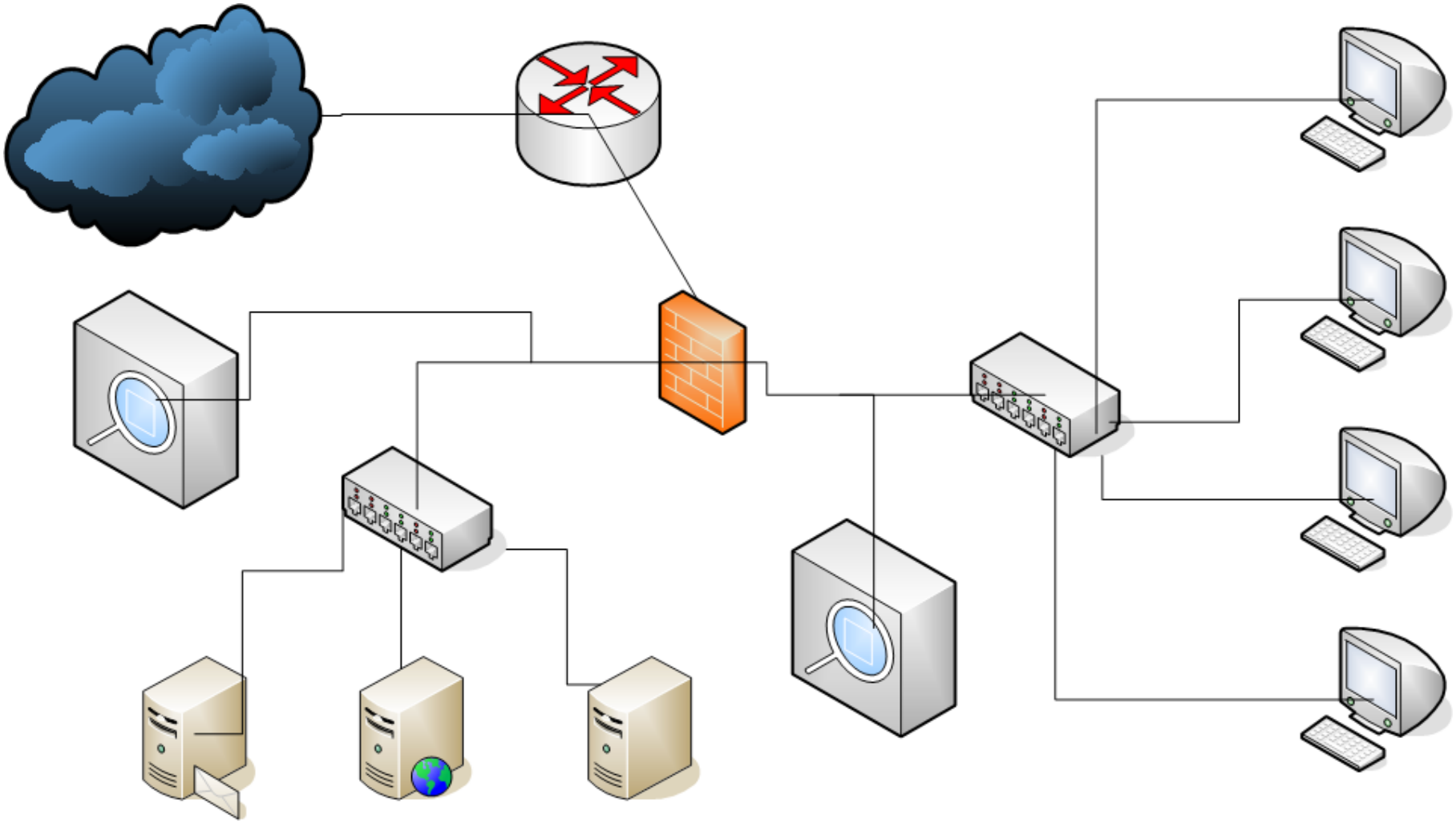
NIDS

- A vantagem de um NIDS é que ele não tem impacto nos sistemas ou na rede monitorada. O comprometimento de algum *host* monitorado também não o afeta;

- Problemas:
  - Esgotar a quantidade de *span ports* disponíveis em uma dada subrede;
  - Esgotar a largura de banda no *span*, saturando o *backplane*.

    Ex.: 20 portas de 100MB espelhadas em uma ~ 2GB

NIDS



HIDS

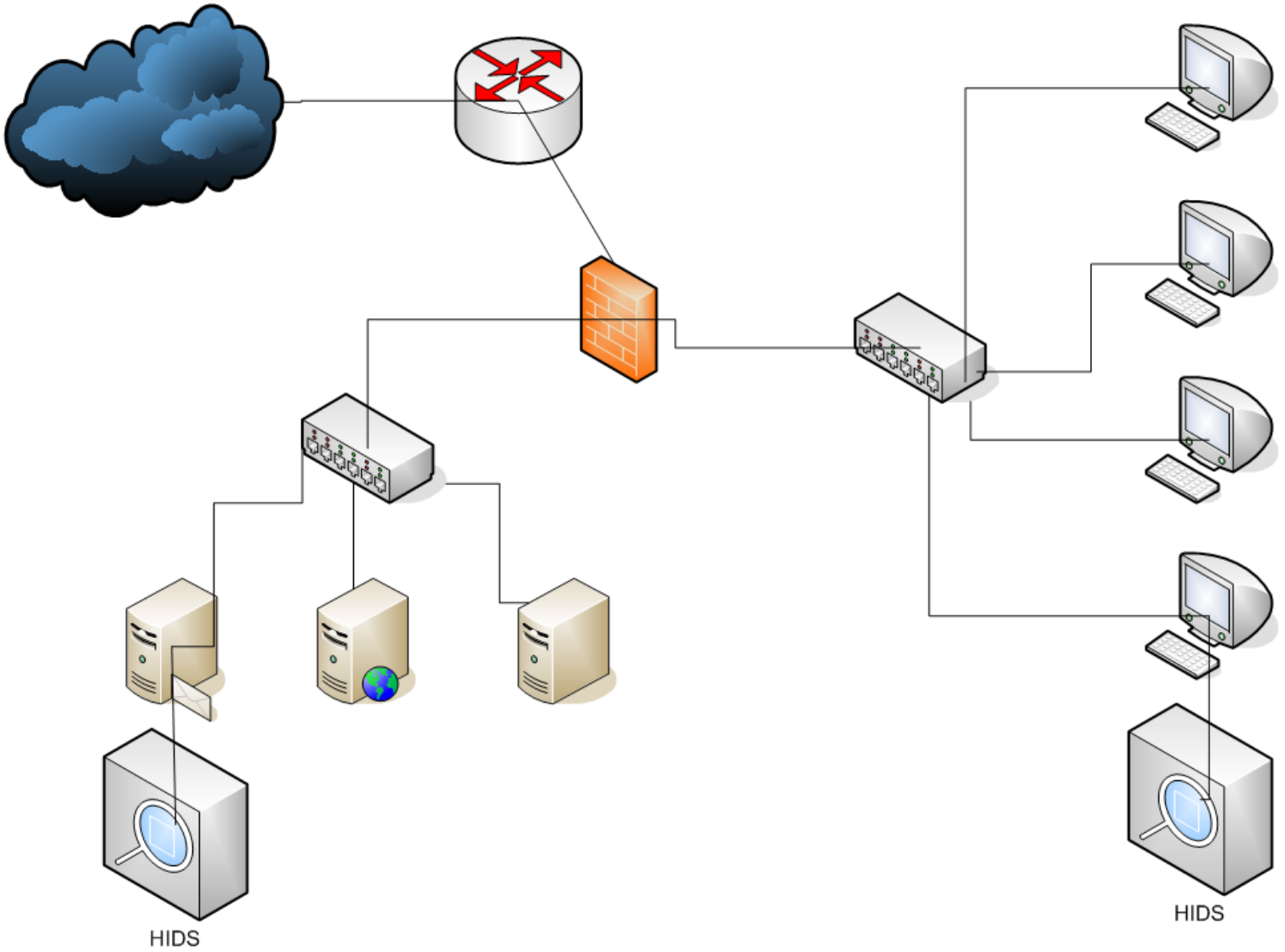
- Diferem dos NIDS em dois modos:
  - Protege apenas o sistema no qual reside;
  - A interface de rede normalmente opera em modo não promíscuo => menos ocupação de CPU.

- Vantagens:
  - Menos regras (mais específicas), menos falsos positivos;
  - Detecta certas mudanças em arquivos e no sistema operacional;
  - Pode interceptar chamadas de sistema maliciosas;
  - Monitoração de tráfego que não atravessa a rede (interno).

HIDS

- Desvantagens:
  - Configuração personalizada leva tempo;
  - Adiciona carga ao *host* hospedeiro (consome recursos);
  - Administração complicada:
    - Muitos sensores;
    - Sistemas operacionais diferentes.
    - Servidores com funções diferentes

HIDS



DIDS

- Combinação de sensores NIDS, HIDS ou ambos, distribuídos através de uma instituição e todos se reportando a um sistema central de correlacionamento.

- *Logs* de ataque são gerados nos sensores e exportados periodicamente para uma estação centralizada onde são armazenados em um banco de dados.

DIDS

- As regras podem ser refinadas para corresponder a necessidades individuais (subrede e *hosts*).

- Alertas podem ser encaminhados para um sistema de envio de mensagens na estação de correlacionamento e utilizados para notificar o administrador do IDS.

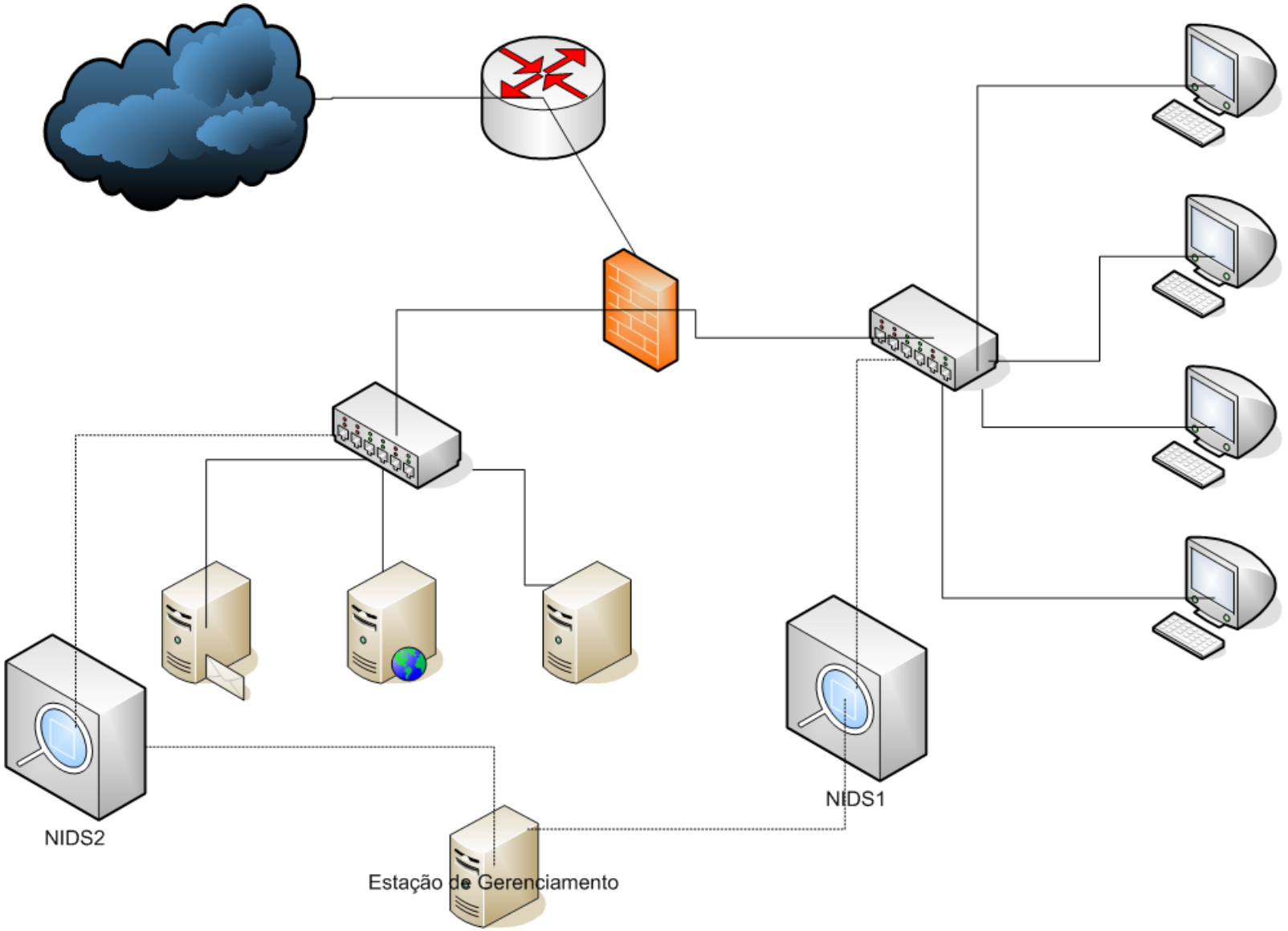
- As transações entre sensores e gerente podem usar uma VPN para proteger a confidencialidade dos dados de gerenciamento.

DIDS

- A principal vantagem de um DIDS é que se pode observar eventos de uma maneira abrangente, a milhares de pés de altitude!

- Desvantagens:
  - Complexidade para projetar e implantar;
  - Requer experiência para refinar as regras;
  - Não é simples correlacionar e gerenciar os dados gerados por todos os sensores

DIDS



Snort

Snort

O que é

O SNORT é uma ferramenta NIDS desenvolvido por Martin Roesch "open-source" bastante popular por sua flexibilidade nas configurações de regras e constante atualização frente às novas ferramentas de invasão . Outro ponto forte desta ferramenta é o fato de ter o maior cadastro de assinaturas, ser leve, pequena, fazer escaneamento do micro e verificar anomalias dentro de toda a rede ao qual seu computador pertence.

Snort

Características

O Snort conta com o permanente desenvolvimento e atualização, que são feitos diariamente, tanto em relação ao código propriamente dito, como das regras de detecção.

Os padrões utilizados na construção das regras de detecção das subversões são introduzidos no sistema de configuração, tão rápido quando são enviados os alertas originados pelos órgãos responsáveis, como por exemplo o CERT, Bugtraq (lista de discussão), entre outros.

Snort

Características

Por ser uma ferramenta peso leve, a utilização do Snort é indicada para monitorar redes TCP/IP pequenas, onde pode detectar uma grande variedade do tráfego suspeito, assim como ataques externos e então, fornece argumento para as decisões dos administradores.

Os módulos que compõe o Snort são ferramentas poderosas, capazes de produzir uma grande quantidade de informação sobre os ataques monitorados, dado que é possível avaliar tanto o cabeçalho quanto o conteúdo dos pacotes, além de disponibilizar, por exemplo, a opção de capturar uma sessão inteira.

Snort

Características

O Snort monitora o tráfego de pacotes em redes IP, realizando análises em tempo real sobre diversos protocolos (nível de rede e aplicação) e sobre o conteúdo (hexa e ASCII). Outro ponto positivo desse software é o grande número de possibilidades de tratamento dos alertas gerados.

O subsistema de registro e alerta é selecionado em tempo de execução através de argumentos na linha de comando, são três opções de registro e cinco de alerta. O registro pode ser configurado para armazenar pacotes decodificados e legíveis em uma estrutura de diretório baseada em IP, ou no formato binário do tcpdump em um único arquivo.

Para um incremento de desempenho, o registro pode ser desligado completamente, permanecendo os alertas. Já os alertas podem, ser enviados ao syslog, registrados num arquivo de texto puro em dois formatos diferentes, ou ser enviados como mensagens WinPopup usando o smbclient.

Snort

Características

Os alertas podem ser enviados para arquivo texto de forma completa e o alerta rápido.

O alerta completo escreve a mensagem de alerta associada à regra e a informação do cabeçalho do pacote até o protocolo de camada de transporte.

A opção de alerta rápido escreve um subconjunto condensado de informação do cabeçalho alerta.

Snort

Características

Existe também, a possibilidade de utilizar métodos como o Database Plug-in por exemplo, para registrar pacotes em uma variedade de bases de dados diferentes (MySQL, PostgreSQL, entre outros), as quais contam com recursos próprios para efetuar consultas, correlações e dispõem de mecanismos de visualização para analisar dados.

Plataformas

O Snort deve trabalhar em todos os lugares que o *libpcap* trabalha, e o mesmo foi compilado com sucesso nas seguintes plataformas:

i386	Sparc	M68k/PPC	Alpha	Other	
X	X	X	X	X	Linux
X	X	X			OpenBSD
X			X		FreeBSD
X		X			NetBSD
X	X				Solaris
	X				SunOS 4.1.X
				X	HP-UX
				X	AIX
				X	IRIX
			X		Tru64
		X			MacOS X Server
X					Win32 - (Win9x/NT/2000)

Snort

Modos de trabalho

O Snort poderá assumir três modalidades a seguir:

- **Sniffer:** Está modalidade simplesmente captura os pacotes e imprime continuamente no console.

- **Packet logger:** Registra os pacotes capturados no disco rígido.

- **Network intrusion detection system:** Esta modalidade é a mais complexa e versátil, permitindo que o Snort analise o trafego da rede de encontro a regras definidas pelo usuário, executando diversas ações baseadas em suas regras.

Snort

IDS - Virtudes do SNORT

Extremamente Flexível:
- Algoritmos de Inspeção baseados em Regras.
- Sem falsos positivos inerentes.
- Controle Total do refinamento das regras.

Metodologias de detecção Multi-Dimensional:
- Assinaturas (Impressões Digitais) do Ataque.
- Anomalias no Protocolo.
- Anomalias no Comportamento.

Imensa Adoção (Comunidade SNORT):
- Dezenas de Milhares de Instalações (42 mil).
- Algumas das maiores empresas do mundo.(Microsoft, Intel,PWC..)
- Milhares de Contribuidores fazendo regras para novas vulnerabilidades.

Infra-estrutura de Suporte da Comunidade Open Source:
- Rápida Respostas às ameaças.
- Velocidade de Inovação.
- Velocidade de Refinamento.

Snort

IDS - Fraquezas do SNORT

Performance Modesta:
- Menos de 30mbps, para redes de até 10Mbps.

Interface Gráfica Limitada:
- Configuração do Sensor.
- Gerenciamento de Regras.

Implementação lenta e cansativa (pelo menos 10 dias).
Capacidade Analítica Limitada.
Sem Suporte Comercial:
- Dependência de pessoas "capacitadas", nem sempre estáveis...
- Gastos Significativos com Recursos Humanos.