INE5429-07208
Segurança em Computação
IDS e IPS

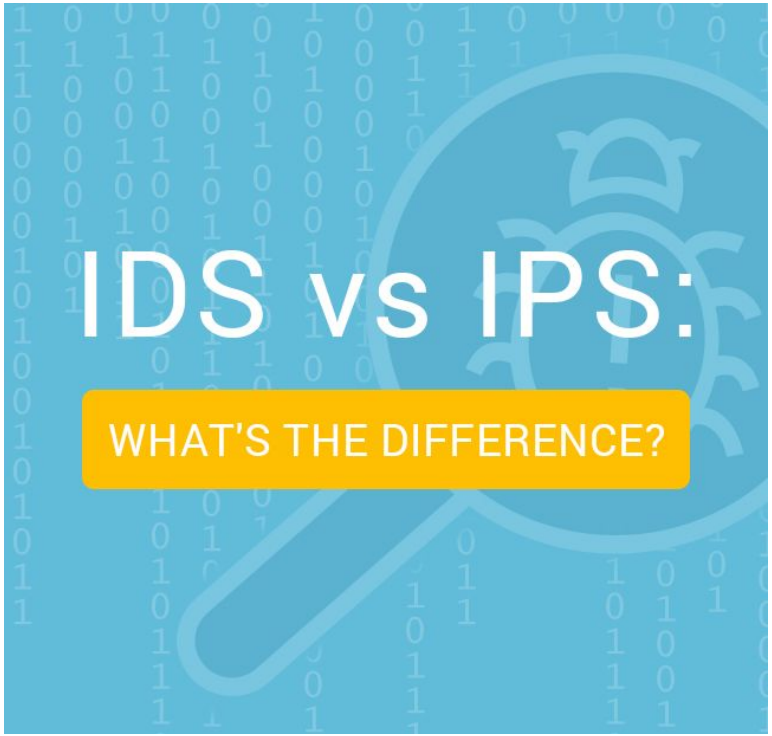
Prof. Jean Everson Martina

Definições

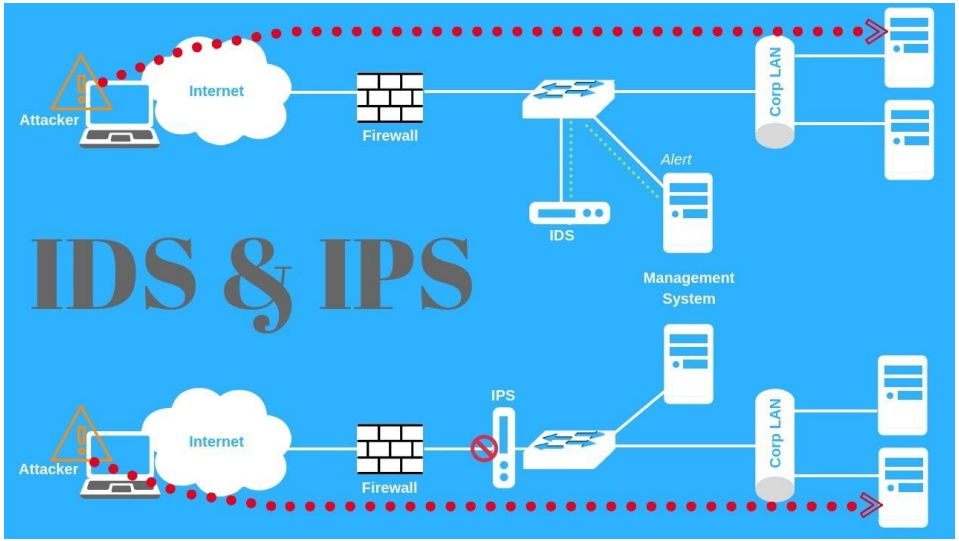
- Intrusão:
  - É qualquer conjunto de ações que tentem comprometer a integridade, confidencialidade ou a disponibilidade
- Os sistemas de Detecção de Intrusão ou de Prevenção de Intrusão são dispositivos de monitoramento de sistemas capazes de perceber e reagir a ocorrência de um ataque ou comportamento anormal e produzir uma resposta.
- As respostas providas pelo IDS/IPS tem por objetivo alertar e proteger um perímetro de rede e seus ativos

IDS versus IPS

- Sistema de detecção de intrusão (IDS): é um software que automatiza o processo de detecção de intrusão. A principal responsabilidade de um IDS é detectar atividades indesejadas e mal-intencionadas.
- Sistema de prevenção de intrusão (IPS): é um software que possui todos os recursos de um sistema de detecção de invasão e também tenta interromper incidentes.
- Hoje não faz mais sentido falar só de IDS!

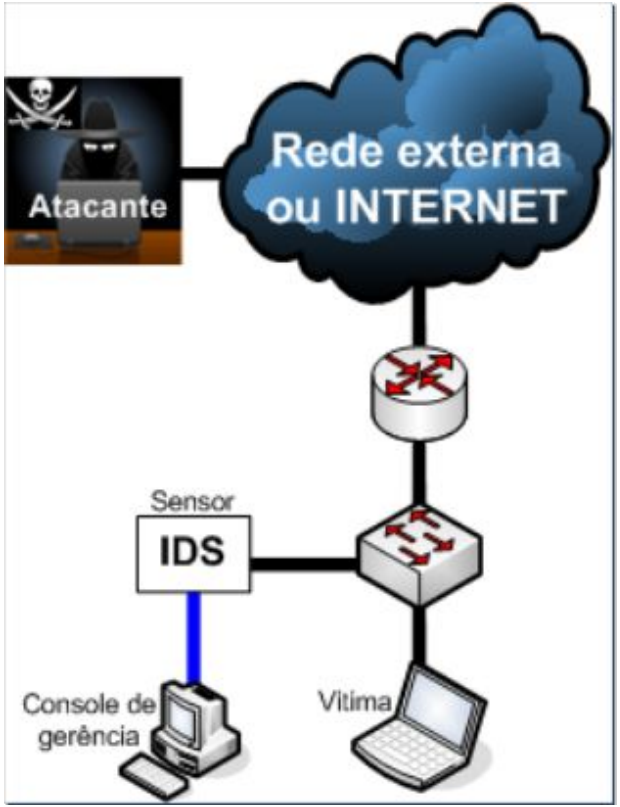


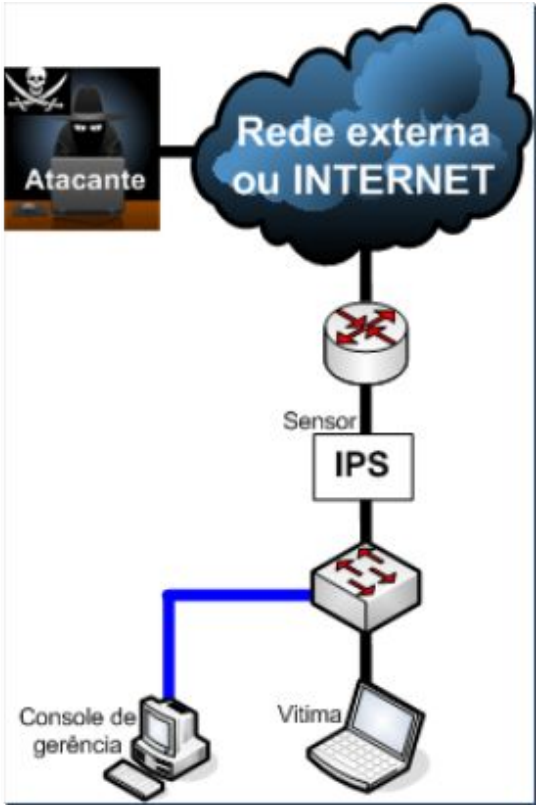
CARACTERÍSTICAS COMUNS DOS IDS E IPS



- Ambas as tecnologias são implantadas através de sensores.
- Ambas as tecnologias usam assinaturas para detectar padrões de uso indevido de tráfego de rede.
- Ambos podem detectar padrões atômicos (single-packet) ou padrões compostos (multi-packet)
- Ambos devem ter uma Política de Segurança bem planejada.

Promiscuous mode x Inline mode





Promiscuous Mode

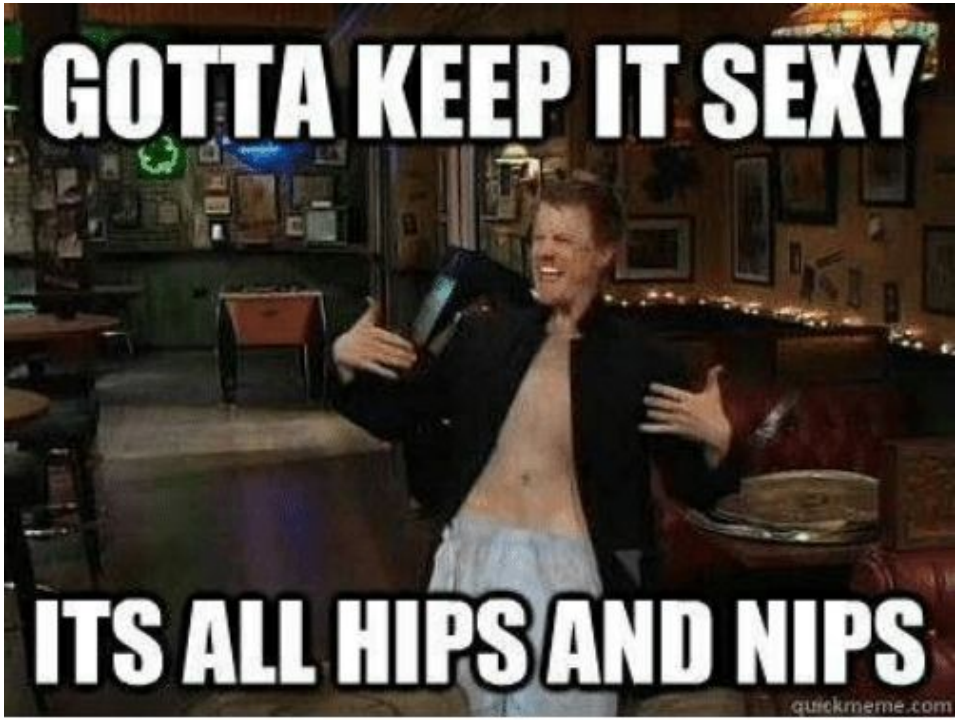
- VANTAGEM
  - Não gera impacto de latência ou jitter na rede
  - Se houver FALHA no sensor NÃO afetará a rede
  - Se houver SOBRECARGA no sensor NÃO afetará a rede
- DESVANTAGEM
  - Ação de resposta não pode parar o pacote que a desencadearam.
  - Ação de resposta necessita de um ajuste fino e preciso

Inline Mode

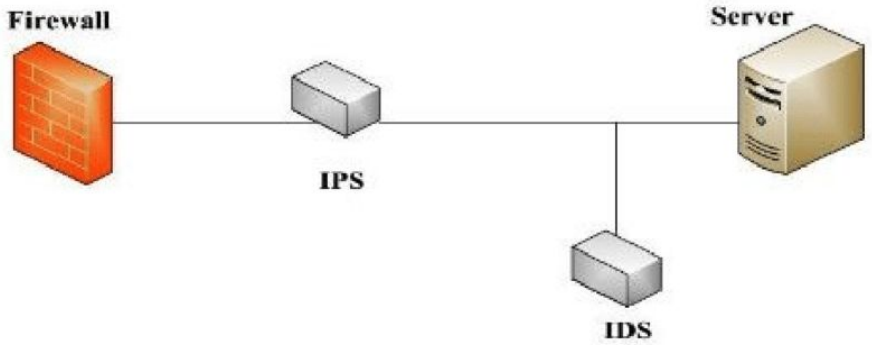
- VANTAGEM
  - Pode parar os pacotes que a desencadearam
  - Pode usar técnicas de normalização de fluxo contínuo
- DESVANTAGEM
  - Questões do sensor podem afetar o tráfego de rede
  - Se houver SOBRECARGA no sensor AFETARÁ a rede
  - Gera algum impacto de latência e jitter na rede

HIPS versus NIPS

- Host Based
  - VANTAGEM
    - É específico do host
    - Protege host após descriptografia
    - Fornece proteção de criptografia em nível de aplicativo
  - DESVANTAGEM
    - Dependente do Sistema Operacional
    - Eventos inferiores ao nível de rede NÃO serão vistos
    - O Host é visível para atacantes



HIPS versus NIPS

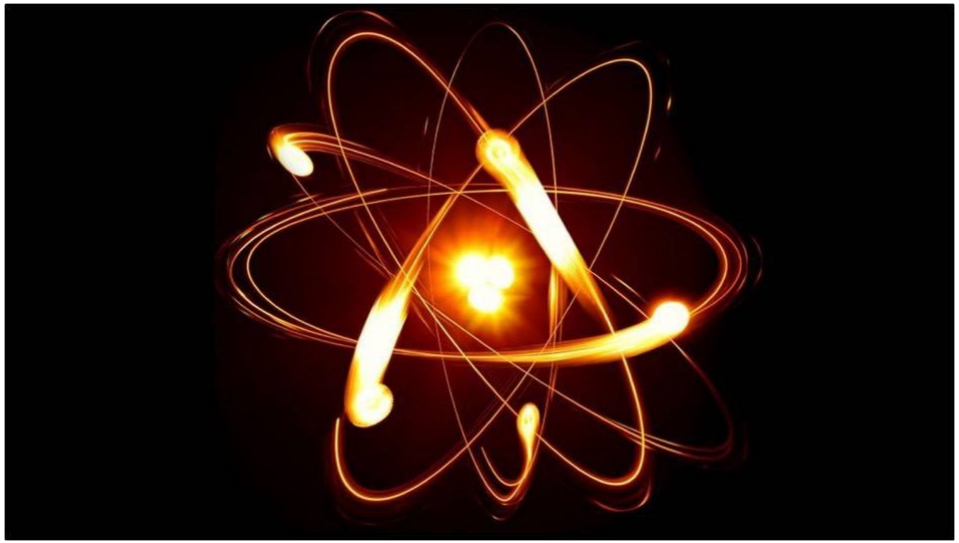


- Network Based
  - VANTAGEM
    - É o custo-efetivo
    - Não é visível na rede
    - Independe do Sistema Operacional
    - Eventos inferiores ao nível de rede serão vistos
  - DESVANTAGEM
    - Não pode examinar o tráfego criptografado
    - Não sabe se um ataque foi bem-sucedido

CARACTERÍSTICAS DA ASSINATURA:

- Um sensor IDS ou IPS realiza a correspondência entre uma assinatura e um fluxo de dados
- O sensor toma ações
- Assinaturas têm três atributos característicos:
  - tipo de assinatura
  - trigger da assinatura (disparo)
  - ação da assinatura

TIPOS DE ASSINATURAS:



- Atômico
  - Forma mais simples
  - Consiste em um único pacote, atividade, ou evento
  - Não necessita de sistema de intrusão para manter informações de estado
  - Fácil de identificar
- Composto ou Stateful
  - Identifica uma sequência de operações distribuídas em vários hosts
  - Assinatura deve manter um estado conhecido

TRIGGERS DE ASSINATURAS (DISPAROS):

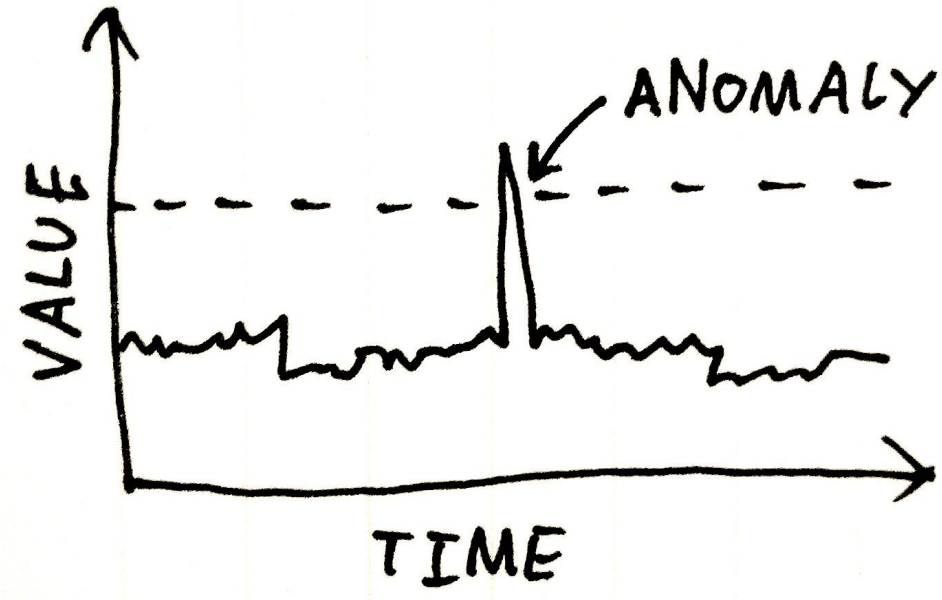
- Detecção baseada em padrões
- Detecção baseada em anomalia
- Detecção baseada em política
- Detecção baseada em Honeypot

Detecção baseada em padrões

- VANTAGENS
  - Fácil de configurar
  - Poucos falsos positivos
  - Bom design de assinatura
- DESVANTAGENS
  - NÃO detecta assinaturas desconhecidas
  - Grande quantidade de falsos positivos
  - Assinaturas devem ser criadas, atualizadas e sofrer um ajuste fino

Detecção baseada em anomalia

- VANTAGENS
  - Simples e confiável
  - Políticas personalizadas
  - Pode detectar ataques desconhecidos
- DESVANTAGENS
  - Saída genérica
  - Deve ser criada uma política

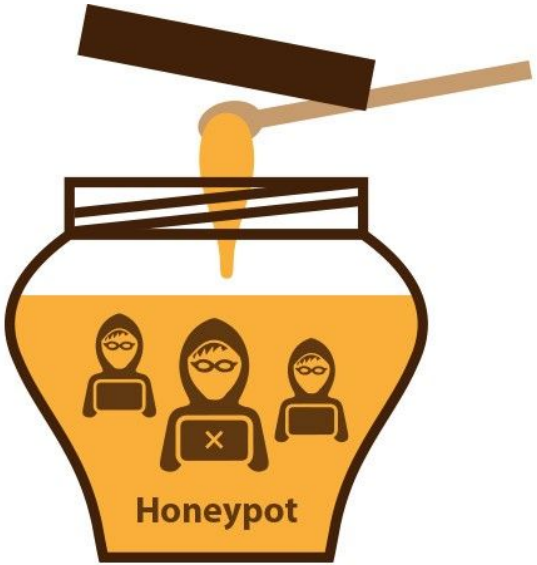


Detecção baseada em política

- VANTAGENS
  - Fácil configurar
  - Pode detectar ataques desconhecidos
- DESVANTAGENS
  - Perfil de tráfego deve ser constante

Detecção baseada em Honeypot.

- VANTAGENS
  - Janela para visualizar ataques
  - Distrair e confundir os atacantes
  - Diminuir a velocidade e evitar ataques
  - Coletar informações sobre o ataque
- DESVANTAGENS
  - Servidor de honeypot dedicado
  - Servidor de honeypot não deve ser confiável



Ação da assinatura

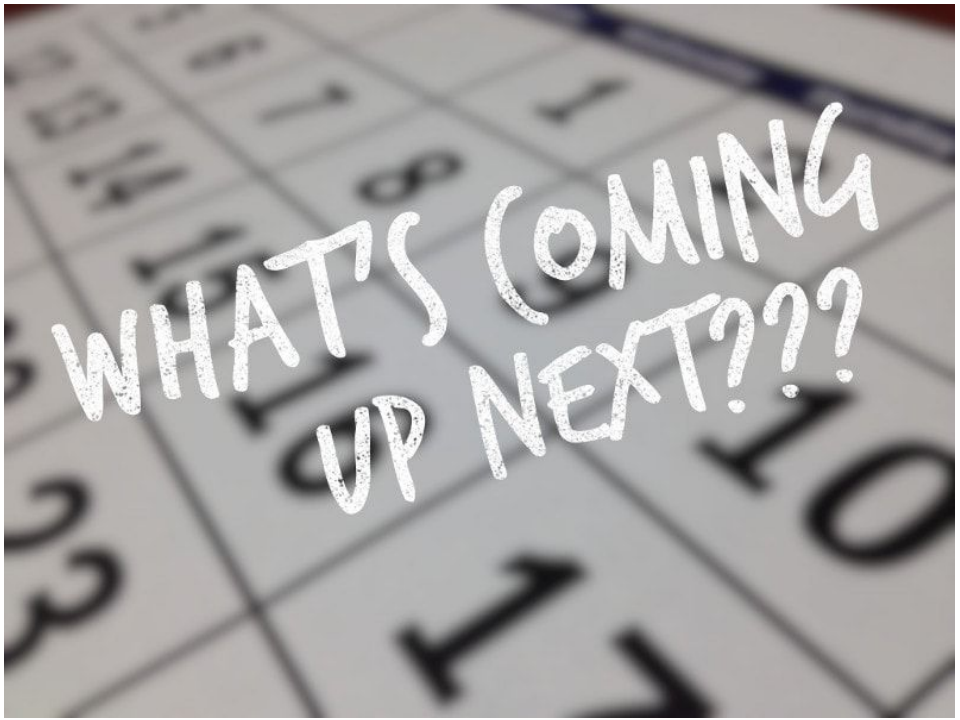
- Reportar
  - Pode gerar muitos dados
  - Processá-los pode ser tornar difícil
- Bloquear
  - Pode gerar negação indevida
  - Mas é extremamente eficaz
- Contra-atacar
  - Deve ser considerado o ultimo recurso
  - O contra-ataque é difícil de ser implementado e pode instigar o atacante a revidar.

BOAS PRÁTICAS

- Grandes redes devem atualizar os pacotes preferencialmente de forma automática;
- Quando a atualização dos pacotes de assinatura for necessária, deve ser baixada para um servidor seguro na rede de gerência, com um HIDS/HIPS instalado;
- Criar uma nova assinatura para detectar e mitigar um ataque específico, se a atualização não existir;

Próximas Aulas

- Prática:
  - Trabalho Individual V
    - Envolve todo este conteúdo que vimos na aula de hoje e o que veremos nas próximas.
  - Próxima Aula Teorica:
    - Detecção, Contenção e Resposta / Recuperação de desastres



Perguntas?

jean.martina@ufsc.br