Detecção de Intrusão com Snort

Professora: Kalinka Branco
Estagiário PAE: Daniel Pigatto

Instituto de Ciências Matemáticas e de Computação
Universidade de São Paulo

Organização

1. Intrusão
2. Sistemas de Detecção de Intrusão
   - Classificação
   - Taxonomia
   - Forças e Fraquezas
3. Snort
   - Requisitos
   - Funcionamento
4. Cenário da Aula Prática

Intrusão

Intrusão

É o ato de avançar ou tentar ganhar acesso a informações sem convite, direito ou boas vindas.

Objetivo

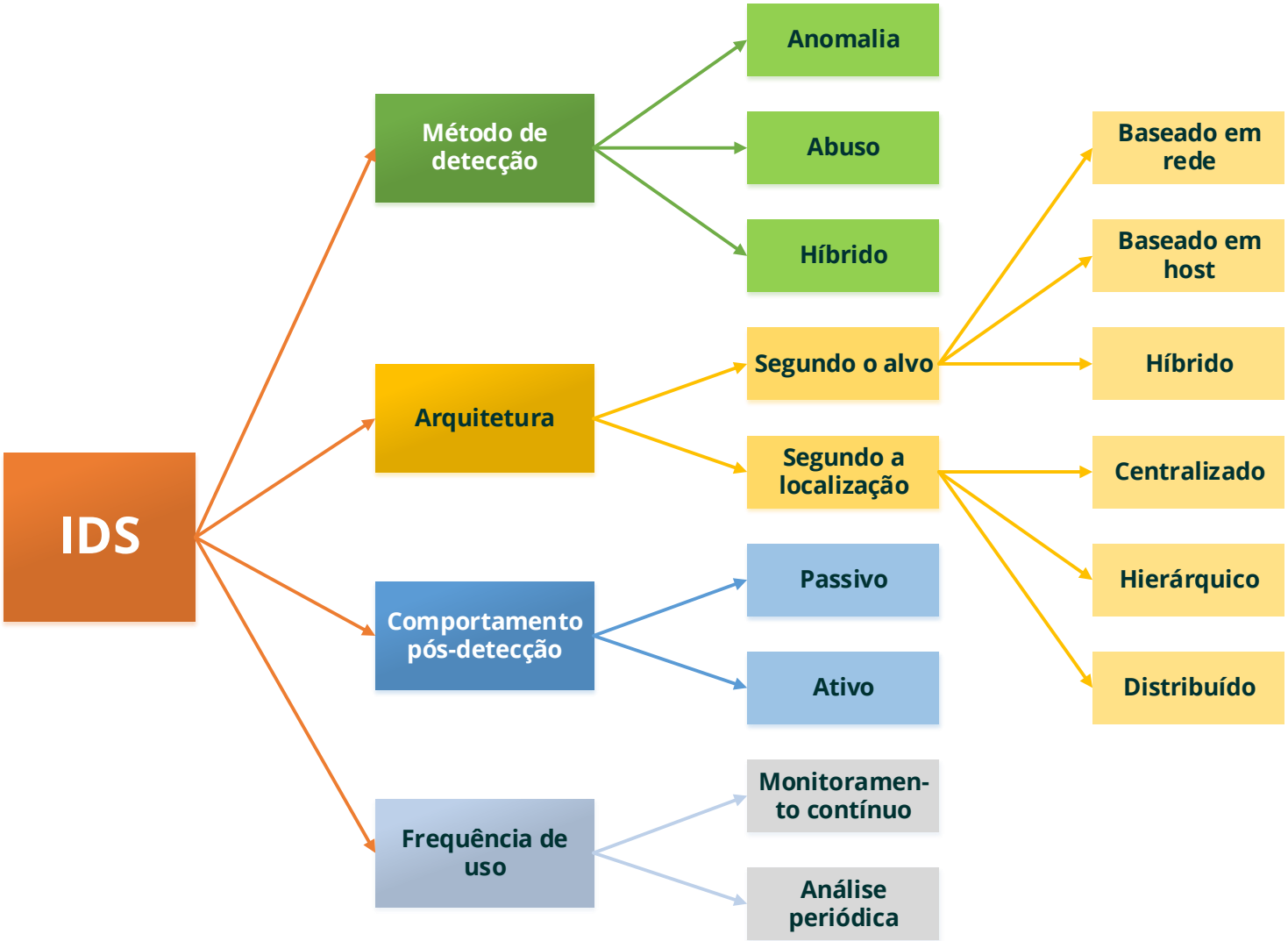
Danificar o sistema ou causar distúrbios às informações existentes/gerenciadas pelo sistema.

Sistemas de Detecção de Intrusão

Intrusion Detection System – IDS

É um dispositivo ou software que monitora a rede e o sistema a fim de encontrar atividades maliciosas. Quando algo suspeito é identificado, o IDS notifica uma estação de monitoramento, que vai tomar as medidas adequadas.

Classificação IDS



Taxonomia

- IDS (*Intrusion Detection System*)
  - NIDS (*Network-based IDS*)
  - HIDS (*Host-based IDS*)
  - DIDS (*Distributed IDS*)
  - GIDS (*Gateway IDS*)
- IPS (*Instrusion Prevention System*)
  - NIPS
  - HIPS

Forças e Fraquezas

Forças

- Detecta ataques remotos;
- Tempo real;
- Pouco impacto no desempenho dos sistemas;
- Prevenção (IPS).

Fraquezas

- Perda de pacotes em redes com tráfego elevado;
- *Switches*: dividem as redes em pequenos segmentos e e provêm ligações lógicas diretas entre as estações por meio de portas, dificultando a detecção.
- Criptografia.

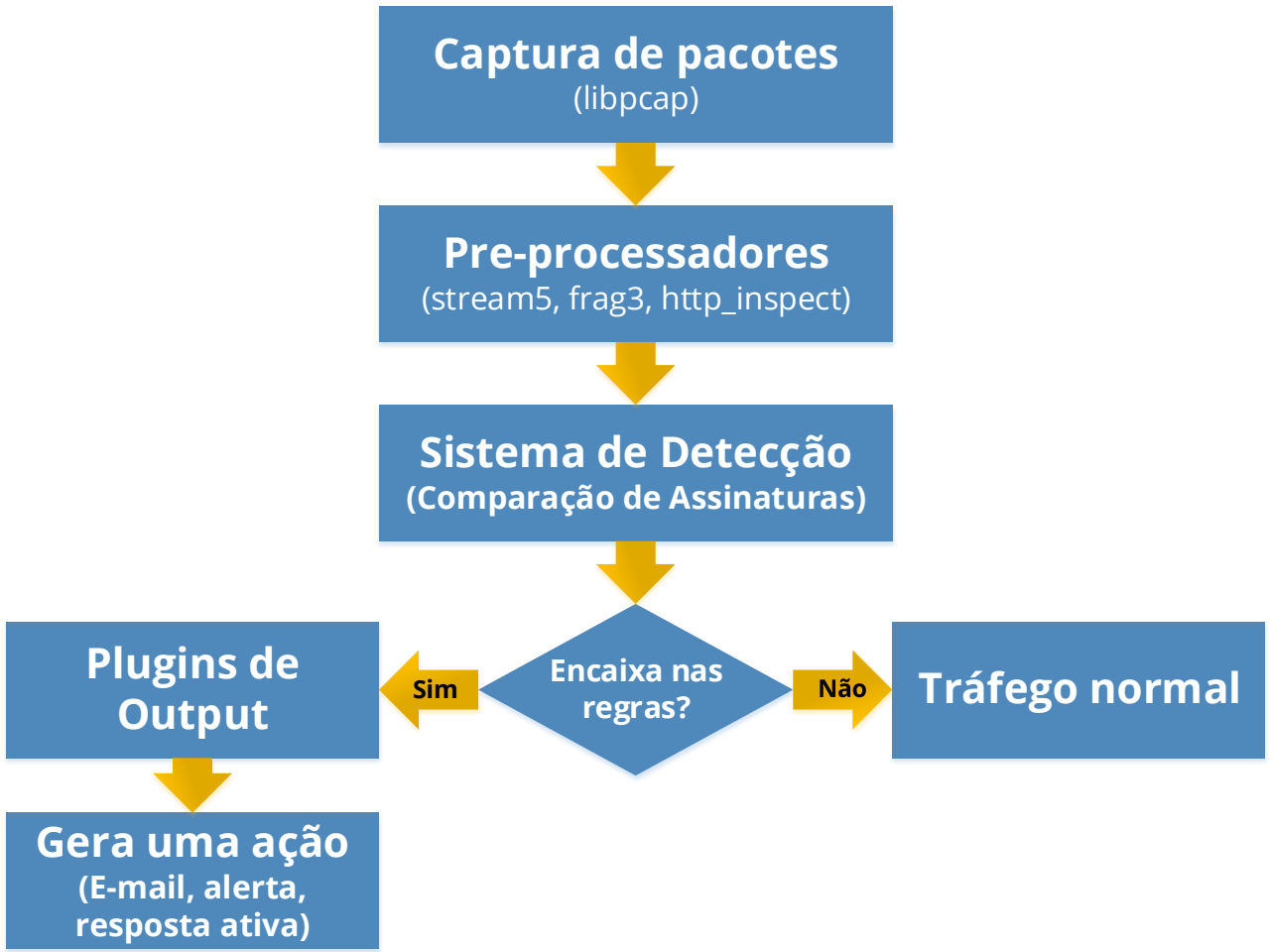
Snort

- NIDS;
- É o mais utilizado;
- Bastante eficiente;
- Possui vários modos de operação;
- Suporte ágil da comunidade *Open Source*.

Requisitos

- Disco rápido;
- Rede rápida (interface);
- Memória RAM (quanto mais, melhor).

Funcionamento



Cenário da Aula Prática (Netkit)