Universidade Federal do Pará
Centro de Tecnologia da Informação e Comunicação

Sistemas de Detecção e Prevenção de Intrusão - IDS/IPS

Glenon Mateus Barbosa Araújo

11 de abril de 2017

Sumário

IDS/IPS

Definição

- O que é Sistema de Detecção e Prevenção de Intrusão (IDS/IPS)?
  - mecanismo capaz de identificar ou detectar a presença de atividades intrusivas
  - processos utilizados na descoberta de utilizações não autorizadas de dispositivos de rede ou de computadores
  - tem por objetivo impedir possíveis ataques
  - trabalha maneira reativa e informativa
  - diminui o risco de comprometimento de um ambiente

IDS/IPS

Tipos

- *Network Based*
  - monitora o tráfego da rede
  - analisa a rede e a atividade dos protocolos para identificar atividades suspeitas
- *Host Based*
  - monitora características do dispositivo e os eventos que acontecem no *host*
  - tráfego da rede para o dispositivo, os processos em execução, os *logs* do sistema e o acesso e alteração em arquios e aplicações

IDS/IPS

Tipos

- Conhecimento
  - banco de dados (assinaturas) de perfis de vulnerabilidades de sistemas já conhecidos, para identificar tentativas de intrusão ativas
  - política de atualização continua das assinaturas
- Comportamento
  - analisa o comportamento do tráfego seguindo uma linha de base ou padrão de atividade normal do sistema

IDS/IPS

Tipos

- Ativo
  - bloqueia ataques e atividades suspeitas, sem qualquer intervenção humana
  - importante uma parametrização adequada a fim de minimizar falsos positivos, bloqueando conexões legítimas
- Passivo
  - monitora o tráfego, identificando potenciais ataques, gerando alertas
  - não interfere na comunicação

Fases de Implantação

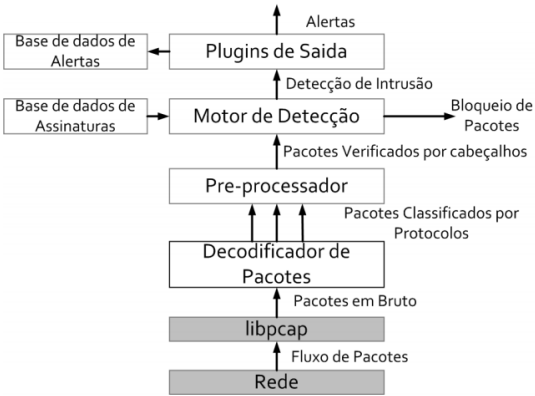
Levantamento

- Definir quais as ferramentas mais conhecidas de IDS/IPS
  - Suricata
  - Snort
- Identificar diferença entre elas
  - *multithread*

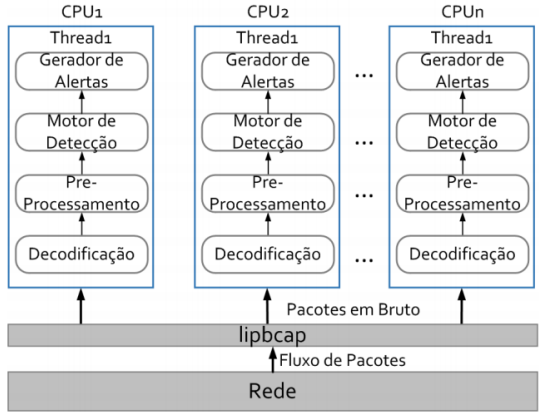
Fases de Implantação

Levantamento

Snort



Suricata



Fases de Implantação

Preparação do Ambiente

- Escolher uma rede com um tráfego considerado - ILC
- *Port mirroring* dessa rede para nosso servidor de teste
- Instalação e configuração das VMs com as mesmas configurações (memória, processamento)
- Problema com a formatação dos arquivos de logs do Snort (unified2 - json) - idstools-u2json

Fases de Implantação

Testes

- Escolha da base de assinaturas
  - p2p
  - *botnet*
  - DDOS
  - *worms*
  - *exploit*
  - *scan*
- Ferramentas para simulação de ataques
  - Pytbull
  - Kali Linux

Fases de Implantação

- Análise do comportamento de cada IDS/IPS
  - falsos positivos/negativos
  - quantidade de recurso usado num determinado período
  - quantidade de log gerado