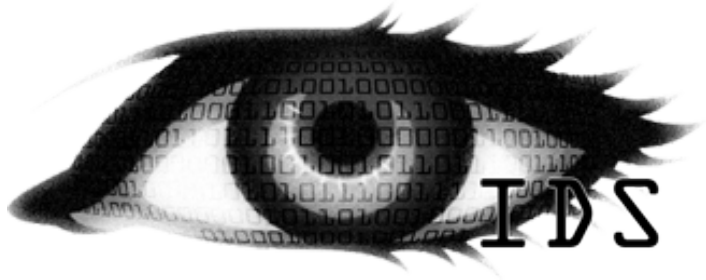
Sistemas de Detecção de Intrusão

André Silveira de Araujo
Luciano Silva Leite
Lygia Marina Mendes da Costa



IDS

Detecção de intrusão é o monitoramento de eventos ocorrentes em um sistema ou rede de computadores em busca de ações suspeitas.

IDS

Funções:

- Monitorar atividades de interesse.
- armazenar informações sobre eventos observados.
- Emitir alerta para os administradores.

Métodos de detecção

- *Signature-Based Detection*.
  - Detectar ameaças conhecidas.
- *Anomaly-Based Detection*.
  - Detectar atividades incomuns.
- Stateful Protocol Analysis

IDPS

Respostas a atividades suspeitas:

- Interrompe a comunicação
- Configurar outros dispositivos.
- Altera conteúdo.

IDPS

- Identificar problemas na politica de segurança.
- Coleta informações sobre ameaças.
- Coibe tentativas de ações não permitidas.

Tipos de IDPS

- Network-based.
- Wireless.
- Network Behavior Analysis.
- Host-based.

Network-based IDPS

- Monitora trafego em um seguimento de rede.
- Analiza protocolos de rede, transporte e aplicação.
- Não detecta ameaças com tráfego de dados criptografados.

Wireless IDPS

- Semelhante ao network-based.
- Um sensor monitora apenas um canal por vez.
- Monitora apenas protocolo de rede Wireless.
- Mais precisa que as outras tecnologias.

Network Behavior Analysis System

- Identifica fluxo de rede anormal.
- Mais eficiente contra ataques DoS.

Host-based IDPS

- Monitora hosts (críticos).
- Monitora alterações em arquivos do sistema, modificações em privilégios dos usuários, processos do sistema e programas.

Componentes dos IDPS

- Sensor or Agent.
- Management Server.
- Database Server.
- Console.

A arquitetura de rede do IDPS

- Na própria rede monitorada.
- Management network.
- Virtual manangement network.

Dificuldades

- Técnicas de evasão.
- Falsos negativos e falsos positivos.
- Tunning.

Integrando tecnologias IDPS

- Impacto de falhas é reduzido.
- Integração direta ou indireta.
- Firewalls e Anti-vírus.

Exemplos de IDS

- RealSecure
  http://www.iss.net
- Snort
  http://www.snort.org
- Open Source Tripwire
  http://sourceforge.net/projects/tripwire/
- Bro
  http://bro-ids.org

Bibliografia

[1] Patrício, Daiane; Raimundo, Lidiane; Correa, Rosana; Pezzi, Daniel (2006) “Detecção de Intrusão”, In Sulcomp

[2] Werlinger, Rodrigo; Hawkey, Kirstie; Muldner, Kasia; Jaferian, Pooya; Beznosov, Konstantin (2008) “The Challenges of Using an Intrusion Detection System: Is It Worth the Effort?”, In Proceeding, 4th Symposium on Usable Privacy and Security

Bibliografia

[3] Scarfone, Karen; Mell, Peter (2007) “Guide to Intrusion Detection and Prevention Systems (IDPS)”, In National Institute of Standards and Technology, Information Technology Laboratory, Computer Security Division

[4] Fuchsberger, Andreas (2005) “Intrusion Detection Systems and Intrusion Prevention Systems”, In Information Security Technical Report, Issue 10, p. 134-139

Bibliografia

[5] Vaz, Tiago; Camões, Tássia; Araújo, Gorgonio (2004) “Sistemas de Detecção de Intrusão Livres: suas limitações e uma arquitetura proposta sobre concentração de mensagens e correlacionamento de eventos”, In IV ERBASE

[6] Ferreira, Eduardo (2011) “Detecção autônoma de intrusões utilizando aprendizado de máquina”, In USP, Instituto de Ciências Matemáticas e de Computação, Dissertação de Mestrado