This work is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License.

To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-sa/3.0/

Hugo González

@hugo_glez

http://atit.upslp.edu.mx/~hugo/

10 años UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Análisis de Sistemas de Detección de Intrusos

Hilda Rocio Puente
Hugo Francisco González Robledo

MCIS 2006

Agenda

- Antecedentes
- Sistemas de detección de intrusos
- Tipos de IDS
  - NIDS
  - HIDS
- Problemas
- Herramientas
- Snort
- Más alla, complementos
- Conclusiones

Antecedentes

- En estos tiempos la inseguridad en la red es algo inminente.
- Múltiples peligros ataques profesionales los menos, y automáticos los más.
- Existen muchas herramientas de seguridad, nos enfocamos a describir los IDS, su funcionalidad y sus alcances.

Sistema de Detección de Intrusos IDS's

- Los IDS's son herramientas de seguridad que sirven para detectar y avisar de posibles ataques o intrusiones.

Funciones

- Proteger la red de las amenazas que aparecen al incrementar la conectividad
- Puertos abiertos y actividades permitidas:
  - DNS, Web, Correo electrónico, IRC, etc.
- Ataques conocidos contra estos servicios :
  - Patrones de ataques

Funcionamiento

- Gran capacidad de análisis de datos
- Son capaces de registrar intentos de ataques
- Pueden activar alarmas en tiempo real
- Junto con los Firewalls forman una pieza fundamental en la infraestructura de seguridad de una organización

Clasificación de IDS’s

- IDS de red (NIDs)
- IDS de sistemas (HIDs)

IDS de red (NIDs)

- Capturan y analizan el trafico de la red
- Los métodos para el análisis son:
  - detección basado en firmas
  - detección de anomalías

  - Intrusion detection
  - Extrusion detection

IDS de sistemas (HIDs)

- Su funcionamiento se basa en la información local del equipo
- Generalmente basado en logs y modificaciones al sistema.

- OSSEC

Problemas de los NIDS

- Técnicas de evación (como la fragmentación)
- Ataques polimorficos
- Ataques de denegación de servicos
- Redes de alta velocidad
- Falsos positivos
- Falsos negativos

Herramientas libres y comerciales

- Dragón Enterasys Networks
- NetRanger
- Internet Security Systems
- Snort
- Shadow
- etc.

SNORT

- Es open source
- Es el estándar de facto.
- Multiplataforma
- Flexible
- Estable
- Escalable

Snort

- Modos de trabajo:

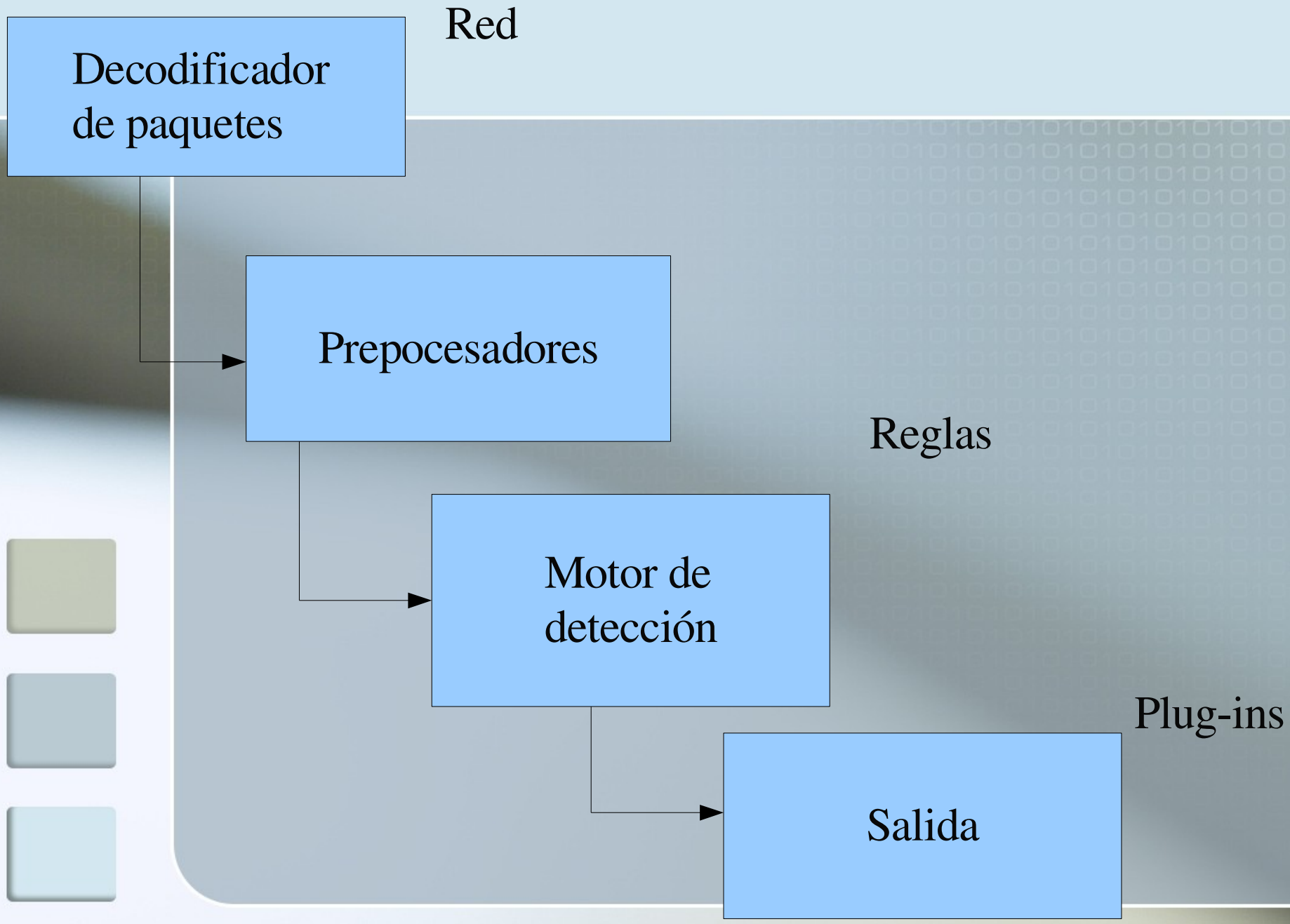
  -Es un Sniffer

  -Detecta y alerta los ataques en tiempo real

- Es un NIDs
- Diferentes formas de implementarlo, un solo sensor, múltiples sensores.

Arquitectura de Snort

- Decodificador de paquetes
- Preprocesadores
  - (Reglas)
- Motor de detección
- Etapa de salida
  - logs, BD


Red
Decodificador de paquetes
Prepocesadores
Reglas
Motor de detección
Plug-ins
Salida

Consolas

- ACID
  - Analisis Console Intrusion Detection
- BASE
  - Basic Analisis and Security Engine
- Sguil (la mejor según Bejtlich)

Mas allá de la detección

- Añadiéndole un modulo al IDS este cambia a un estado activo que le permite realizar ciertas tareas de prevención y se convierte en un IPS
- Como funciona:
  - detiene el ataque en el momento
  - puede desviar el ataque a equipos o redes preparados (honeypot, honeynets)

Funcionamiento

- Primero se procesa el trafico
- Se comparan los patrones en las reglas preconfiguradas (actualizarlas constantemente)
- Alertas logueadas
- Snort-online: posibilidad de interactuar con las reglas de iptables (IPS)

Complementos de Snort

- Oinkmaster = actualización de reglas de Snort
- Blockit = monitoriza los archivos de alerta de Snort y crea reglas para IPTables, IPChains, IPFWADM, o Checkpoint Firewall
- Barnyard = sistema de salida para Snort

Resultados

- Durante el último año al red el ITSLP se ha monitoreado con snort de 3 formas.
  - Fuera del firewall (detección de ataques)
  - Dentro del firewall (detección de intrusiones de red)
  - Dentro del firewall con diferente configuración (detección de virus y ataques internos)
- ACID permite analizar los resultados

- Ataques en los últimos dias
  - 800 (escaneos, ftp brute force, http XSS, DCOM exploit)
- Intrusiones
  - 80 Ataques a aplicaciones, el firewall de estados no los detiene, la aplicación si. (ftp, ssh brute force, http XSS, SQL)
- Extrusiones
  - 1 virus o gusano. Laptop externa.

Conclusiones

- Los IDS’s no sustituyen a ninguna de las soluciones de seguridad existentes, sino por el contrario la idea es complementar los elementos actuales y fortalecer la seguridad de cualquier infraestructura.
- Futuro
  - Aplicaciones integradas
  - IPS/IDS inteligentes
  - Self Defending Networks

Recomendaciones

- Definir una política de seguridad y darla a conocer
- Contar con herramientas para minimizar los problemas como son: antispam, antivirus, antispyware, firewall (todo en uno)
- NIDS y HIDS en equipos principales y sobre todo actualizados.

Preguntas !

hugo.gonzalez@itslp.edu.mx

- Under CC 2.5, by: