Propuesta de modelo para un Sistema Inteligente de Detección de Intrusos en Redes Informáticas (SIDIRI)

VII Jornada Nacional de Seguridad Informática

COMPUTACIÓN FORENSE: RASTREANDO LA INSEGURIDAD INFORMÁTICA

JUNIO 20, 21 Y 22 DE 2007

Biblioteca Luis Ángel Arango
Calle 11 No 4-14
Bogotá D.C., Colombia.

Conferencista:

Juan David Arroyave

ifjuar@eia.edu.co

ACIS

Agenda

- Introducción
- Amenazas y herramientas aliadas a la seguridad de la información
- Sistemas de Detección de Intrusos (IDS)
- Redes Neuronales Artificiales (RNA)
- Ventajas de usar RNA en IDS
- Modelo SIDIRI
- Desventajas y conclusiones

Introducción

La información es la base de las actividades humanas, del desarrollo social y económico. Estamos en la bien llamada era de la información, en donde se hace cada vez más patente la necesidad de mantener la información segura, íntegra, y disponible, una labor no muy fácil.

Las empresas tienen que pensar en proteger la información que mantiene el negocio, ya que la internet es desde cualquier punto de vista una pasarela de información indispensable para obtener ventajas competitivas, conocer entonces a quienes pueden atentar contra la seguridad de la información y tener medios para impedirlo es una obligación.

Amenazas y herramientas aliadas a la seguridad de la información

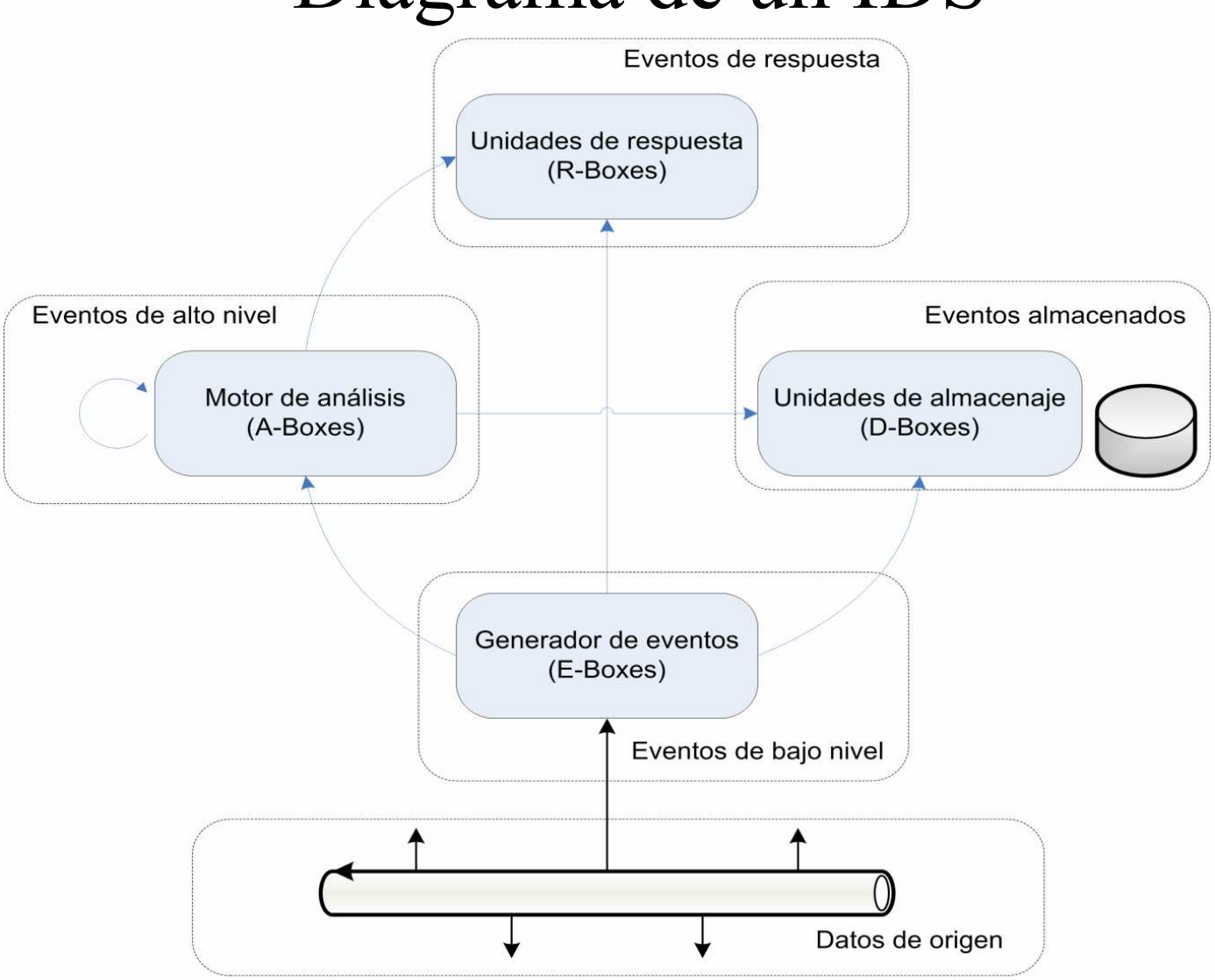
- **Amenazas**
  Hackers
  Script Kiddies
  Personal inconforme o desprevenido

- **Herramientas aliadas**
  Firewalls
  VPN
  Antivirus
  Antispam
  IDS

Sistemas de Detección de Intrusos (IDS)

Es un programa que detecta intrusiones a una red determinada, es el guardián de nuestra red, la alarma que nos indica los posibles ataques de los cuales estamos siendo víctimas.

Diagrama de un IDS



Redes Neuronales Artificiales (RNA)

- Se trata de un sistema conexionista de nodos en una red que colabora para producir un estímulo de salida.

- Las RNA tienen una concepción que basa su versatilidad y simplicidad en el sistema nervioso animal con cualidades como: aprendizaje, auto organización, tolerancia a fallos, flexibilidad, respuesta en tiempo real.

Ventajas de usar RNA en IDS

- La red aprenderá de manera autónoma a partir de los ejemplos, lo que disminuirá el tiempo y esfuerzo del proceso de "*finetunning*" que se necesita para su correcto funcionamiento

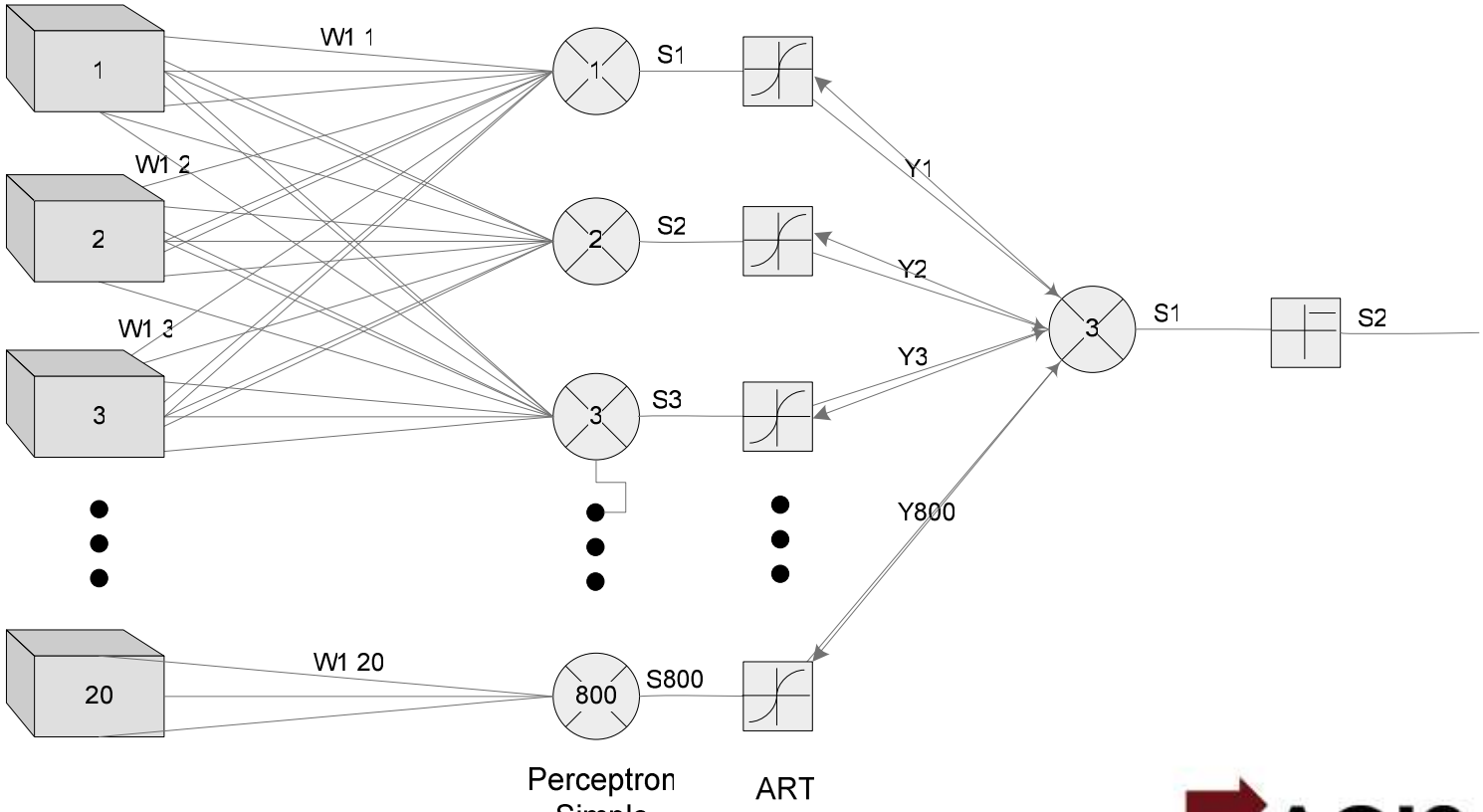
- La red neuronal artificial se puede adaptar a nuevos comportamientos, la cual hace al sistema mucho más flexible a variaciones y modificaciones de los métodos de intrusión actualmente conocidos (Base de conocimiento)

- Disminuir la cantidad de falsos positivos y falsos negativos que presentan los sistemas IDS basados en firmas

- La red infiere ataques que no aprendió, y puede adaptarse a los que el administrador de red cual lo convierte en un sistema, de cierta manera, heurístico.

Modelo SIDIRI

El modelo SIDIRI es una propuesta de A-box para un IDS basado en redes neuronales artificiales, para protocolos TCP/IP.



Desventajas y conclusiones

Desventajas

- Variabilidad del sistema
- Posee muchos parámetros configurables y esto crea muchos problemas a la hora de hacerle *finetunning*.
- La representación de los datos para que el sistema opere con ellos, y su adquisición por medio de los elementos de E-box
- Posible pérdida de información discriminante valiosa al hacer conversión de datos
- Poca o nula trazabilidad de los ataques.

Conclusiones

- El desarrollo de IDS es un complejo campo que debe ser abordado con una perspectiva que ayude a enfrentar el problema gigante que representa la seguridad de la información, es por esta razón que se hace necesario abordar el problema de manera distinta a la que se usa actualmente, una opción para hacerlo son los sistemas inteligentes, en nuestro caso las redes neuronales artificiales.
- Esta investigación y propuesta de modelo SIDIRI será desarrollada como trabajo de grado por los ponentes del presente artículo.

Referencias bibliográficas

- Wikipedia: La Enciclopedia Libre. *Ataque de denegación de servicio* [en línea]. [ref. de 27 de Abril de 2007]. http://es.wikipedia.org/wiki/Ataque_de_denegaci%C3%B3n_de_servicio
- Wikipedia: La Enciclopedia Libre. *Red neuronal artificial* [en línea]. [ref. de 21 de Abril de 2007]. http://es.wikipedia.org/wiki/Red_neuronal_artificial
- BARRERA GARCÍA-OREA, Alejandro. Universidad Politécnica de Madrid. *Presente y Futuro de los IDS* [en línea]. 2005. [ref. de 16 de Febrero de 2007] http://www.neurosecurity.com/whitepapers/futureIDS.pdf
- BALUJA GARCÍA, Walter; ESCANDÓN BON, Rebeca. Instituto Superior Politécnico José Antoni Echevarría. *Empleo de las redes neuronales en la detección de intruso*. VIII Seminario Iberoamericano de Seguridad en las TICs 2007. http://www.segurmatica.co.cu/descargas/info2007/redesneuronales_ids.ppt
- PINACHO, Pedro Pablo; VALENZUELA Tito. Universidad de Santiago (Chile). *Una Propuesta de IDS Basado en Redes Neuronales Recurrentes* [en línea]. México DF, Octubre de 2003. [ref. de 13 de Marzo de 2007] http://www.criptored.upm.es/guiateoria/gt_m291b.htm

MUCHAS GRACIAS POR SU ATENCIÓN

Preguntas e Inquietudes