CONCEPTES AVANÇATS DE SISTEMES OPERATIUS
Departament d'Arquitectura de Computadors

NIDS(Network Intrusion Detection System)

(Seminaris de CASO)

Autors

Alberto Rodrigo Fernández

¿Qué es?

- Un IDS es un sistema de detección de intrusos.

- HIDS (Host Intrusion Detection System):
  - IDS que trabaja con la información recogida dentro de un solo host.

- NIDS (Network Intrusion Detection System):
  - IDS que trabaja con los datos que circulan a través de la red.

¿Qué es un NIDS?

- IDS que trabaja con los datos que circulan a través de un segmento de red.
- Se dedica a monitorizar la red en busca de intentos de posibles accesos no autorizados.
- Complemento al sistema de seguridad.
- Funciona como un sniffer.

¿Por qué es necesario un NIDS?

- Alerta ante ataques.
- Capacidad de reacción.
- Análisis posterior en caso de intrusión.
- No debe ser substituto de una política de seguridad.

¿Para qué sirve?

- Monitoriza todo el tráfico que pasa por un segmento de red en busca de intentos de posibles malos usos o accesos no autorizados.
- Filtra el tráfico.
- Detecta tráfico maligno, habitualmente mediante un conjunto de reglas.
- Lanza alertas.

¿Qué conceptos utiliza?

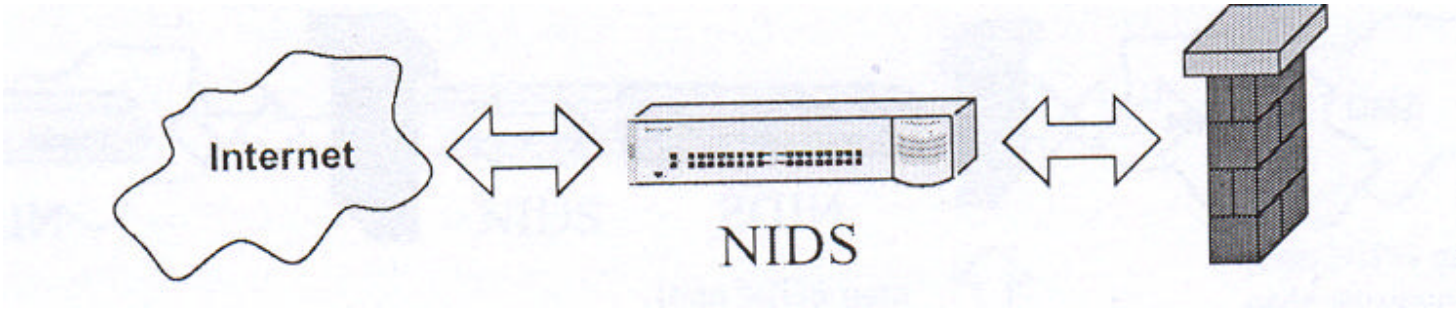
- Poder leer todo el tráfico de red :
  - Interface de red en modo promiscuo.
- Filtros que descartan el tráfico que no interesa analizar :
  - Reduce la cantidad de trabajo a realizar.
- Detectar tráfico dañino :
  - Mediante conjuntos de reglas que crean una serie de alertas.
  - Comparación del tráfico detectado con las reglas del programa.
- Alertas :
  - Se tratan como quiera el usuario.
  - Más habituales : logs en ficheros de texto o bases de datos.
  - Incluso envio de correos electrónicos o SMS al móvil.

¿Dónde colocar un NIDS?

- Al instalar un NIDS debe estudiarse en que lugar de la red lo vamos a situar.
- No hay reglas fijas. Depende de la estructura de la red.
- Varias formas :
  - Delante del firewall.
  - Detrás del firewall.
  - Combinación de los dos casos.
  - Firewall/NIDS.
  - Combinaciones avanzadas.

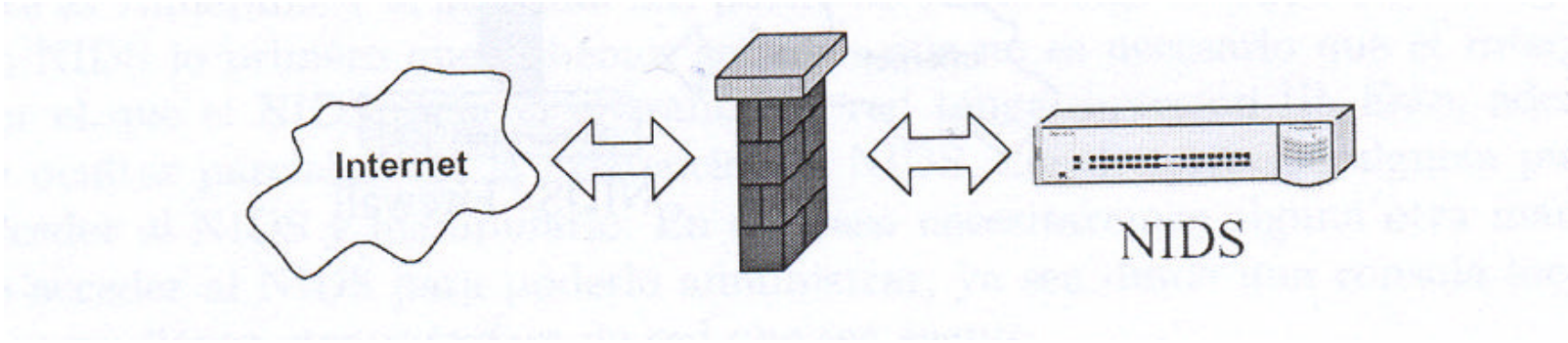
¿Dónde colocar un NIDS? (2)

- Delante del firewall :
  - Se pueden comprobar todos los ataques que se produzcan. No todos tendrán éxito.
  - Genera gran cantidad de información en los logs.
  - Firewall bloqueará los ataques.
  - Exceso de información puede ser contraproducente. Perder de vista ataques efectivos.



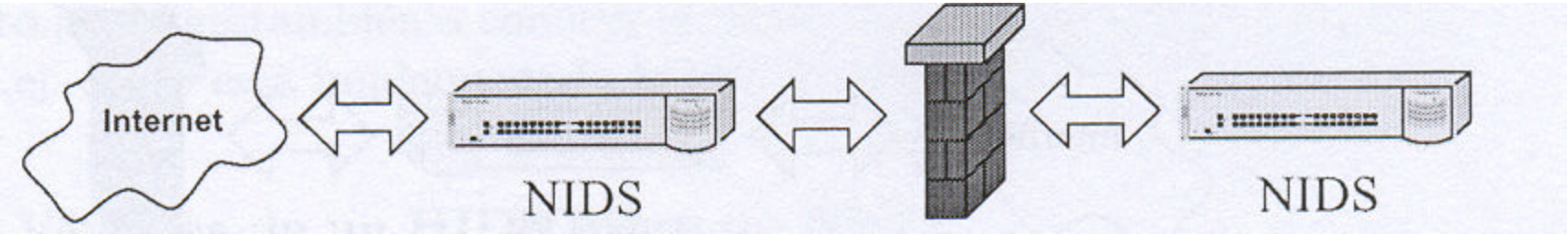
¿Dónde colocar un NIDS? (3)

- Detrás del firewall :
  - Monitoriza únicamente el tráfico que haya entrado realmente en la red, no ha sido bloqueado por el firewall.
  - Cantidad de logs inferior.
  - Ataques detectados potencialmente mucho más peligrosos.



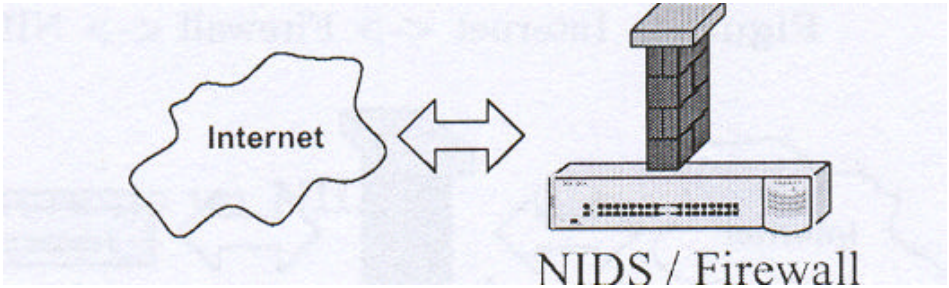
¿Dónde colocar un NIDS? (4)

- Combinación de los dos casos anteriores :
  - Control mucho mayor.
  - Ir mejorando la seguridad en caso de encontrar que deja pasar tráfico que no debería.
  - Correlación entre ataques detectados en un lado y otro.
  - Contrapartida : dos máquinas para implementarlo.



¿Dónde colocar un NIDS? (5)

- Firewall / NIDS:
  - En caso de no tener máquinas suficientes :
    - Una máquina hace de firewall y de NIDS a la vez.
  - Igual que primer caso. Monitoriza todo el tráfico de la red.



- Combinaciones avanzadas :
  - Necesidades de seguridad más altas. Cada NIDS monitorice un segmento de red o hosts individuales.

Ataques a un NIDS

- Importancia de la seguridad del NIDS.
- No sirve de nada registrar los accesos no deseados si el atacante puede borrar los logs creados.
- NIDS no pueda escuchar el tráfico.
  - Mediante DOS o desactivando la máquina que implementa el NIDS.
- Logs.
  - Borrando logs o creando muchos logs.
- Sistema de análisis de paquetes del NIDS.
  - El NIDS no reconozca los mismos paquetes que el objetivo.

Algunos sistemas comerciales

- Snort
  - Desarrollado por Marty Roesch.
  - Open-source.
  - Además soporte comercial(de pago).
- BlackICE by Network ICE.
- Http:// www.cs.purdue.edu/coast/ids.
  - Lista de varios sistemas comerciales y freeware.

Bibliografia

- Revisión práctica de IDS por Sacha Fuentes.
- www.snort.org
- http://www.robertgraham.com/pubs/network-intrusion-detection.html
- http://www.cerias.purdue.edu/about/history/coast_resources/intrusion_detection/