Seguridad en Sistemas Informáticos

Detección de intrusión

Área de Ingeniería Telemática
Dpto. Automática y Computación
http://www.tlm.unavarra.es/

Hasta ahora...

- Tipos de ataques al host y a la red
- La cadena de seguridad: host, red local, perimetral...
- Seguridad perimetral
  - Herramientas: firewalls, proxies, redes y hosts expuestos y bastion hosts

- Hoy:
  - Sistemas de detección de intrusión

Introducción

- Cortafuegos

  Permiten elegir que dejamos pasar a nuestra red (o nuestro host)
- Algunos principios básicos de seguridad
  - **Eslabon mas debil (weakest link)**
  - **Mínimos privilegios (least privilege)**

    Un objeto (usuario, programa, systema...) debe tener los minimos privilegios necesarios para cumplir su función asignada pero ninguno más
  - **Cuello de botella (choke point)**

    Forzar a los atacantes a seguir un canal estrecho que pueda ser controlado y vigilado
  - **Seguridad en profundidad (security in depth)**

    Varios niveles de medidas de seguridad (no tengo que suponer que son infranqueables). ¿Para que poner una camara detrás de una puerta que se supone que no puede abrirse?

Introducción

- **Sistemas de Detección de Intrusión**

  monitoriza de un modo automático todos los **eventos** que ocurren en una red, un host, en una aplicación...

  en busca de señales que puedan indicar la existencia **de problemas de seguridad.**

- Problema típico con un firewall:

  He sufrido un ataque en uno de mis servidores, el atacante ha conseguido ser root.

  Intento reconstruir lo que ha pasado. Examino los logs del firewall en busca de pistas de lo que ha pasado

  Los logs del firewall contienen los paquetes que han filtrado... eso son los ataques que no han conseguido pasar

Tipos de IDS

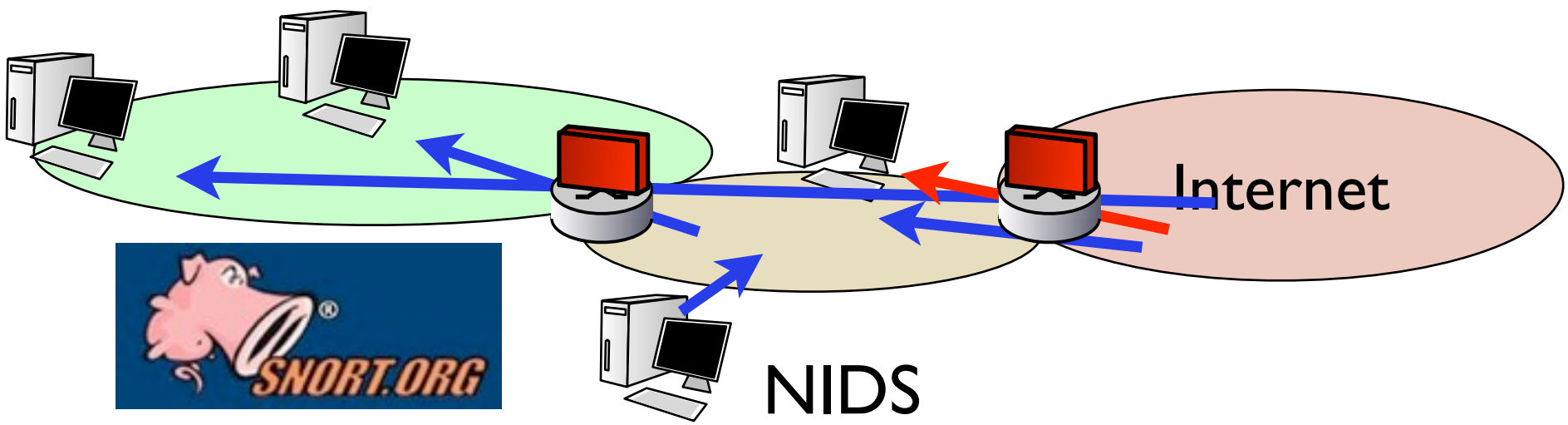
- Clasificaciones
  - según la fuente de información utilizada.
  - según el modo de análisis empleado.
  - según la respuesta proporcionada.
  - según la arquitectura utilizada.

Tipos de IDS

- Clasificaciones
  - según la fuente de información utilizada.
    - Network IDS
    - Host IDS
    - Application/protocol IDS
  - según el modo de análisis empleado.
  - según la respuesta proporcionada.
  - según la arquitectura utilizada.

NIDS (Network IDS)

- **Sistemas de Detección de Intrusión basados en red**
- Los más comunes (sistemas comerciales suelen ser de estos)
- Capturan y analizan tráfico que pasa por un segmento de red (por ejemplo la DMZ) y observan si se producen ataques
- Pueden ser distribuidos
  - varias sondas en diversos puntos que capturan trafico y lo analizan
  - una consola central que procesa las alarmas



- Ejemplo de NIDS: Snort

NIDS (Network IDS)

- **Sistemas de Detección de Intrusión basados en red**
- **Ventajas**
  - Un IDS protege varias máquinas (y es independiente del SO)
  - Con varios distribuidos pueden monitorizar redes muy grandes
  - Puesta en marcha sin interrumpir servicios (son pasivos)
  - Son difíciles de detectar por los atacantes (sensores sin IP)
  - Son muy efectivos detectando y deteniendo ataques que se basan en manipulaciones de las cabeceras IP (por ejemplo LAND o Teardrop).
- **Desventajas**
  - Rendimiento limitado (pocos pueden analizar un segmento cargado)
  - En redes conmutadas necesitan port mirroring (que un switch saque todo el trafico por un puerto para el IDS) eso convierte el puerto en cargado
  - Es capaz de ver muchos ataques pero no de saber si han tenido éxito

    Alarma y que decida el administrador/encargado de seguridad
  - No se pueden utilizar si el trafico va cifrado (cuando veamos VPNs...)

HIDS (Host IDS)

- **Sistemas de Detección de Intrusión basados en host**
- Software
- Monitorizan la actividad del host
  - Intercepción de llamadas al sistema y otros parámetros del kernel
  - Ficheros de log del sistema operativo o diversas aplicaciones
  - Fechas de modificación de ficheros críticos
  - Combinados con sistemas de detección de integridad (algo ha sido modificado??)
- Ejemplo de HIDS:
  - Tripwire: Open source, basado sobre todo en detectar si se modifican ficheros que no debieran
  - Los antivirus serian HIDS ?
  - El TPM sería un HIDS ?

    Normalmente hablamos de sistemas más configurables que dejen elegir lo que quiero proteger...

HIDS (Host IDS)

- **Sistemas de Detección de Intrusión basados en host**
- Ventajas
  - Son capaces de detectar si el ataque ha tenido éxito (menos falsos positivos)
  - No necesitan hardware adicional
  - Un sistema en cada host, no tan sensible a la carga de la red
  - No importa que el trafico de red sea encriptado
- Inconvenientes
  - Configuración más compleja
  - Un sistema en cada host, afecta al rendimiento del servidor que protejamos (ademas de requerir parar el servidor para instalarlo)
  - Ataques de denegación de servicio contra el HIDS
  - Protegen a un solo host

IDS de aplicación

- **IDSs basados en aplicación / protocolo**

  Tipo de HIDS especializados
- Diseñados especificamente para aplicaciones o protocolos concretos
- Interceptan la comunicación de aplicaciones especificas y observan ataques
- Ejemplos:
  - Analizadores de HTTP/HTTPS
    - Peticiones que llegan a un servidor web
    - Peticiones que llegan a un servidor web con SSL
  - Analizadores de peticiones que llegan a una base de datos desde el servidor web
  - ...

Tipos de IDS

- Clasificaciones
  - según la fuente de información utilizada.
  - según el modo de análisis empleado.
    - IDS detector de malos usos
    - IDS detector de anomalías
  - según la respuesta proporcionada.
  - según la arquitectura utilizada.

Detección de malos usos

- Aproximación más común
- El IDS busca patrones conocidos de ataques
  - Un NIDS busca paquetes con contenidos conocidos o que van puertos peligrosos (reglas y alarmas como los firewalls)
  - Un HIDS modificaciones en ficheros concretos o ataques a llamadas al sistema concretas

- Aplicación del principio: **enumerate-badness**

Detección de malos usos

- **Ventajas**
  - muy efectivos y generan pocos falsos positivos
  - detectan los ataques de un modo muy preciso
  - Generalmente conocen además de los patrones de ataques, información sobre las consecuencias, como detectar el ataque, cómo responder, etc lo cual resulta de gran utilidad (sistema experto)
  - Hay algunos capaces de detectar variaciones sobre los ataques conocidos pero no son aun muy comunes
- **Desventajas**
  - No son capaces de detectar ataques que no conocen

    Ataques de día cero (zero-day exploits)

    Ataque que se detecta al mismo tiempo que se hace publica la vulnerabilidad

Detección de anomalías

- Intentan aprender el comportamiento/tráfico "normal" de usuarios y aplicaciones y avisan cuando se producen anomalías
  - Diferentes técnicas: estadísticas, detección de umbrales, inteligencia artificial...

    Son aun campo de investigación
- Ventajas
  - Puede detectar ataques que no conoce
  - Pueden generar información de patrones que debe buscar un detector de malos usos
- Desventajas
  - La detección es poco precisa

    Alarma: "Ha pasado algo raro" pero el administrador deba averiguar que ha ocurrido
  - Gran número de falsos positivos
  - Su utilización requiere gran trabajo de parametrización y en general mayores conocimientos que los IDSs de detección de malos usos
- Los sistemas comerciales más avanzados utilizan una combinación de las dos técnicas

Tipos de IDS

- Clasificaciones
  - según la fuente de información utilizada.
  - según el modo de análisis empleado.
  - según la respuesta proporcionada.
    - De respuesta pasiva
    - De respuesta activa / Inline
  - según la arquitectura utilizada.

IDS de respuesta pasiva

- Recopilan información
- Generan alarmas que se guardan o se envían a sistemas de gestión
- Las alarmas pueden disparar mensajes al administrador por correo electrónico o SMS.

- El administrador debe reaccionar

IDS de respuesta activa

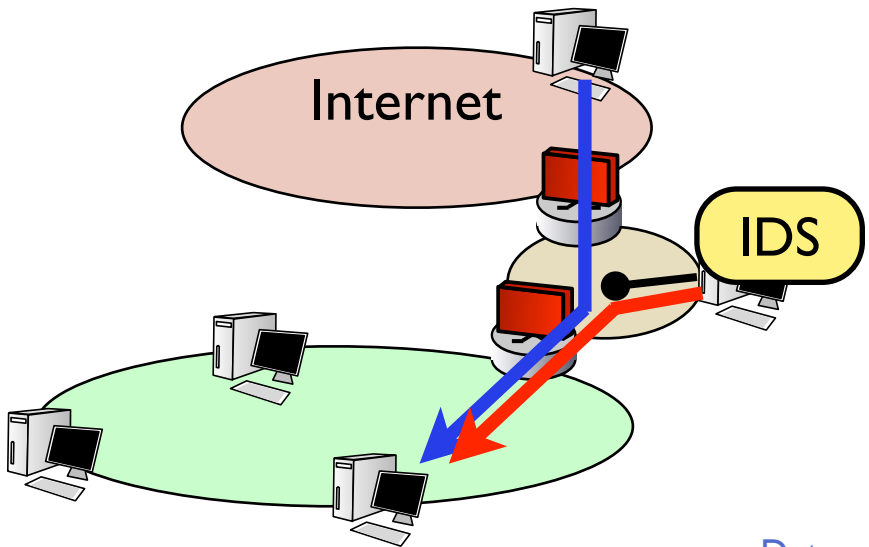
- responden de un modo automático ante la detección de un ataque.
  - **Recolección de información adicional,** modificando el número de eventos almacenados.
    - para analizar y hacer frente al ataque
    - como soporte para emprender acciones legales contra el agresor.
  - **Modificación del entorno.**
    - interactúa con otros dispositivos como routers (modificación de ACLs) o firewalls (modificación de reglas) para detener el ataque (por ejemplo bloqueando una dirección IP determinada, etc).
    - resetear la conexión TCP del atacante inyectando RSTs con IP spoofed
    - bloquear todo el tráfico proveniente del atacante
  - **Contrataque**. No es una opción muy apropiada
    - implicaciones legales que pudiera tener y posibilidad de spoofing
    - hay sistemas que hacen traceroutes y escaneos a la dirección de que viene el ataque

IDS de respuesta activa

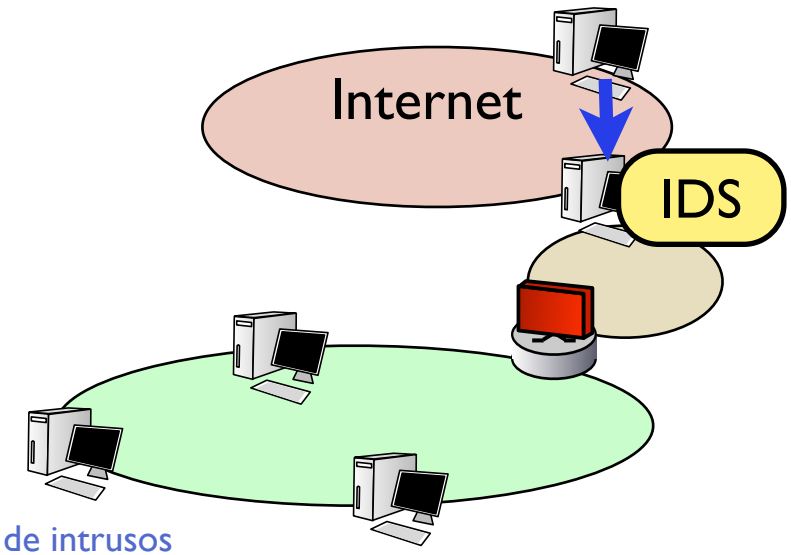
- Si impiden ataques se suelen llamar también IPS (intrusion prevention systems)

  Pero es más bien un nombre de marketing y el nombre IPS está bastante desprestigiado entre los expertos
- Normalmente se llaman IDS-inline si el IDS esta en el camino del ataque (firewall inteligente) y puede decidir no reenviar paquetes y IDS de respuesta activa si es un sistema aparte que envia RSTs o da ordenes a los firewalls

IDS de respuesta activa



IDS en línea



Tipos de IDS

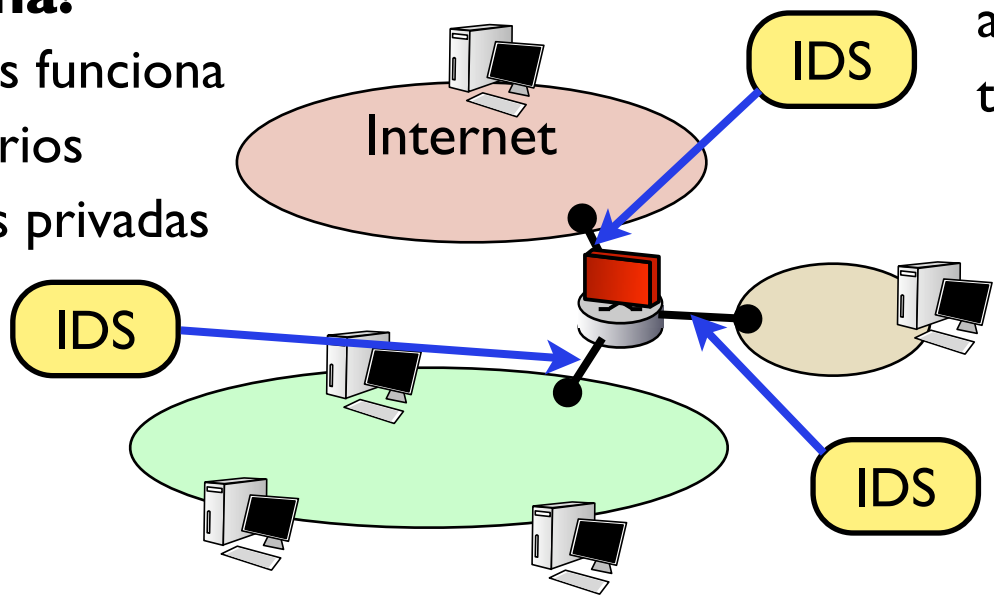
- Clasificaciones
  - según la fuente de información utilizada.
  - según el modo de análisis empleado.
  - según la respuesta proporcionada.
  - según la arquitectura utilizada
    - Un host
    - Distribuidos

Arquitecturas de IDS

- **IDS de un host**
  - El IDS es una máquina que observa un punto de la red y analiza el tráfico generando alarmas o respuestas activas.

    Se basa en el trafico en un único punto. ¿En qué punto conviene vigilar?

En la red interna?
ve si el cortafuegos funciona
protege a los usuarios
ve trafico de redes privadas



En la red exterior?
ve ataques al cortafuegos y a la DMZ
todo el tráfico entrante
mucha información
pero mucha carga

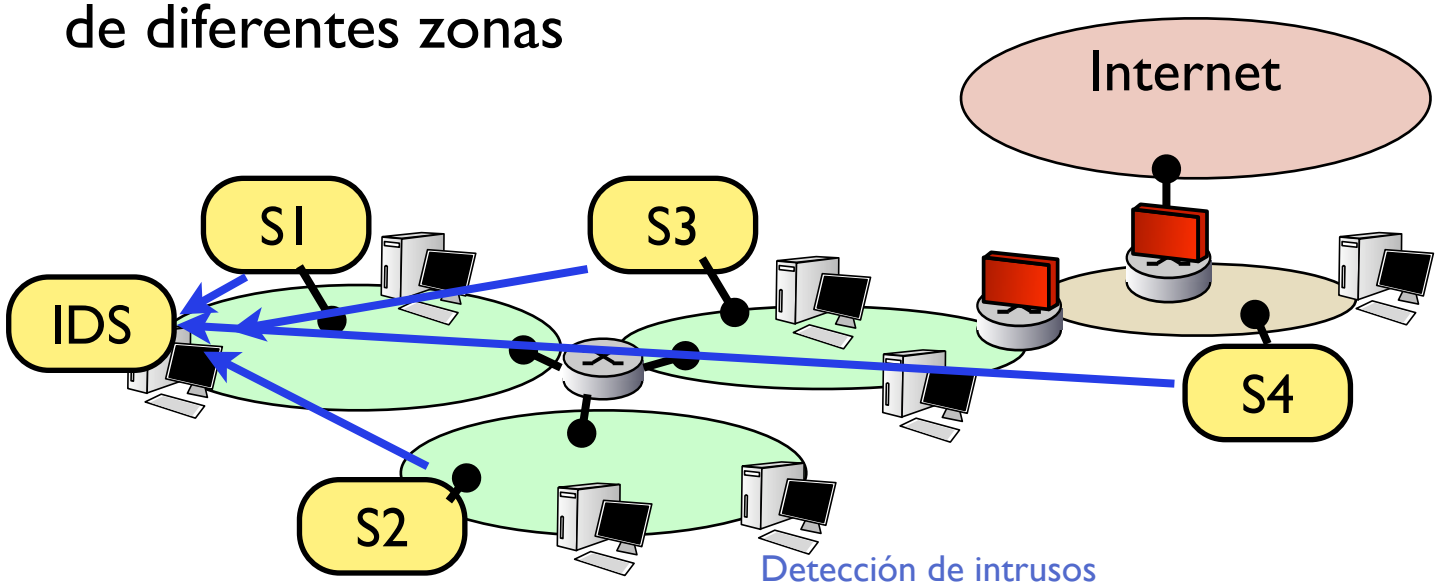
En la DMZ?
no ve ataques al cortafuegos
menos tráfico
menos información
menos carga = más análisis

Arquitecturas de IDS

- **IDS distribuidos**

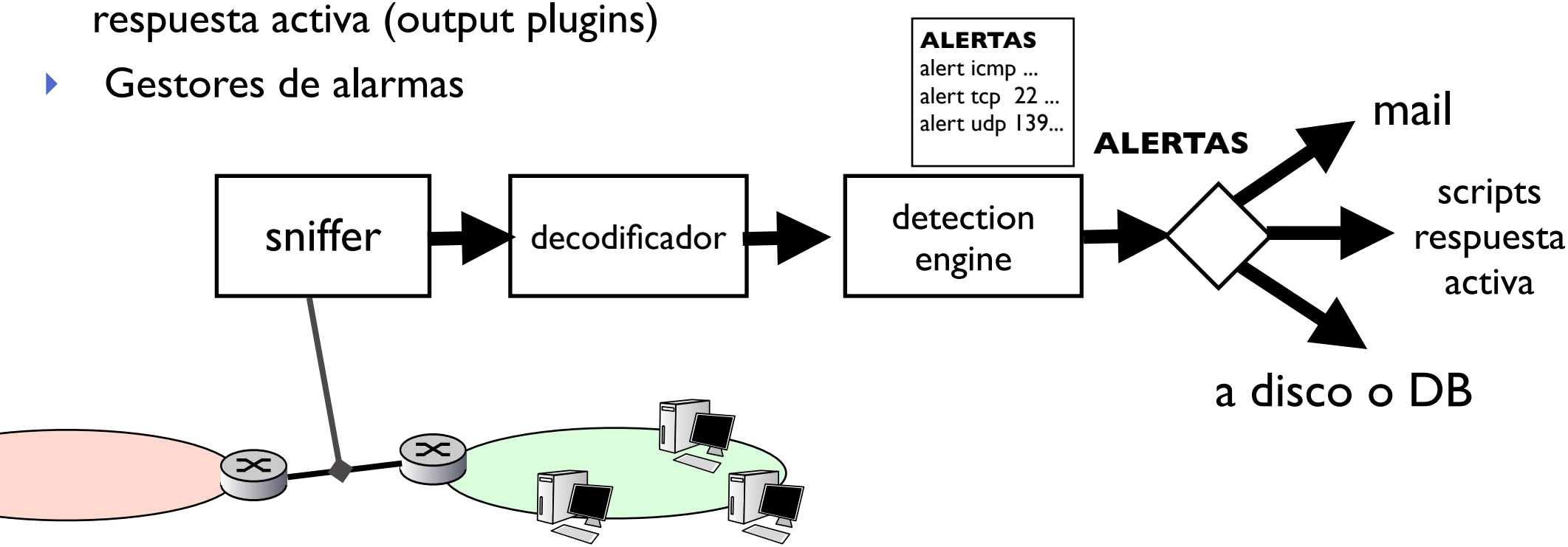
  También llamados IDS de correlación

  - Varias sondas en distintos puntos de la red observan tráfico y generan eventos
  - Los eventos se envían a un sistema central (preferiblemente encriptadas y por red aparte)
  - El sistema central muestra todo al administrador
  - Puede hacer analisis de correlación aplicando reglas a los eventos de diferentes zonas



Un ejemplo: Snort

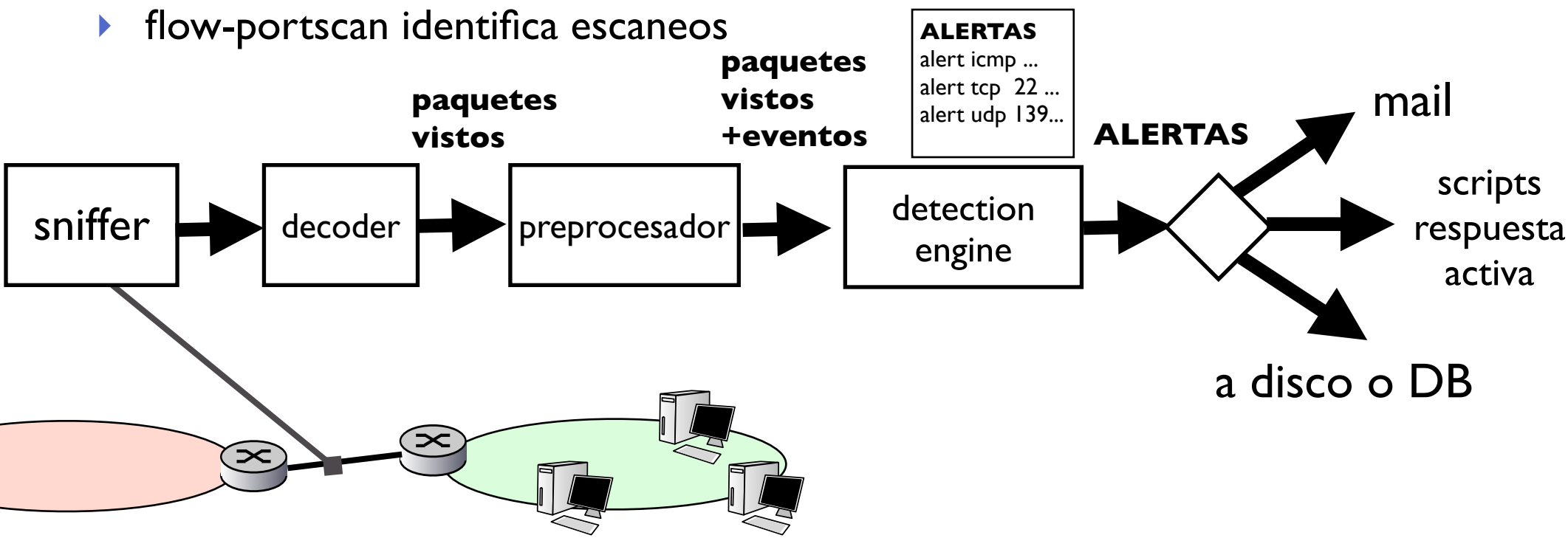
- Sniffer y decodificador que extrae campos de los paquetes
- Lenguaje de reglas para alertas
  - generan alertas etiquetadas con prioridad y tipo de ataque o evento
- Las alertas se mandan a disco o a base de datos (MySQL soportado por ejemplo)
- Sistemas de interfaz para configurar reglas y o interfaz con scripts para respuesta activa (output plugins)
- Gestores de alarmas



Snort

- Pero no está limitado a reglas de un solo paquete

  ¿Que ocurre si el atacante fragmenta los paquetes o el ataque va en varios paquetes de una conexión TCP?
- Preprocesadores: agrupan paquetes con ciertos criterios y disparan eventos
  - frag2 reconstruye paquetes fragmentados
  - stream4 reconstruye conexiones TCP (se puede buscar en los datos)
  - flow-portscan identifica escaneos



Snort: reglas

- Lenguaje de reglas

  `accion protocolo origen direccion destino` `(mas condiciones y resultados)`

- Acciones:
  - **alert** genera una alerta
  - **log** solo guarda el evento en disco
  - **pass** ignora este paquete/evento (para ignorar ciertas maquinas por ejemplo)
  - **tag** marca este origen o esta conexion (para fijarse en el resto de paquetes de una IP si genera un ataque)
- Protocolo, direccion (y puerto origen) y destino

Snort: reglas

- Ejemplo

```
alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25 (msg:"EXPLOIT sniffit
overflow"; flow:stateless; dsize:>512; flags:A+; content:"from|3A 90 90
90 90 90 90 90 90 90 90|"; nocase; reference:arachnids,273;
reference:bugtraq,1158; reference:cve,2000-0343; classtype:attempted-
admin; sid:309; rev:10;)
```

- paquetes TCP de la red externa (cualquier puerto) a los servidores de correo (puerto 25)
- en el ( ) van más condiciones
- con tamaño>512 [`dsize:>512`]
- que lleven en los datos la cadena " **`from|3A 90 90 90 90 90 90 90 90 90 90|`** "

Snort: reglas

- Ejemplo

```
alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25 (msg:"EXPLOIT sniffit
overflow"; flow:stateless; dsize:>512; flags:A+; content:"from|3A 90 90
90 90 90 90 90 90 90 90|"; nocase; reference:arachnids,273;
reference:bugtraq,1158; reference:cve,2000-0343; classtype:attempted-
admin; sid:309; rev:10;)
```

- Y resultados
- msg: mensaje que aparecera en el log "EXPLOIT sniffit overflow"
- tipo del evento: ataque de intento de ser admin **`attempted-admin`**
- id de la regla sid: 309 (puede llevar tambien priority gravedad de la alerta)
- referencias a la vulnerabilidad en bases de datos de vulnerabilidades

Gestión de alertas

- Interfaces gráficos para usar snort y gestionar las alertas
- Si instalo Snort y mantengo actualizado su conjunto de reglas desde la pagina de snort.org sólo tengo que mirar de vez en cuando si ocurre alguna alerta... (o que me la mande por mail)

  Cada cuánto tiempo me hacen un escaneo de purtos o un ataque?
- La respuesta es en minutos...
- Y si eres una red de una empresa grande muy pocos minutos

Gestión de alertas

- Post-procesado de las alertas
- Solo enviar al administrador las mas graves (ejemplo: ataques que hayan tenido exito, accesos de root conseguido...)
- Las menos graves contarlas y reaccionar según su volumen
  - Aumenta mucho el número de escaneos por hora
  - Aumenta el número de ataques de un tipo (un gusano funcionando?)
  - Aumenta mucho el número de conexiones SSH cortas (intentos de login?)
  - Detectores de anomalías?
- El problema es
  - Va a haber muchos falsos positivos y hay que encontrar los buenos
  - El trabajo de filtrar los falsos positivos nos hace olvidarnos de que tambien hay falsos negativos (=aun así hay ataques que no estamos viendo)

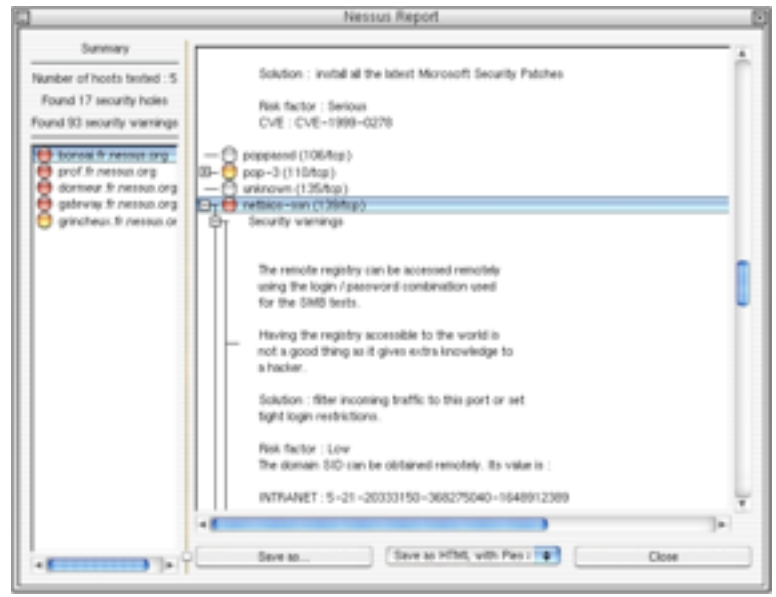
Otras herramientas

- Existen diferentes herramientas que pueden ser utilizadas para completar y mejorar las funciones de los sistemas de detección de intrusión; de hecho muchas veces estas herramientas están integradas en los IDSs:

  - Herramientas de análisis de vulnerabilidades (Auditoria)
  - Herramientas de comprobación de integridad de ficheros.
  - Honey Pots.
  - Padded Cell systems.

Otras herramientas

- **Herramientas de análisis de vulnerabilidades:**
- Son herramientas que permiten determinar si una red, un conjunto de hosts o un host son vulnerables a ataques conocidos. Lo ideal es ejecutar periódicamente estas herramientas para lograr obtener una "foto" del nivel de seguridad del sistema a modo de auditoría.



- Ejemplos:
  - Nessus.
  - MBSA (entornos MS).
- Problemas
  - Es una buena herramienta tambien para los atacantes
  - Google hacking: buscar informes de Nessus

Otras herramientas

- **Herramientas de comprobación de integridad de ficheros:**

  - Mediante este tipo de utilidades se puede verificar que ningún atacante haya modificado ninguno de los ficheros del sistema. Además, al tener una "foto" del sistema, cualquier recuperación es más fácil de realizar.

  - Una de las herramientas más populares es Tripwire:

    http://www.tripwiresecurity.com/

Otras herramientas

Honey Pots:

- Los "tarros de miel" son sistemas pensados para **atraer atacantes y distraerlos** de los verdaderos sistemas de red. Los objetivos que se buscan son aprender sobre el modo de actuar de los hackers, poner un sistema fácilmente accesible en nuestra red de modo que el atacante se quede en ese sistema y no en los de producción y tener tiempo para reaccionar ante ataques. (http://www.enteract.com/~lspitz/honeypot.html)

- **Construyendo un honey pot**

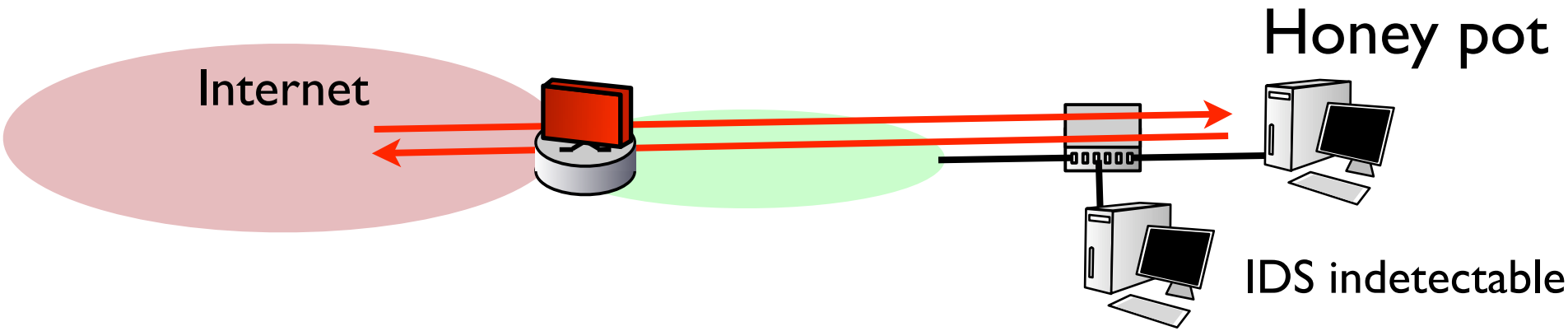
  1 PC viejo. Se reinstala un sistema operativo

  se hacen usuarios y se insatlan los servicios que quiera

  se configura en la red

  Y nunca más se vuelve a tocar

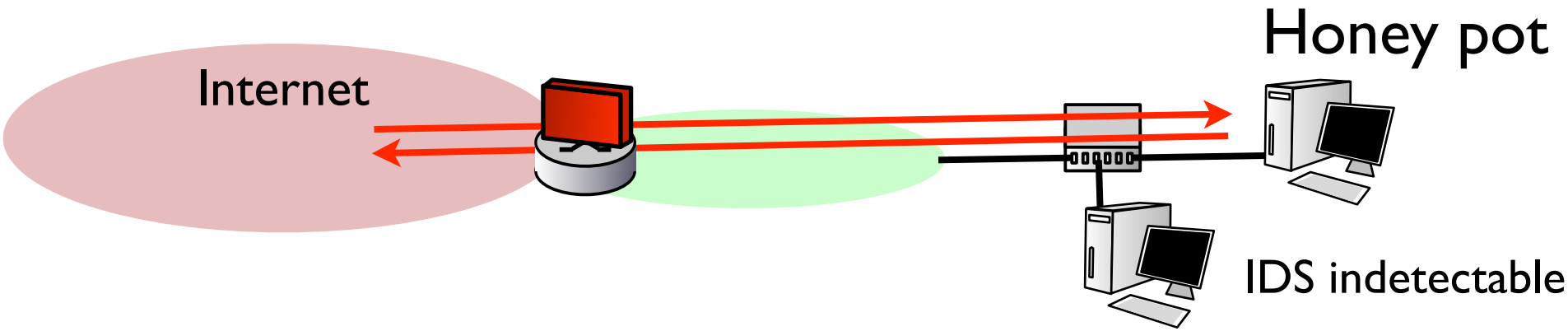
Honey pots



- Colocamos un IDS que vea sólo el tráfico del honey pot
- Muy útil para aprender de los hackers
  - Si alguien hace un ataque contra el honey pot lo veremos
  - Si alguien escanea nuestra red lo veremos
  - Si alguien controla el honey pot veremos que hace desde alli
- Que inteligencia necesita el IDS?

  Cómo distinguimos el tráfico causado por hackers/ataques del tráfico normal?

Honey pots



- Sacrificamos un ordenador para cada honey pot (Honey pot hardware)
- Hoy en día:
  - Virtualización: es fácil hacer una maquina virtual honey pot
  - Honey pots software: simulan solo la pila TCP/IP y varios servicios (honeyd) el mismo software puede simular toda una red

Otras herramientas

- **Padded Cell systems:**

  - Son sistemas muy similares a los anteriores con la diferencia de que trabajan de un modo conjunto con los IDSs. Es decir, cuando un IDS detecta un atacante éste es redirigido a un entorno simulado (Padded Cell) ubicado en un host específico de manera que se puede monitorizar sus actividades sin riesgo para nuestros sistema.

  - Tanto los tarros de miel como las celdas acolchadas son herramientas que están actualmente muy de moda pero que a la hora de la verdad no resultan de fácil implantación ya que requieren poseer un gran conocimiento y dedicar mucho esfuerzo a las mismas. En la mayoría de los casos resulta más productivo dedicar esos recursos al resto de componentes de seguridad por lo que generalmente estas herramientas sólo resultan útiles a empresas que se dedican a desarrollar soluciones de seguridad, universidades, etc

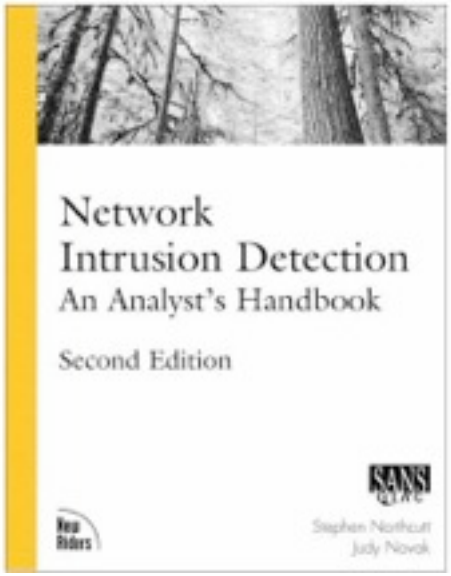
Con FIREWALL + IDS estoy protegido?

- **Hay técnicas para saltar firewalls**
  - Usando fragmentación IP para que el firewall no pueda inspeccionar las cabeceras TCP/UDP
  - Usando tuneles o backchannels una vez que controlas un host dentro del firewall
  - Usando trafico que pase por el firewall
- **Hay técnicas para confundir IDSs**
  - Spoofing
  - Camuflar escaneos, haciendolos durante mucho tiempo los preprocesadores se olvidan de los eventos lejanos
  - Atacar desde varias direcciones IP y en diferentes días

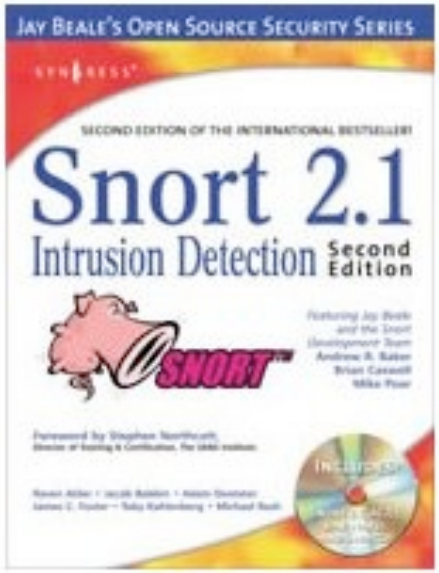
    desde una escaneo, desde otra hago el exploit para conseguir que el objetivo se conecta a una tercera
  - Sobrecargar al IDS

    genero muchos ataques conocidos desde varias direcciones IP falsas. El IDS dará muchas alarmas y el administrador no podrá examinarlas todas y encontrar el ataque real

BIBLIOGRAFÍA



NETWORK INTRUSION DETECTION
An Analyst´s Handbook (2nd Edition)
New Riders
Stephen Northcutt, Judy Novak
ISBN: 0735710082



Snort 2.1 Intrusion Detection, Second Edition
By Jay Beale,
ISBN: 1931836043

Conclusiones

- Los IDSs son herramientas que permiten avisar de que se ha producido una intrusión
- Pero aun su inteligencia artificial no es demasiado alta así que sus servicios son basicamente:
  - Dar alarmas y reaccionar ante ataques bien conocidos

    Enumerate baddness y problemas con zero-day exploits
  - Dar alarmas ante condiciones anómalas que deben ser analizadas (falsos positivos)
  - Seguimos necesitando al administrador experto