Detección de Intrusos

Curso 2013/14

Grado Gestión Informática Empresarial

Asignatura Auditoría y Seguridad Informática

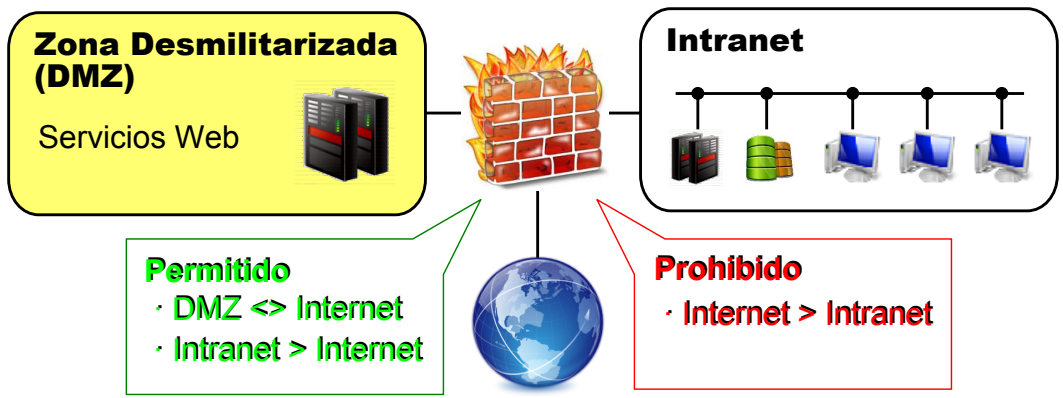
Profesores Alfredo Cuesta Infante
alfredo.cuesta@ajz.ucm.es
Alberto Herrán González
aherran@ajz.ucm.es

Contenidos

Seguridad perimetral

Cortafuegos

- Separar servicios web de una empresa de la red interna (intranet).
- Los hosts que dan dichos servicios web se agrupan en la zona desmilitarizada (DMZ) mediante cortafuegos.
- El tráfico de la intranet y la DMZ hacia internet está permitido, pero el cortafuegos bloquea las peticiones hacia la intranet y sólo aceptará el tráfico hacia la DMZ.
  El servidor de bases de datos se queda en la intranet!



- 4 tipos según sus características y la capa OSI en la que funcionan:
  1. de pasarela: telnet, ftp
  2. de capa de red: ip, puerto de origen/destino
  3. de aplicación: http,
  4. personales: sobre el equipo de escritorio

Ataques por intrusión

Tipos de intrusos

Impostor *Masquerader*

- Individuo **no** autorizado para usar el computador
- que atraviesa los controles de acceso
- para hacer uso de la cuenta de un usuario legítimo.

Abuso de autoridad *Misfeasor*

- Usuario legítimo
- que accede a ciertos a/i a los que no está autorizado
- o que hace mal uso de sus privilegios.

Usuario clandestino *Clandestine user*

- Individuo que logra privilegios de administrador
- y lo utiliza para eludir herramientas de auditoría y rastreo.

Patrones de comportamiento

- **Hackers.** Comunidad *meritocrática* interesada en investigar el funcionamiento de los sistemas y comparten conocimientos.
  - El status depende de la habilidad
  - Aprovechan las oportunidades $\rightarrow$ sin objetivo concreto.
- **Criminales.** Tienen objetivos más especificos y actuan rápido.
  - *Ej.:* Ficheros de tarjetas de crédito en comercio electrónico.
- **Ataques desde dentro.** Generalmente motivados por venganza o despecho.
  - Los más difíciles de detectar ya que actuan como usuarios legítimos.

Técnicas de detección

IDS = Intrusion Detection Systems

Clasificación IDS

- **Basado en hosts:** Monitoriza la actividad y los eventos que ocurren en un host.
- **Basado en redes:** Monitoriza el tráfico de red, transporte, protocolos de aplicación, etc de un segmento de la misma.

Requerimientos

Un IDS debe:

1. funcionar continuamente, con mínima supervisión humana, y sin sobrecargar al sistema;
2. ser capaz de recuperarse de caidas y reinicializaciones;
3. monitorizarse a si mismo y detectar si ha sido modificado;
4. ser configurable para adaptarse a las políticas de seguridad del sistema y sin necesidad de reiniciarse (reconfiguración dinámica);
5. ser escalable, para monitorizar un gran numero de hosts;
6. si alguno de sus componentes deja de funcionar, el impacto en los demás debe ser el menor posible.

Componentes lógicos

1. **Sensores:** Recopilación de datos.
2. **Analizadores:** Reciben información de uno o más sensores y determinan si ha ocurrido un ataque por intrusión. También puede guiar sobre los procedimientos a seguir.
3. **Interfaz de usuario:** Necesario para la comunicación al exterior.

Detección basada en hosts

HIDS = Host based IDS

- **Proposito principal:** Detectar intrusiones externas e internas, reportar eventos sospechosos y emitir alertas.
- **Beneficio principal:** Los IDS basados en red no detectan intrusiones internas.

Hay dos tendencias...

1. **Detección de anomalías.** Almacenar datos sobre el comportamiento de usuarios legítimos y aplicar técnicas estadísticas o IA para rechazar comportamientos de usuarios no legítimos.
   - Basada en perfiles de actividad de cada usuario.
   - Basada en umbrales, independientemente de los usuarios.
2. **Detección de firmas.** Por *firma* se entiende un patrón de comportamiento específico de un ataque o un atacante.
   - Basada en reglas creadas a partir de la observación del comportamiento.

La diferencia entre IA y reglas es la ausencia de conocimiento previo en el primero.

...y una herramienta común

Los registros o grabaciones para posteriores auditorías.

- **Nativos en el SO.** Todos los SO tienen comandos para registrar las actividades de los usuarios.
- **Específicos para la IDS.** Necesarios cuando hay que registrar información específica.

Ejemplos de HIDS

Algunas medidas

Medida	Qué detectan
Frecuencia de conexiones por día y hora o desde diferentes localizaciones	Intrusos conectando *fuera de hora* o desde lugares poco frecuentes
Tiempo transcurrido por sesión	Grandes desviaciones de la media pueden indicar impostores
Utilización de recursos por sesión	Niveles de entrada/salida del procesador inusuales
Fallos de la contraseña al conectar	Intentos de adivinar la contraseña
Fallos de conexión desde terminales concretos	Intentos de abuso de autoridad
Frecuencia de ejecución o de su negación	El intento o el éxito de haber penetrado a través de un usuario legítimo o de querer obtener mayores privilegios
Frecuencia de lectura, escritura, borrado o creación de ficheros	Puede indicar la presencia de un impostor navegando por las carpetas

Algunas reglas heurísticas

1. Los usuarios no deberían leer ficheros de los directorios personales ajenos.
2. Los usuarios no deben escribir en los ficheros ajenos.
3. Los usuarios que se conectan fuera de horas de oficina suelen acceder a los ficheros que usaron antes.
4. Los usuarios no suelen conectarse al sistema más de una vez al mismo tiempo.
5. Los usuarios no hacen copias de los archivos del sistema.

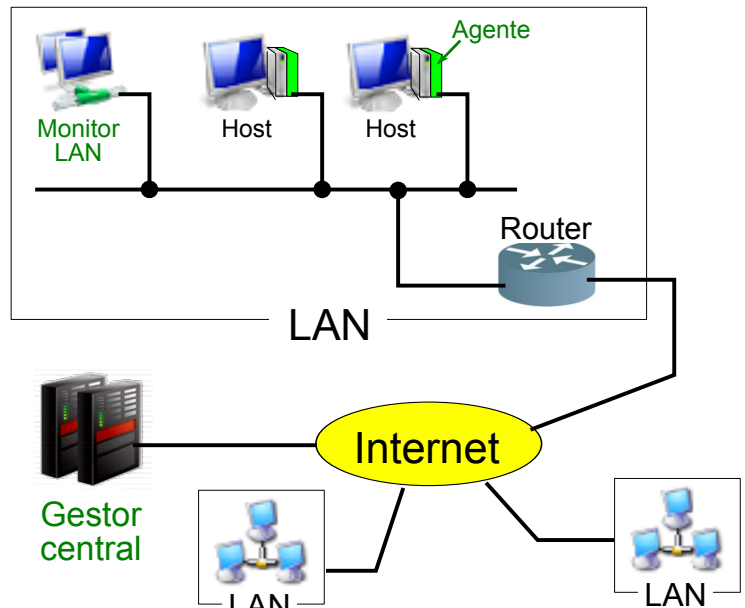
Detección basada en redes (1/3)

NIDS = Network based IDS

- **HIDS-distribuido:** Evita instalar un HIDS en cada host.
- **NIDS:** Monitoriza el tráfico de paquetes en una red o un conjunto de redes interconectadas, en diferentes niveles (aplicación, transporte, red) y en tiempo (casi-)real. Por tanto cubre un objetivo diferente del HIDS, más centrado en examinar el comportamiento del usuario y del SW.
- **Cuestiones importantes:**
  - Selección de arquitectura:
    Centralizada: 1 punto de recogida y análisis de datos.
    Descentralizada: Más de un punto, pero necesita coordinación para el intercambio de información y el desarrollo de las tareas.
  - Ser capaz de trabajar con registros de auditoria de diferentes formatos
  - Los sensores transmiten los datos recogidos a otros hosts de la red
    $\rightarrow$ Requerimientos adicionales en la integridad y confidencialidad de estos datos.

Componentes

1. **Agente:** Módulo en el host encargado de la recogida de datos relacionados con eventos de seguridad.
   Los envía al gestor central.
   Opera como proceso en 2º plano.
2. **Monitor LAN:** Igual que el agente pero encargado de monitorizar la red.
3. **Gestor central:** Recibe y analiza los datos.



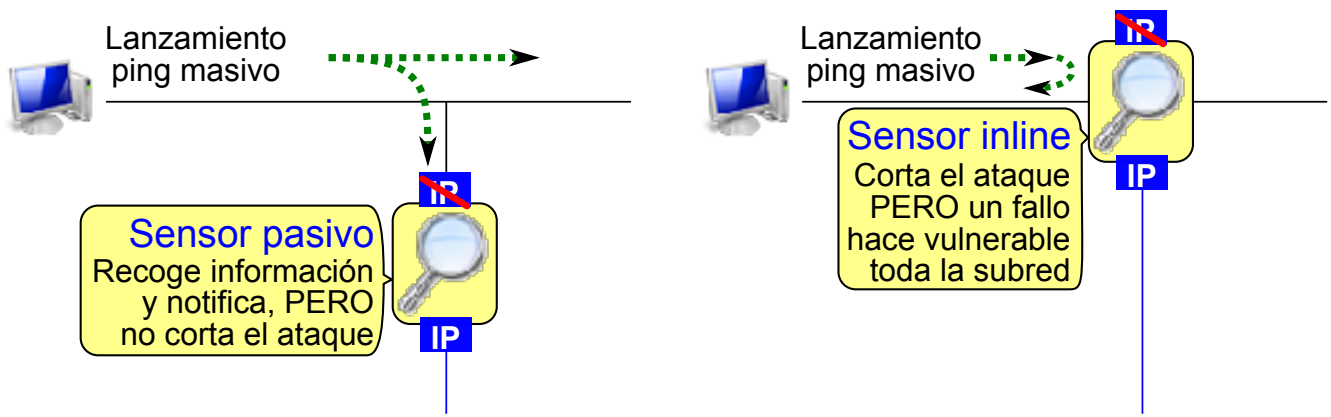
Detección basada en redes (2/3)

Tipos de sensores

- Los agentes y los monitores LAN son módulos añadidos a hosts de una LAN.
- Los sensores son elementos desplegados en la red para medir el tráfico en los niveles de red, transporte y aplicación, especialmente aquel dirigido hacia puntos potencialmente vulnerables.

Los sensores pueden ser:

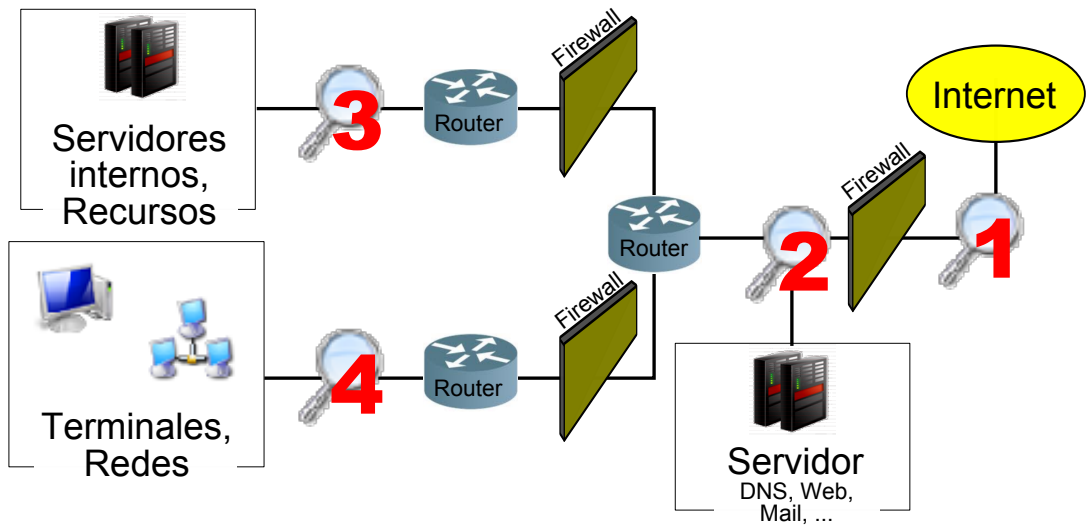
- **Pasivos.** Más comunes. Se limitan a escuchar y copiar el tráfico en modo *promiscuo* con su propia tarjeta de red. Desde el punto de vista del tráfico de red no añade retardos pero no pueden bloquear un ataque.
- **En línea.** Se inserta en el segmento que se quiere monitorizar. De este modo el tráfico debe atravesarle para llegar al destino. Añade retardo pero defiende el segmento.



El sensor suele tener 2 tarjetas, una con IP para poder acceder a él por una vía segura, y otra sin IP para hacerlo *invisible*, que es la que se conecta a la red.

Detección basada en redes (3/3)

Posicionamiento de los sensores



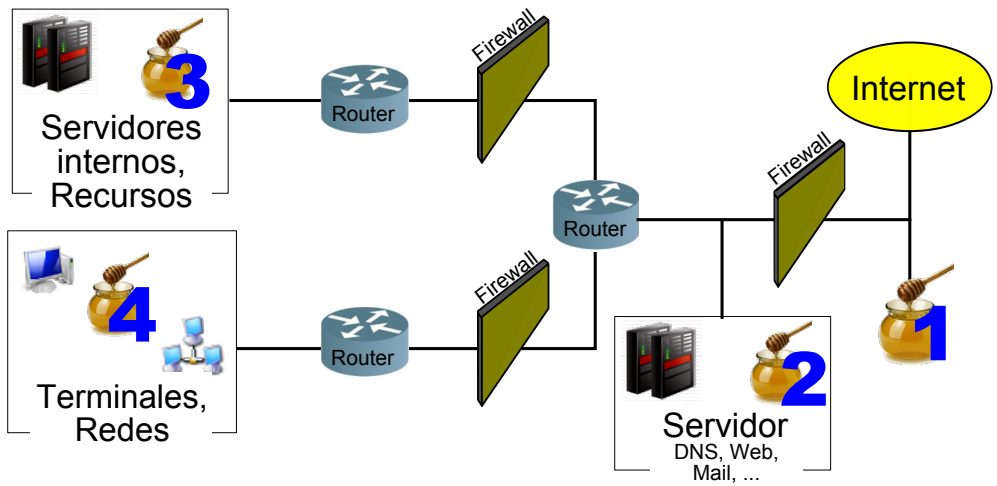
1. Monitoriza todo el tráfico sin filtrado.
   Documenta el número y tipo de ataques originados desde internet.
   Conlleva una gran carga computacional.
2. Documenta los ataques que atraviesan las defensas *perimetrales*.
   Protege de ataques contra servicios web.
   Puede reconocer el tráfico de salida resultante de un servidor atacado.
3. Detecta abusos de autoridad (*misfeasor*) ya que se producen desde dentro.
4. Detecta ataques a sistemas y recursos críticos.

Honeypots

Honeypot = Tarro de miel

Los *honeypots* son señuelos para desviar al atacante de los sistema críticos
a la vez que se recoje información de su actividad.
Mientras está engañado permanece más tiempo, dando ventaja a los administradores.

- Son recursos que no tienen valor pero se les dota de todas las medidas de seguridad para que parezcan *reales*.
- Inicialmente consistían en hosts conectados a un IP,
  pero ya se construyen redes enteras simulando el tráfico de la empresa.



1. Atrae ataques exteriores descargando las defensas interiores de trabajo, pero no defiende frente a abusos de autoridad.
2. Aquí sus efectos son limitados debido al firewall exterior.
3. Atrapa ataques internos, detecta defensas mal configuradas.
   Puede suponer un problema si a través del honeypot se ataca a otros sistemas internos.
   Al igual que 2, los firewall limitan sus efectos.
4. Igual que 3.