Tecnologías de
Detección de Intrusos

Carlos Fragoso Mariscal

Director Técnico

carlos@jessland.net

Microsoft TechNet

Jessland Security Services

Agenda

- Introducción
- HIDS: nivel de host
- NIDS: nivel de red
- Respuesta activa y prevención de intrusiones
- Gestión de eventos de seguridad
- Máquinas y redes trampa
- Conclusiones
- Referencias

Introducción (I)

- **¿ Por qué pueden interesarse en mi ?**
  - Ataques oportunistas
  - Ataques dirigidos
  - Ataques internos
- **NO** es una cuestión de '**SI**' sino de '**CUANDO**'
- Tipos de ataques:
  - Nivel de enlace
  - Nivel de red
  - Nivel de aplicación → web !!!
- Detección de Intrusiones vs Detección de Ataques

Introducción (II)

> "La prevención es idonea pero la detección es imprescindible"

- **… pero … ¡¡¡ si ya tengo un cortafuegos !!!**
  - Los cortafuegos se preocupan de tus perímetros
  - ¿ Qué ocurre si se logra penetrar en el perímetro ?
    - Adjuntos maliciosos de correo, páginas web maliciosas, VPN's, redes inalámbricas, etc.
- Función de auditoría:
  - Nos dicen que ocurre en nuestras redes
- Valor "**forense**":
  - Clave para una recuperación efectiva
    - ¿ Que hicieron en el sistema ?
    - ¿ Cómo consiguieron entrar ?
    - ¿ Que debo parchear o fortificar ?

Perfiles de intruso informático

- Las motivaciones de los intrusos informáticos son muy variadas: diversión, egocentrismo, económicas, políticas, ideológicas, etc
- Según sus conocimientos:
  - Hacker de élite ~ *Elite hacker*
  - Ciberpiltrafillas ~ *Script kiddies*
- Considerando sus intenciones:
  - Blackhat, Grayhat, Whitehat
- Desde que el negocio está en la red las motivaciones económicas han llevado a la delincuencia a la red:

  Spammers, extorsiones por revelación de secretos, *hacking* entre gobiernos, etc.

"It is a well-known fact that no other section of the population avail themselves more readily and speedily of the latest triumphs of science than the criminal class"

- Inspector John Bonfield, Chicago police (1888)

¡¡¡ Conoce a tu enemigo !!!

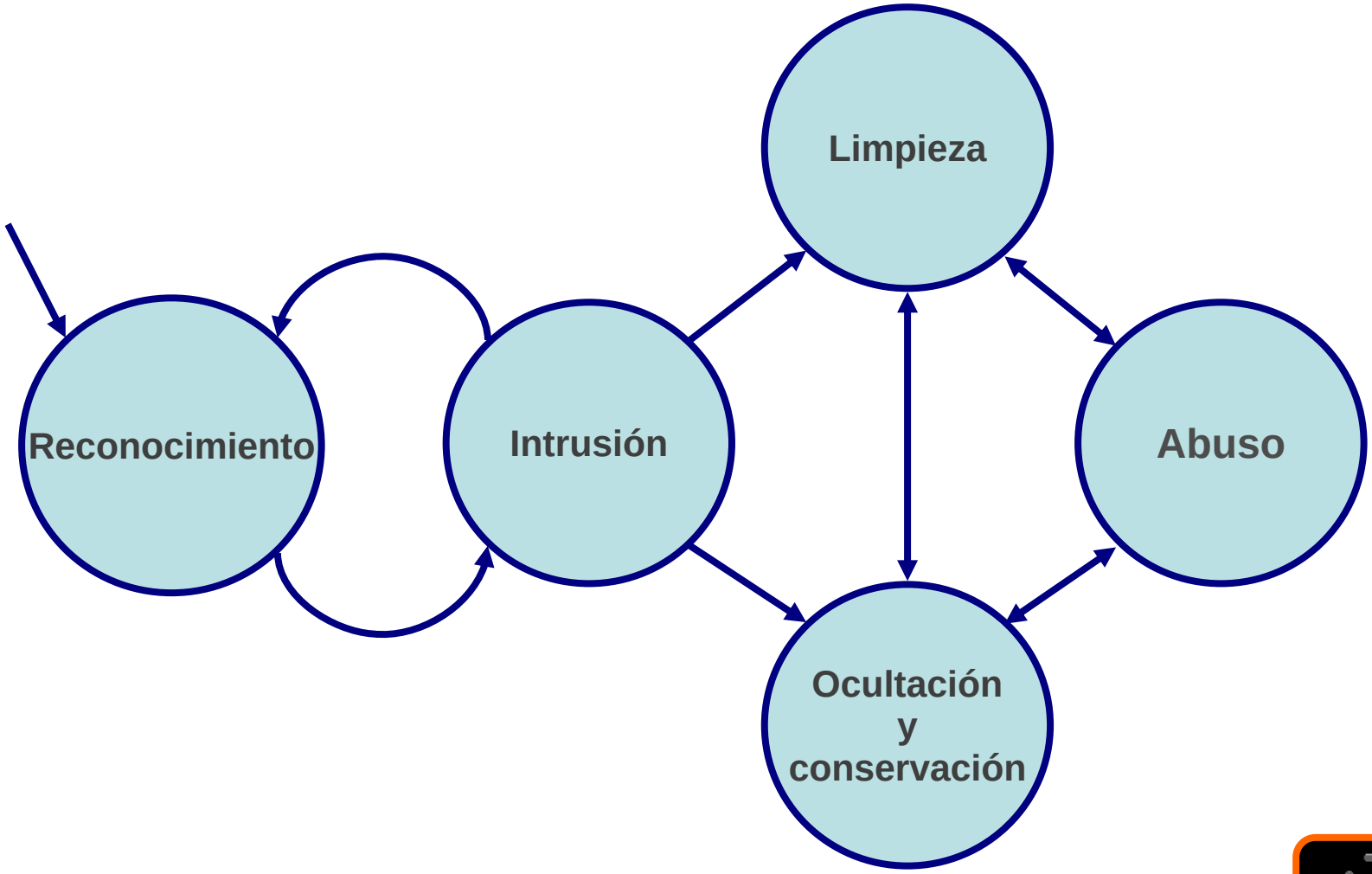
"Know Your Enemy and know yourself; in a hundred battles, you will never be defeated. When you are ignorant of the enemy but know yourself, your chances of winning or losing are equal. If ignorant both of your enemy and of yourself, you are sure to be defeated in every battle"

- Sun Tzu (The Art of War)

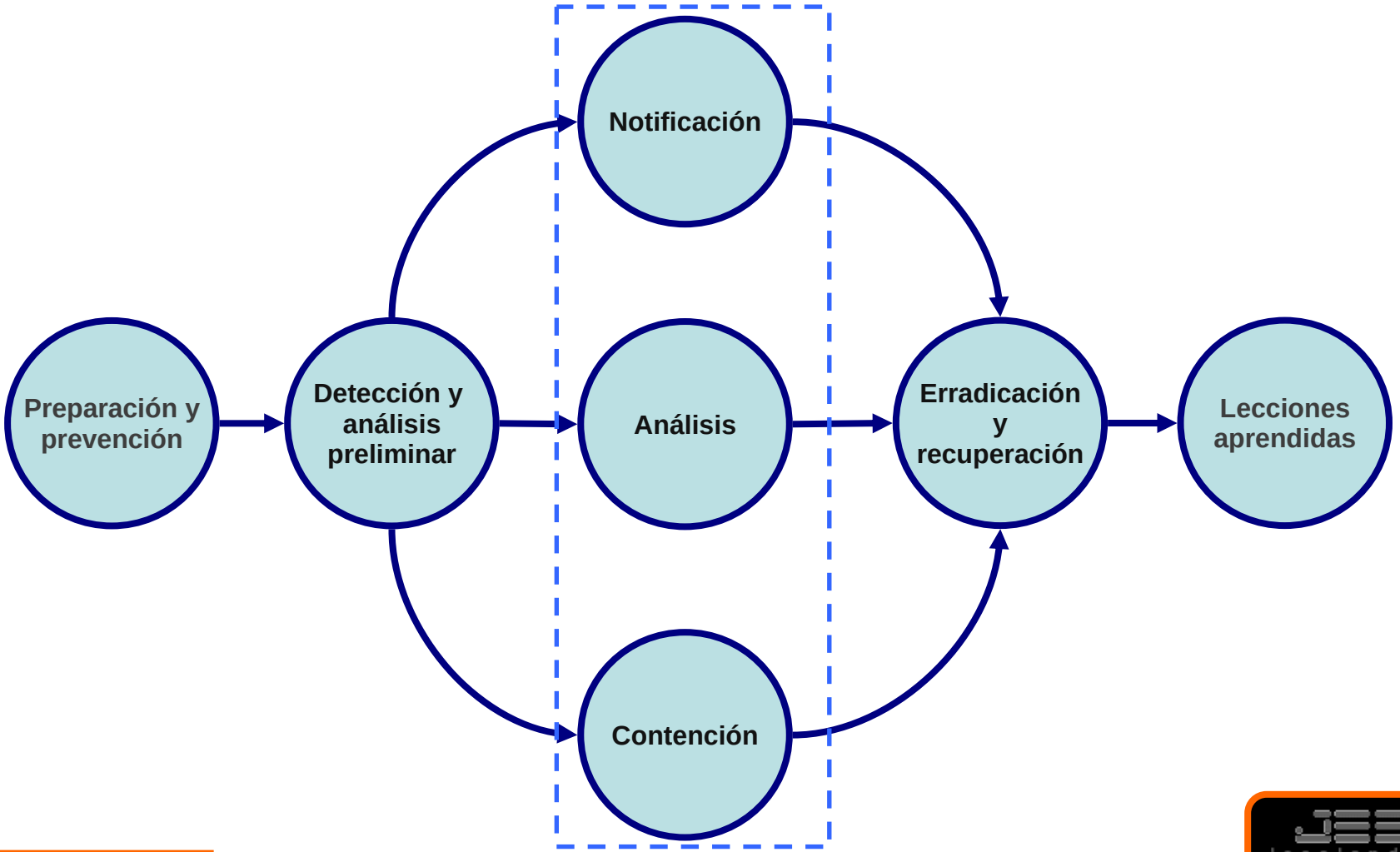
"Si no puedes con tus enemigos, aprende de ellos" ☺

- Carlesun Fragotzu

Ciclo de vida de una intrusión



Respuesta a incidentes



Tecnologías IDS

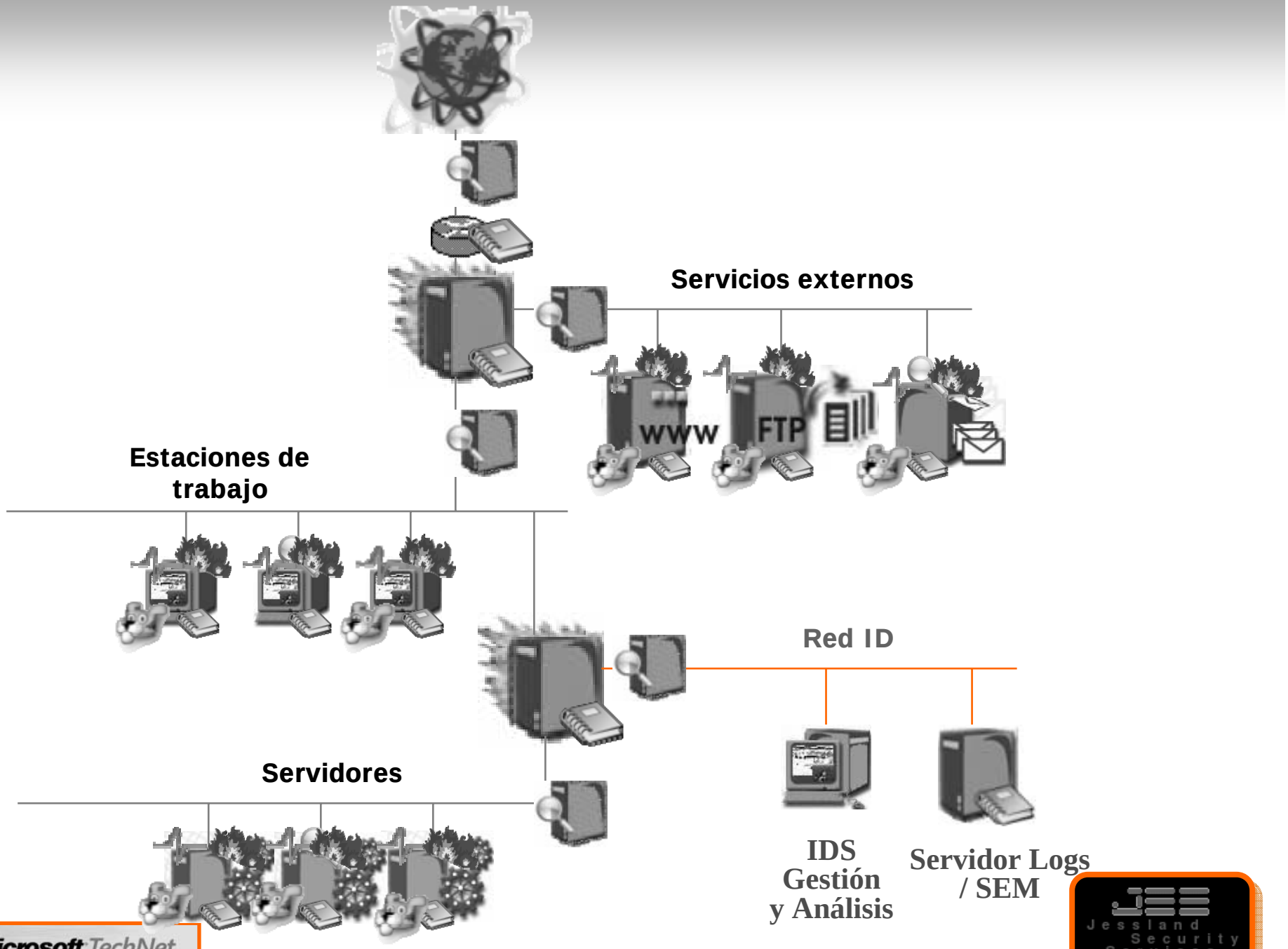
- Ámbito de actuación:
  - A nivel de sistema (HIDS)
  - A nivel de red (NIDS)
  - Máquinas y redes trampa
- Detección basada en:
  - Uso indebido
    - Patrones / firmas
  - Anomalías
    - Estadístico
  - Otros:
    - Políticas
    - Sistemas trampa

Agenda

- Introducción
- **HIDS: nivel de host**
- NIDS: nivel de red
- Respuesta activa y prevención de intrusiones
- Gestión de eventos de seguridad
- Máquinas y redes trampa
- Conclusiones
- Referencias

HIDS: nivel de host

- Motivaciones:
  - Ataques contra NIDS
  - Ataques desde el interior (*perimeter bypass*)
- Tecnologías:
  - Control de integridad de ficheros
  - Monitorización de trazas de sistema / aplicación
  - Monitorización y perfilado de procesos
  - Monitorización y perfilado de red
  - Monitorización de eventos del núcleo (*kernel*)
  - Auditoria de configuración
  - Verificadores de integridad del sistema (*rootkits*)
  - Cortafuegos a nivel de sistema


Servicios externos
WWW
FTP
Estaciones de trabajo
Red ID
Servidores
IDS Gestión y Análisis
Servidor Logs / SEM

HIDS: ventajas y limitaciones

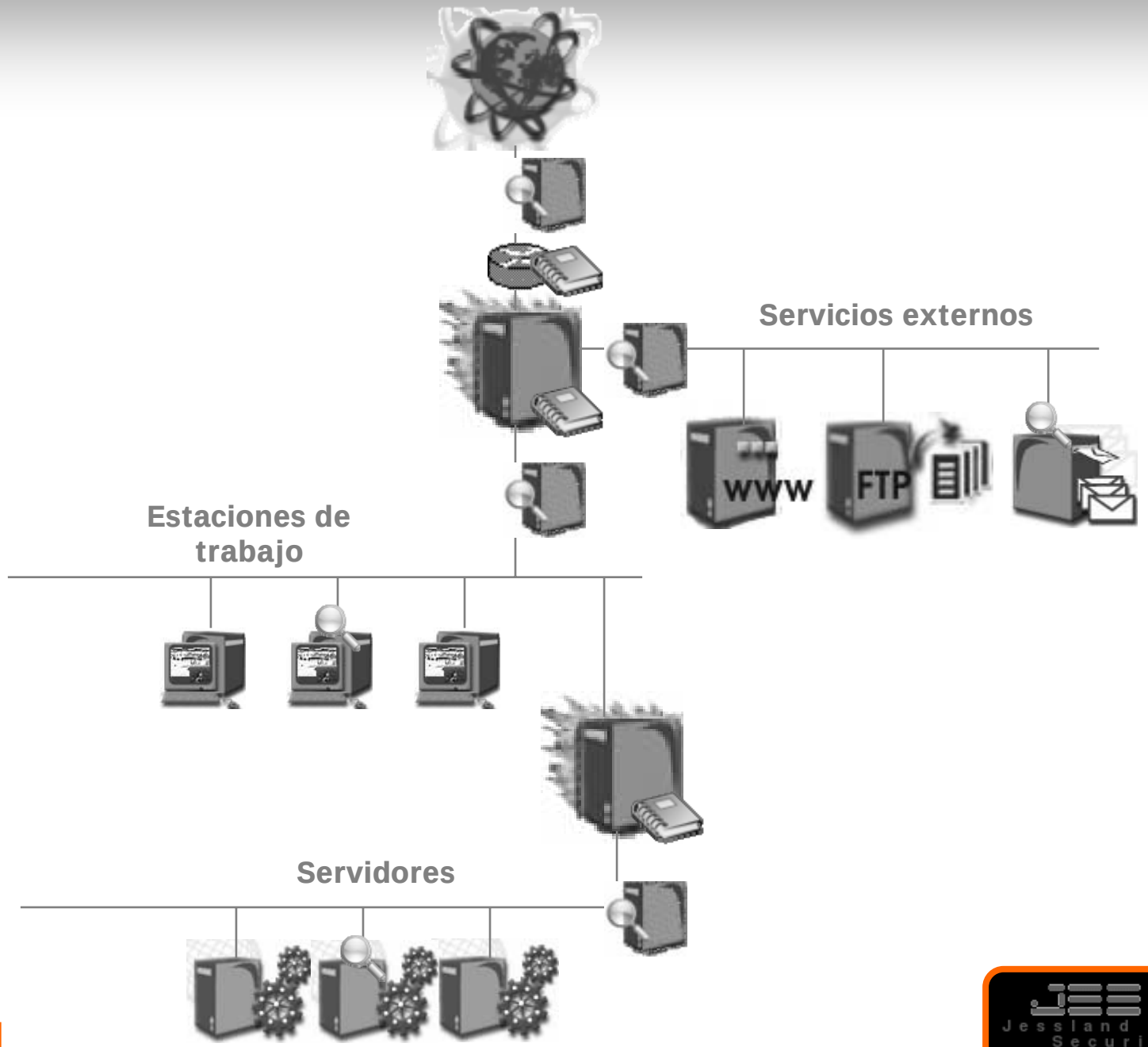
- Ventajas:
  - Funcionalidades HIDS nativas en los SO recientes, fácil activación en el momento de instalación
  - Punto de vista de los ataques desde el sistema
  - Ubicuidad
- Limitaciones:
  - Inútil (incluso desorientador) después de un compromiso
    - Uso de rootkits
  - Gestión compleja para un gran número de sistemas
  - Carga en el sistema (disco, CPU, etc.)
  - Alto coste en despliegues corporativos al utilizar herramientas comerciales

Agenda

- Introducción
- HIDS: nivel de host
- **NIDS: nivel de red**
- Respuesta activa y prevención de intrusiones
- Gestión de eventos de seguridad
- Máquinas y redes trampa
- Conclusiones
- Referencias

NIDS: nivel de red

- Tipos:
  - Sensor de red [+ consola remota]
  - Sensor de nodo
  - Sistema en línea (IPS)
- Formato:
  - Software
  - Appliances
- Técnicas de captura de tráfico (sniffing):
  - TAP's de red
  - Concentradores (*hub*) [+ cables de sólo lectura]
  - Conmutadores (*switch*) con puertos en modo "Span"
  - Balanceadores


Servicios externos
WWW
FTP
Estaciones de trabajo
Servidores

NIDS: ventajas y limitaciones

- Ventajas
  - Faciles de desplegar
  - Efectivos:
  - Buena escalabilidad
- Limitaciones
  - Falsos positivos:
    - Reglas demasiado genéricas o ataques de inserción
  - Falsos negativos:
    - Nuevos ataques, evasión o perdida de paquetes
  - Alarmas sin contexto (*non-textuals*):
  - Gran volumen de datos
  - Cifrado

Agenda

- Introducción
- HIDS: nivel de host
- NIDS: nivel de red
- **Respuesta activa y prevención de intrusiones**
- Gestión de eventos de seguridad
- Máquinas y redes trampa
- Conclusiones
- Referencias

Respuesta Activa y Prevención de Intrusiones

- Tipos de respuesta:
  - Respuesta Pasiva: verificación de la intrusión
    - Escaneo de vulnerabilidades, recogida de tráfico, etc.
  - Respuesta Activa: bloqueo del ataque
    - Reglas en cortafuegos (shunning), ruptura de conexiones TCP, etc.
- Prevención de Intrusiones:
  - Capacidad de bloquear un ataque o tráfico malicioso en la red, evitando su impacto en los sistemas
  - Híbrido entre tecnologías IDS y cortafuegos
  - Niveles de eficacia muy altos frente a niveles de bloqueo bajos depurando al máximo la probabilidad de falsos positivos
- **Son extremadamente útiles para dar un paso adelante en la lucha automatizada contra las intrusiones**
- **No son ninguna "bala de plata" que permita eliminar el resto de tecnologías asociadas**

Agenda

- Introducción
- HIDS: nivel de host
- NIDS: nivel de red
- Respuesta activa y prevención de intrusiones
- **Gestión de eventos de seguridad**
- Máquinas y redes trampa
- Conclusiones
- Referencias

Integración, Correlación y Minería de Datos

- Integración de registros y alertas
  - Integrar todos los eventos de seguridad de manera que puedan ser adecuadamente supervisados
  - Permite lidiar con ingentes cantidades de trazas
- Correlación
  - Manera de diferenciar incidentes de eventos de forma eficaz
  - Es importante poder valorar si un evento corresponde con un incidente real o no
- Análisis y alertas
  - Una vez que un incidente ha sido detectado, un sistema de análisis genera alertas y operaciones en forma de "*triggers*"

Gestores de eventos de seguridad

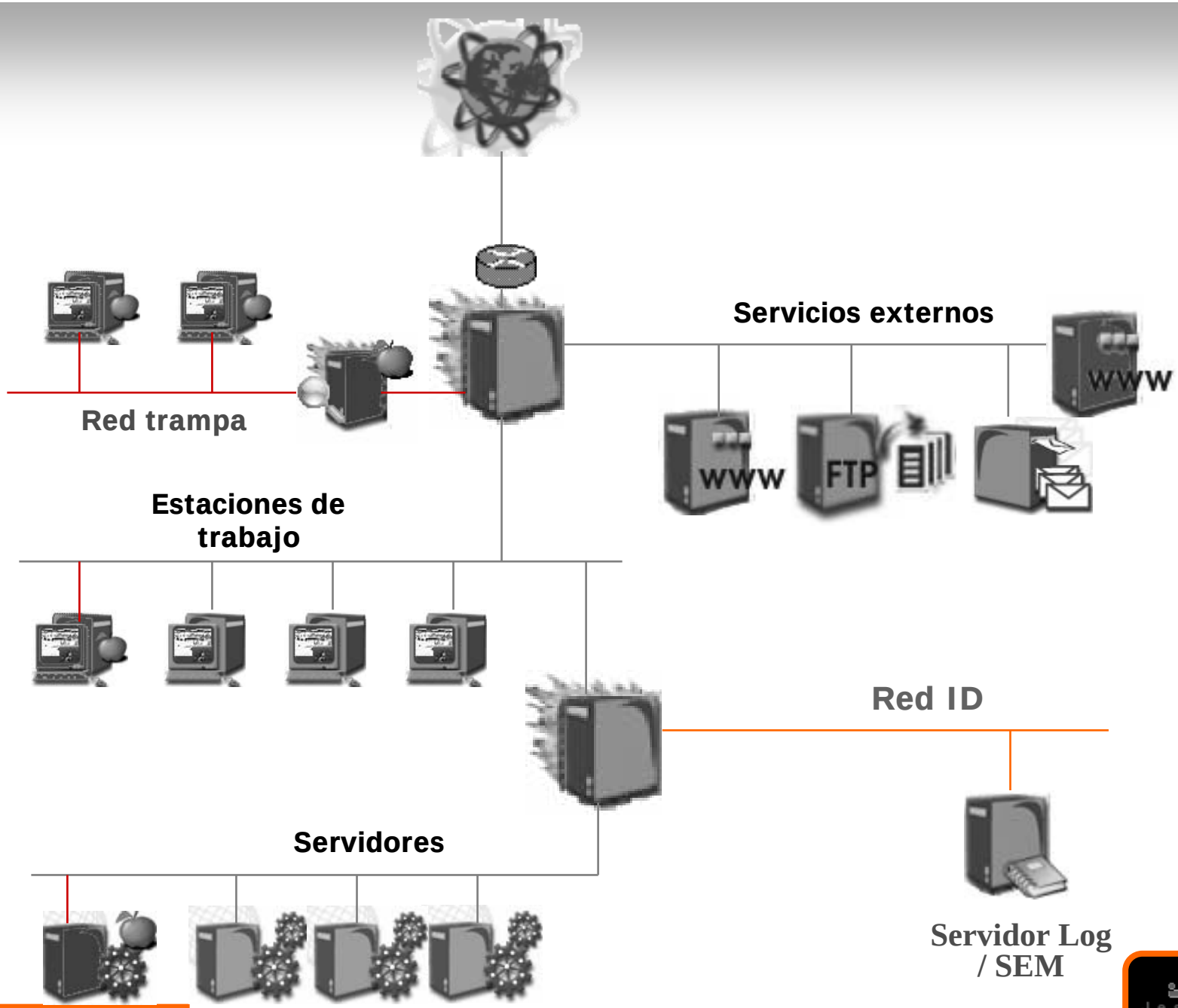
- Permiten una integración entre los sistemas de detección de intrusos a nivel de red y de sistema, con otro tipo de herramientas de seguridad:
  - Cortafuegos
  - Escáneres de vulnerabilidades
  - Herramientas de auditoria
- Funciones:
  - Agregar
  - Correlacionar
  - Priorizar
- Ayudan a rebajar el nivel de falsos positivos
- Su calidad reside en la cantidad de fuentes de datos que pueden agregar y calidad en el motor de correlación

Agenda

- Introducción
- HIDS: nivel de host
- NIDS: nivel de red
- Respuesta activa y prevención de intrusiones
- Gestión de eventos de seguridad
- **Máquinas y redes trampa**
- Conclusiones
- Referencias

Máquinas y redes trampa

- Tipos:
  - Baja interacción
  - Alta interacción
- Uso:
  - Cualquier tráfico es sospechoso
  - Excelente herramienta IDS
- Estrategias:
  - Redes externas
  - Redes internas
  - Redirección de tráfico bloqueado a las máquinas trampa


Servicios externos
WWW
WWW
FTP
Red trampa
Estaciones de trabajo
Red ID
Servidores
Servidor Log / SEM

Honeypots/nets: ventajas y limitaciones

- Ventajas:
  - Máquinas trampa:
    - Sistema IDS de 0 falsos positivos
    - Posibilidad de “tarpitting”
  - Redes trampa:
    - Conocer a los atacantes
    - Probar los procedimientos de respuesta a incidentes
    - Entrenamiento para equipos IR/Forensic
- Limitaciones:
  - Redes trampa:
    - Alto riesgo (especialmente si no se implementan correctamente)
    - Alto consumo en tiempo

Agenda

- Introducción
- HIDS: nivel de host
- NIDS: nivel de red
- Respuesta activa y prevención de intrusiones
- Gestión de eventos de seguridad
- Máquinas y redes trampa
- **Conclusiones**
- Referencias

Agenda

- Introducción
- HIDS: nivel de host
- NIDS: nivel de red
- Respuesta activa y prevención de intrusiones
- Gestión de eventos de seguridad
- Máquinas y redes trampa
- Conclusiones
- **Referencias**

Referencias

- “JISK: Intrusion Detection and Prevention”, JSS
  URL: http://www.jessland.net/JISK/IDS_IPS/
- “JISK: Honeypots”, JSS
  URL: http://www.jessland.net/JISK/Honeypots/
- “Inside Network Perimeter Security”, S.Northcutt, Lenny Zeltser
  ISBN: -
- “Network Intrusion Detection”, S.Northcutt & Judy Novak
  ISBN: -
- “The Tao of Network Security Monitoring”, R.Beijlitch
  ISBN: -
- “Intrusion Signatures and Analysis”, S.Northcutt, Mark Cooper
  ISBN: -
- “Honeypots: Tracking Hackers”, Lance Spitzner
  ISBN: -
- “Know your Enemy”, The Honeynet Project
  ISBN: -