“La tecnología IDS ha muerto”

Gartner Group

Detección de Intrusos

desde el **interior** y a **vista de pájaro**

✚ Objetivos

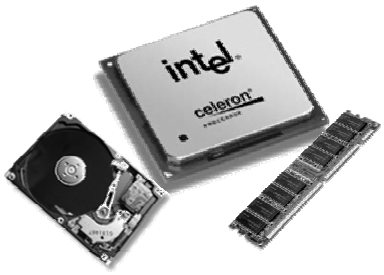
- Mostrar la importancia de la detección de intrusos desde el interior y a vista de pájaro.
- Describir tecnologías existentes para la **detección de intrusos a nivel de sistema**.
- Descubrir el potencial existente en las aproximaciones de **centralización y gestión de eventos** de seguridad.
- Poder aprender algo "**nuevo**" para llevarlo a vuestras instituciones. ☺

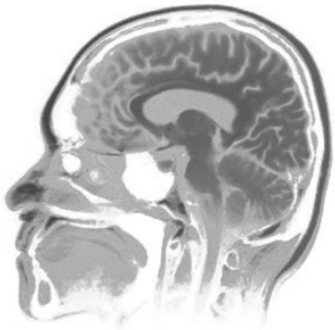
✚ Agenda

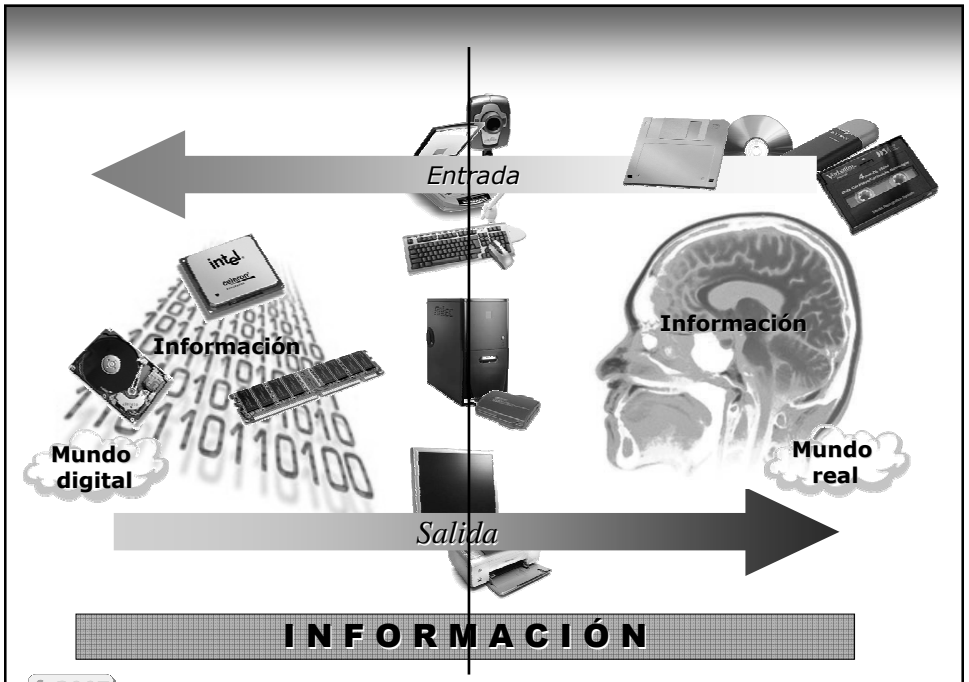
- Introducción
- IDS a nivel de sistema
- Recogida y centralización de eventos
- Gestión de eventos de seguridad
- Conclusiones
- Referencias

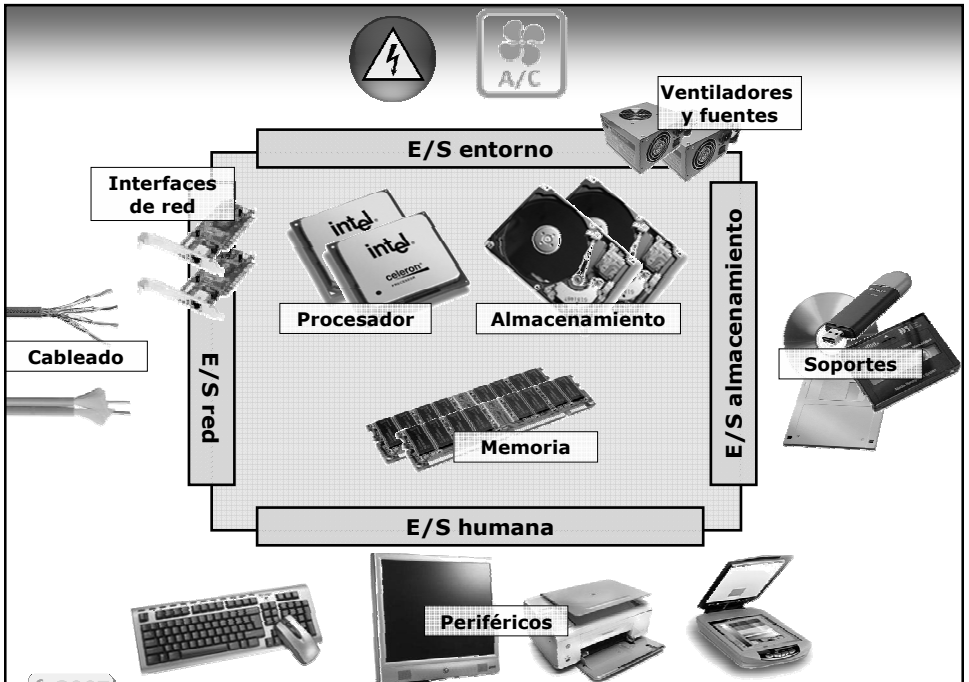
Agenda

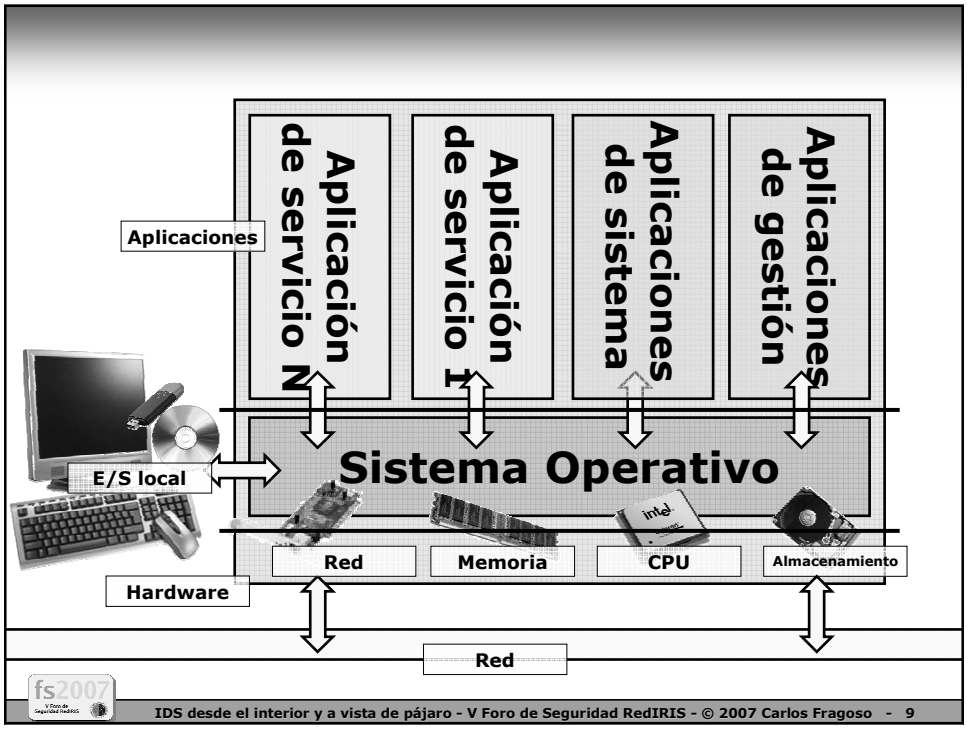
- **Introducción**
  - IDS a nivel de sistema
  - Recogida y centralización de eventos
  - Gestión de eventos de seguridad
  - Conclusiones
  - Referencias

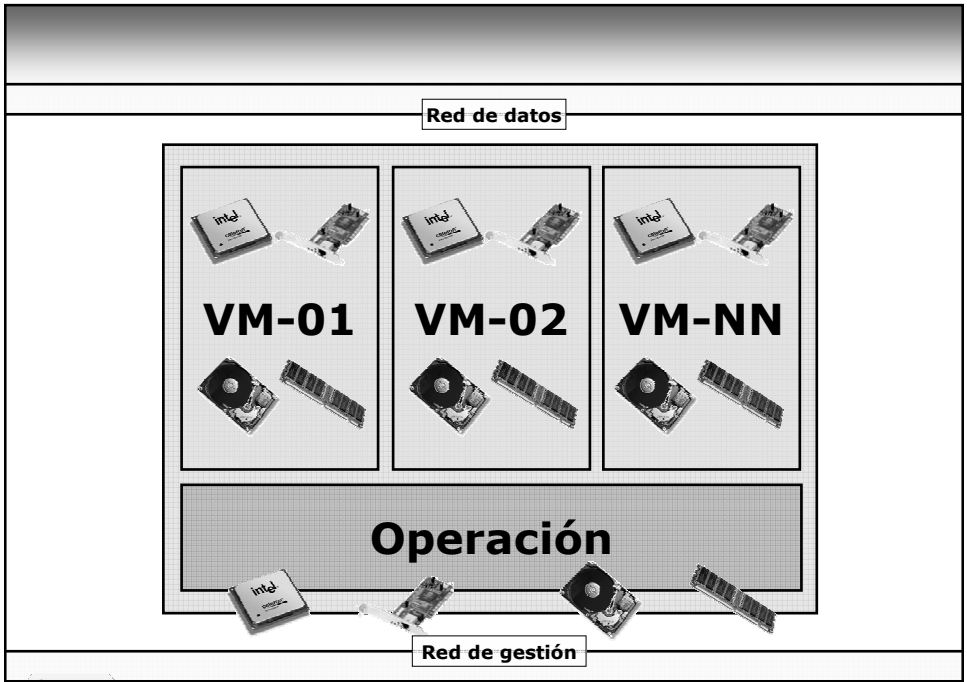


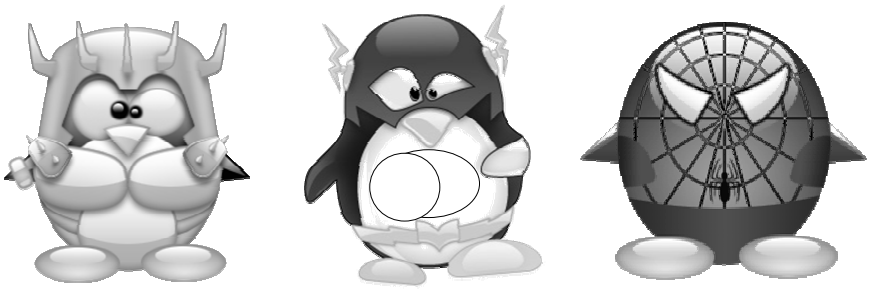



Entrada
Información
Información
Mundo digital
Mundo real
Salida
I N F O R M A C I Ó N

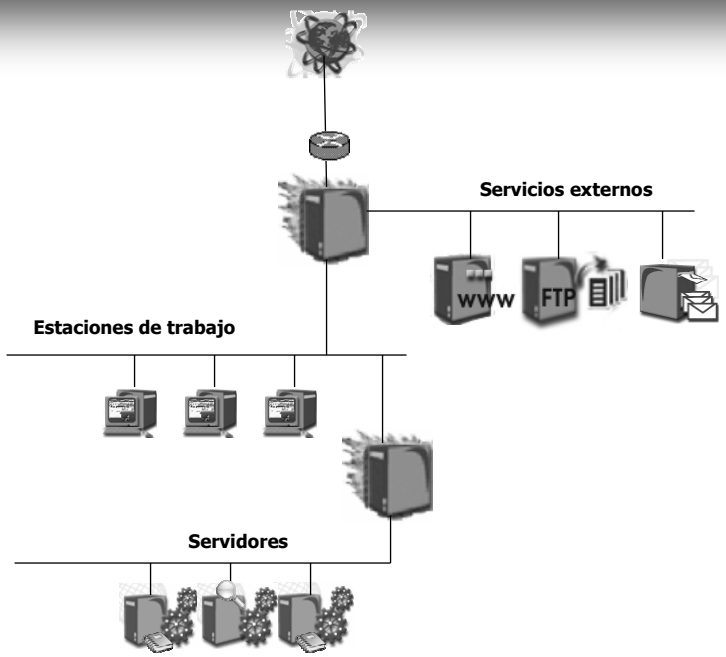

A/C
Ventiladores y fuentes
E/S entorno
Interfaces de red
Procesador
Almacenamiento
E/S almacenamiento
Cableado
E/S red
Soportes
Memoria
E/S humana
Periféricos


Aplicación de servicio N
Aplicación de servicio 1
Aplicaciones de sistema
Aplicaciones de gestión
Aplicaciones
Sistema Operativo
E/S local
Red
Memoria
CPU
Almacenamiento
Hardware
Red


Red de datos
VM-01
VM-02
VM-NN
Operación
Red de gestión

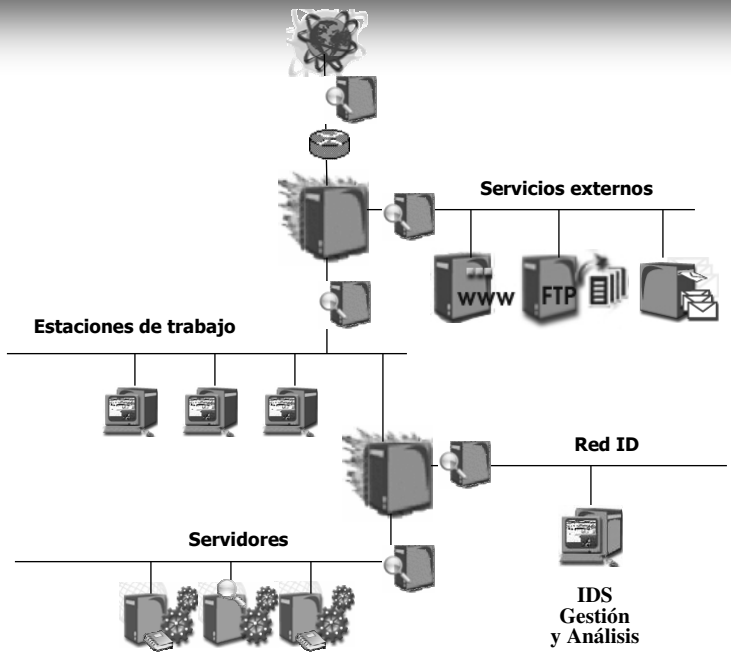


Protección **Detección** **Reacción**



Introducción 1/2

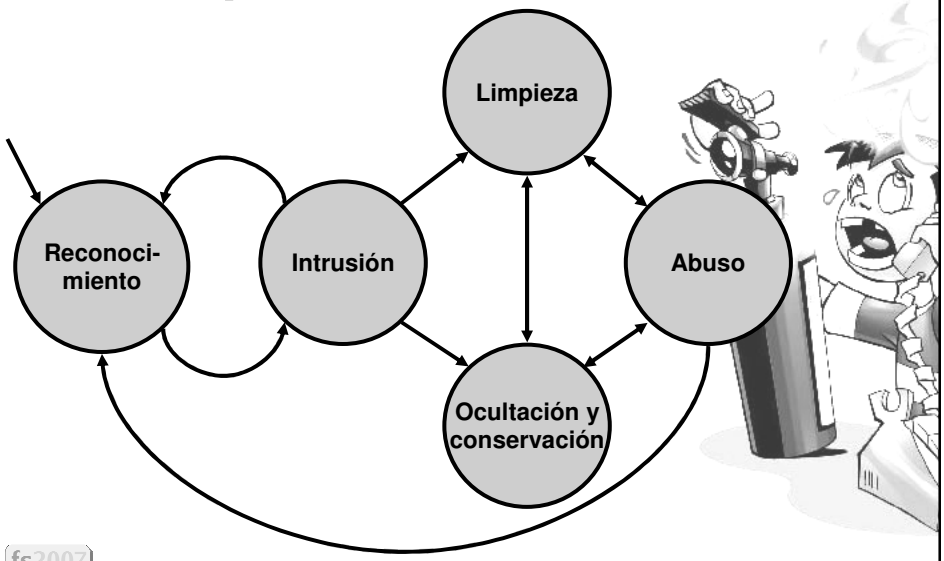
- Si protejo mis perímetros de red con cortafuegos y dispongo de mecanismos a nivel de sistema de control de código malicioso ... ¿Qué puede pasarme?
- Además tengo un fantástico NIDS justo antes del cortafuegos para ver todos los ataques! ☺
  - Detección de ataques vs detección de intrusos
- ¿ Qué ocurre si se logra penetrar en el perímetro ?
  - Adjuntos de correo y páginas web maliciosas, VPN no autorizadas, redes inalámbricas desprotegidas, etc.
- ¿ Qué ocurre si el atacante utiliza nuevos vectores, herramientas y mecanismos de ataque ?
  - Vulnerabilidades de día 0, polimorfismo, evasión NIDS, etc.
- "La prevención es idónea pero la detección es imprescindible"



Introducción 2/2

- ¿ Por qué pueden interesarse en mi ?
  - Ja ja ! ¿ todavía lo pones en duda ?
  - Ataques oportunistas, dirigidos, internos, etc.
- No es una cuestión de 'si' sino de 'cuando'
- Funciones:
  - Detección
    - Respuesta a incidentes más completa y ágil.
  - Auditoria ☺
    - Nos dicen que ocurre en nuestras redes
  - Forense
    - ¿ Que hicieron en el sistema ?
    - ¿ Cómo consiguieron entrar ?
    - ¿ Que debo parchear o fortificar ?

Etapas de una intrusión



"No soy **único**
en mi **equipo**

...pero...

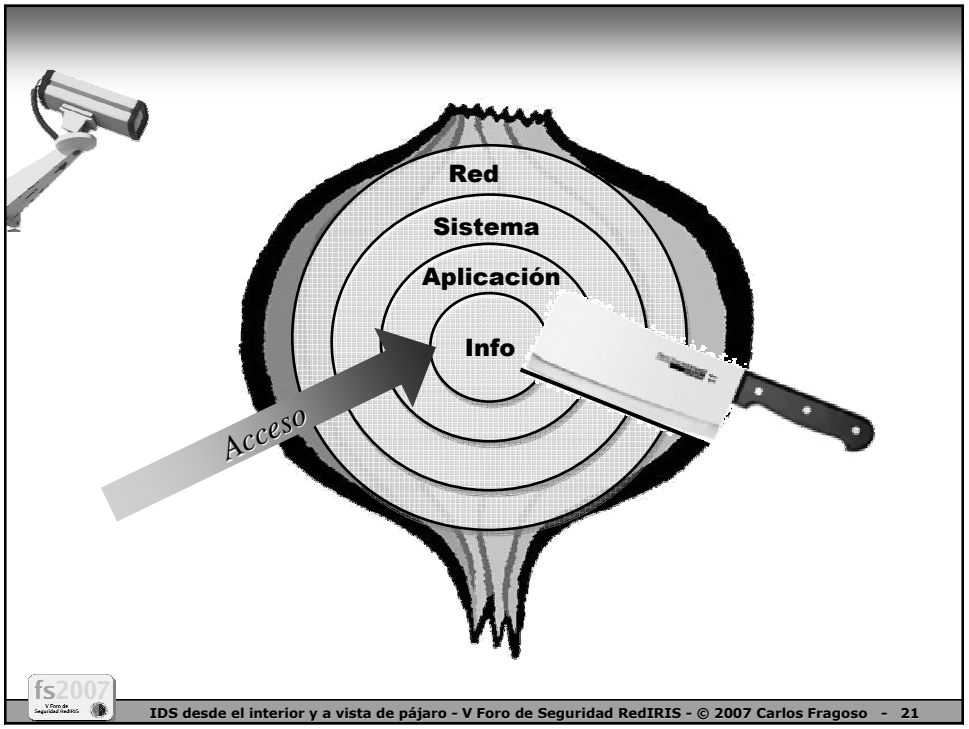
...en mi **equipo**
soy **único**"

=

Equipos
Multidisciplinares

Equipos: conocimientos

- El "conocimiento" es crítico en las tecnologías IDS para un despliegue y operación efectivas:
  - Redes
  - Sistemas Operativos
  - Aplicaciones
  - Conceptos de seguridad
  - Adecuación a la política de la organización
  - Habilidades en *scripting* y uso de herramientas

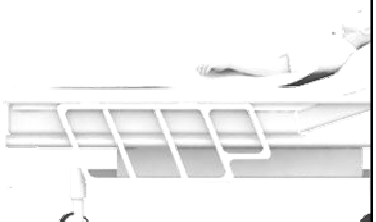


✚ Agenda

- Introducción
- ✚ **IDS a nivel de sistema**
- Recogida y centralización de eventos
- Gestión de eventos de seguridad
- Conclusiones
- Referencias

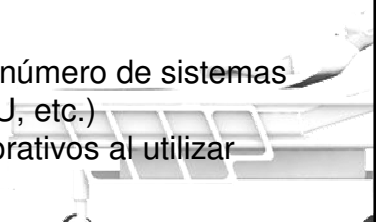
IDS a nivel de sistema (HIDS)

- **Monitorización y detección local a nivel de sistema operativo o aplicación.**
- **Motivaciones:**
  - Evasión o ataques contra NIDS
  - Ataques desde el interior (*perimeter bypass*)
- **Implementaciones:**
  - Herramientas específicas
  - Agente con módulos HIDS



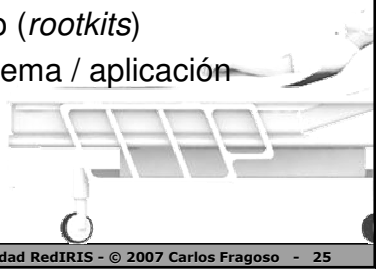
HIDS: ventajas y limitaciones

- 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



IDS a nivel de sistema (HIDS)

- Tecnologías:
  - Control de integridad de ficheros
  - Monitorización y perfilado de procesos
  - Tráfico y eventos de red
  - Monitorización de eventos del núcleo (*kernel*)
  - Perfilado y auditoria de sistema (configuración)
  - Verificación de código malicioso (*rootkits*)
  - Monitorización de trazas de sistema / aplicación
  - Cortafuegos a nivel de sistema



HIDS: Integridad de ficheros

- Verificación de cambios en el sistema de ficheros ya sea en contenido o metadatos:
  - Simple
  - Multicapa
- Base de datos de ficheros críticos utilizando firmas digitales
- Contrastado con bases de datos de terceros
- Consideraciones:
  - Carga de procesamiento en los sistemas
  - Copia remota (centralización) de la base de datos

Integridad de ficheros
AIDE 1/2

- Advanced Intrusion Detection Engine
- Fichero de configuración: aide.conf
- Crea firmas criptográficas:
  - Sha1, sha256, sha512, md5, rmd160
- Almacenamiento en base de datos
- Plataformas soportadas:
  - Solaris
  - Linux
  - FreeBSD, OpenBSD
  - AIX, HP-UX, Tru64
  - Windows (cygwin)

Integridad de ficheros
AIDE 2/2

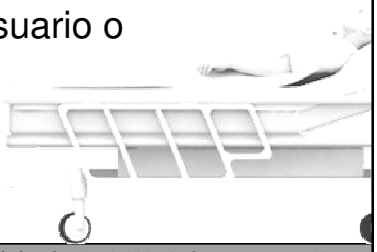
```
# You can alse create custom rules - my home made rule
   definition goes like this
MyRule = p+i+n+u+g+s+b+m+c+md5+sha1

# Next decide what directories/files you want in the
   database

/etc p+i+u+g     #check only permissions, inode, user and
   group for etc
/bin MyRule      # apply the custom rule to the files in
   bin
/sbin MyRule     # apply the same custom rule to the files
   in sbin
/var MyRule
   !/var/log/.*     # ignore the log dir it changes too
   often
   !/var/spool/.*   # ignore spool dirs as they change too
   often
   !/var/adm/utmp$  # ignore the file /var/adm/utmp
```

HIDS: Monitorización y perfilado de procesos

- Supervisión continua de los procesos del sistema y su comportamiento:
  - Consumo de recursos, acceso a la red, etc.
- Alertas:
  - Informativas
  - Consulta confirmación al usuario o administrador del sistema



Tráfico y eventos de red

- Captura y perfilado de tráfico para la detección de anomalias.
- En algún caso se suele denominar NIDS a nivel de nodo
- Niveles:
  - Nivel 2: red de área local
  - Nivel 3/4: información de sesión
  - Nivel 7: nivel de aplicación

Eventos y tráfico de red

SANCP 1/2

- Security Analyst Network Connection Profiler
- Versión actual 1.6.1 del 24/08/2006
- Realiza un perfilado del tráfico de red a nivel de sesión recogiendo información estadística, flujos de red y datos.
- Cuenta con un lenguaje de reglas para describir el tráfico normal y así diferenciarlo de las anomalias.
- Niveles de registro:
  - *Pcap*: todo el tráfico en formato pcap
  - *Realtime*: conexiones basadas en el primer paquete
  - *Stats*: conexiones según su finalización o fin por inactividad
- Puede integrarse con otras herramientas para correlar actividad o investigar incidentes. Ej: Sguil NSM

Eventos y tráfico de red

SANCP 2/3

```
var ip 8                # ether proto 0x0800  # ip traffic
var arp 1544            # ether proto 0x0806  # arp
  traffic
var loopback 144        # ether proto 0x9000  # Loopback:
  used to test ethernet interfaces
var 802.3 1024          # ether proto 0x0004  # IEEE 802.3
  traffic
var mailserver1  10.10.11.29
var ntpserver  210.121.2.64
var icmp 1
var tcp 6
var udp 17
var http 80
var https 443
known_ports tcp http,https,ssh,telnet,irc_ports,dns
known_ports udp dns
```

Eventos y tráfico de red

SANCP 3/3

```
arp any any any any any, ignore # ignore arp traffic
loopback any any any any any, ignore # ignore local
  ethernet loopback test packets
802.3 any any any any any, ignore  # ignore IEEE
  802.3 traffic on the switch

ip any dnsserver1 17 any 53, realtime=pass,
  status=303, rid=15 #2003-12-14 19:19:27
ip any dnsserver2 17 any 53, realtime=pass,
  status=303, rid=16 #2003-12-14 19:19:27
```


Eventos y tráfico de red

ARPWatch 1/2

- Herramienta de monitorización de nivel 2 que realiza un seguimiento de los pares IP/Ethernet.
- Desarrollada por Berkeley National Laboratory
- Controla la actividad de tipo ARP:
  - Nuevas estaciones: "*new station*"
  - Cambios de MAC: "*changed ethernet address*"
  - Conmutación: "*flip flop*"
- Nos permite especialmente detectar ataques de intercepción mediante envenenamiento ARP.
- Notificación mediante correo electrónico.

Eventos y tráfico de red

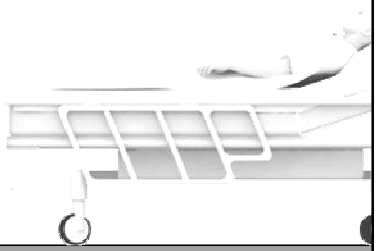
ARPWatch 2/2

```
            hostname: <unknown>
          ip address: 172.16.237.69
           interface: eth1
    ethernet address: 0:c:29:ae:2b:2c
     ethernet vendor: Vmware, Inc.
           timestamp: Wednesday, April 11, 2007 19:35:43 -0500

            hostname: <unknown>
          ip address: 172.16.237.2
           interface: eth1
    ethernet address: 0:c:29:ae:2b:2c
     ethernet vendor: Vmware, Inc.
old ethernet address: 0:50:56:f7:12:20
 old ethernet vendor: Vmware, Inc.
           timestamp: Wednesday, April 11, 2007 19:37:11 -0500
  previous timestamp: Wednesday, April 11, 2007 19:37:04 -0500
               delta: 7 seconds
```


HIDS: Eventos del núcleo

- Registro de los eventos del núcleo del sistema operativo para registrar las acciones en el sistema
- Soportado en gran parte de los sistemas operativos actuales
- Consideraciones:
  - Granularidad
  - Impacto en eficiencia



Perfilado y auditoría de sistema

- Realización de auditorias de configuración del sistema
- Factores:
  - Volumen
  - Protocolos
  - Destinos
- Consideraciones:
  - Complejidad debido a las posibles variaciones en el tiempo

Perfilado y auditoría de sistema

tiger 1/2

- Herramienta de auditoria y detección de intrusiones.
- Revisa debilidades y vulnerabilidades habituales en el sistema:
  - Permisos
  - Archivos de configuración
  - Cuentas no habilitadas
- Está totalmente escrita en Shell, utiliza herramientas POSIX del sistema.
- Configuración en fichero tigerrc

Perfilado y auditoría de sistema

tiger 2/2

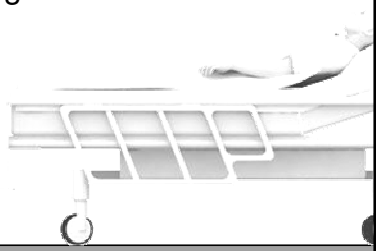
```
:~# tiger -c /etc/tiger/tigerrc
Tiger UN*X security checking system
   Developed by Texas A&M University, 1994
   Updated by the Advanced Research Corporation, 1999-2002
   Further updated by Javier Fernandez-Sanguino, 2001-2005
   Covered by the GNU General Public License (GPL)

Configuring...

Will try to check using config for 'i686' running Linux 2.6.18-4-
   686...
--CONFIG-- [con005c] Using configuration files for Linux 2.6.18-
   4-686. Using
           configuration files for generic Linux 2.
Tiger security scripts *** 3.2.1, 2003.10.10.18.00 ***
23:26> Beginning security report for lin-srv-int.
23:26> Starting file systems scans in background...
23:26> Checking password files...
23:26> Checking group files...
23:26> Checking user accounts...
```

Verificación de código malicioso

- Detección de la presencia de *rootkits*
  - *A nivel de sistema*
  - *A nivel de núcleo*
- Busqueda de patrones conocidos
  - Cambios en binarios especiales
  - Entradas sospechosas en los logs
  - Interfaz en modo “sniffer”
  - Métodos indirectos
- Consideraciones:
  - Utilidad limitada



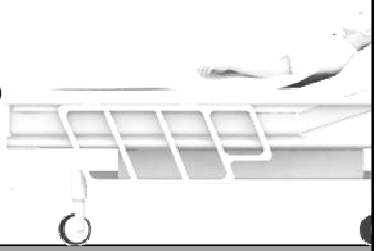
Revisión de código malicioso

chkrootkit

- Búsqueda local de signos de compromiso mediante rootkit.
- Identificación de diferentes ítems:
  - Troyanos conocidos
  - Interfaz en modo promiscuo
  - Modificación de binarios del sistema
- Sistemas soportados:
  - FreeBSD, OpenBSD, NetBSD
  - Solaris
  - HP-UX, Tru64
  - MacOSX

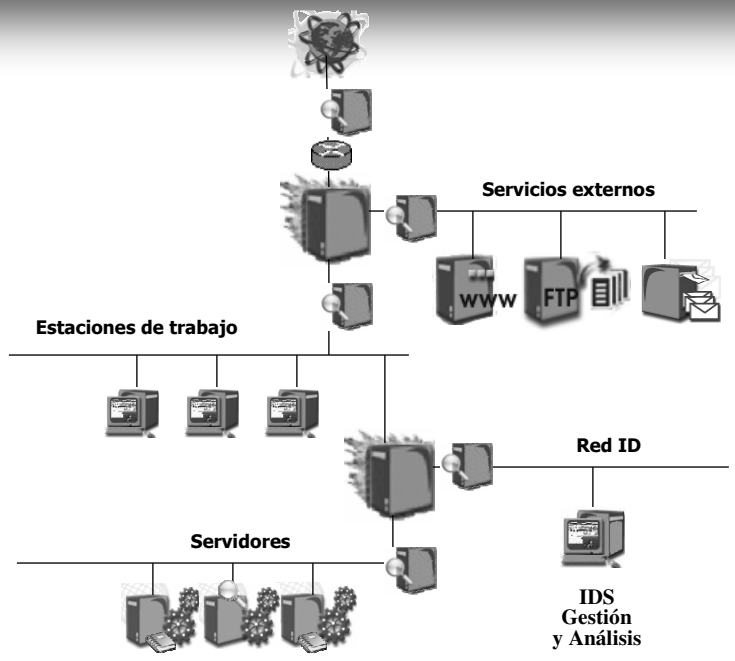
Monitorización de *logs* de sistema y aplicaciones

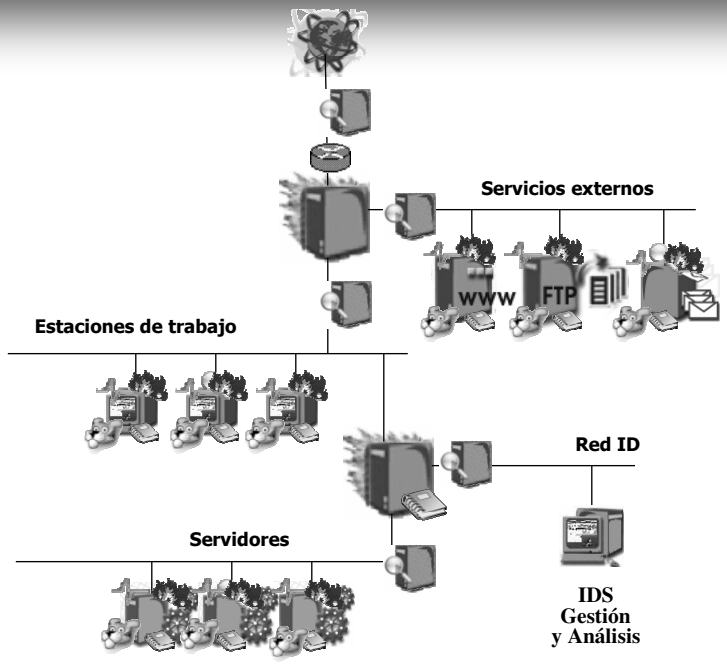
- Son una excelente fuente de información
- Análisis:
  - Continuo
  - Periódico
- Ubicación
  - Local
  - Servidor de registro remoto
    - Garantia de entrega (TCP)
    - Cifrado (SSL)



Híbridos

- Combinan grupos de las técnicas anteriores.
- Suelen consistir en un agente conformado por un grupo de plug-ins o módulos.
- Habitualmente se comunican con un punto centralizado donde se:
  - Centraliza configuraciones, BBDD...
  - Notifación de eventos/anomalias



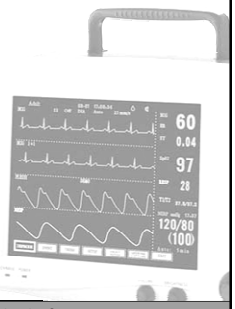


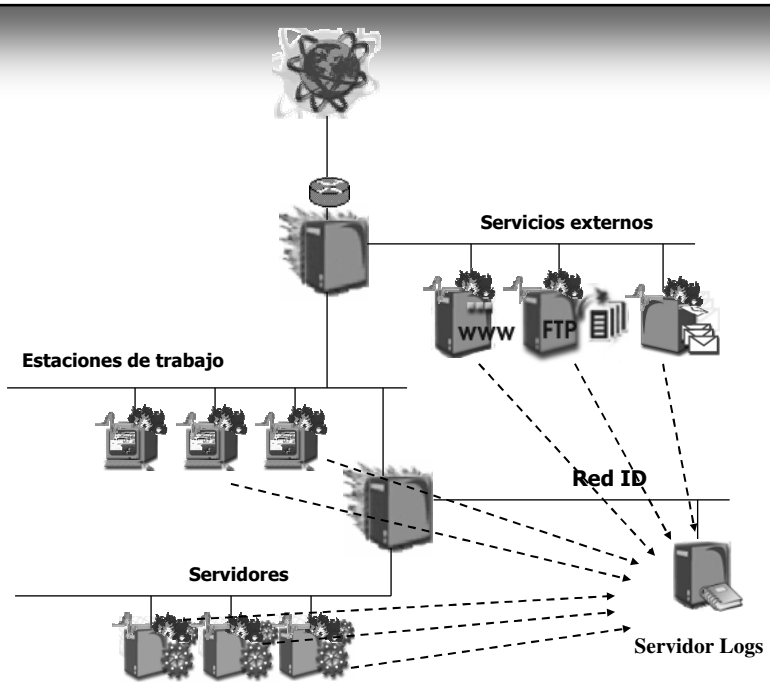
✚ Agenda

- Introducción
- IDS a nivel de sistema
- ✚ **Recogida y centralización de eventos**
- Gestión de eventos de seguridad
- Conclusiones
- Referencias

Eventos de seguridad

- Mecanismos de envío:
  - Syslog
  - Correo electrónico
  - SNMP traps
  - Propietarios
- Formato:
  - Texto plano vs XML
  - Línea vs multilínea
- Sincronización horaria centralizada (NTP)
- Centralización
- Estándares relacionados:
  - IDMEF e IDXP en IETF IDWG
- Poca aceptación de los fabricantes:
  - Mecanismos propietarios y integración mediante APIs, plug-ins, etc.





¿ Quienes generan *logs* ?

- Sistemas Operativos
- Aplicaciones
- Herramientas de seguridad
  - NIDS, VPN, FW, Antivirus, etc.
- Dispositivos de red
  - Cortafuegos, enrutadores, etc.
- Herramientas de gestión
- ...etc.

¡¡¡ Dame logs !!!

- "LogAnalysis Log Samples"
  - http://www.loganalysis.org/sample-logs/samples.html
- "OSSEC Log Samples"
  - http://www.ossec.net/wiki/index.php/Log_Samples

Problemáticas

- Cuanta información recoger
- Cómo clasificar los eventos
- Cuales eventos enviar por red
- Cómo buscar una aguja en un pajar
  - Análisis de la información recogida
- Intentar garantizar:
  - Confidencialidad: cifrado
  - Disponibilidad futura: almacenamiento masivo

Recogida y centralización de eventos

Syslog

- Definido en RFC3164
- Protocolo para el envío de logs por red
- Problemáticas:
  - Uso de protocolo no fiable UDP
  - Confidencialidad: texto plano
  - Integridad: falta de autenticación
  - Disponibilidad: susceptible de DoS
- Soluciones actuales:
  - Uso de wrappers SSL o IPSec. Ej: stunnel
  - Implementaciones propietarias con TCP, cifrado, etc.
- Futuras soluciones:
  - Syslog-sign: firma de eventos
  - Reliable syslog: uso de protocolo BEEP

Recogida y centralización de eventos

Syslog-NG 1/2

- Mantenida por Balabit IT Security
- Características destacables:
  - Transporte fiable mediante TCP
  - Configuración intuitiva y flexible
  - Filtrado y control granular
- Configuración por niveles:
  - Source: define origen de los eventos
  - Destination: define su destino
  - Filter: filtrado aplicado al orígen
- Cada 'log' queda definido uniendo los componentes source, destination y filter.

Recogida y centralización de eventos

Syslog-NG 2/2

```
source s_net { udp(); };
destination d_net_dev-acl {
  file("/var/log/net/acl");
};
filter f_net_dev-acl { match("IPACCESSLOG"); };
filter f_net_router { host("192.168.0.1"); };
log {
        source(s_net);
        filter(f_net_dev-acl);
        filter(f_net_router);
        destination(d_net_dev-acl);
};
```

Lasso

- Esponsorizado por Loglogic
- Basado en el desarrollo pasado del proyecto Snare de Intersect Alliance
- Cliente de captura y envío de eventos:
  - Estándard de Windows
  - Específicos de aplicaciones
- Fiabilidad mediante TCP: *Syslog-NG*

Swatch

```
Ignore /news|CROND/

watchfor /[dD]enied|/DEN.*ED/
  echo bold
  mail=alert@pisa.org.hk, subject=Log_Denial
  exec "/etc/call_pager 5551234 08"

watchfor /router/
  mail=alert@pisa.org.hk, subject=Log_Router
  exec
```

Recogida y centralización de eventos

Algunas herramientas de análisis

- Tiempo real:
  - Logsurfer
  - Logcheck
- Periódico:
  - Logwatch

✚ Agenda

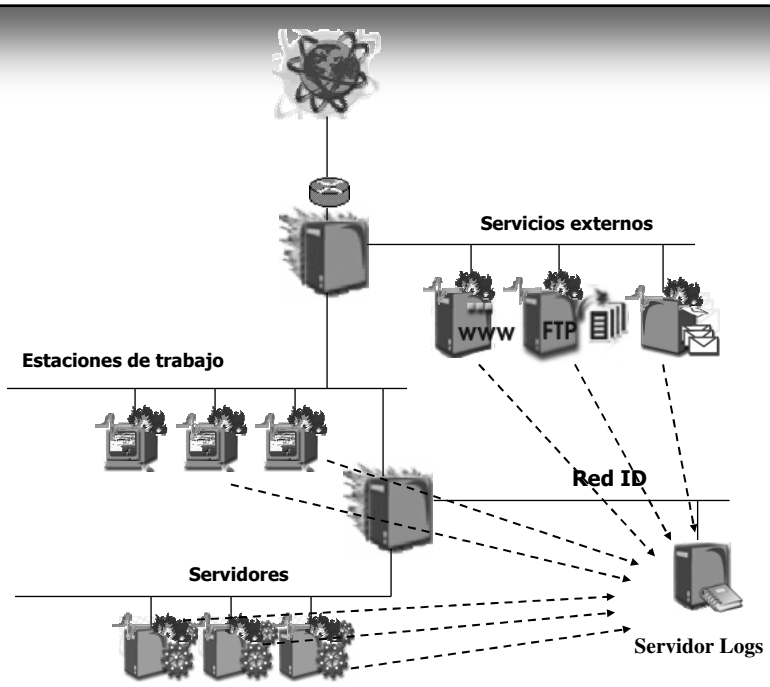
- Introducción
- IDS a nivel de sistema
- Recogida y centralización de eventos
- ✚ **Gestión de eventos de seguridad**
- Conclusiones
- Referencias

Gestión de eventos:
Integración, Correlación y Análisis

- 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 acciones en forma de "*triggers*"

Gestión de eventos:
Integración, Correlación y Análisis

- 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:
  - Consolidar
  - 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



Gestión de eventos de seguridad

SEC 1/2

- Security Event Correlator
- Desarrollado por Risto Vaarandi
- Herramienta simple de correlación que utiliza juegos de reglas basados en expresiones regulares
- Tipos de correlación:
  - Single (withScript, withSuppres, withThreshold)
  - Pair (withWindow)
  - Suppress
  - Calendar

Gestión de eventos de seguridad

SEC 2/2

- Ej: Mostrar un único mensaje de filesystem lleno durante 900 segundos por cada uno de los servidores (srv1 y srv2)

```
type=SingleWithSuppress
ptype=RegExp
pattern=(\S+) \[kern\.crit\] vmunix: (\S+): [fF]ile system
   full
context=_FILE_EVENT_/logs/srv1.messages ||
   _FILE_EVENT_/logs/srv2.messages
desc=$1:$2 file system full
action=pipe 'File system $2 at host $1 full' mail -s 'FS
   full' root
window=900
```


Gestión de eventos de seguridad

OSSEC 1/3

- Proyecto Open-Source liderado por Daniel Cid
- Gran evolución y soporte de la comunidad
- Funcionalidades:
  - Motor de análisis y correlación de eventos
  - Respuesta Activa
  - Librería de reglas para múltiples formatos de log conocidos.
  - Módulos HIDS
- Plataformas soportadas (POSIX):
  - Linux: Slackware, RedHat, Ubuntu, Debian, Suse
  - BSD: OpenBSD, FreeBSD
  - Windows: XP/2000/2003
  - MacOSX
  - UNIX: AIX, HP-UX, Solaris
- Componentes:
  - Rootcheck: Rootkit detection (bbdd con patrones en servidor)
  - Syscheck: Integrity checking (bbdd en servidor)

Gestión de eventos de seguridad
OSSEC 2/3

- Tipos de instalación
  - Servidor
  - Agente
  - Local
- Eventos soportados:
  - NIDS: Snort, Cisco IOS IDS/IPS
  - Cortafuegos: iptables, ipfilter, netscreen, windows firewall, Cisco PIX/ASA/FWSM, etc.
  - Concentradores VPN: Cisco VPN concentrator, Racoon SSL
  - Security Tools: nmap, arpwatch, spamd, symantec antivirus, etc.
  - Servidores: Named, Squid, Apache, IIS, Postfix, Sendmail, MS Exchange, ProFTPd, vsftpd, samba, etc.
  - Sistema: OpenSSH, sudo, PAM, Windows Event Viewer, etc.
- Comunicación por syslog o segura propia.
  - Clave precompartida entre agente y servidor
- Particularidades:
  - OSSEC Web User Interface (WUI)
  - En Windows solo versión agent (extra registro y eventos de sistema)

Gestión de eventos de seguridad
OSSEC 3/3

```
<rule id="1608" level="13" timeframe="120">
    <regex>^sshd[\d+]: fatal: Local: crc32
  compensation attack</regex>

    <if_matched_regex>^sshd[\d+]: \.+Corrupted check
  by bytes on</if_matched_regex>

    <comment>SSH CRC-32 Compensation
  attack</comment>

  <info>http://www.securityfocus.com/bid/2347/info/<
  /info>

</rule>
```

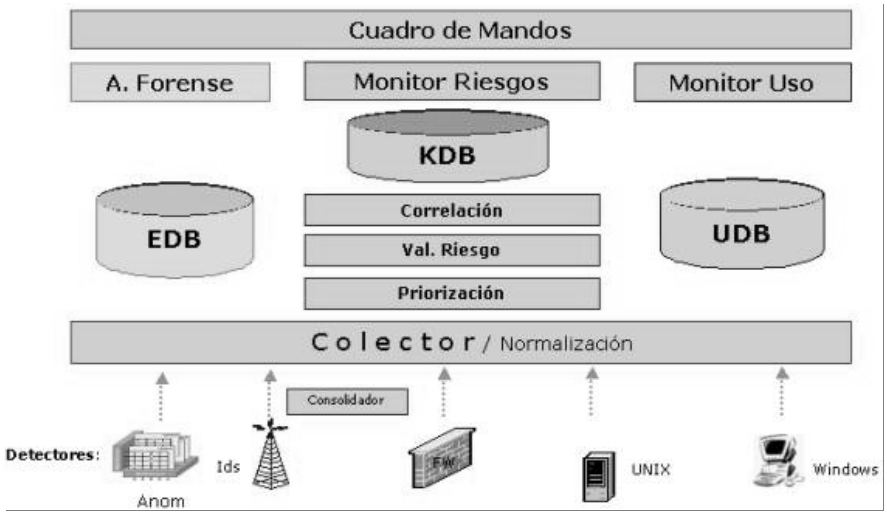
Gestión de eventos de seguridad

OSSIM 1/3

- Open Source Security Information Management
- Desarrollado por un grupo de españoles de IT Deusto:
  - Julio Casal, Fabio Ospitia, David Gil y Dominique Karg
- Características:
  - Correlación
  - Priorización
  - Valoración de Riesgos
- Carencias:
  - Imposibilidad de agregar eventos procedentes de herramientas comerciales

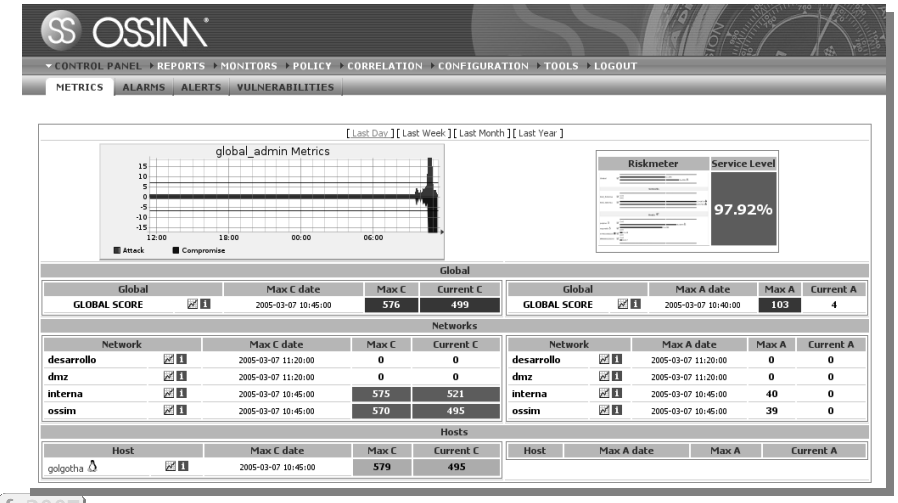
Gestión de eventos de seguridad

OSSIM 2/3



Gestión de eventos de seguridad

OSSIM 3/3



Gestión de eventos de seguridad

Soluciones comerciales

- Bitácora
- Cisco Security MARS
- Microsoft Operations Manager (MOM)
- NetForensics
- CA eTrust Security Management Suite
- Loglogic
- Arcsight
- Network Intelligence
- Symantec Security Information Manager
- ...etc...

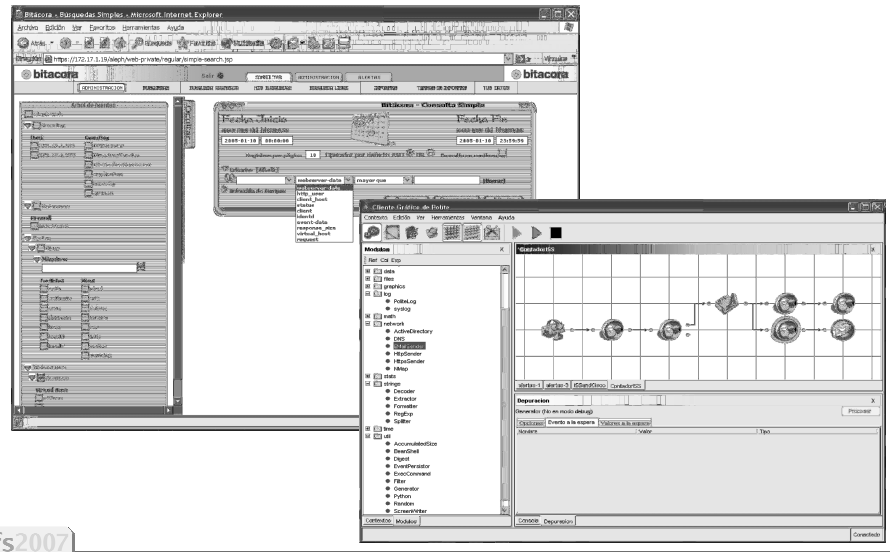
Gestión de eventos de seguridad

bitacora 1/2

- Desarrollado por S21Sec
- Producto de centralización y análisis de eventos de seguridad
- Características:
  - Arquitectura modular con alta disponibilidad
  - Multiplataforma soportando múltiples fabricantes
  - Recolector en tiempo real y diferido mediante múltiples protocolos
  - Almacenamiento a largo plazo
  - Potente motor de búsquedas
  - Alertas, informes, gráficas, etc.

Gestión de eventos de seguridad

bitacora 2/2



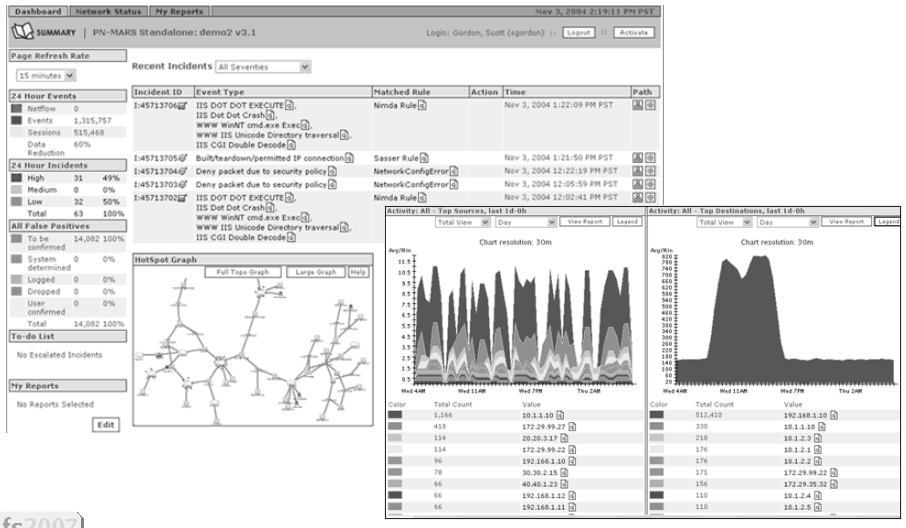
Gestión de eventos de seguridad

Cisco MARS 1/2

- Cisco Monitoring, Analysis and Response System
- Sistema para la gestión de amenazas de los sistemas de información:
  - Potente motor de correlación de eventos para la detección de anomalias
  - Integración con múltiples fabricantes
  - Mecanismos de autodescubrimiento
  - Entorno de investigación forense y respuesta a incidentes manual y automatizada
  - Análisis de vulnerabilidades bajo demanada
  - Revisión y ajuste de configuraciones de dispositivos

Gestión de eventos de seguridad

Cisco MARS 2/2

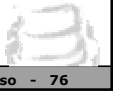


✚ Agenda

- Introducción
- IDS a nivel de sistema
- Recogida y centralización de eventos
- Gestión de eventos de seguridad
- ✚ **Conclusiones**
- Referencias

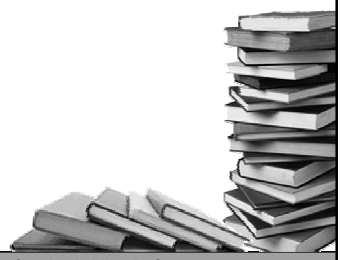
✚ Conclusiones

- **"La prevención es idónea pero la detección es imprescindible"**
- Madurez de las tecnologías IDS tanto de las NIDS como de las HIDS, mientras SIM/SEM está en crecimiento.
- Gran abanico de técnicas y herramientas HIDS para utilizar en nuestros sistemas de información.
- Correlar eventos dispersos mejora sustancialmente la capacidad de detección.
- Las herramientas de centralización y correlación son el núcleo duro de la gestión de la seguridad.
- Elegir un despliegue efectivo según los riesgos y necesidades de nuestra organización.



✚ Agenda

- Introducción
- IDS a nivel de sistema
- Recogida y centralización de eventos
- Gestión de eventos de seguridad
- Conclusiones
- ✚ **Referencias**



✚ Referencias

Generales

- **"Detección y Prevención de Intrusos"**
  Jessland Security Services (JSS)
  URL: http://www.jessland.net/JISK/IDS_IPS.php
- **"Logging News and Information"**
  LogAnalysis
  URL: http://www.loganalysis.org
- **"Top 5 Intrusion Detection Systems"**
  Insecure.org
  URL: http://sectools.org/ids.html

Referencias

Libros

- **"Intrusion Detection and Prevention"**
  Osborne McGraw-Hill

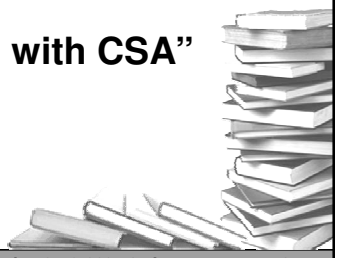
  ISBN: 9780072229547

- **"Security Threat Mitigation with Cisco MARS"**
  Cisco Press

  ISBN: 9781587052606

- **"Advanced Intrusion Detection with CSA"**
  Cisco Press

  ISBN: 9781587052521



Referencias

Estándares y guías de buenas prácticas

- **"CCN-STIC Seguridad Perimetral: Detección de Intrusos"**
  Centro Criptológico Nacional (CCN)

  URL: http://www.cert.ccn.cni.es

  URL: http://www.ccn.cni.es

- **"Guide to Intrusion Detection and Prevention Systems"**
  "Guide to Computer Security Log Management"
  National Institute for Standards and Technology (NIST)

  URL: http://csrc.nist.gov/publications/

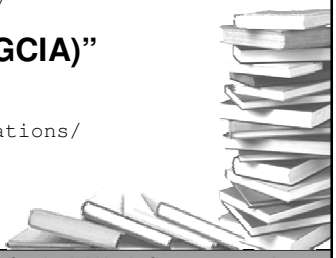
- **"Syslog Working Group"**
  "Intrusion Detection Working Group"
  Internet Engineering Task Force (IETF)

  URL: http://www.ietf.org/

Referencias

Cursos y certificaciones

- **"Curso de Acreditación STIC: Detección de Intrusos"**
  Centro Criptológico Nacional (CCN)
  - URL: http://www.cert.ccn.cni.es
  - URL: http://www.ccn.cni.es
- **"SEC503: Intrusion Detection In-Depth"**
  SANS Institute
  - URL: http://www.sans.org/training/
- **"GIAC Certified Intrusion Analyst (GCIA)"**
  Global Information Assurance Certification
  - URL: http://www.giac.org/certifications/



¡¡¡ Gracias por vuestra atención !!!

http://www.cesca.es

http://www.jessland.net

http://carlos.fragoso.es carlos@fragoso.es

E3B5 8908 57CA 5B67 83DD 9400 085A 29FF D539 69A3