

TEMA 5:

Seguridad en sistemas

SEGURIDAD

Grado de Ingeniería Informática
en Sistemas de Información



Índice



1. Introducción
2. Configuración segura
3. Protección frente a código malicioso
4. Gestión de actualizaciones y parches
5. Monitorización y registros
6. Sistemas de detección de intrusiones en hosts (HIDs)

1.Introducción



Siguiendo con la progresión físico->lógico pasamos de seguridad física a **seguridad lógica** en equipos.

Los equipos, y sobre todo los sistemas operativos, tienen cada día más funcionalidades y complejidad. Por tanto, más posibilidades de ser vulnerables.

Las configuraciones estándares no suelen ser muy seguras. Deben revisarse y mejorarse tras la instalación.

1.Introducción



Los programas suelen tener fallos de seguridad

- Hay que protegerlos de código malicioso y, en general, de actividades maliciosas (intrusiones)
- Hay que resolver los fallos mediante parches/actualizaciones

Hay que tener constancia de lo que está pasando en los sistemas, monitorizando y registrando su actividad.



1. Introducción
2. **Configuración segura**
3. Protección frente a código malicioso
4. Gestión de actualizaciones y parches
5. Monitorización y registros
6. Sistemas de detección de intrusiones en hosts (HIDs)



2. Configuración segura

Se deben tener estándares de configuración para

- servidores
- equipos de sobremesa
- portátiles
- electrónica de red
- ...

Se consigue un entorno homogéneo. Equipos configurados de igual forma, lo que facilita la administración.

2. Configuración segura



Estándares que definen configuraciones específicas (longitud mínima de contraseñas, cierre de puertos, parámetros TCP...)

para

- Servidores Windows [w2kchk] [cis-win]
- Servidores Solaris [cis-sol]
- Servidores Linux (distintas distribuciones) [cis-lnx] [auscertchk]

... y para...

- Clientes Windows
- Clientes Linux
- Portátiles

2. Configuración segura



...además de...

- servidores de BD [cis-ora]
- servidores de aplicaciones [cis-apache][cis-iis]

... y para...

- switches
- routers
- impresoras de red

2. Configuración segura



A un equipo o servicio se le aplican una serie de estándares. Se rellenan una serie de listas de comprobación (*checklists*) del tipo

- Fecha de aplicación del checklist / persona que lo aplica
- Control / forma de implantarlo / [hecho][pendiente][no aplicable->motivo]

La aplicación de las configuraciones debe hacerse, en lo posible, con el equipo sin conectar a red: estamos *asegurándolo*; hasta que no esté seguro, mejor que no esté disponible

2. Configuración segura



Deben cambiarse las **claves por defecto** [dpl]
[dpl2]

Deben eliminarse los **usuarios de prueba o invitados**: pueden hacernos vulnerables a **escalada de privilegios** [escalada]

Deberían configurarse “*login banners*” o avisos del tipo

“Sistema propiedad de Desconéctese si no está autorizado. Toda actividad puede ser monitorizada”



2. Configuración segura

Debe habilitarse en el sistema la política de contraseñas [winpp][lnxpp]:

- longitud mínima: p. ej., nueve caracteres
- complejidad:
 - requerir uso de mayúsculas, minúsculas, dígitos y símbolos
 - búsqueda en diccionario de la nueva clave
- caducidad: cambio de clave cada 6 meses, por ejemplo
- histórico: la nueva clave no puede ser una de las X anteriores
- permanencia mínima para evitar el cambio+cambio y vuelta a la clave inicial

2. Configuración segura



... y deben controlarse los accesos fallidos, con una política de bloqueo de cuentas:

- X fallos de acceso antes del bloqueo.
- Tras ese número de accesos erróneos consecutivos, bloqueo de la cuenta por Y minutos
- Se pone a cero el contador de fallos
 - tras un acierto, o...
 - tras Z minutos

Esto evita los ataques por fuerza bruta...

... pero puede causar denegación de servicio.

2. Configuración segura



Sólo se deben ejecutar los servicios necesarios.

El resto deben ser desactivados

Debe desinstalarse el software innecesario:

- Un servidor de producción no debe tener software de desarrollo
- Un servidor Unix/linux no necesita entorno gráfico (X11)
- Un servidor no necesita un agente de transferencia de correo / Mail Transfer Agent (MTA), al menos, visible desde fuera
- ...

2. Configuración segura



El acceso remoto al servidor debe estar encriptado:

- ssh [wp-ssh] en lugar de telnet
- sftp [wp-sftp] en lugar de FTP
- Acceso gráfico:
 - “X11 forwarding” sobre ssh: túnel ssh para X11
 - RDP [wp-rdp] (Terminal Server/rdesktop) encriptado
 - VNC encriptado

2. Configuración segura



Siguiendo el principio general de *defensa en profundidad*, se debería instalar un cortafuegos en el equipo, con política gestionada de forma centralizada.

Debería configurarse el protector de pantalla con clave, o un fin de sesión automático por inactividad (*auto-logout*)

2. Configuración segura



La modificación de parámetros TCP del núcleo del SO sirve para [tcpip-sec, cap.2]

- proteger contra ataques de DoS (SYN flood) [wp-syn]
 - Intento de inicio de conexión que luego no se sigue.
- proteger contra *spoofing* (falsificación) de direcciones
- proteger contra ataques de *source routing* [ibm-sr]
 - Podrían permitir, entre otras cosas, el acceso a máquinas protegidas dentro de una red privada mediante una pasarela.
- ocultar al equipo deshabilitando las respuestas a los ICMP/PING

Se hace con [hardening-tcp]

- modificación del registro en Windows
- sysctl en Linux (usado para visualizar, configurar y automatizar configuraciones del kernel en el directorio /proc/sys/)

2. Configuración segura



Debe establecerse una sincronización con un servidor de hora

Varios motivos:

- veracidad y correlación de registros de sucesos (logs)
- requisitos de los protocolos de autenticación
- sincronización de clusters

Se suele usar el *Network Time Protocol* [wp-ntp]

2. Configuración segura



Sincronización de hora

- En equipos Windows integrados en dominios Active Directory (AD), automáticamente contra los controladores de dominio
- En equipos independientes y controladores AD Windows, no. Modificaciones del registro para sincronizarlos con fuente externa
- En otros sistemas operativos:
 - Demonio NTPD
 - Ejecución de comando ntpdate periódico (en tarea cron)

2. Configuración segura



Debe configurarse la auditoría del sistema (logs/registro de sucesos)

En determinados casos, deben exportarse los logs a servidores remotos, ya sea por seguridad (para evitar la destrucción de evidencias) o para unirlos con otros logs.

2. Configuración segura



Listas de comprobación (checklists) disponibles:

<http://www.cisecurity.org>

<http://checklists.nist.gov>

<http://iase.disa.mil/stigs/checklist>

<http://www.nsa.gov/snac>

2. Configuración segura



Automatización

Hay proyectos de estandarización: Extensible Configuration Checklist Description Format [xccdf]

- Define una serie de requisitos de configuración
- Permite auditar si están implantados

Automatización de la configuración:

- Herramientas de bastionado [bastille][lynis]
- Sistemas de configuración distribuida [puppet] [cfengine]
- “Security templates” [ms-sectpl] [ms-sectpl] [ws-sectpl]
- Distribución de políticas: Active Directory GPOs [gp] [ms-gp]

2. Configuración segura



Automatización

Automatización de la auditoría: comprobación automatizada y periódica de las configuraciones.



1. Introducción
2. Configuración segura
3. **Protección frente a código malicioso**
4. Gestión de actualizaciones y parches
5. Monitorización y registros
6. Sistemas de detección de intrusiones en hosts (HIDs)

3. Protección frente a código malicioso



Malware o código malicioso [mw1] :

Código que ha sido diseñado para infiltrarse en un sistema informático o para causar daño en él.

Más en general: código con la intención de comprometer uno o varios aspectos de la seguridad de un Sistema Informático.

Disponéis de la cronología en [cronologia] [cronologia2]

3. Protección frente a código malicioso



Posibles clasificaciones de malware:

Según forma de distribución:

- autorreplicante (al ejecutarse crea copias de sí mismo; incluso modificadas si es *polimórfico*)
- no autorreplicante

Según su independencia

- requiere estar adosado a otro código
- es independiente

3. Protección frente a código malicioso



Según su carga útil (*payload*)

- Destrucción de archivos
- Intercepción de información (keyloggers, spyware...)
- Subversión del sistema (rootkits, backdoors...) -> Creación de *Botnets* [bots] [bots2]: redes de *zombies* controlados desde un centro de control difícil de trazar
- Denegación de servicio distribuida (DDoS)
- Extorsión (!) (encriptación de disco+petición de rescate)

3. Protección frente a código malicioso



DIRECCIÓN GENERAL DE LA POLICÍA

CUERPO NACIONAL DE POLICÍA



Se han grabado todas las actividades de este ordenador. Todos sus ficheros están cifrados.

¡ATENCIÓN!

Ha violado la ley de derechos de autor (video, música, software) y ha utilizado o distribuido ilegalmente contenidos con derechos de autor, infringiendo con ello el artículo 1, sección 8, cláusula 8, también conocido como el artículo 17 del código penal de los España.

El artículo 1, sección 8, cláusula 8 del código penal de los España, multa de dos a quinientos salarios mínimos o la privación de libertad de uno a tres años.

Ha estado viendo o distribuyendo contenidos prohibidos (se encontraron fotos porno de niños etc. en su ordenador). Por violación del código penal de los España, el artículo 202 del código penal de los España, multa de dos a quinientos salarios mínimos o la privación de libertad de uno a tres años.

Se ha iniciado un acceso ilegal a su ordenador personal. El artículo 17 del código penal de los España, multa de dos a quinientos salarios mínimos o la privación de libertad de uno a tres años. Si el uso negligente del ordenador personal, el artículo 17 del código penal de los España, multa de dos a quinientos salarios mínimos o la privación de libertad de uno a tres años.

De conformidad con la ley de mayo de 2011, esta infracción de la ley (en caso de que se considere como una infracción de la ley) puede considerarse como una infracción de la ley (en caso de que se considere como una infracción de la ley).

Para desbloquear el ordenador, el artículo 17 del código penal de los España, multa de dos a quinientos salarios mínimos o la privación de libertad de uno a tres años. Se le obliga a pagar unas tasas de 100€. Puede pagar a través de la tarjeta Ukash, cargarla con 300€ e introducir el código de la tienda o gasolinera. Ukash está disponible en tiendas de alimentación.

¿Cómo puedo pagar la multa para desbloquear mi PC?

1. Encuentre un punto de venta de Ukash cerca suyo:



2. Escoja Ukash en la selección de prepago y cárguela con dinero en efectivo en la caja registradora.

3. Ingrese su código Ukash y escoja "¡Desbloquear el PC ahora!"



Su IP: [redacted]
Ubicación: Madrid,
Madrid,
Spain



Beveiligd betalingsformulier

Introduzca el código Ukash

Por favor, introduzca el código Ukash con el teclado numérico de abajo.

1 2 3 4 5 6 7 8 9 0 Borrar

¡Desbloquear el PC ahora!

Nota: Las multas sólo se pueden pagar en el plazo de 12 horas. Al transcurrir 12 horas vence la posibilidad de pagar la multa. Se confiscarán todos los datos de su PC y se iniciarán procedimientos penales en su contra si no paga la multa.

3. Protección frente a código malicioso



Distintos tipos de software malicioso

Virus. (Fred Cohen, 1984): “un programa que puede infectar a otros programas modificándolos para insertar una copia de sí mismo, posiblemente evolucionada”

Requiere un *huésped*.

Se activa al ejecutar el programa huésped.

No sólo código máquina: las aplicaciones *scriptables* son vulnerables (virus de macro, por ejemplo).

3. Protección frente a código malicioso



...tipos de software malicioso...

Gusano: aprovecha vulnerabilidades (normalmente en servicios de red) para propagar copias de sí mismo

También puede propagarse por correo.

No necesita huésped.

Aunque la carga útil pueda no ser dañina, el tráfico exponencial causado por su propagación es en sí mismo una DoS (denegación de servicio)

Morris Worm, por ejemplo [morris] [morris20]

Echó Internet abajo!



3. Protección frente a código malicioso



...tipos de software malicioso...

Troyano: código oculto en el interior de un programa legítimo (o que aparenta serlo). No se autorreplica.

Rootkit: un tipo de troyano que sustituye las herramientas de administración o librerías legítimas por versiones ***troyanizadas*** que ocultan el hecho de que el sistema está comprometido.

3. Protección frente a código malicioso



...tipos de software malicioso...

Spyware: recaba información del usuario y la envía al propietario del *malware*.

Keyloggers: un caso especial de *spyware*. Busca contraseñas, números de cuenta, números de tarjeta...

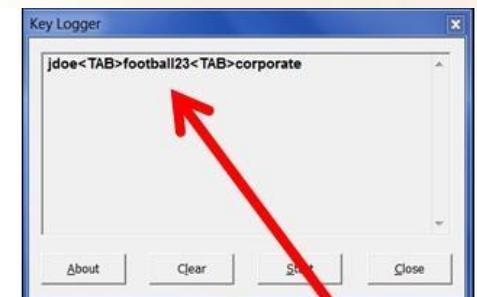


Image above shows Keylogger
Stealing VPN credentials

3. Protección frente a código malicioso



...tipos de software malicioso...

Caso particular: SPAM

No es código

No afecta, en principio, a la seguridad *del destinatario*...

Pero suele enviarse desde/a través de sistemas comprometidos (*bots/zombies*, por ejemplo) o mal configuradores (*mail relays* abiertos)

... y suele ser vía de transmisión de *malware*.

3. Protección frente a código malicioso



Antivirus/antispyware/antispam:

- Basados en patrones. Requieren descarga de actualizaciones frecuente.
- Basados en heurísticas. Aprendizaje. Observación del comportamiento y detección de anomalías. Pueden usar *sandboxes*: entornos restringidos para la ejecución monitorizada

Instalados en cada máquina y/o en *pasarelas* (de correo, web, proxy...) y servidores de ficheros

3. Protección frente a código malicioso



Se tiende a integrar la protección en UTM's (*unified threat management*) [utm-wp]: un *appliance* que incluye cortafuegos, IDS/IPS, antivirus, antispam, filtrado de contenido web...

Gestión centralizada: una consola que permite

- Despliegue de agentes y protecciones
- Distribución de actualizaciones
- Definición de políticas
- Registro de sucesos
- Generación de informes

3. Protección frente a código malicioso



TREND MICRO OfficeScan™ root Log Off ? Help

Current servers:

- Scan Now for All Domains
- Update Server Now

Summary

- Security Compliance
- Networked Computers
- Smart Protection
- Updates
- Logs
- Cisco NAC
- Notifications
- Administration
- Tools

Plug-in Manager

Summary Refresh Help

Activated services: **Desktop/Server Antivirus, Desktop/Server Web Reputation and Anti-spyware, File Reputation, Damage Cleanup Services**

OfficeScan OfficeScan and Plug-ins Smart Protection Network +

Client Connectivity Tab Settings Add Widgets

Latest data refresh: 10/18/2017 12:21 pm

All ▼ Display: [Icons]

Status	Smart Scan	Conventional Scan	Total
Online	105	1	106
Offline	25	12	37
Roaming	0	0	0
Total	130	13	143

Security Risk Detections

Latest data refresh: 10/18/2017 12:21 pm

Type	Detections	Infected Computers
Virus/Malware	87	12
Spyware/Grayware	6	4

Client Connectivity

Latest data refresh: 10/18/2017 12:21 pm

All ▼ Display: [Icons]

Status	Smart Scan	Conventional Scan	Total
Online	105	1	106
Offline	25	12	37
Roaming	0	0	0
Total	130	13	143

Outbreaks

View Top 10 Security Risk Statistics Latest data refresh: 10/18/2017 12:21 pm

Alert	Type	Current Outbreak	Last Outbreak	
[Icon]	Virus/Malware	None	None	Reset
[Icon]	Spyware/Grayware	None	None	Reset

Client Updates

Online Clients: 106, Smart Scan: 105, Conventional Scan: 1 Latest data refresh: 10/18/2017 12:21 pm



1. Introducción
2. Configuración segura
3. Protección frente a código malicioso
4. **Gestión de actualizaciones y parches**
5. Monitorización y registros
6. Sistemas de detección de intrusiones en hosts (HIDs)



4. Gestión de actualizaciones

Todo software tiene defectos

Algunos afectan solo a su funcionalidad

Otros tienen implicaciones en materia de seguridad.

Según Metrica v3, el mantenimiento puede ser

- **correctivo:** errores del producto
- **evolutivo:** cambios en las necesidades
- **adaptativo:** cambio en entorno (BD, comunicaciones, servidores...)
- **perfectivo:** calidad interna, rendimiento

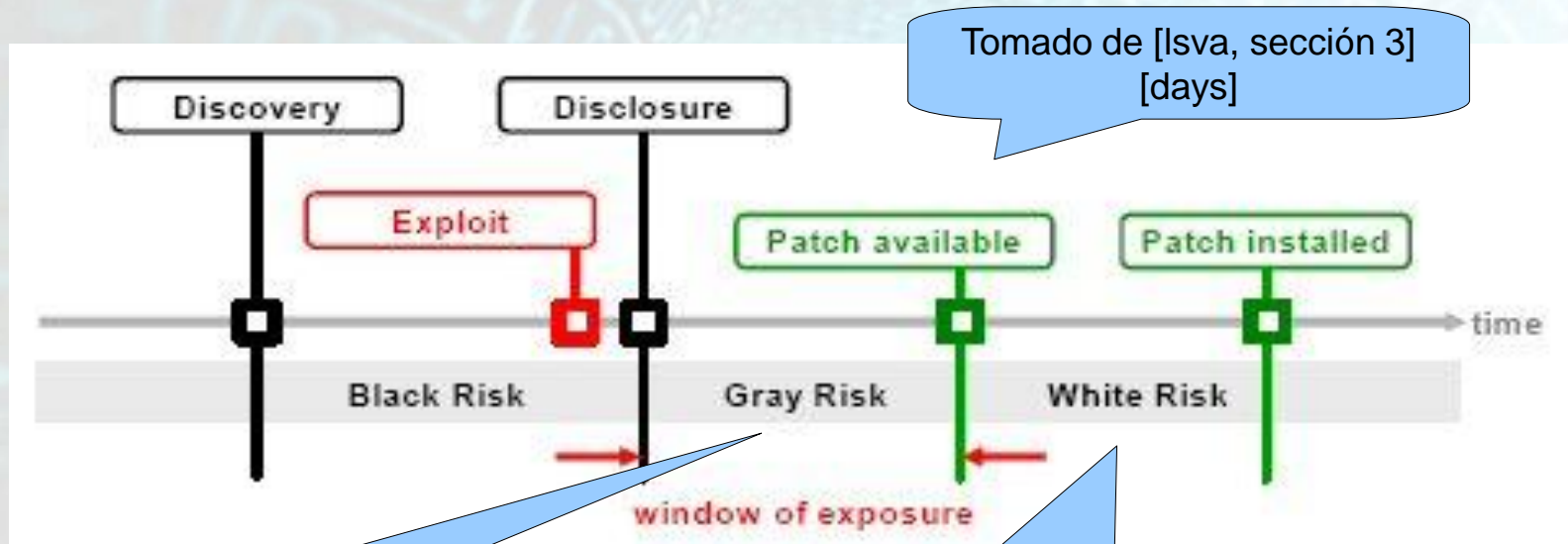
4. Gestión de actualizaciones



Ciclo de vida de un parche de seguridad

- *Descubrimiento de la vulnerabilidad.* Por amigos o enemigos
- *Explotación de la vulnerabilidad.* exploit: código que la aprovecha
- *Difusión de herramientas de explotación automática – la hora de los script-kiddies* [script-kiddie]
- *Publicación de la vulnerabilidad* (disclosure). El problema de la publicación completa [fulldisclosure]
- *Publicación del parche*
- *Aplicación del parche*

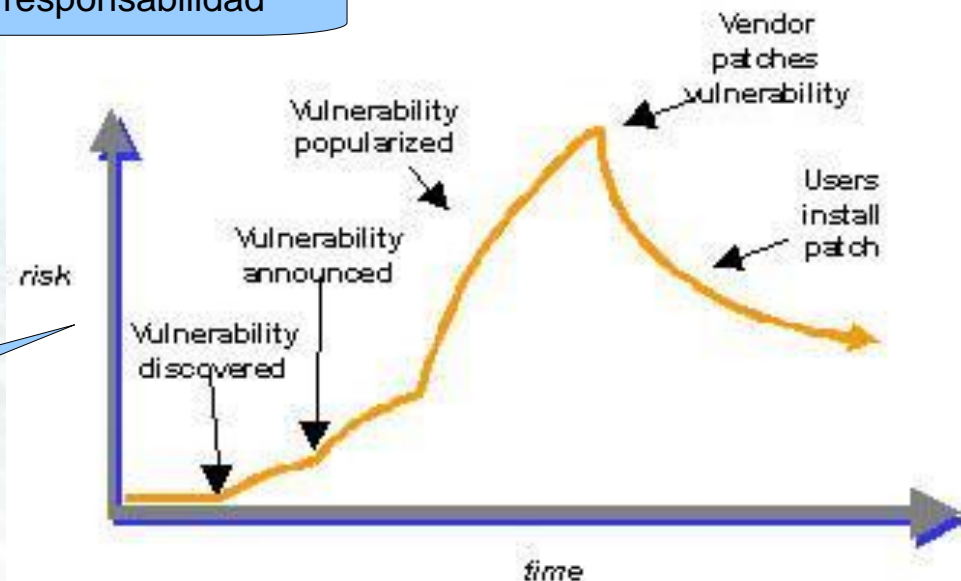
4. Gestión de actualizaciones



Responsabilidad del fabricante del software

Nuestra responsabilidad

Tomado de [schneier]



4. Gestión de actualizaciones



Proceso de actualización por nuestra parte

- **Información del estado del sistema:** nivel de parches, versiones instaladas...
- **Búsqueda de actualizaciones.** En base de datos del fabricante, por ejemplo. Hay servicios de seguridad gestionada (MSS) que proporcionan información para múltiples productos.
- **Búsqueda de dependencias:** una actualización puede requerir otras, en cascada

4. Gestión de actualizaciones



...proceso de actualización...

- **Descarga** (posible proxy). Si hay gran cantidad de equipos a parchear, una sola descarga a un servidor local (proxy). Cada equipo descarga desde el proxy. No todos a la vez: tráfico de red elevado
- **Instalación:** ¿inmediata, desatendida, programada, al apagar el equipo?
- **¿Reconfiguración?. Cuidado con las desconfiguraciones**
- **¿Reinicio? Problema en servidores con necesidad de alta disponibilidad. En *clusters* no hay problema: se reinicia por partes**

4. Gestión de actualizaciones



Actualización de múltiples equipos

- Centralización de información de estado
- Informe de actualizaciones disponibles
- Instalación de equipo(s) piloto. Se suele recomendar probar los parches antes de desplegarlos: posibles interacciones con aplicaciones existentes
- Pruebas
- Descarga y despliegue completo de los parches

4. Gestión de actualizaciones



Automatización de actualizaciones

- Debian/Ubuntu: apt / apt-cacher / apt-dater
- Solaris: pkg...
- RedHat: up2date (hasta RH4), yum. RedHat Network
- Microsoft: *Windows Software Update Services* (WSUS)



1. Introducción
2. Configuración segura
3. Protección frente a código malicioso
4. Gestión de actualizaciones y parches
5. **Monitorización y registros**
6. Sistemas de detección de intrusiones en hosts (HIDs)

5. Monitorización y registros

Monitorización

Control de los indicadores de funcionamiento de los sistemas

Permite establecer una línea de base (***baseline***) como comportamiento “normal”...

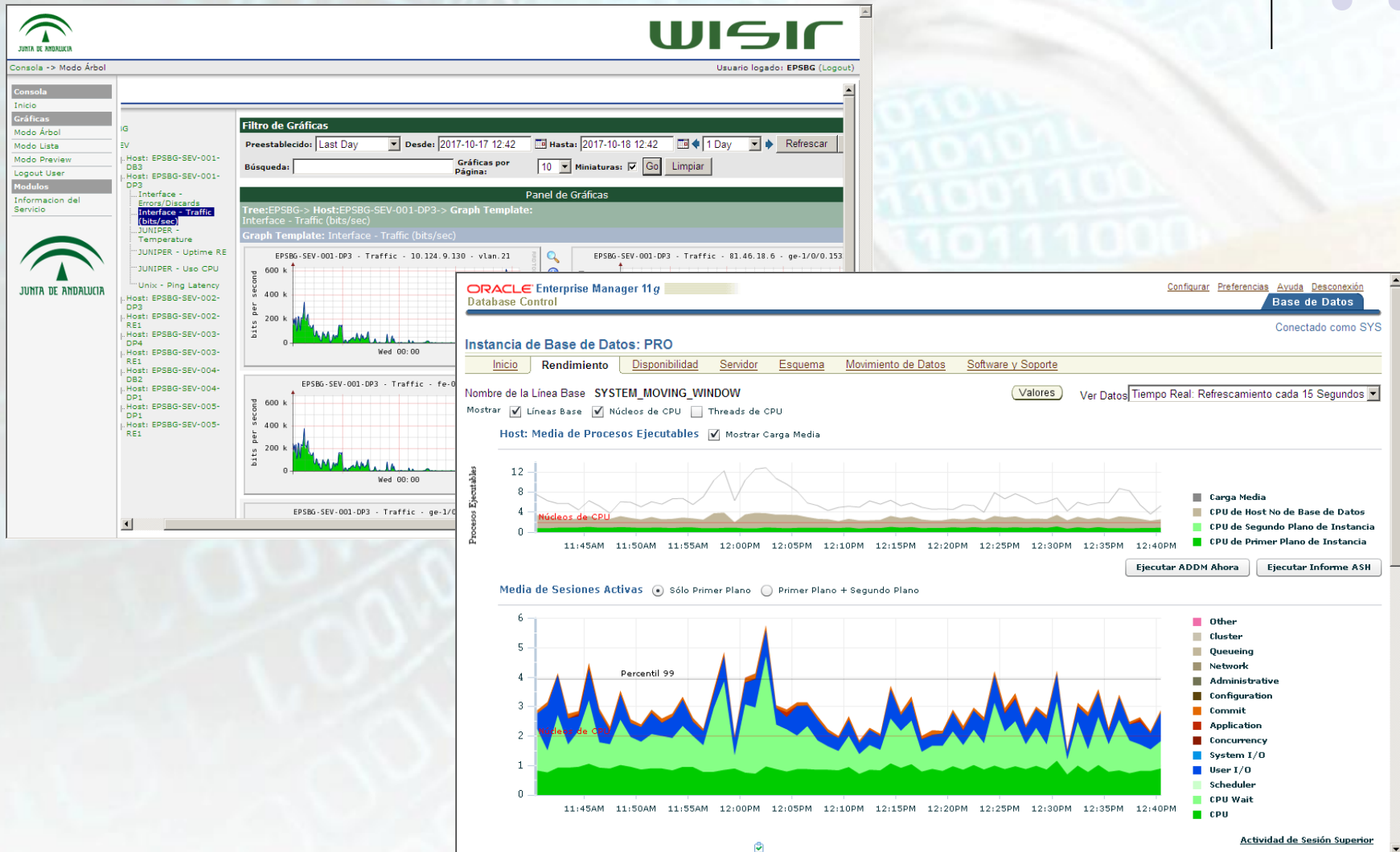
... y detectar cuándo los sistemas se salen de ella

El estudio de las tendencias facilita la continuidad y garantiza la disponibilidad:

podemos estimar cargas y necesidades futuras para estar preparados



5. Monitorización y registros



5. Monitorización y registros



SNMP [snmp-wpe]

Simple Network Management Protocol

Permite monitorizar (y en algunos casos configurar) dispositivos de red

Primitivas: GET, GETNEXT, SET, TRAP...

5. Monitorización y registros



SNMP

Componentes:

- dispositivos: los sistemas a monitorizar
- agentes: software que obtiene y publica las variables de los dispositivos
- sistemas de gestión: software que gestiona los dispositivos

La información se almacena de forma jerárquica en la *Management Information Base* (MIB), y cada variable se identifica mediante su *Object Identifier* (OID)

5. Monitorización y registros



Tipos de monitorización:

Monitorización cuantitativa:

- Bytes E/S en interfaces de red
- Espacio usado en discos
- %iowait (tiempo gastado en espera de E/S)
- %cpu (usuario, sistema, inactivo -- *idle* -- ..)
- N° de peticiones/segundo en servidores web
- ...

5. Monitorización y registros



Tipos de monitorización:

Monitorización cualitativa: servicios disponibles/indisponibles. Varios niveles

- Localmente: ¿está el proceso ejecutándose?
- Remotamente:
 - ¿podemos conectar al puerto de red del servicio
 - ¿lo que obtenemos es válido? ¡Puede que sea una página de error!
 - ¿podemos hacer *login* y ejecutar alguna(s) acción(es)?

5. Monitorización y registros



Los sistemas de monitorización, en caso de alerta, deben generar avisos por correo electrónico y, en casos específicos, por SMS.

Si en un tiempo determinado no se “reconoce” (*acknowledge*) el problema, se produce un escalado a más técnicos.

Software de monitorización: hay muchísima variedad. Comerciales y libres (Cacti, Nagios, OpenNMS, Zabbix...)

5. Monitorización y registros



Nagios - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://cacti/nagios/

Google

None

->gr ->gmail GC GBmk Not ced upo invest Lngjes Linux Ref Afic Educ E-buy seg desvan

Cacti Nagios

Inicio

- Mapas de Trafico
 - Seneca
 - Balanceadores
 - Moodle
 - Red SAN
 - Fabrics SAN
- Consola Syslog

Grupos

- Seneca
- @Firma
- Pasen
- Formacion
- Portal
- Intranet
- Oracle
- Comunicaciones
- Servidores
- Solaris

Monitoring

- Tactical Overview
- Service Detail
- Host Detail
- Hostgroup Overview
- Hostgroup Summary
- Hostgroup Grid
- Servicegroup Overview
- Servicegroup Summary
- Servicegroup Grid
- Status Map
- 3-D Status Map
- Service Problems
- Host Problems
- Network Outages

Show Host:

Current Network Status

Last Updated: Mon May 5 17:42:07 CEST 2008
Updated every 90 seconds
Nagios@ - www.nagios.org
Logged in as *nagiosadmin*

[View Service Status Detail For All Service Groups](#)
[View Status Summary For All Service Groups](#)
[View Service Status Grid For All Service Groups](#)

Host Status Totals

Up	Down	Unreachable	Pending
124	4	0	1

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
380	0	4	12	3

All Problems All Types





4	129
---	-----

All Problems All Types









16	399
----	-----

Service Overview For All Service Groups

Servicios de @Firma (SG_@FIRMA)

Host	Status	Services	Actions
MON_EXTERNA	UP	4 OK	 
MON_INTERNA	UP	5 OK	 

SG_COMUNICACIONES (SG_COMUNICACIONES)

Host	Status	Services	Actions
Alteon-DMZ-1	UP	2 OK	 
Alteon-DMZ-2	UP	2 OK	 
Alteon-SSL-DMZ-1	UP	2 OK	 
Alteon-SSL-DMZ-2	DOWN	1 UNKNOWN 1 CRITICAL	 

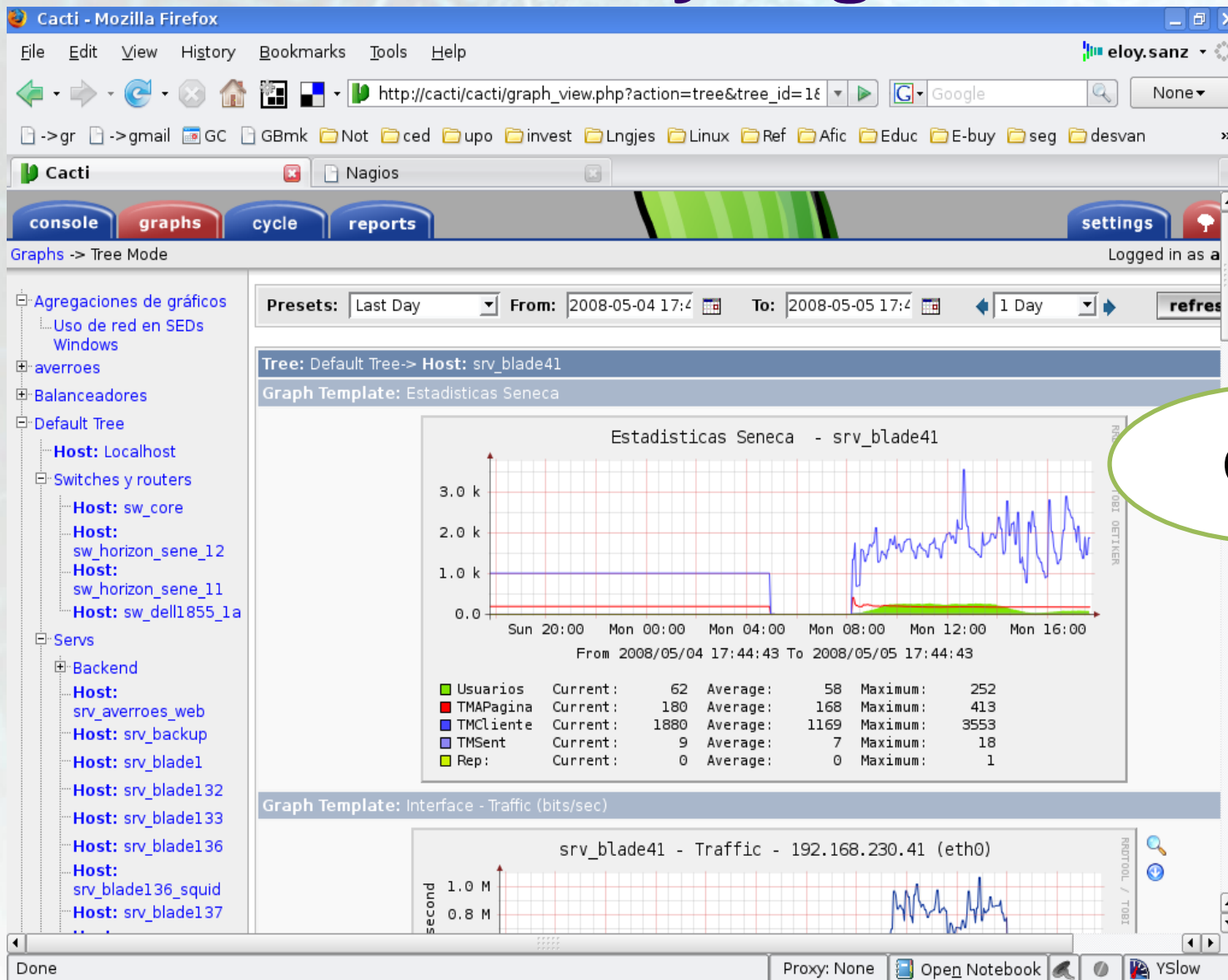
Servicio

Host
MON_I
MON_I
blade1
blade1
proteo

Done Proxy: None Open Notebook YSlow

Nagios

5. Monitorización y registros

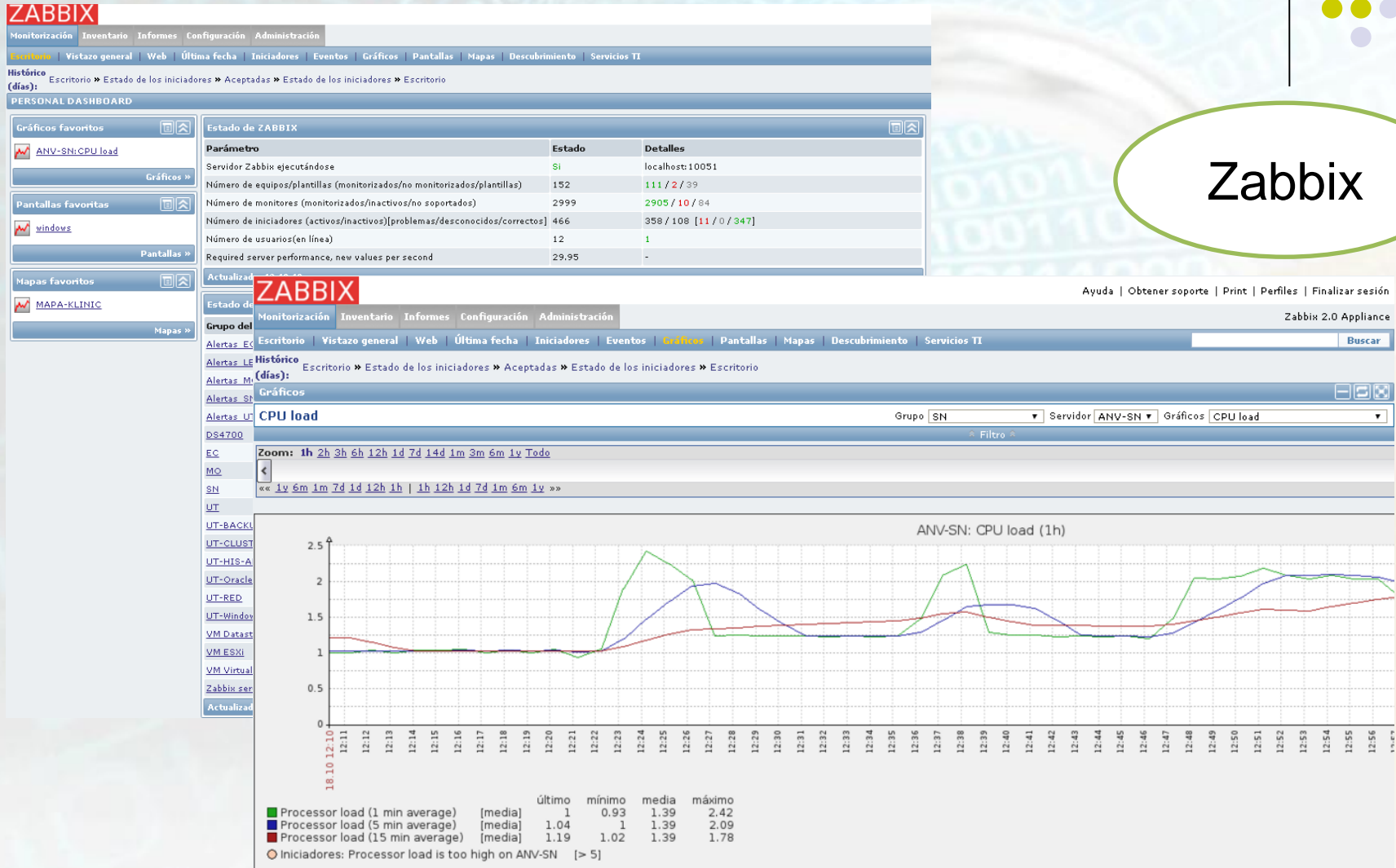


Cacti

5. Monitorización y registros



Zabbix



5. Monitorización y registros



Registros

Llamados también *logs*, registros de eventos, registros de sucesos, bitácoras...

Detalle temporal de los principales sucesos ocurridos en el sistema.

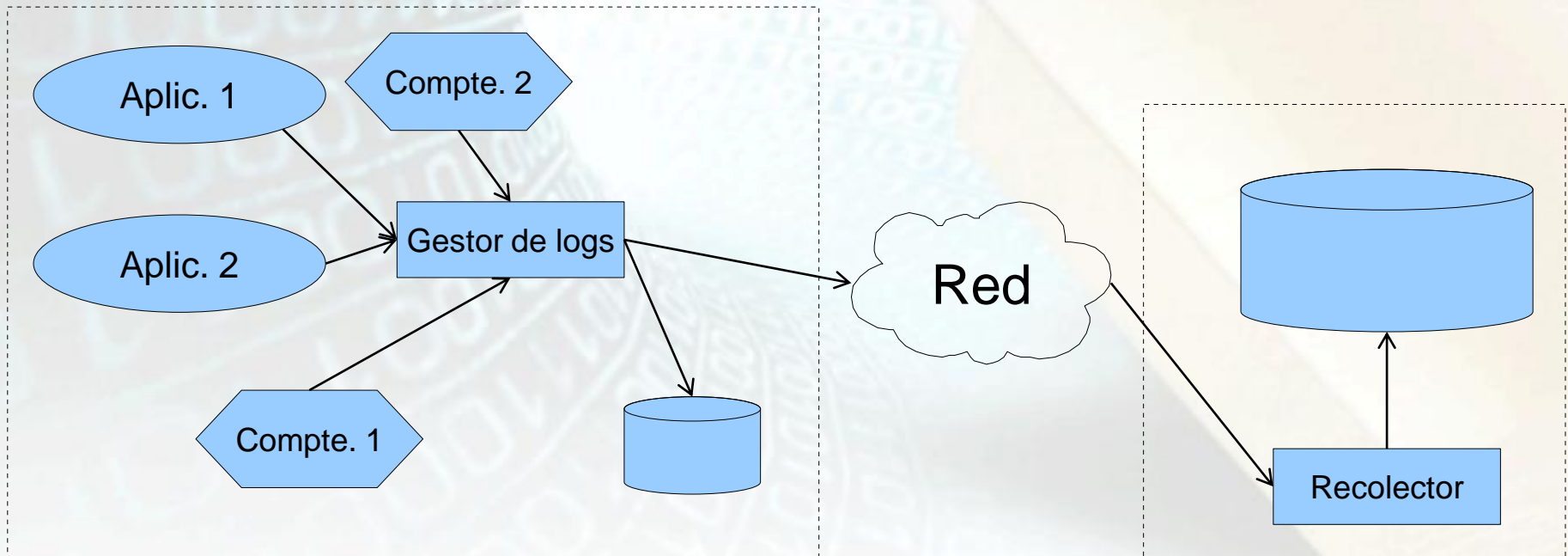
Permiten

- descubrir comportamientos anómalos
- detectar causas de errores
- obtener estadísticas
- ¡cumplir la ley!

5. Monitorización y registros



Las aplicaciones y los componentes del S.O. generan registros. Éstos se centralizan en un gestor de registros que los almacena en disco y/o los envía a un recolector centralizado



5. Monitorización y registros



En Windows: registro de sucesos

En Unix/Linux: syslog / syslog-ng

Tendremos una práctica sobre ellos

Se debe prestar atención a la sincronización de hora entre los equipos

Sobre todo al correlar registros de diferentes servidores

5. Monitorización y registros



Aspectos adicionales de la gestión de registros:

- normalización: distintos sistemas y aplicaciones generan diferentes formatos de mensaje.
- almacenamiento: suelen almacenarse históricos comprimidos, con el límite temporal que convenga: una semana, un mes, un año... y van borrando los anteriores (rotación de logs).
- correlación: una ingente cantidad de registros no sirve de nada si no se pueden buscar patrones en ellos para detectar anomalías.



1. Introducción
2. Configuración segura
3. Protección frente a código malicioso
4. Gestión de actualizaciones y parches
5. Monitorización y registros
6. **Sistemas de detección de intrusiones en hosts (HIDs)**

6. Sistemas de detección de intrusiones en hosts (HIDs)



Un *Host Intrusion Detection System* (HIDS) es un tipo de IDS [intro-ids] [ids-s21] especializado en vigilar un servidor exclusivamente.

Veremos los NIDS, especializados en tráfico de red, en el próximo tema.

Detecta y avisa de cambios en el sistema.

6. Sistemas de detección de intrusiones en hosts (HIDs)



Monitoriza el estado del sistema (archivos, puertos, kernel...) y el comportamiento dinámico del mismo: logs, creación de procesos...

Algunos HIDSs:

Tripwire: monitorización de integridad de ficheros

Samhain: monitorización de integridad de ficheros centralizada

OSSEC: control centralizado; monitoriza logs, integridad de ficheros, puertos, procesos... Basado en reglas libremente modificables

Referencias



[w2kchk]

[https://technet.microsoft.com/en-us/library/hh831360\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/hh831360(v=ws.11).aspx)

[cis-win] [cis-linx] [cis-ora]

<https://benchmarks.cisecurity.org/en-us/?route=downloads.multiform>

Ver PDFs en referencias.

Referencias



[auscert-chk] <http://www.auscert.org.au/5816>

[dpl] <http://cirt.net/passwords>

[dpl2] <http://default-password.info/>

[escalada]

http://en.wikipedia.org/wiki/Privilege_escalation

Referencias



[winpp] <https://technet.microsoft.com/en-us/library/hh994572.aspx>

[Inxpp] <http://xmodulo.com/set-password-policy-linux.html>

[wp-ssh] <http://en.wikipedia.org/wiki/Ssh>

[wp-sftp]
http://en.wikipedia.org/wiki/SSH_File_Transfer_Protocol

[wp-rdp]
http://en.wikipedia.org/wiki/Remote_Desktop_Protocol

Referencias



[tcpip-sec]

http://www.linuxsecurity.com/resource_files/documentation/tcpip-security.html

[wp-syn]

http://en.wikipedia.org/wiki/SYN_flood

[ibm-sr]

http://www.iss.net/security_center/advice/Underground/Hacking/Methods/Technical/Source_Routing/default.htm

[hardening-tcp] <http://www.securityfocus.com/infocus/1729>

[wp-ntp] http://en.wikipedia.org/wiki/Network_Time_Protocol

[xccdf] <http://nvd.nist.gov/xccdf.cfm>

Referencias



[bastille] <http://www.bastille-unix.org/>

[lynis] <https://cisofy.com/lynis/>

[puppet]

<http://reductivelabs.com/trac/puppet/wiki/AboutPuppet>

[cfengine] <http://www.cfengine.org/>

[ms-sectpl] <http://support.microsoft.com/kb/816585>

[ws-sectpl]

<http://www.windowsecurity.com/articles/Hardening-Servers-Security-Templates.html>

[gp] http://en.wikipedia.org/wiki/Group_Policy

[ms-gp] <http://technet.microsoft.com/en-us/windowsserver/grouppolicy/default.aspx>

[nessus] <http://www.nessus.org>

Referencias



[mw1] <http://www.infospyware.com/articulos/que-son-los-malwares>

[cronologia]
http://replay.waybackmachine.org/20090123201053/http://alerta-antivirus.es/virus/ver_pag.html?tema=V&articulo=4&pagina=1

[cronologia2] <http://www.eset-la.com/threat-center/1600-cronologia-virus-informaticos>

[kruegel] [kruegelChpt2--malware.pdf](#)

[bots] [NetLivingDead\(20080225\).pdf](#)

LECTURA [bots2] <http://www.eset-la.com/threat-center/1573-botnets-redes-organizadas-crimen>

Referencias



[morris] <http://snowplow.org/tom/worm/worm.html>

[morris20]

<http://www.itworld.com/security/57044/morris-worm-turns-20-look-what-its-done>

[mwpdf] <http://blogs.eset->

[la.com/laboratorio/2007/10/30/malware-archivos-pdf/](http://blogs.eset-la.com/laboratorio/2007/10/30/malware-archivos-pdf/)

[utm-wp]

http://en.wikipedia.org/wiki/Unified_Threat_Management
t

Referencias



[schneier] <http://www.schneier.com/crypto-gram-0009.html#1>

[Isva] Large-Scale Vulnerability Analysis,
<http://www.techzoom.net/publications/papers.en#Isad06>

[days]
http://blogs.csoononline.com/basic_guide_to_days_of_risk

[script-kiddie] http://en.wikipedia.org/wiki/Script_kiddie

[fulldisclosure]
http://en.wikipedia.org/wiki/Full_disclosure

Referencias



[snmp-wpe]

http://es.wikipedia.org/wiki/Simple_Network_Management_Protocol

[intro-ids]

<http://www.cs.ucsb.edu/~kemm/courses/cs177/IDSintro.pdf>

[ids-s21] <http://blog.s21sec.com/2008/11/ids-sistemas-de-deteccion-de-intrusiones.html>