

# **Seguridad de los Sistemas Informáticos**

## **Tema 5: Seguridad de los sistemas operativos**

# Introducción

- Un sistema informático puede considerarse compuesto por un conjunto de “capas”:
  1. La instalación donde se encuentra el sistema.
  2. El hardware del mismo y de comunicaciones con el resto del mundo.
  3. El sistema operativo, como software que soporta todas las aplicaciones que ofrece el sistema.
  4. Los servicios instalados, que ofrecen las funcionalidades a los usuarios (servidor web, servidor de ficheros, servidor de aplicaciones, etc.)
  5. Las aplicaciones del usuario.

# Introducción

- Los niveles 1 y 2 se corresponden con la seguridad física estudiadas en un tema anterior.
- El nivel 3 se corresponde con la seguridad del sistema operativo.
  - Es lo que estudiaremos en este tema.

# Introducción

Desde otro punto de vista, la seguridad lógica del sistema se puede estructurar en tres puntos:

1. Seguridad del sistema. Trata de los mecanismos a utilizar para asegurar el sistema en sí y todo lo que contiene.
2. Seguridad perimetral. Intenta aislar el sistema de los ataques externos, pero posibilitando los accesos que estén autorizados.
3. Seguridad en las comunicaciones. Pretende garantizar que las comunicaciones con otros sistemas cumplen los requisitos de integridad, confidencialidad y disponibilidad.

Con este esquema, este tema trata del punto 1.

# Aspectos a considerar por el SO

- En lo que respecta a la seguridad, el sistema operativo debe proveer mecanismos para:
  1. Evitar vulnerabilidades en su funcionamiento.
  2. Realizar una autenticación efectiva de los usuarios que acceden al sistema.
  3. Controlar de manera efectiva el uso de los recursos.

# Actualización del sistema

- Todo sistema operativo recién instalado debe actualizarse inmediatamente:
  - Desde la fecha de distribución del sistema, **seguro** que se han descubierto vulnerabilidades en el sistema o en las aplicaciones que lo acompañan.
  - Es preciso, pues, descargar e instalar las actualizaciones de seguridad disponibles.
- Todos los sistemas operativos actualmente disponen de herramientas que facilitan la tarea:
  - Windows Update (o Windows Server Update Services –WSUS para instalaciones con muchos ordenadores).
  - apt-get, yum, rpm, ..., en Linux (según distribución).
  - Actualizaciones en el Mac App Store.

# Actualización del sistema

## Elija la forma en que Windows puede instalar las actualizaciones

Cuando el equipo está conectado, Windows puede comprobar automáticamente las actualizaciones e instalarlas usando esta configuración. Cuando estén disponibles nuevas actualizaciones, puede instalarlas antes de apagar el equipo.

[¿Cómo me puede ayudar la actualización automática?](#)

### Actualizaciones importantes

Descargar actualizaciones, pero permitirme elegir si deseo instalarlas

Instalar nuevas actualizaciones: Todos los días a las 3:00

### Actualizaciones recomendadas

☒ Ofrecerme actualizaciones recomendadas de la misma forma que recibo las actualizaciones importantes

### Quién puede instalar actualizaciones

☒ Permitir que todos los usuarios instalen actualizaciones en este equipo

### Microsoft Update

☒ Ofrecer actualizaciones de productos de Microsoft y comprobar si hay nuevo software opcional de Microsoft al actualizar Windows

### Notificaciones de software

☒ Mostrar notificaciones detalladas cuando haya disponible nuevo software de Microsoft

Nota: es posible que Windows Update se actualice automáticamente antes de que busque otras actualizaciones. Lea nuestra [declaración de privacidad en línea](#).

# Actualización del sistema

```
root@kali:~# apt-get update
Get:1 http://archive-4.kali.org/kali kali-rolling InRelease [30.5 kB]
Get:2 http://archive-4.kali.org/kali kali-rolling/main amd64 Packages [14.9 MB]
Get:3 http://archive-4.kali.org/kali kali-rolling/non-free amd64 Packages [163 kB]
Get:4 http://archive-4.kali.org/kali kali-rolling/contrib amd64 Packages [107 kB]
Fetched 15.2 MB in 14s (1,034 kB/s)
Reading package lists... Done
root@kali:~# apt-get upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
gdebi-core iproute libcrypto++6 libjavascriptcoregtk-1.0-0 libladr4
libmm-gtk-common libqt4-opengl libqtwebkit4 libvp3 libwebkitgtk-1.0-0
prover9 python-cluster python-darts.lib.utils.lru python-esmre python-git
python-gitdb python-guess-language python-halberd python-ipaddr
python-ndg-httpsclient python-nltk python-pdfminer python-phply python-ply
python-psutil python-pybloomfiltermmap python-pyclamd python-pycryptopp
python-pygithub python-ruamel.orderdict python-smmmap python-tbllib
python-vulndb python-webkit python-xdot w3af w3af-console
Use 'apt autoremove' to remove them.
The following packages have been kept back:
aapt afflib-tools axel bluez cadaver clamav clamav-base clamav-daemon
clamav-freshclam clamscan clang crda curl dirmngr dradis dsiff erlang-asn1
erlang-base erlang-crypto erlang-eunit erlang-inets erlang-mnesia
erlang-os-mon erlang-public-key erlang-runtime-tools erlang-snmp erlang-ssl
erlang-syntax-tools erlang-tools erlang-xmerl evolution-data-server
evolution-data-server-common ewf-tools folks-common ftp gdb
gir1.2-mutter-3.0 gir1.2-networkmanager-1.0 gir1.2-totem-1.0 gjs
gnome-contacts gnome-core gnome-online-accounts gnome-packagekit
gnome-session gnome-session-bin gnome-session-common gnome-shell
gnome-shell-common gnome-shell-extension-workspace-dock
gnome-shell-extensions gnome-sushi gnupg gnupg-agent gnupg2 gnuplot-data
gnuplot-qt graphviz gstreamer1.0-libav gstreamer1.0-plugins-bad
guile-2.0-libs gvfs gvfs-backends gvfs-bin gvfs-common gvfs-daemons
```



# Actualización del sistema

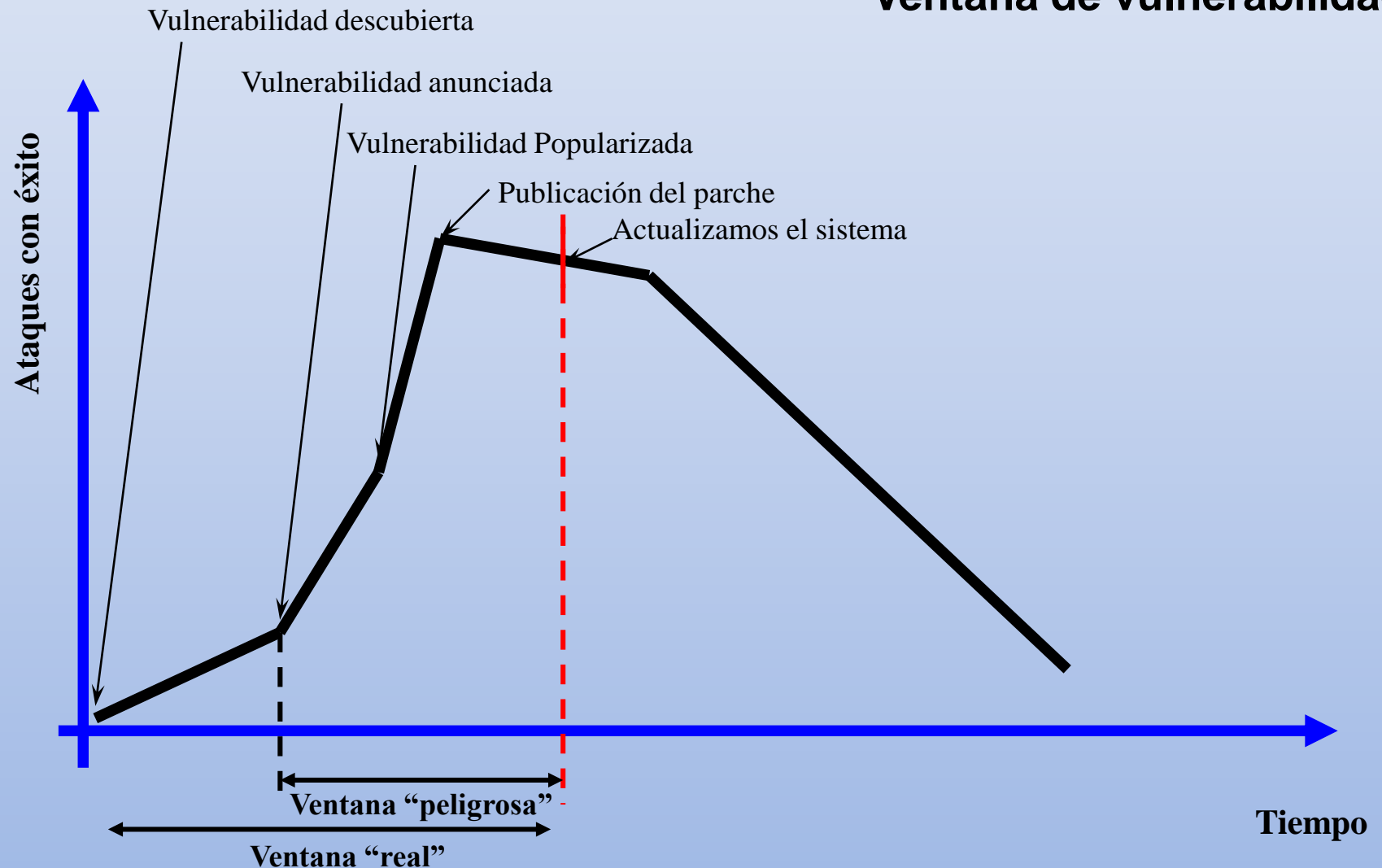
- Después de la actualización inicial, ha de establecerse un calendario de actualización para mantener el sistema a salvo de *exploits*.
- Hay que considerar que NO se puede estar al tanto de TODAS las vulnerabilidades:
  - Según Wietse Venema: *“Hay aproximadamente un bug de seguridad por cada 1000 líneas de código fuente”*
  - Si el S.O. tiene 100 millones de líneas de código (Windows Server 2003 tiene unas 50 millones, Un Linux completo >300 , Mac OS X >86 millones), hay cientos de miles de bugs de seguridad potenciales en el S.O.
  - El CERT (*Computer Emergency Response Team*) descubre una media de 5000 bugs/año -> 20 años en descubrir

# Actualización del sistema

- Existen bases de datos públicas sobre vulnerabilidades conocidas:
  - [www.cvedetails.com](http://www.cvedetails.com)
  - [cve.mitre.org](http://cve.mitre.org)
  - [nvd.nist.gov](http://nvd.nist.gov)
  - [www.secunia.com](http://www.secunia.com)
  - [www.sans.org](http://www.sans.org)
  - [www.osvdb.org/](http://www.osvdb.org/)
  - [www.kb.cert.org/vuls/](http://www.kb.cert.org/vuls/)
  - ...
- El objetivo de estas bases de datos **NO** es dar pistas a posibles atacantes sobre lo que pueden hacer ante un sistema determinado, sino dar a conocer a los administradores de sistemas los problemas que puede tener su sistema y cómo corregirlos.
- Por lo tanto, lo que hay que lograr es que, al menos, las soluciones para vulnerabilidades conocidas estén instaladas.
- Aún así, podemos sufrir “ataques de día 0”.

# Actualización del sistema

## Ventana de vulnerabilidad



# Configuración del sistema

Además de actualizar el sistema, hay que prestar especial cuidado con la **configuración** inicial del mismo.

1. En concreto, es importante instalar únicamente aquellos servicios que se van a utilizar:
  - Los servicios no utilizados son un peligro adicional:
    - No ofrecen nada a los usuarios (no se utilizan).
    - Proveen nuevos frentes de ataque.
    - Nadie suele estar pendiente de ellos, con lo que cualquier ataque puede pasar mucho tiempo inadvertido.
  - Además de que consumen recursos innecesariamente (disco, memoria, CPU...).

# Configuración del sistema

2. Además, hay que configurar los límites (de disco, de memoria, de procesos, etc.) que puede utilizar cada usuario para evitar el acaparamiento de recursos por parte de algún usuario (de forma intencionada o no). Bombas fork, mala programación...
3. Hay que asignar privilegios a usuarios con mucho cuidado (*mínimo privilegio*):
  - No permitir acceder a programas *delicados* (programas de configuración del sistema, de gestión de usuarios, etc.).
  - No permitir acceder a ficheros de configuración (ficheros de contraseñas, configuración de red, configuración firewall, etc.)
  - No dejar instalar aplicaciones.
  - Restringir el uso de recursos (como la red).
  - Ejecutar los servicios con los mínimos permisos posibles.

# Configuración del sistema

4. Bloquear o eliminar las cuentas por defecto del sistema que no se utilicen
  - Las que se utilicen tienen que tener contraseñas que no sean las que vienen “por defecto”.
5. No habilitar comunicaciones no encriptadas (o con debilidades conocidas ftp, rsh....).
6. Restringir las máquinas desde las que se pueden realizar operaciones *delicadas* (acceso de administración, *backups*, etc.)
  - Ciertas operaciones sólo deberían hacerse desde la consola física.
7. Tener en cuenta las precauciones específicas de sistemas concretos.

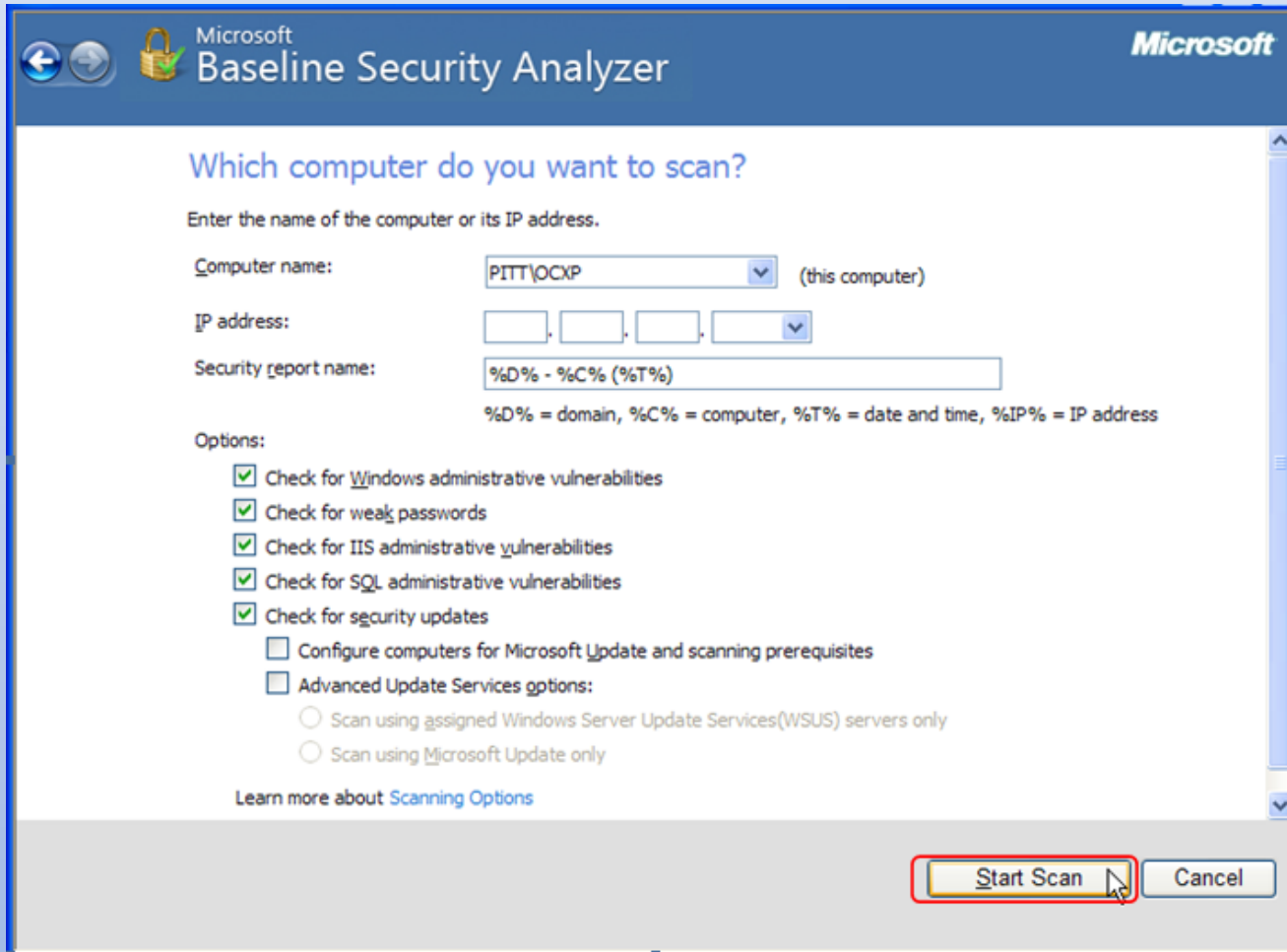
# Configuración del sistema

## Herramientas de análisis

- Dados los problemas de seguridad que puede haber por una configuración inadecuada del sistema, los fabricantes de S.S.OO. y otras personas y compañías han desarrollado herramientas para verificar dicha configuración.
- Microsoft tiene la herramienta MBSA (*Microsoft Baseline Security Analyzer*). Y otras como SCCM, SCM, etc.
- Para sistemas Unix se dispone de herramientas como Bastille, Lynis o tiger.

# Configuración del sistema

## Herramientas de análisis



Microsoft Baseline Security Analyzer

Which computer do you want to scan?

Enter the name of the computer or its IP address.

Computer name: PITT\OCXP (this computer)

IP address: . . .

Security report name: %D% - %C% (%T%)

%D% = domain, %C% = computer, %T% = date and time, %IP% = IP address

Options:

- ☒ Check for Windows administrative vulnerabilities
- ☒ Check for weak passwords
- ☒ Check for IIS administrative vulnerabilities
- ☒ Check for SQL administrative vulnerabilities
- ☒ Check for security updates
- ☐ Configure computers for Microsoft Update and scanning prerequisites
- ☐ Advanced Update Services options:
  - ☐ Scan using assigned Windows Server Update Services (WSUS) servers only
  - ☐ Scan using Microsoft Update only

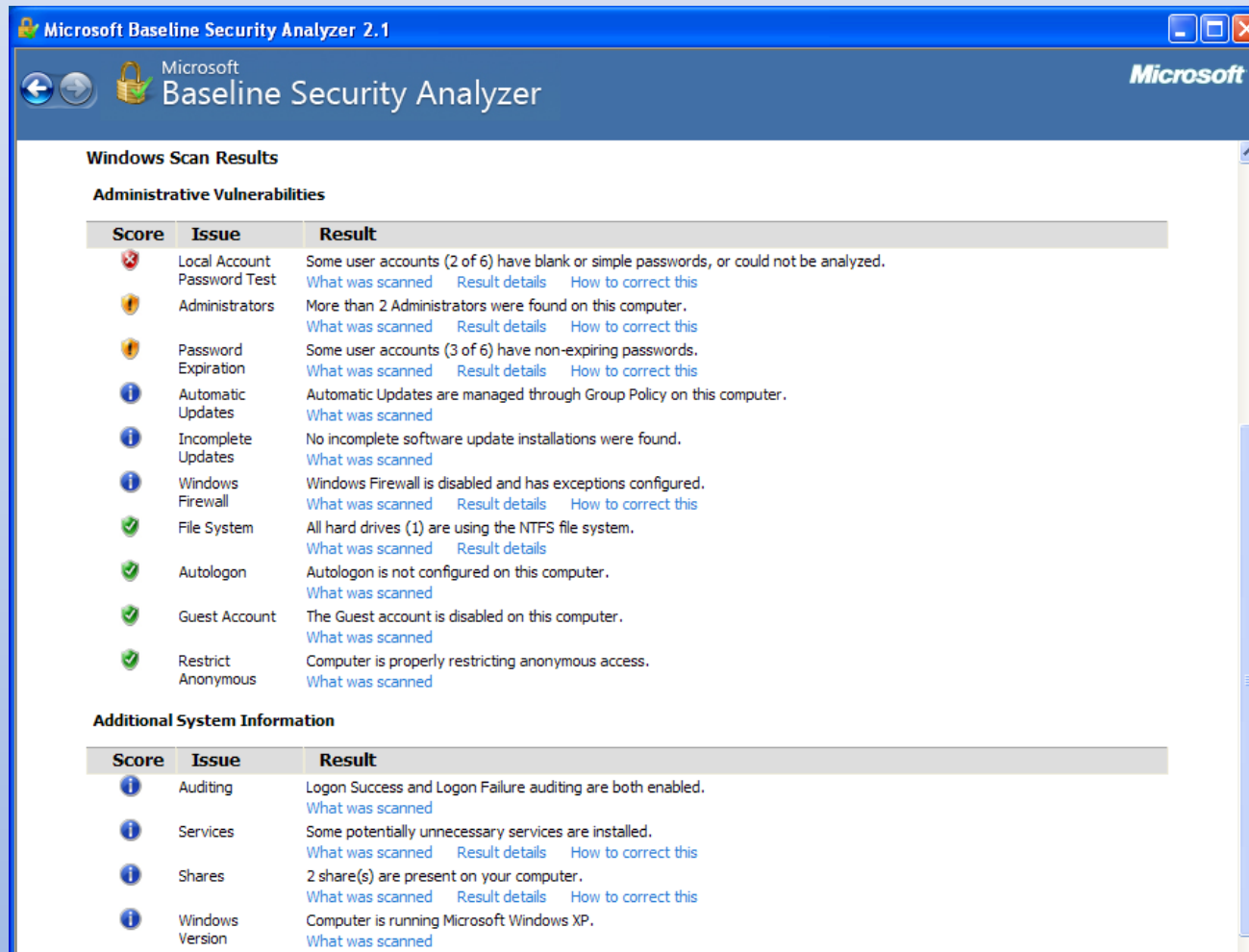
Learn more about [Scanning Options](#)

Start Scan Cancel



# Configuración del sistema

## Herramientas de análisis



The screenshot displays the Microsoft Baseline Security Analyzer 2.1 application window. The title bar reads "Microsoft Baseline Security Analyzer 2.1". The main content area is titled "Windows Scan Results" and contains a section for "Administrative Vulnerabilities". This section lists various security issues with their scores, descriptions, and links for further action. Below this, there is a section for "Additional System Information" which provides details about system configuration and status.

Score	Issue	Result
✗	Local Account Password Test	Some user accounts (2 of 6) have blank or simple passwords, or could not be analyzed. <a href="#">What was scanned</a> <a href="#">Result details</a> <a href="#">How to correct this</a>
⚠	Administrators	More than 2 Administrators were found on this computer. <a href="#">What was scanned</a> <a href="#">Result details</a> <a href="#">How to correct this</a>
⚠	Password Expiration	Some user accounts (3 of 6) have non-expiring passwords. <a href="#">What was scanned</a> <a href="#">Result details</a> <a href="#">How to correct this</a>
i	Automatic Updates	Automatic Updates are managed through Group Policy on this computer. <a href="#">What was scanned</a>
i	Incomplete Updates	No incomplete software update installations were found. <a href="#">What was scanned</a>
i	Windows Firewall	Windows Firewall is disabled and has exceptions configured. <a href="#">What was scanned</a> <a href="#">Result details</a> <a href="#">How to correct this</a>
✓	File System	All hard drives (1) are using the NTFS file system. <a href="#">What was scanned</a> <a href="#">Result details</a>
✓	Autologon	Autologon is not configured on this computer. <a href="#">What was scanned</a>
✓	Guest Account	The Guest account is disabled on this computer. <a href="#">What was scanned</a>
✓	Restrict Anonymous	Computer is properly restricting anonymous access. <a href="#">What was scanned</a>

Score	Issue	Result
i	Auditing	Logon Success and Logon Failure auditing are both enabled. <a href="#">What was scanned</a>
i	Services	Some potentially unnecessary services are installed. <a href="#">What was scanned</a> <a href="#">Result details</a> <a href="#">How to correct this</a>
i	Shares	2 share(s) are present on your computer. <a href="#">What was scanned</a> <a href="#">Result details</a> <a href="#">How to correct this</a>
i	Windows Version	Computer is running Microsoft Windows XP. <a href="#">What was scanned</a>

# Configuración del sistema

## Herramientas de análisis

### Lynis

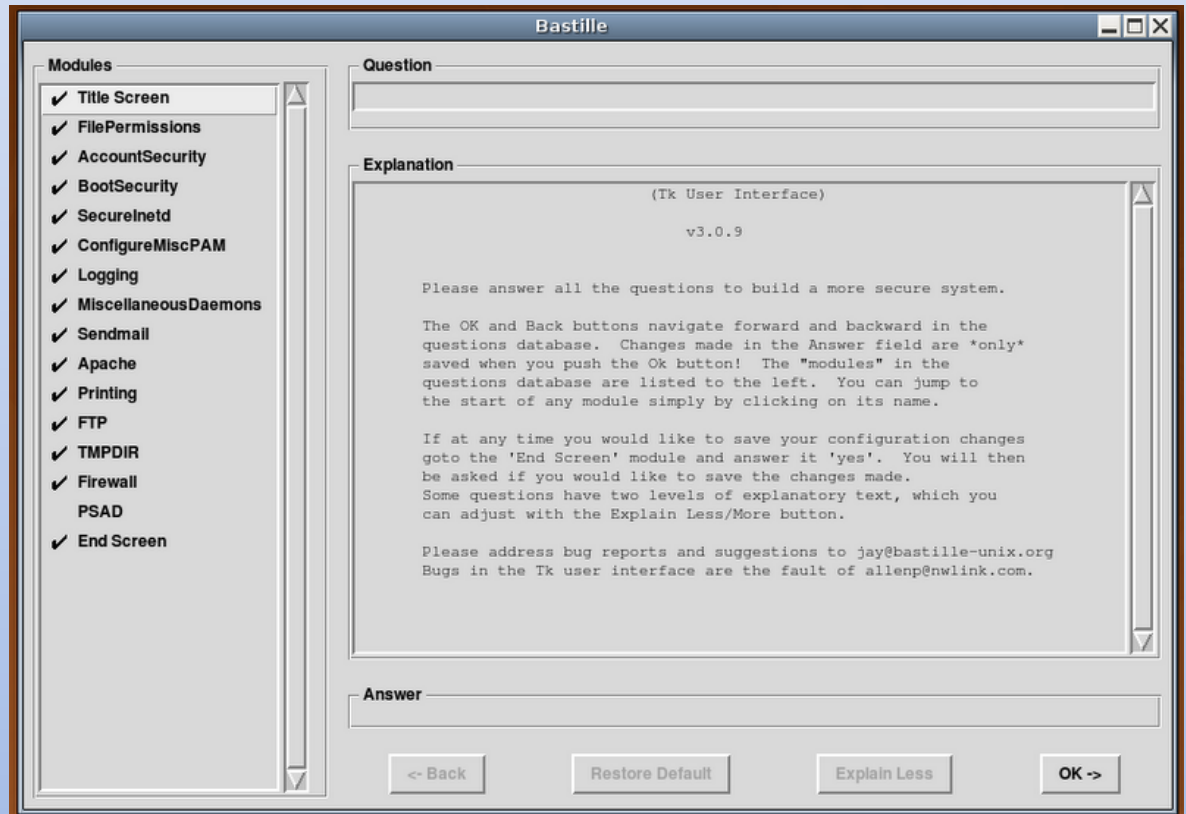
```
[+] Kernel
- Checking active kernel modules... [ OK ]

[+] Users, Groups and Authentication
- Search administrator accounts... [ DONE ]
  Result: Found one or more administrator accounts
- Checking UIDs... [ WARNING ]
- Checking chkgpt tool... [ FOUND ]
- Consistency check /etc/group file... [ OK ]
- Checking login shells... [ WARNING ]

[+] Home directories
- Checking shell history files... [ OK ]
- Checking PATH variable vulnerabilities... [ OK ]
- Checkin TTys... [ WARNING ]

[+] File and Directory permissions
- Checking skel file permissions (/usr/share/skel)... [ OK ]
- Checking skel file permissions (/etc/skel)... [ EMPTY ]
- Checking /tmp sticky bit... [ OK ]

[+] Ports and packages
- Checking portaudit to obtain vulnerabilities... [ WARNING ]
- Searching package managers...
- Searching pkg_info... [ FOUND ]
  - Querying pkg_info for installed packages... [ DONE ]
  - Querying pkg_info for double installed packages... [ OK ]
- Searching RPM package manager... [ NOT FOUND ]
- Searching dpkg package manager... [ NOT FOUND ]
```



# Autenticación de usuarios

- Debe asegurarse:
  - Que los usuarios **NO** autorizados **NO** puedan acceder al sistema.
  - Que los usuarios **SÍ** autorizados **SÍ** puedan acceder al sistema.
- La autenticación de usuarios puede estar basada en:
  - Algo que **sabe** el usuario: *contraseña, pin, ...*
  - Algo que **tiene** el usuario: *tarjeta magnética, llave, ...*
  - Quién **es** el usuario: biométricos (*huella dactilar, geometría de la mano, retina, iris, cara, firma, voz, ...*)
  - Varios de los anteriores.

# Autenticación de usuarios

## Acceso por contraseña

- Es el mecanismo más utilizado:
  - No requiere hardware especial.
  - La tasa de falso rechazo (FRR – *False Rejection Rate*) es nula.
  - La tasa de falsa aceptación (FAR – *False Acceptance Rate*) también es nula.

# Autenticación de usuarios

## Acceso por contraseña

- Es el más fácilmente atacable:
  - Cualquiera puede intentar averiguar contraseñas.
  - Las contraseñas deben almacenarse en el sistema, luego alguien puede intentar conseguirlas.
    - Para solventar este problema, se almacenan encriptadas (preferiblemente con cifrado no reversible→hash).
  - Independientemente de si se consigue el fichero de contraseñas encriptado o no, se puede intentar averiguarlas:
    - Por ingeniería social:
      - Obteniéndolas directamente del usuario.
      - Usando información relacionada con el usuario.
    - Por ataque de “fuerza bruta”.

# Autenticación de usuarios

## Acceso por contraseña: Precauciones a tomar

- Algunas precauciones que pueden tomarse:
  - Asegurarse que todos los usuarios tienen contraseñas seguras.
  - No dejar ninguna cuenta sin contraseña.
  - No almacenar contraseñas en ficheros accesibles por usuarios normales.
  - No almacenar contraseñas sin cifrar o con cifrado reversible.
  - No dejar sesiones abiertas desatendidas.
  - Bloquear cuentas con exceso de intentos infructuosos de acceso.
  - Vigilar los ficheros de *log* para localizar accesos sospechosos.
  - Inhabilitar cuentas no utilizadas.
  - Cambiar el nombre de cuentas conocidas (administrador, invitado, ...)
- Algunas cuestiones son de educación del usuario y/o del administrador; otras pueden vigilarse por medios técnicos.

# Autenticación de usuarios

## Acceso por contraseña: Precauciones a tomar

- Cuando el usuario cambia una contraseña, el sistema impone algunas restricciones (mayor de 6 caracteres, mezcla de letras y/o dígitos y/o otros, no tener relación con información del usuario, ...)
- Sin embargo, no suele ser suficiente: hay que educar al usuario para que elija una contraseña segura:
  - Cuanto más larga, más segura.
  - Que no tengan significado (diccionario).
  - Que no tengan relación con el usuario (nombre, mascota, matrícula del coche, teléfono, ...)
  - Que sea fácil de recordar (¡¡Ojo con los *Post-it* en pantallas!!)
- Periódicamente, el administrador podría utilizar algún programa “revienta contraseñas”, para estudiar la seguridad de las contraseñas creadas.
  - *John the Ripper password cracker.*
  - *Ophcrack.*

# Autenticación de usuarios

## Acceso por elementos que posea el usuario

- Los usuarios se identifican con algo que poseen: una tarjeta magnética, una tarjeta inteligente, DNle, un chip, etc.
- Es fácilmente utilizable:
  - Requiere hardware especial, pero no suele ser muy costoso.
  - La tasa de falso rechazo (FRR – *False Rejection Rate*) es nula.
  - La tasa de falsa aceptación (FAR – *False Acceptance Rate*) también es nula.
  - Casi todos los sistemas operativos proveen mecanismos para incorporarlos como elemento de control de acceso.

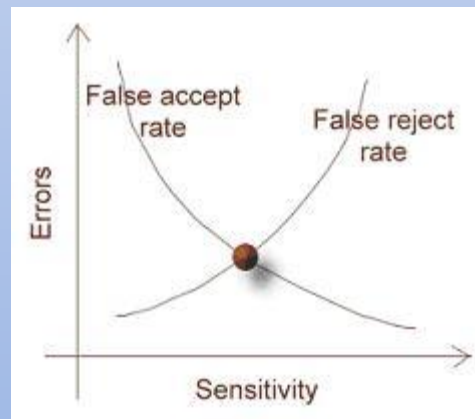
Una empresa belga implanta un «chip» de identificación bajo la piel sus empleados



# Autenticación de usuarios

## Acceso por métodos biométricos

- Los usuarios se identifican con alguna característica propia: huella dactilar, iris, retina, voz, ...
- No suele utilizarse demasiado:
  - Requiere hardware especial, relativamente costoso.
  - Puede ser engorroso para los usuarios.
  - La tasa de falso rechazo (FRR – *False Rejection Rate*) puede llegar a ser inaceptable.
  - La tasa de falsa aceptación (FAR – *False Acceptance Rate*) puede ser peligrosamente alta.



# Autenticación de usuarios

## Acceso por biométricos

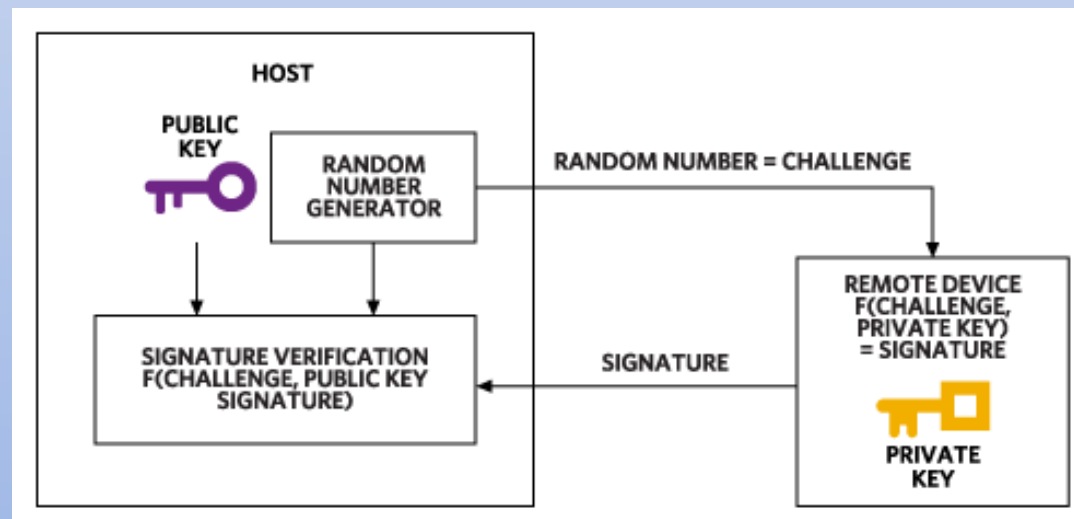
- Los fabricantes suelen ajustar el umbral de aceptación prefiriendo rechazar usuarios legales que aceptar usuarios no autorizados.
- Casi todos los sistemas operativos proveen mecanismos para incorporarlos como elemento de control de acceso.

	Ojo (Iris)	Ojo (Retina)	Huellas dactilares	Vascular dedo	Vascular mano	Geometría de la mano	Escritura y firma	Voz	Cara 2D	Cara 3D
<b>Fiabilidad</b>	Muy alta	Muy Alta	Muy Alta	Muy Alta	Muy Alta	Alta	Media	Alta	Media	Alta
<b>Facilidad de uso</b>	Media	Baja	Alta	Muy Alta	Muy Alta	Alta	Alta	Alta	Alta	Alta
<b>Prevención de ataques</b>	Muy alta	Muy Alta	Alta (con dudas)	Muy Alta	Muy Alta	Alta	Media	Media	Media	Alta
<b>Aceptación</b>	Media	Baja	Alta	Alta	Alta	Alta	Muy Alta	Alta	Muy alta	Muy alta
<b>Estabilidad</b>	Alta	Alta	Alta	Alta	Alta	Media	Baja	Media	Media	Alta

# Autenticación de usuarios

## Otros mecanismos

- Utilizando un par de claves privada – pública o certificados de usuario:
  - En este caso sólo se puede acceder desde las máquinas que tengan instalada la parte privada de la clave del usuario.
  - La parte pública se queda en el host que tiene una lista de las claves autorizadas (requiere que previamente haya sido añadida).



# Autenticación de usuarios

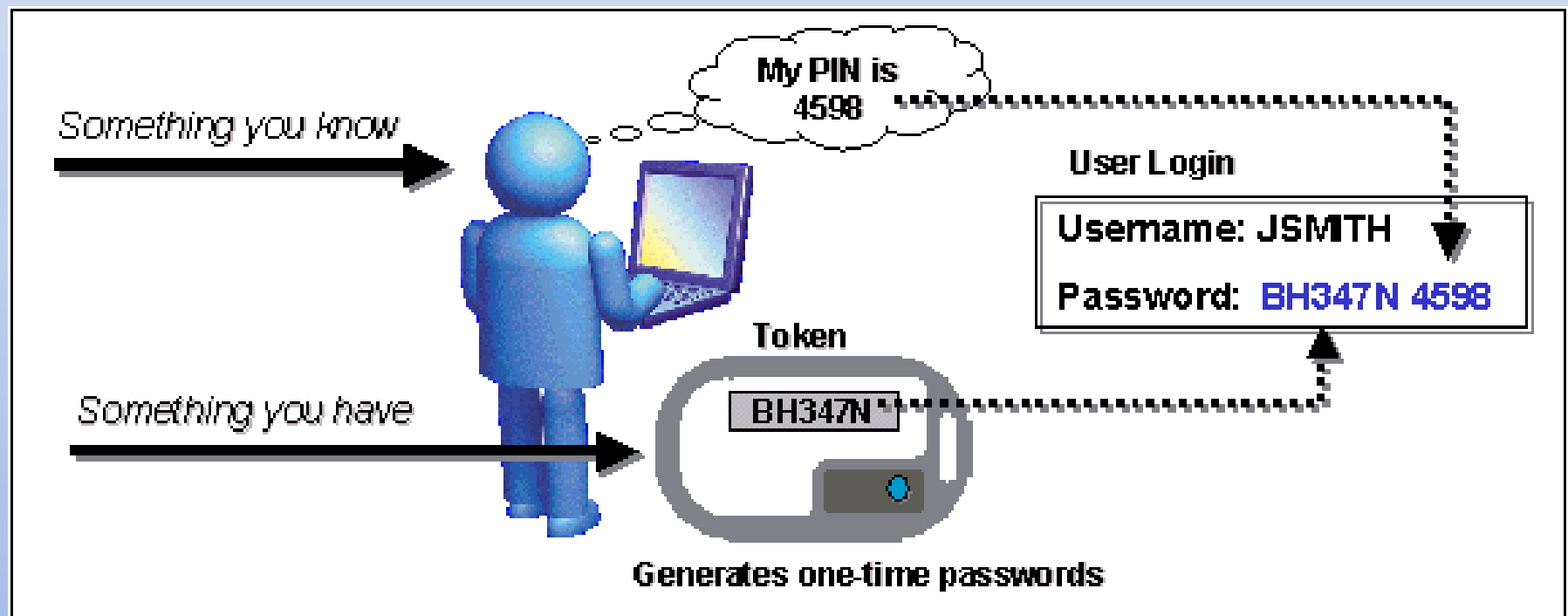
## Otros mecanismos

- Utilizando “claves de un solo uso” (*one time passwords*).
  - Algoritmo HMAC-Based One-time Password (HOTP)
  - Algoritmo Time-based One-time Password (TOTP)
  - El proveedor de servicio genera una clave secreta de 80 bits para cada usuario la cual se le suministra al cliente previamente de una forma segura/secreta.
  - El cliente crea un mensaje HMAC-SHA1 usando esta clave secreta. Puede basarse en
    - El tiempo pasado desde “Tiempo UNIX”.
    - Un contador que se incrementa con cada nuevo código generado.
  - Una porción de la HMAC se extrae y es convertida a un código de 6 dígitos que es lo que el usuario debe introducir junto a su usuario y contraseña para acceder al sistema.

# Autenticación de usuarios

## Otros mecanismos

- *Ej: Google Authenticator...*



# Control de acceso a recursos

En general, debe gestionarse una **matriz de acceso** como principal modelo de protección. **Filas: clientes; columnas: recursos**

$M[i,j]$  = Permisos del cliente  $i$  sobre el recurso  $j$

Dos implementaciones de la matriz

## Listas de control de acceso (por columnas)

- Cada recurso guarda la lista de clientes con sus permisos (vector columna de la matriz) → Un local tiene la lista de “invitados” a los que se permitirá acceder.

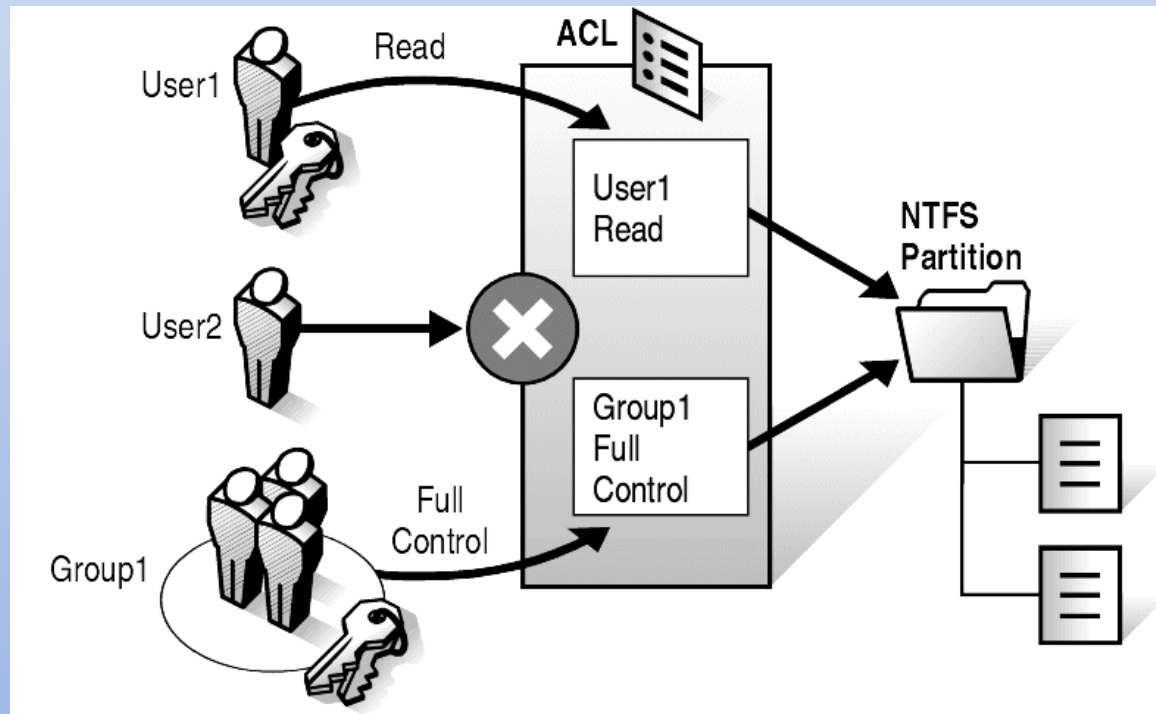
## Capacidades (por filas)

- Cada cliente guarda la lista de capacidades (recurso+permisos) que tiene disponibles. → Un cliente acude a un local con una entrada que le da derecho a acceder al mismo.

# Control de acceso a recursos

## Mecanismo de control de acceso con Listas de Control de Acceso

Cuando un cliente realiza una petición sobre un recurso el S.O (mecanismo de protección) comprueba si el cliente está en la LCA del recurso.



# Control de acceso a recursos

## Mecanismo de control de acceso con Listas de Control de Acceso

Mecanismo usado por Unix y Windows para el control de acceso a ficheros y a otros recursos.

## Inconvenientes de las LCA

Falta de escalabilidad

Muchos clientes → LCA muy grandes

Muchos recursos → muchas LCA

Solución:

Agrupar los clientes → disminuye el nº de entradas de la LCA

Agrupar recursos → Disminuye el nº de LCA



# Control de acceso a recursos

## Dominios de protección

- Cada sistema operativo determina a quién garantiza o niega unos determinados tipos de acceso a los recursos.
- En Unix se distinguen tres dominios: *propietario*, *grupo* y *resto de usuarios*.
- En Unix, con el paquete ACL instalado, se pueden incluir  $n$  dominios: usuarios independientes en cualquier número, grupos en cualquier número y “otros”.
- En Windows se pueden incluir  $n$  dominios: usuarios independientes en cualquier número y grupos en cualquier número.

# Control de acceso a recursos

## Tipos de acceso

- Cada sistema operativo determina entre qué tipos de accesos distingue, pudiendo permitirlos o negarlos.
- En Unix, los tipos tradicionales son tres: *lectura*, *escritura* y *ejecución*.
  - La combinación de los permisos de los ficheros y de los directorios que los contienen dan más flexibilidad (pero poca).

# Control de acceso a recursos

## Tipos de acceso

- Unix también soporta *atributos extendidos*. En este caso, los tipos de acceso que se distinguen son:
  - (s): *secure deletion*\*. Al borrarlo, se reescriben sus bloques.
  - (u): *undelete*. Al borrarlo, se podrá recuperar.
  - (c): *compress*\*. Se almacena comprimido.
  - (S): *synchronous*. Las modif. se realizan síncronamente.
  - (i): *immutable*\*. No se puede modificar, enlazar, borrar, ...
  - (a): *append only*\*. Sólo se puede modificar añadiendo.
  - (d): *no dump*. No se puede usar la utilidad *dump* con él.
  - (A): *no atime*. No se actualiza la hora de acceso.

*(Los atributos i y a sólo pueden ser establecidos por root; s y c no están soportados actualmente en Linux)*

# Control de acceso a recursos

## Tipos de acceso

### Windows

Operaciones básicas por dominio:

- Control Total
- Modificar
- Lectura y ejecución
- Mostrar contenido de carpeta
- Leer
- Escribir

### Windows

Operaciones avanzadas por dominio:

- control total,
- recorrer carpeta/ejecutar archivo
- listar carpeta/leer datos
- atributos de lectura
- atributos extendidos de lectura
- crear archivos/escribir datos
- crear carpetas/anexar datos
- atributos de escritura
- atributos extendidos de escritura
- eliminar archivos/carpetas
- eliminar
- permisos de lectura
- cambiar permisos
- tomar posesión

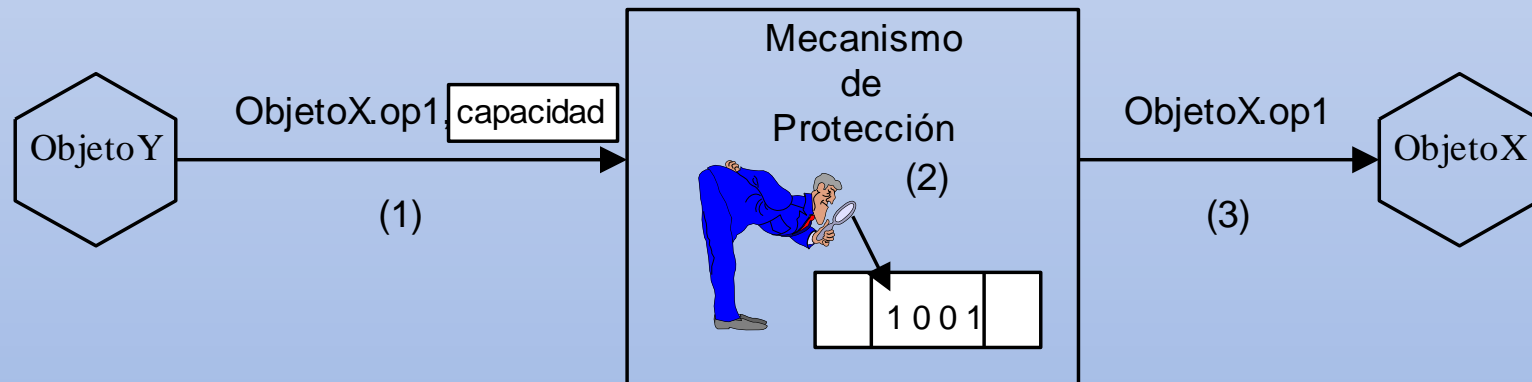
Todos los permisos pueden ser heredados o explícitos.

# Control de acceso a recursos

## Mecanismo de control de acceso con capacidades

Cuando un cliente realiza una petición sobre un recurso:

- El cliente presenta la capacidad sobre el recurso.
- El S.O. (mecanismo de protección) comprueba si en la capacidad existe permiso para la operación solicitada. Análogo a entrada a cine.
- No hay que acceder a ninguna ACL ni similar.



# Control de acceso a recursos

## Mecanismo de control de acceso con capacidades

Muchos sistemas comerciales o de investigación utilizan esta aproximación:

- POSIX (Borrador 1003.1 )
- Tahoe-LAFS
- KeyKOS, EROS, CapROS, Coyotos
- kaneton
- Cambridge CAP computer
- IBM System/38, AS/400
- Intel iAPX 432
- Plessey System 250
- Symbian
- Flex
- L4 microkernel
- Amoeba

# Cuestiones adicionales

Otros aspectos importantes que hay que considerar para reforzar la seguridad de cada máquina son:

- **Utilización de programas antivirus.**

- Muchos ataques se producen a través de distintos programas malignos, con lo que un sistema de detección, eliminación y/o bloqueo de estos es altamente recomendable.
- Se basan en el empleo de heurísticos, búsqueda de patrones, base de datos de virus conocidos (los virus tienen una “firma” que los identifica), etc.
- Nos protegen de virus conocidos y de programas con comportamiento “sospechoso”.
- Pueden monitorizar la memoria, los accesos a discos, el tráfico de red, etc. analizando si puede haber un virus (de cualquier variedad) y bloqueando su actividad y eliminando la amenaza.



# Cuestiones adicionales

- **Configuración del cortafuegos del sistema.** (nos referimos en este caso dentro del equipo).
  - El cortafuegos o *firewall* es un software que se ejecuta en la máquina y que limita qué puertos de comunicaciones se pueden utilizar y por qué aplicaciones.
  - Se configuran reglas mediante las que se indica qué tráfico entrante y/o saliente debe permitirse o limitarse.
  - Puede limitar el tráfico a ciertos programas, IPs de origen o destinos, protocolos, puertos, etc.
  - Hoy en día, teniendo nuestros equipos conectados a Internet es imprescindible contar con una protección así.
- **Utilización de TCP Wrappers.**
  - Estos sistemas permiten definir qué máquinas están autorizadas a usar servicios de la nuestra. Funcionan mediante ACL (listas de control de acceso).
  - Funcionan en la capa de aplicación.
  - Existen para sistemas Unix/Linux.

# Cuestiones adicionales

- Utilización de herramientas como:
  - **Sistemas de detección de intrusos (IDS).**
    - Analizan la actividad y buscan patrones de comportamiento conocidos por ser ataques o que puedan ser sospechosos.
  - **Comprobadores de la integridad de los sistemas de ficheros.**
    - Las modificaciones de ficheros, en especial de ejecutables del sistema, puede indicar que han sido modificados/infectados por algún tipo de virus.
  - **Analizadores de los ficheros de *log*.**
    - En los ficheros de log del sistema se registran las operaciones “importantes”, como pueden ser accesos con usuarios con privilegios, intentos de logging fallidos, intentos de acceso a recursos (servicios, ficheros, etc) fallidos.
    - Su análisis puede dar indicaciones sobre ataques sufridos, etc.

# Resumen

Para garantizar la seguridad de la máquina, debemos:

1. Instalar y configurar adecuadamente el sistema.
2. Instalar las actualizaciones de seguridad del sistema y las aplicaciones instaladas regularmente.
3. Instalar sólo las aplicaciones y servicios que se utilicen.
4. Utilizar mecanismos de autenticación efectivos.
5. Usar adecuadamente los mecanismos de control de acceso a recursos.
6. Instalar programas antivirus.
7. Configurar adecuadamente el cortafuegos del sistema.
8. Utilizar *TCP Wrappers* o similar.
9. Utilizar Sistemas de detección de intrusos (IDS).
10. Utilizar Comprobadores de la integridad de los sistemas de ficheros.
11. Utilizar Analizadores de los ficheros de *log*.
12. Usar todas aquellas otras medidas que se crean necesarias.

Y, sobre todo, regirse por el **sentido común**.

# Seguridad en la red local

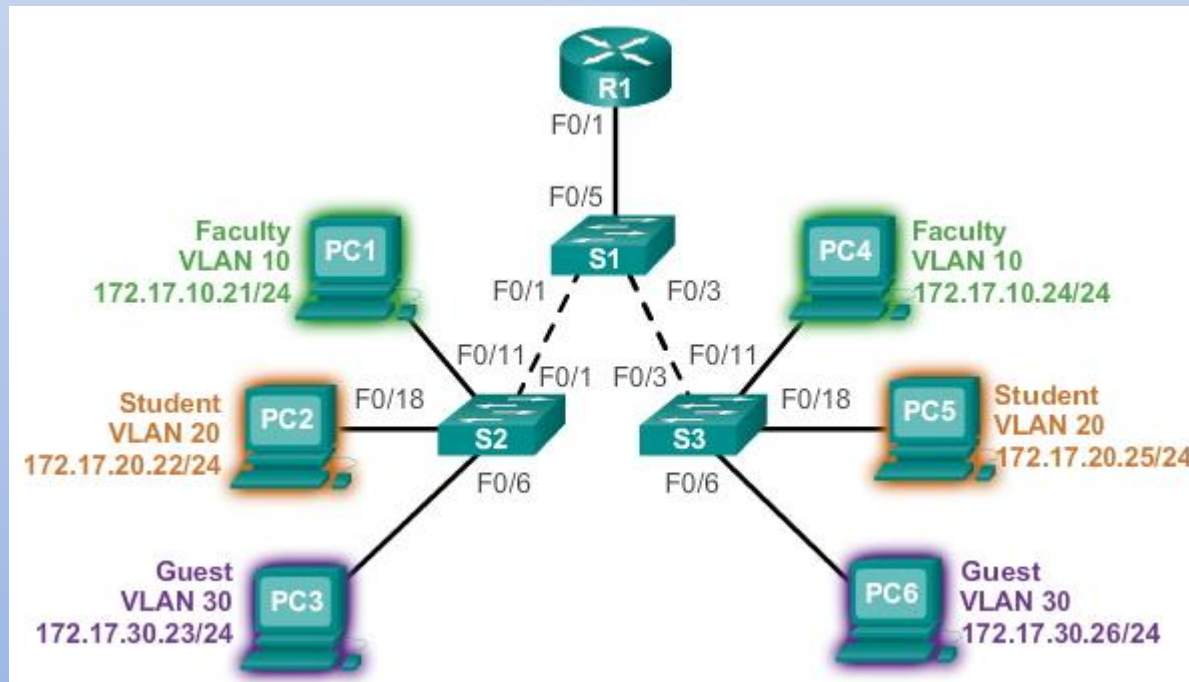
Una vez fortalecida la seguridad en los equipos, siguiendo el esquema de “dentro hacia fuera”, el siguiente paso es fortalecer la seguridad de la red local. Para ello, las medidas a tomar pueden empezar por:

- *Configuración del HW de red en modo no promiscuo*. El modo promiscuo permite a una máquina atrapar todo el tráfico que circula por la red, pudiendo un usuario malintencionado hacerse con información confidencial, contraseñas, etc.
- Empleo de herramientas anti *sniffers*. Existen técnicas y herramientas para detectar máquinas sospechosas de estar accediendo a todo el tráfico de la red. Existen diversas técnicas como pueden ser:
  - Test DNS
  - Test del Ping
  - Test ARP
  - Test ICMP o ping de latencia

# Seguridad en la red local

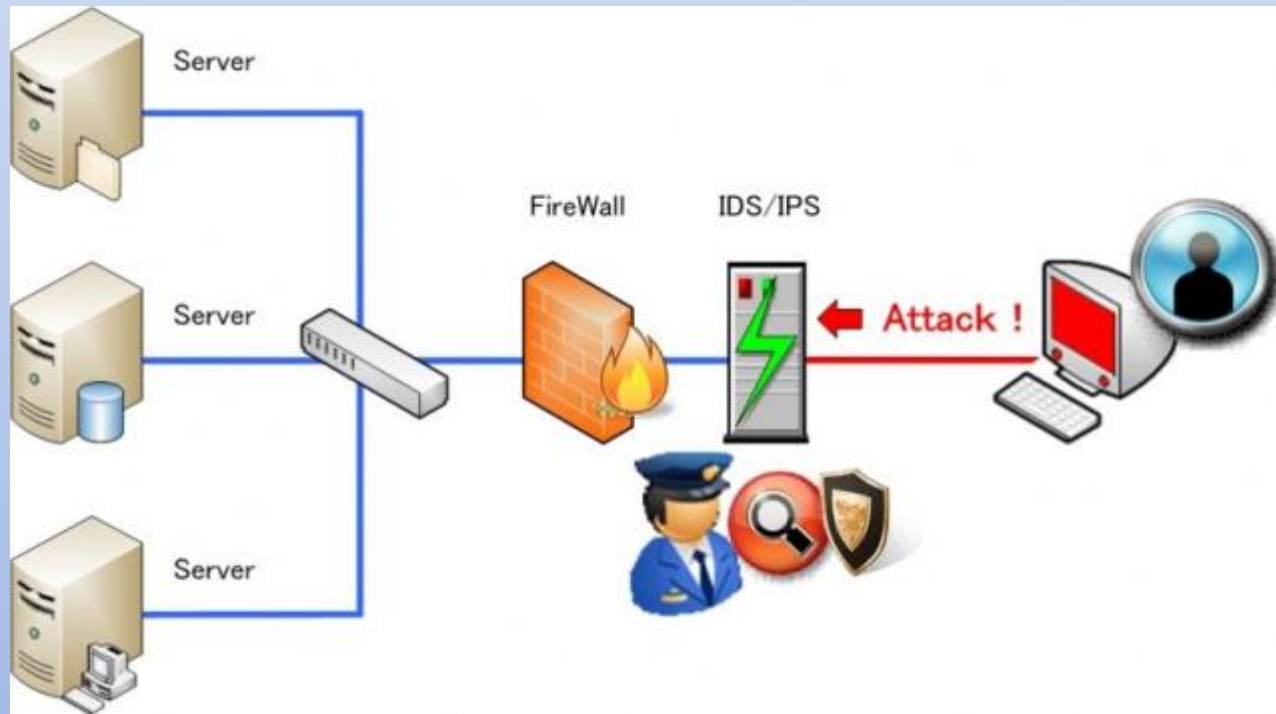
- *Utilización de VLANs (Virtual LAN).*

- Las VLAN (Virtual LAN) permiten la creación de redes de área local virtuales independientes funcionando sobre la misma red física. De esa manera el tráfico de cada red virtual es independiente.
- Se puede asignar una directiva de seguridad individual a cada VLAN. Los ordenadores conectados a una VLAN no *ven* los ordenadores (y el tráfico) de las otras VLAN.
- Si una red VLAN se ve atacada el resto de redes no se ven afectadas.



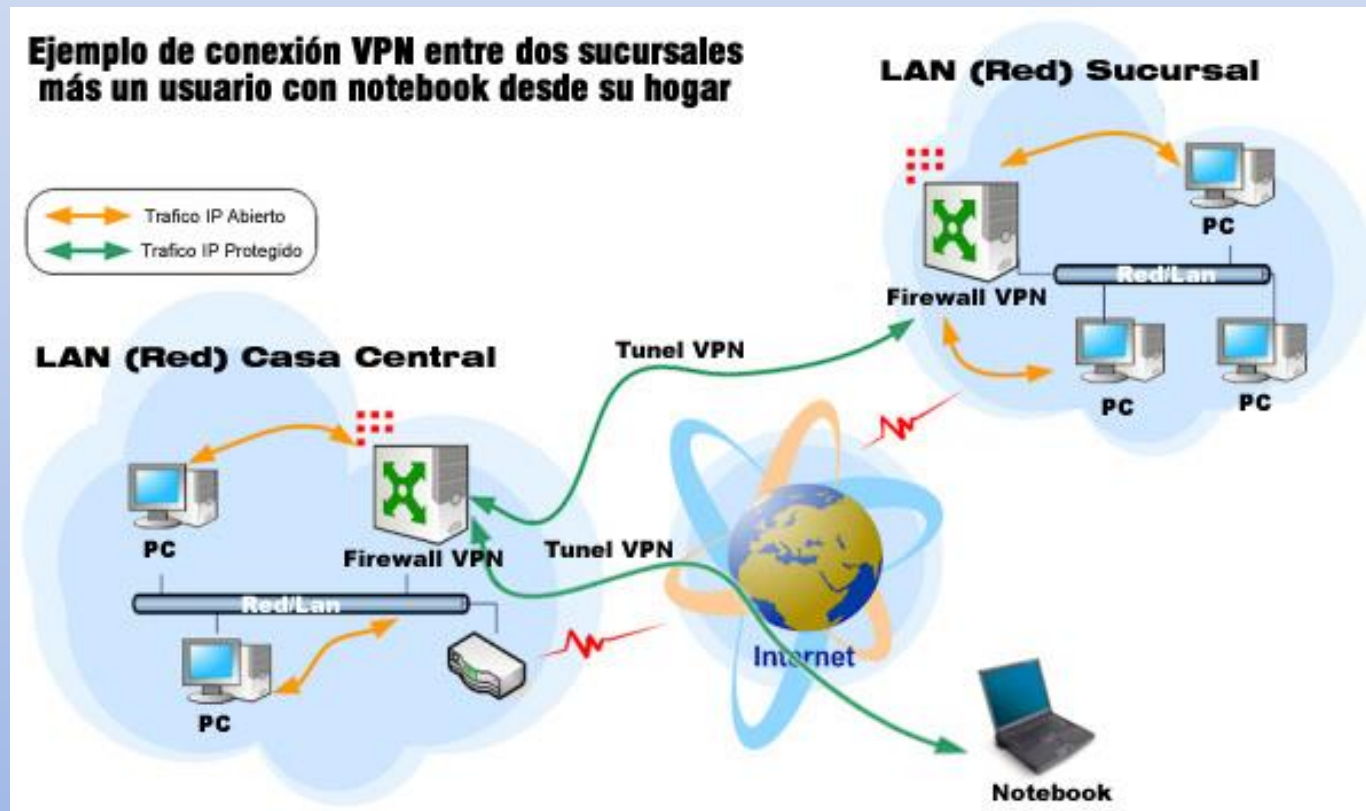
# Seguridad en la red local

• *Utilización de IDSs de red.* Los sistemas de detección de intrusos (IDS) –Y los IPS, sistemas de protección ante intrusos- de red permiten localizar, por medio de análisis del tráfico de la red, posibles intrusos y, en su caso, bloquearlos.



# Seguridad en la red local

- Utilización de VPN (Virtual Private Network). Mediante software o hardware se crea una red privada en la que todas las comunicaciones viajan de forma cifrada, de tal forma que sea imposible de descifrar para alguien ajeno a la VPN.





# Seguridad en la red local

- Seguridad de los dispositivos de red. Todo el equipamiento de red debe estar adecuadamente protegido desde el punto de vista físico para evitar posibles ataques destructivos o escuchas no deseadas.
- Hoy en día cada vez existen más dispositivos conectados a nuestra red (IoT, impresoras en red, domótica, etc.). Estos dispositivos muchas veces no cuentan con unas medidas de seguridad adecuadas y pueden ser utilizados para *pivotar* y acceder a nuestra red. (<https://www.osi.es/servicio-antibotnet>)

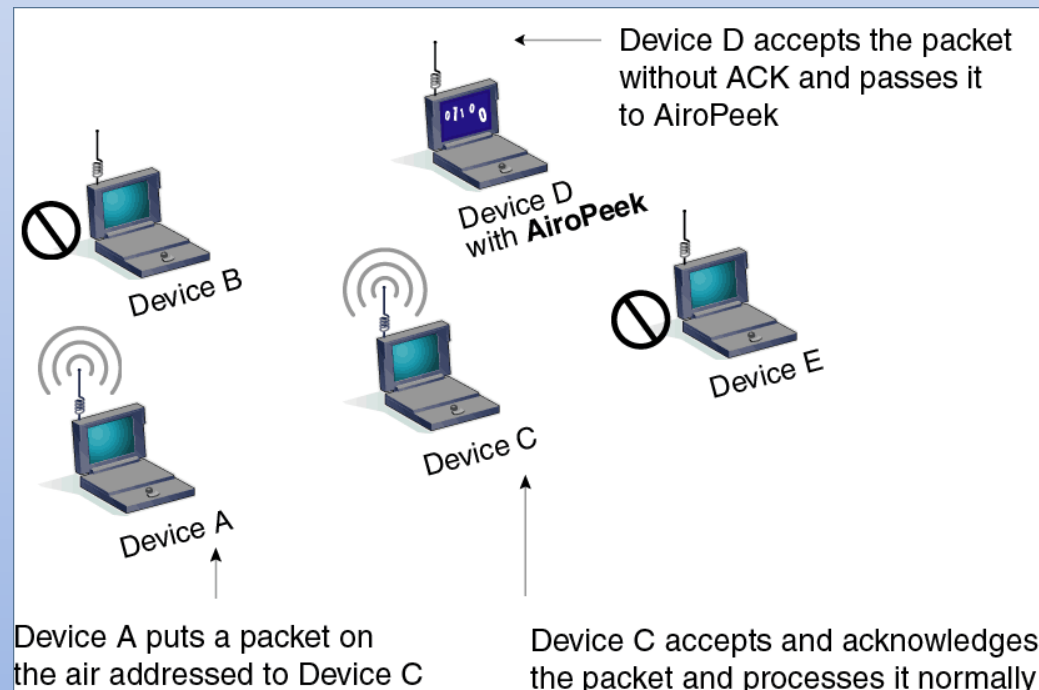
**Confirmado: el ataque DDoS que tumbó la red en EEUU surgió de una *botnet* en el Internet de las Cosas**

Ataque mirai DDoS 2016 → Cámaras IP y DVR



# Seguridad en la red local

- Redes WiFi. Por definición las redes inalámbricas son objetivos fácilmente atacables. Al viajar la información a través del aire es sencillo capturar todo el tráfico de red sin ser detectado (monitorización del tráfico).



# Seguridad en la red local

- Por ello en las redes WiFi hay que ser extremadamente precavidos:
  - Todo el tráfico debe ir cifrado convenientemente. No usar aplicaciones que no cifren la comunicación. Contraejemplo: caso Deusto-Whatsapp. (ahora Whatsapp ya es más seguro)
  - La red no debe estar abierta y el mecanismo de autenticación debe ser seguro. Por ejemplo WPA2 con cifrado AES (WEP no es seguro).
  - Cambiar contraseñas por defecto de los elementos de la red.
  - Si es posible, filtrar el acceso por MAC. (no protege pero ayuda).
  - Vigilar los dispositivos que se conectan a la red.
  - Utilizar una VPN para acceder a nuestros recursos cuando se esté conectado a una WiFi.