# Seguridad en los Sistemas Informáticos
# Tema 2: Seguridad de los sistemas operativos

Grado en Ingeniería Informática

Departamento de Ingeniería Informática
Universidad de Cádiz

Curso 2024–2025

# Índice

# Seguridad en el sistema

La seguridad de un sistema debe contemplar 3 aspectos fundamentales:

- Control de acceso al sistema.
- Control de acceso a los datos.
- Administración del sistema y de la seguridad.

# Control de acceso al sistema

Los sistemas operativos suelen proporcionar un mecanismo de control del acceso de los usuarios. Este suele constar de dos pasos:

1. Identificación del usuario.
2. Autenticación del usuario.

# Métodos de autenticación

Los métodos de autenticación se suelen dividir en tres grandes categorías:

1. Algo que el usuario sabe.
2. Algo que el usuario posee.
3. Una característica física del usuario (autenticación biométrica).

# Autenticación Multifactorial (MFA)

- Con el paso de los años cada vez es más usual que los servicios utilicen autenticación multifactorial.
- La autenticación multifactor consiste en un proceso de seguridad que requiere dos o más factores de verificación para probar la identidad de un usuario.
- Este proceso requiere la combinación de, al menos, dos factores de dos categorías diferentes.
- Un ejemplo de esta autenticación sería requerir la contraseña de un usuario y además el código proporcionado por alguna aplicación, por ejemplo, *Google Authenticator*.

# La elección de las contraseñas (I)

## Principio general

Una buena contraseña debe ser difícil de adivinar (tanto por las personas como mediante métodos automatizados).

## Recomendaciones

- Deben ser lo más largas posible (mínimo 8 caracteres).
- Conviene combinar caracteres numéricos y alfanuméricos, letras mayúsculas, minúsculas y caracteres especiales ( %, $, &, . . . )
- Deben evitarse las palabras de cualquier idioma y los nombres propios.
- No deben utilizarse combinaciones simples de datos personales: iniciales del nombre, fecha de nacimiento, DNI, teléfono, matrícula del coche, etc.
- Utilizar contraseñas fáciles de recordar, para evitar tenerlas apuntadas.
- Son especialmente recomendables los acrónimos de frases que uno recuerde fácilmente.

# La elección de las contraseñas (II)

## Recomendaciones

- Si nos basamos en el número de combinaciones posible como medida para determinar la dificultad de rotura de una contraseña, siempre será preferible aumentar el número de carácteres de la misma a la combinación de diferentes tipos de carácteres.
- Esto nos ayudará a recordarla más fácilmente.

| | Cantidad de caracteres de la contraseña | | | |
|---|---|---|---|---|
| | 10 | 12 | 15 | 20 |
| Solo minúsculas o mayúsculas | 141E+12 | 95E+15 | 1677E+18 | 19928E+24 |
| Combinar minúsculas/mayúsculas (80%) y números (20%) | 20E+12 | 14E+15 | 95E+18 | 436E+24 |
| Combinar minúsculas/mayúsculas (80%) y caracteres especiales (20%) | 213E+12 | 144E+15 | 3127E+18 | 45727E+24 |
| Combinar aleatoriamente minúsculas, mayúsculas, caracteres especiales y números | 53E+18 | 475E+21 | 395E+27 | 2901E+36 |

Fuente: `https://www.welivesecurity.com/la-es/2013/11/28/tamano-si-importa-construyendo-contrasena-larga-segura/`

# Protección de las contraseñas

## Precauciones a tomar por los usuarios

- No compartir nunca su contraseña.
- Cambiarla cada cierto tiempo.
- No escribir ni teclear su contraseña delante de otras personas.
- No enviar la contraseña por correo electrónico.
- Si la contraseña se guarda por escrito, hacerlo en un lugar de difícil acceso para otras personas y de forma que no pueda ser adivinada su función.
- También podemos usar webs para comprobar si nuestra contraseña ha sido filtrada en algún momento. Un ejemplo es *Have I Been Pwned*: `https://haveibeenpwned.com/`

# Protección de las contraseñas (cont.)

## Precauciones a tomar por el administrador

- No debe crear nunca cuentas sin contraseña.
- Cambiar la contraseña después de instalar el sistema.
- Proteger de forma adecuada el fichero del sistema donde se almacenan las contraseñas.
- Vigilar las cuentas de los usuarios accidentales, ya que son las más propensas a la penetración por parte de intrusos.

# Protección de las contraseñas (cont.)

## Protección automatizada:

- Número limitado de intentos de acceso.
- Control de calidad de las contraseñas.
- Caducidad de contraseñas.
- Generación automática de contraseñas.
- Bloqueo de cuentas.
- Registro de entradas.

# Protección de las contraseñas (cont.)

## Protección del fichero de contraseñas

- Las contraseñas tienen que guardarse cifradas. El método criptográfico utilizado debe ser irreversible para que no sea posible descifrarlas.
- El fichero que contiene las contraseñas no debería ser visible a los usuarios.

# Las contraseñas en UNIX/Linux

## El sistema clásico

- Las contraseñas se guardaban cifradas en el fichero `/etc/passwd` (lectura pública).
- Formato del fichero:
  `login:passwd:UID:GID:varios:dir-entrada:shell`
- Problemas: Se podían adivinar contraseñas comparando palabras de un diccionario cifradas con las almacenadas en el fichero `/etc/passwd`.

# Las contraseñas en UNIX/Linux (cont.)

## Mejora de la seguridad de las contraseñas

- El fichero `/etc/passwd` no contiene la contraseña codificada.
- Esta se encuentra en el fichero /etc/shadow que no es de lectura pública.

# Autenticación local en Windows

## *Local Security Authority Server Service* (LSASS)

LSASS es el servicio encargado del control de acceso al sistema. Su principal función es la de gestionar los accesos a *Security Accounts Manager* (SAM).

## SAM

Base de datos local donde se almacenan el usuario y las credenciales hasheadas (hash NTLM o hash LM) de los usuarios con medios de autenticación local, es decir, los usuarios locales y usuarios de dominio autenticados de manera local.

# Autenticación a nivel de dominio en Windows

## Directorio activo

- Uno de los principales usos de un entorno de directorio activo es gestionar el acceso a diversos recursos de la organización.
- Permite autenticar a un usuario desde cualquier equipo dentro del entorno.
- Para ello, existen diversos métodos de autenticación; los más comunes son Kerberos y NTLM.

## NTDS.dit

- Similar a la base de datos SAM usada para la autenticación local pero con la información de todos los usuarios del dominio.
- Este archivo se encuentra en los controladores de dominios.

# Sistemas de autenticación biométrica

- Pueden utilizar cualquier característica única y mensurable del individuo. Se han utilizado:
  - Iris del ojo.
  - Retina del ojo.
  - Huellas dactilares.
  - Geometría de la mano.
  - Firma.
  - Voz.

# Sistemas de autenticación biométrica (cont.)

## Fases

1. Captura o lectura de los datos que el usuario presenta para su validación.
2. Extracción de ciertas características de la muestra.
3. Comparación de tales características con las guardadas en una base de datos.
4. Decisión de si el usuario es válido o no.

## Problemas

| | |
|---|---|
| Tasa de falso rechazo | Probabilidad de que el sistema de autenticación rechace a un usuario legítimo. |
| Tasa de falsa aceptación | Probabilidad de que el sistema autentique correctamente a un usuario ilegítimo. |

# Sistemas de autenticación biométrica (cont.)

## Ejercicio 2.1

Si un sistema de autenticación biométrica tiene una tasa de falso rechazo elevada:

- ¿Para quién sería más perjudicial, para los usuarios o para el sistema?
- ¿Y si fuera elevada la tasa de falsa aceptación?

# Mecanismos de control de acceso a la información

- Determinan qué información puede ser utilizada por cada usuario del sistema.
- Pueden constituir una segunda barrera ante los intrusos que consigan saltarse los mecanismos de control de acceso al sistema.

# Modelo de control de acceso

## Elementos básicos

**Sujeto** Es una entidad capaz de acceder a los objetos. En general, podemos equiparar el concepto de sujeto con el de proceso.

**Objeto** Cualquier recurso cuyo acceso deba controlarse, por ejemplo, ficheros, partes de ficheros, segmentos de memoria, etc.

**Derecho de acceso** La forma en que un sujeto accede a un objeto, por ejemplo, lectura, escritura y ejecución.

| | Fichero1 | Fichero2 | Fichero3 |
|---|---|---|---|
| Usuario A | r w | r | |
| Usuario B | | r w | r |
| Usuario C | | | r w |

# Listas de control de acceso y listas de capacidades

## Listas de control de acceso

- Resultan de la descomposición por columnas de la matriz de acceso.
- Existe una por cada objeto del sistema y enumera los usuarios y los derechos de acceso de estos al objeto.

## Listas de capacidades

- Resultan de la descomposición por filas de la matriz de acceso.
- Hay una por cada sujeto y enumera los derechos de acceso de este a los objetos del sistema.

# Control por niveles de seguridad

## Acceso discrecional y obligatorio

**Acceso discrecional** Deja en manos de los usuarios la decisión de qué tipos de acceso permite para los ficheros que posee.

**Acceso obligatorio** Es el sistema el que toma todas las decisiones sobre el acceso a los datos basándose en unas reglas fijas y en un esquema de clasificación que establece los niveles de seguridad de los distintos sujetos y objetos que comparten el sistema. Esta política puede ser implementada por medio del denominado control por niveles de seguridad.

# Control por niveles de seguridad (cont.)

- Es apropiado para organizaciones que tienen requisitos elevados de seguridad y los usuarios operan de modo jerárquico y disciplinado (organizaciones militares, agencias de inteligencia, empresas con altos requisitos de seguridad).
- Cada sujeto y objeto tiene asociada una etiqueta.
- La etiqueta consta de dos partes: **Clasificación** y un conjunto de **Categorías**.
- Ejemplo de etiqueta:
  Secreto [Armas-Químicas Oriente-Medio]

# Control por niveles de seguridad (cont.)

## Niveles de seguridad en entorno militar

1. Alto secreto
2. Secreto
3. Confidencial
4. No clasificado

## Niveles de seguridad en entorno empresarial

1. Propietario
2. Directivo
3. Jefe de Departamento
4. Empleado
5. Público

# Control por niveles de seguridad (cont.)

## Categorías

- Las categorías no son jerárquicas.
- Representan las distintas áreas de información del sistema.
- Ejemplo de categorías en una empresa: Ventas, Personal, Producción, Marketing...

## Decisión:

- Etiqueta del sujeto
- Etiqueta del objeto
- Tipo de acceso que se quiere realizar

# Utilidad de las copias de seguridad

## Único mecanismo para recuperar datos perdidos

### Casos en que son necesarias

- Un usuario o un administrador ha borrado de forma no intencionada alguna información que era importante.
- Un intruso ha borrado información importante.
- Fallo de hardware.
- Un robo.
- Desastres naturales: inundación, incendio...

# ¿Qué debemos copiar?

## Hay dos tendencias: copiar todo o solo una parte

### Copia completa

Copiamos todos los ficheros del sistema.

| | |
|---|---|
| Ventajas | La recuperación del sistema, en caso de tener que recuperarlo completo, es más sencilla. |
| Inconvenientes | Consume más recursos (soporte y tiempo). |

### Copia parcial

Copiamos aquello que sea específico de nuestro sistema: ficheros de usuarios, ficheros de configuración...

| | |
|---|---|
| Ventajas | Consume menos recursos. |
| Inconvenientes | Si hay que recuperar todo el sistema, tendremos que empezar instalando el SO, todo el software adicional instalado (más parches...) y, por último, la copia de seguridad. |

# Tipos de copias de seguridad

## Completas

Copia todos los ficheros de interés.

## Progresivas

Solo se copian aquellos ficheros que han sido creados o modificados desde la última copia completa o progresiva efectuada.

## Diferenciales

Solo se copian los ficheros que han sido creados o modificados desde la última copia completa realizada.

# Plan de copias de seguridad

## Contenidos

- Tipos de copias que se van a realizar.
- Ciclos de copia y rotación de soportes.
- Frecuencia.
- Momento en que se van a realizar las copias.

## Otros aspectos a considerar

- Protección.
- Comprobación.
- Recursos para la realización de copias de seguridad.

# Ejercicios de copias de seguridad

## Ejercicio 2.2

- Considere los siguientes escenarios:
  - Copias completas y progresivas.
  - Copias completas y diferenciales.
- Explique cómo llevaría a cabo estas acciones en cada caso:
  - Recuperar el sistema completo.
  - Recuperar un fichero individual.

# Auditorías

## Concepto de auditoría

Consiste en la monitorización del funcionamiento del sistema de forma automatizada y sistemática mediante el registro de los sucesos clave que se producen en este.

## El trabajo de un auditor

Consiste en comprobar la seguridad de una infraestructura mediante diversos estándares, así como proponer mitigaciones para los fallos de seguridad detectados.

# Auditorías (cont.)

## Objetivos

- Revisar accesos por usuarios a los objetos del sistema.
- Revisar la efectividad de mecanismos de seguridad del sistema.
- Descubrir intentos de saltarse los mecanismos de seguridad.
- Descubrir usuarios con privilegios excesivos.
- Servir de elemento disuasor para los atacantes.
- Ayudar a la recuperación de desastres informáticos.
- Proporcionar pruebas materiales de los ataques.

# Auditorías (cont.)

## Evento auditable

- Acciones que queremos que queden registradas en el sistema de auditoría.
- Ejemplos: Arranque o parada del sistema, conexión o desconexión de un usuario, cambio de privilegios de acceso a los objetos de un sistema, creación/modificación/borrado de un objeto...

## Información auditable

- Datos relacionados con el evento auditable que pueden ser útiles.
- Ejemplos: Fecha y hora en que se produce el evento, tipo de evento, éxito o fracaso, datos del usuario que lo desencadena...

# Detección de ataques

## Tipos más comunes

- Intentos fallidos de entrada al sistema.
- Suplantaciones.
- Flujos de información prohibidos.
- Obtención de información restringida.
- Caballos de Troya.
- Virus.
- Abuso de recursos.

# Mecanismos para la detección de ataques

## Perfil de usuario

- Recoge las acciones que cada usuario realiza normalmente en el sistema.
- Si un intruso utiliza la cuenta de un usuario se puede detectar debido a que se aparta del perfil del usuario.
- Puede avisar de acciones legales que se aparten del perfil.

## Perfil de intruso

- Los intrusos suelen actuar de una forma similar cuando entran en un sistema ajeno: mirar quién está conectado al sistema, examinar el sistema de ficheros, moverse por los directorios tratando de obtener información, no suelen estar conectado mucho tiempo.

# Mecanismos para la detección de ataques (cont.)

## Acciones puntuales

Hay ciertas acciones que por sí mismas denuncian la presencia de un ataque o intento de ataque:

- Intento de acceso a la administración del sistema.
- Intento de explotación de agujeros de seguridad conocidos.
- Uso de herramientas que detectan agujeros de seguridad.
- Uso de órdenes de otros sistemas operativos.

# Prácticas recomendadas

- Disponer de un administrador.
- Parametrizar de forma adecuada el sistema de auditoría:
  - Establecer los eventos y la información auditables.
  - Definir perfiles.
  - Proteger los ficheros de auditoría.
- Compresión y respaldo de los ficheros de auditoría.
- Determinar el método de análisis que se va a realizar sobre los ficheros de auditoría.
- Cuidar las implicaciones de tipo ético.

# Análisis forense (I)

## Definición

- Se encarga de la recolección, preservación, análisis y presentación de evidencias.
- Cuando sucede una intrusión, acceso no permitido o infección de *malware*.
- Permite detectar una posible amenaza.

## Indicios

- Elevado uso de disco/red/CPU en una máquina.
- Actividad anormal de un usuario.
- Duración sospechosa de cierta conexión.
- Conexión remota desde sitios extraños.
- Ejecución de servicios o procesos no habituales.

# Análisis forense (II)

## Metodología (etapas)

- Adquisición.
- Preservación.
- Análisis de memoria.
- Análisis de ficheros y procesos.
- Presentación de evidencias y realización de informe.

## Adquisición

- Captura de evidencias digitales.
- Preserva el estado volátil de la máquina.
- Debe volcarse todo el contenido de los procesos que estén en ejecución.

# Análisis forense (III)

## Preservación

- Resguardar los objetos que supongan una evidencia de una incidencia.
- Su resguardo ha de ser competo, claro, verificable.
- Deben generarse *hashes* de las evidencias.

## Buenas prácticas

- RFC 3227 - Guidelines for Evidence Collection and Archiving: `https://www.ietf.org/rfc/rfc3227.txt` y `https://www.incibe-cert.es/blog/rfc3227`
- UNE 71505-1:2013: Sistema de Gestión de Evidencias Electrónicas (SGEE).
- UNE 71506:2013: Metodología para el análisis forense de las evidencias electrónicas.

# Adquisición de evidencias (I)

## *Triage*

- Consiste en adquirir datos de un dispositivo u ordenador.
- Las herramientas utilizadas deben ser no intrusivas, conocidas y reproducibles, y estar bien documentadas.
- Se requieren privilegios de administrador.

## *Scripts*

- ((date /t) & (time /t)): fecha y hora del sistema.
- ipconfig /all: adaptadores de red del equipo.
- netstat -nr: lista de interfaces y tablas de enrutamiento.
- nbtstat -c: dirección IP de un ordenador.

# Adquisición de evidencias (II)

## Herramientas

- RamCapturer: gratuita de Belkasoft, realiza un volcado de memoria (*dump*) completo.
- RawCopy: realiza volcado de ficheros en ejecución o *locked*.
- FTK Imager Lite: gratuita de Access Data, extrae ficheros y realiza volcado de memoria.
- Lastactivityview: de Nirsoft (`https://www.nirsoft.net/`), realiza un *timeline* de la actividad de un usuario autenticado y genera un informe en HTML.
- Winaudit: genera un informe de la actividad y el estado de un sistema.
- Windows Registry Recovery: `http://www.mitec.cz/wrr.html`

# Adquisición de evidencias (III)

## Herramientas

- Windows File Analyzer: `http://www.mitec.cz/wfa.html`
- Shadow Explorer: `https://www.shadowexplorer.com/downloads.html` (copias *shadow* es una copia oculta realizada por Windows).
- Autopsy: `https://www.autopsy.com/`
- Everything: `https://www.voidtools.com/es-es/`
- WMIC: Windows Management Instrumentation.
- SimpleWMIView: `http://www.nirsoft.net/utils/simple_wmi_view.html`

# Adquisición de evidencias (IV)

## WMIC

- wmic useraccount list brief: listado de cuentas de usuario.
- wmic partition get name,size,type: listado de particiones.
- wmic process list brief: listado de procesos.
- wmic bios get serialnumber: número de serie de la BIOS.
- wmic bios get manufacturer,name,version /format:list: fabricante, nombre y versión de la BIOS.
- wmic computersystem get model,name,manufacturer,systemtype: modelo, nombre, fabricante y tipo de sistema del equipo.
- wmic process call create "notepad.exe": ejecuta el Notepad.
- wmic process where name="notepad.exe" call terminate: cierra el Notepad.
- wmic os list brief: versión y número de serie del sistema operativo.

# Adquisición de evidencias (V)

## Clonado de discos

- Clonado bit a bit.
- El destino deberá contener los mismos errores que haya en el origen.
- El clonado se realiza de disco a disco (mientras que una imagen de disco a un sistema de ficheros).
- Tipos de clonado: hardware y software.
- Herramientas de clonado: Guymager y FKT Imager.

# Artefactos (I)

## Definición

- Conjunto de ficheros, aplicaciones, registros, configuraciones y rutas de acceso que permiten detectar actividad de usuario malicioso o *malware*.
- Contienen información muy relevante para llevar a cabo la investigación.
- Evidencias que deben ser buscadas y preservadas.

## Registro de Windows

- Fuente de artefactos forenses.
- Contiene configuraciones para Windows.
- Registra datos específicos del usuario.
- Para interactuar con el registro: *regedit.exe*.

# Artefactos (II)

## Claves del registro de Windows

- HKEY_CURRENT_USER: Registra toda la información del usuario que tiene abierta la sesión en el momento de ejecutar el registro. Se almacenan carpetas del usuario, colores de pantalla, configuración del panel de control, etc.
- HKEY_USERS: Contiene todos los perfiles de usuario cargados activamente en el equipo.
- HKEY_LOCAL_MACHINE: Contiene información de configuración específica del equipo (para cualquier usuario).
- HKEY_CLASSES_ROOT: La información que se almacena aquí se asegura de que se abra el programa correcto al abrir un archivo mediante Windows Explorer.
- HKEY_CURRENT_CONFIG: Contiene información sobre el perfil de hardware que usa el equipo local al iniciar el sistema.

# Artefactos (III)

## Registros de eventos

- Archivos especiales donde Windows registra los eventos relevantes que ocurren en el equipo.
- Por ejemplo, se produce un error de un programa, o un usuario inicia sesión en el equipo.
- En el visor de eventos, estos se agrupan en:
  - Eventos de aplicaciones: cada evento se clasifica como información, advertencia o error, en función de su gravedad.
  - Eventos relacionados con la seguridad: indican si una operación se ha llevado a cabo correctamente o no, por ejemplo, el inicio de sesión.
  - Eventos de configuración.
  - Eventos del sistema: información, advertencia o error.
- Ficheros de eventos (.evtx) se encuentran en: %WINDIR%\System32\winevt\Logs

# Artefactos (IV)

## *Prefetching*

- Permite acelerar el arranque de aplicaciones en Windows (no Windows Server).
- Registra datos de una aplicación, ficheros cargados, número de arranques, etc.
- Permite asegurar que un fichero fue abierto con un programa, cuándo, cuántas veces... (pero no quién lo hizo).
- Tras arrancar el equipo, Windows monitoriza los programas abiertos habitualmente.
- Información (.pf) almacenada en: %WINDIR%\Prefetch
- Los ficheros .pf pueden abrirse con WinPrefetchView: `http://www.nirsoft.net/utils/win_prefetch_view.html`

# Artefactos (V)

## Aplicaciones

- Herramientas para todos los navegadores web: BrowsingHistoryView y MyLastSearch.

# Referencias bibliográficas


- Uso de listas de control de acceso en Linux: `http://www.escomposlinux.org/iarenaza/articulo-acls/acls-linux-samba.html`
- LastPass: `https://www.lastpass.com/es/`
- Comprobadores de contraseñas: `https://password.es/comprobador/` y `https://password.kaspersky.com/es`
- Tar: `http://www.gnu.org/software/tar/manual/`
- Clonezilla: `https://clonezilla.org`
- Unison: `https://github.com/bcpierce00/unison`
- Malwarebytes: `https://es.malwarebytes.com/mwb-download/`
- Desinfecta tus dispositivos: `https://www.osi.es/es/desinfecta-tu-ordenador`
- Herramientas imprescindibles para análisis forense: `http://www.nirsoft.net/`
- Herramientas de clonado: FTK Imager, Guymager.