6. SOFTWARE AMPLIADO

Contenidos

1. COMPRESIÓN / DESCOMPRESIÓN DE ARCHIVOS
2. MANTENIMIENTO, MONITORIZACIÓN Y OPTIMIZACIÓN DEL SISTEMA
3. GESTIÓN DE DISCOS, FICHEROS Y RECUPERACIÓN DE DATOS
4. UTILIDADES DE SEGURIDAD
5. OTRAS HERRAMIENTAS

1. Compresión / Descompresión

Su objetivo es reducir el tamaño de los ficheros de datos.

Ejemplo: “ZZZZZZZZZ” se puede comprimir por “9Z”

Ratio de compresión (RC): indica cuánto están comprimidos los datos

Ejemplo: 10:1 indica que de cada 10 bits en el fichero origen se tendrá 1 en el fichero destino (los datos comprimidos ocuparán diez veces menos)

1. Compresión / Descompresión

Tipos de compresión

Con pérdidas: al descomprimir los datos no se obtienen los originales, se pierde información.
Ejemplo: JPG (ajusta la compresión en función de la calidad)

Sin pérdidas: la información descomprimida no pierda nada con respecto a la original.
Ejemplo: algoritmo Huffman de los ficheros ZIP (basado en el estudio de los símbolos más frecuentes de un alfabeto)

1. Compresión / Descompresión

Función hash o resumen

Es un tipo especial de compresión.

Mediante un algoritmo matemático se transforma un bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija

1. Compresión / Descompresión

Función hash o resumen

Permite analizar la integridad de un archivo descargado mediante la comprobación de su valor resumen calculado.

Algoritmos utilizados: SHA-1, SHA-2, SHA-256, MD5

En Linux se utiliza el comando md5sum

2. Mantenimiento, monitorización y optimización del sistema

El objetivo es poder verificar que todos los elementos del sistema funcionan correctamente (CPU, memoria, red, …)

Dentro de esta categoría podemos encontrar:

- Utilidades para la limpieza del registro de Windows
- Utilidades para la administración de tareas
- Utilidades de monitorización del rendimiento

2. Mantenimiento, monitorización y optimización del sistema

Algunas de estas herramientas en Windows son:

- Administrador de tareas
- Programador de tareas
- Visor de eventos
- Monitor de rendimiento

3. Gestión de discos, ficheros y recuperación de datos

- Herramientas de sincronización de datos: sincroniza todos los datos del usuario (carpetas, ficheros, fotos, documentos, favoritos, …) o varias carpetas entre sí (Ej: Drive)

  A nivel empresarial o gubernamental estas herramientas son fundamentales cuando se tienen datos procedentes de varias fuentes (Ej: CRM, censos, elecciones, …)

3. Gestión de discos, ficheros y recuperación de datos

- Recuperación de datos: para recuperar datos borrados accidentalmente del disco o pendrive

  File carving: técnica usada principalmente en informática forense. Analiza los discos a nivel profundo. Se basa en que los ficheros empiezan y terminan por una serie de bloques de datos fijos (magic numbers), diferentes para cada tipo de archivos.

3. Gestión de discos, ficheros y recuperación de datos

	MP4	MPEG-4 video file
[4 byte offset] 66 74 79 70 69 73 6F 6D		[4 byte offset] ftypisom

	ACCDB	Microsoft Access 2007 file
00 01 00 00 53 74 61 6E 64 61 72 64 20 4A 65 74 20 44 42		....Stan dard Jet DB
	MDB	Microsoft Access file
00 01 00 08 00 01 00 01 01		....

4D 5A	MZ
COM, DLL, DRV, EXE, PIF, QTS, QTX, SYS	Windows/DOS executable file

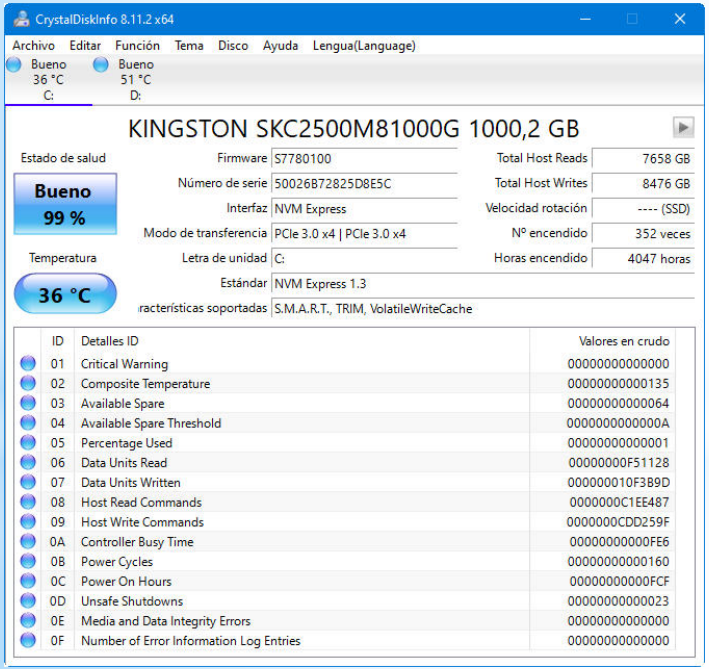
3. Gestión de discos, ficheros y recuperación de datos

- Herramientas de gestión de discos:
  - Defragmentación
  - Particiones
  - Herramientas SMART (Self Monitoring Analysis and Reporting Technology). Estas se utilizan para detectar fallos en el disco

3. Gestión de discos, ficheros y recuperación de datos

- Herramientas de gestión de discos:
  - Herramientas SMART
    Su objetivo es adelantarse a los errores críticos en disco y al menos poder salvar la información
    Su uso no es sencillo. Implica conocer muchos parámetros: tasas de error, tiempo de encendido, ciclos de carga, …

3. Gestión de discos, ficheros y recuperación de datos



ID	Attribute Name	Current	Worst	Threshold	Raw Values
01	Read Error Rate	116	99	6	0000066831F9
03	Spin-Up Time	96	95	0	000000000000
04	Start/Stop Count	80	80	20	0000000051BE
05	Reallocated Sectors Count	100	100	36	000000000000
07	Seek Error Rate	84	60	30	00022318B12E
09	Power-On Hours	62	62	0	00000000833C
0A	Spin Retry Count	100	100	97	000000000000
0C	Power Cycle Count	95	95	20	0000000017CD
B7	Vendor Specific	91	91	0	000000000009
B8	End-to-End Error	100	100	99	000000000000
BB	Reported Uncorrectable Errors	100	100	0	000000000000
BC	Command Timeout	100	94	0	0007000A0131
BD	High Fly Writes	100	100	0	000000000000
BE	Airflow Temperature	66	44	45	000327160022
C2	Temperature	34	56	0	000C00000022
C3	Hardware ECC recovered	30	19	0	0000066831F9
C5	Current Pending Sector Count	100	100	0	000000000000
C6	Uncorrectable Sector Count	100	100	0	000000000000
C7	UltraDMA CRC Error Count	200	190	0	000000000C47
F0	Head Flying Hours	100	253	0	F64A0000CBD8
F1	Total Host Writes	100	253	0	000039102950
F2	Total Host Reads	100	253	0	0000325B5AD3

4. Utilidades de seguridad

Se trata de un software especialmente diseñado para proteger el sistema. La seguridad informática tiene como objetivo identificar qué partes del sistema son vulnerables y ofrecer recursos para evitar dichas debilidades.

- Herramientas de encriptado
- Antimalware
- Antiespías
- Cortafuegos

4. Utilidades de seguridad

Herramientas de encriptado

El objetivo es traducir un archivo en una secuencia ininteligible de caracteres mediante una clave. Su contenido solo puede ser accesible para los que disponen de la clave de descifrado.

Claves simétricas / Claves asimétricas

Se pueden encriptar tanto los archivos como las particiones o los discos.

4. Utilidades de seguridad

Antimalware

En general, el malware es el término genérico para designar a todo el software malicioso diseñado para infiltrarse en un dispositivo con fines poco lícitos.

Hasta hace no mucho, el único tipo de malware eran los virus. Ahora el espectro es muy amplio: virus, gusanos, troyanos, spyware, adware, ransomware, botnets, keyloggers, honeypots, …

4. Utilidades de seguridad

Antivirus

No es fácil saber si un sistema tiene un virus o no. A veces, cuando se muestran sus efectos ya es tarde.

Funciones de los antivirus: detectar los virus, prevenir posibles infecciones, analizar el sistema en busca de virus y eliminarlos.

Importante la actualización frecuente.

4. Utilidades de seguridad

Antivirus

Sus principales medios de propagación son:

- Internet: email, descargas de información, …
- Unidades de almacenamiento: discos externos, unidades USB
- Redes de ordenadores: la comunicación entre equipos posibilita también el paso de malware de unos a otros

4. Utilidades de seguridad

Antivirus

Los síntomas más habituales son:

- Cambio de fecha/hora de archivos
- Sistema ralentizado
- Cambios en la ruta de los programas
- Ejecución de programas extraños
- Errores en el arranque del sistema
- Ventanas emergentes

4. Utilidades de seguridad

Antivirus

Scanning: se escanea el archivo y se compara su código con los códigos de virus conocidos existentes en unas bases de datos. Si coinciden se determina el archivo ha sido infectado. Actualmente está en desuso ya que no evita que el sistema sea infectado.

4. Utilidades de seguridad

Antivirus

Técnicas heurísticas: se monitorizan los programas para buscar comportamientos “sospechosos” propios de los virus. A veces sospecha de programas que no son realmente virus.

Por lo general, se combinan las dos técnicas.

Se analizan no solo virus sino cualquier tipo de malware (spam, troyanos, spyware, …)

4. Utilidades de seguridad

Antiespías

Software que evita los spyware. Esto son programas que recopilan información del usuario o el equipo y la distribuyen para obtener información.

Indicadores: cambio en la página de inicio del navegador, pop-ups, navegadores lentos, arranque lento, …

4. Utilidades de seguridad

Elegir un antimalware

- Falta de objetividad en la mayoría de los informes ya que muchos están realizados por empresas desarrolladoras de antimalware.
- Los usuarios realizar estudios pero con una muestra muy pequeña.
- La tasa de detección varía de mes en mes.

Ningún antivirus es perfecto
Ninguno detecta al 100%

4. Utilidades de seguridad

Elegir un antimalware

Los estudios con más validez son los realizados por laboratorios independientes:

- AV Comparatives (https://www.av-comparatives.org)
- AV-Test.org (https://www.av-test.org/es/)
- ICSA Labs (https://www.icsalabs.com/)
- Virus Bulletin (https://www.virusbulletin.com/)

4. Utilidades de seguridad

Cortafuegos

Sistemas hardware o aplicación software que controla el tráfico de entrada o salida de la red en función de parámetros como el protocolo, la dirección IP o los puertos.

Ejemplos: iptables, firewall de Windows, Comodo, ZoneAlarm, Netdefender, …

5. Otras herramientas

Grabación

Herramientas utilizadas para la grabación de CD y DVD. Ejemplo: CDBurner, Nero, Alcohol 120%, Ashampoo

En las grabaciones y descargas es interesante comprobar la integridad de los archivos originales (p.e. hash)

5. Otras herramientas

Codificadores y conversores multimedia

Herramientas que admiten archivos de audio o vídeo para almacenarlos, transferirlos o reproducirlos.

Codec (Codificador / DECodificador): codifican o decodifican el flujo de datos o señal de audio o vídeo reduciendo su tamaño, a costa de perder calidad en los datos.

Ejemplo: MP3

5. Otras herramientas

Codificadores y conversores multimedia

Los datos codificados necesitan el mismo códec en el equipo destino para poder reproducirlos.

Distribución de codecs en packs.

Ejemplos (vídeo): XviD, DivX, WMV, MPEG
Ejemplos (audio): MP3, WMA, WAV

5. Otras herramientas

Codificadores y conversores multimedia

Los conversores permiten la transformación de los ficheros con distintos formatos.

Por ejemplo, Any Video Converter, VLC, DivX Converter, Format Factory, …

5. Otras herramientas