Seguridad Activa:
Sistema operativo y aplicaciones

Tema 5

Álvaro Rodríguez - IES Alonso de Madrigal (Ávila)
2º SMR

UT5 – S.O. Y APLICACIONES

CONTENIDOS

- Medidas de protección encaminadas a que el usuario se autentifique en el sistema operativo.
- Mecanismos de autentificación del sistema operativo.
- Cuotas.
- Actualizaciones y parches
- Antivirus.
- Monitorización.
- Aplicaciones web.
- Cloud computing.
- Aspectos prácticos.

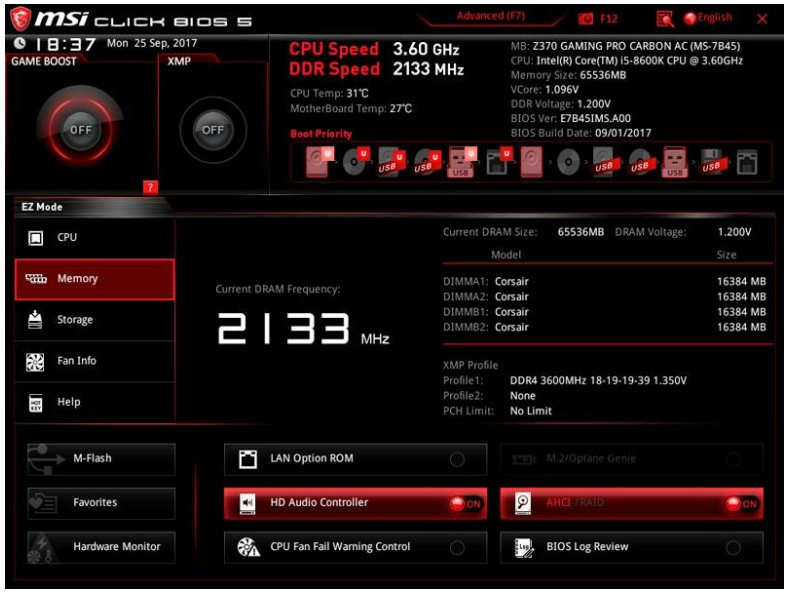
SEGURIDAD ACTIVA: SISTEMA OPERATIVO Y APLICACIONES

LA BIOS O EFI

El primer elemento que debemos proteger y que al mismo tiempo nos sirve para protegernos es la BIOS.

Debemos cuidar:

- El acceso a la BIOS/EFI. Protegiéndolo por contraseña
- El arranque de Sistemas operativos mediante LiveCD. Configurando el orden de arranque
- La versión y actualización controlada del firmware. Siempre desde repositorios fiables, chequeando los hashes, etc.



SEGURIDAD ACTIVA: SISTEMA OPERATIVO Y APLICACIONES

EL SISTEMA OPERATIVO

Uno de los **objetivos** del Sistema Operativo va a ser precisamente ofrecer seguridad al sistema.

El sistema operativo suele ofrecer, entre otras cosas:

- Control de usuarios. Privilegios, cuotas de uso, estadísticas...
- Actualizaciones
- Monitorización
- Antivirus y Firewall
- Cifrado de datos

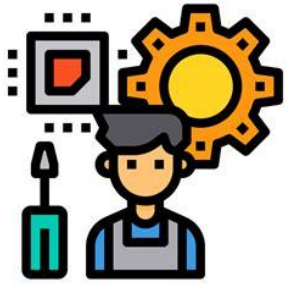
Nuestra tarea como administradores de estos equipos es la de **configurar y monitorizar** que el sistema operativo lleva a cabo correctamente estas acciones y en caso de considerar que no es suficiente, añadir software que aporte la seguridad necesaria a los equipos que administramos.

Algunas herramientas muy útiles para monitorizar los equipos Windows nos las proporciona Nirsoft:
https://www.nirsoft.net/utils/index.html#desktop_utils

SEGURIDAD ACTIVA: SISTEMA OPERATIVO Y APLICACIONES

DEBATE

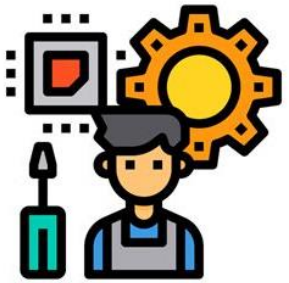
¿Por qué no conviene utilizar de manera habitual un usuario con todos los privilegios de administrador?



SEGURIDAD ACTIVA: SISTEMA OPERATIVO Y APLICACIONES

CUENTAS DE USUARIO

Conviene que, en un sistema compartido, cada usuario utilice su propia cuenta de usuario, de modo que cada uno tenga acceso sólo a sus archivos, y con los permisos que les asignemos.

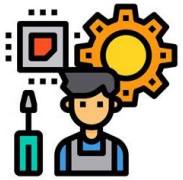


En Windows existe UAC (User Acces Control), con ella el sistema avisa al usuario cuando un programa solicita ejecutar una operación de administración.

Si no estábamos haciendo nada especial, como una instalación de nuevo software, podemos suponer que es un ataque y detenerlo ahí

SEGURIDAD ACTIVA: SISTEMA OPERATIVO Y APLICACIONES

USUARIOS EN LINUX



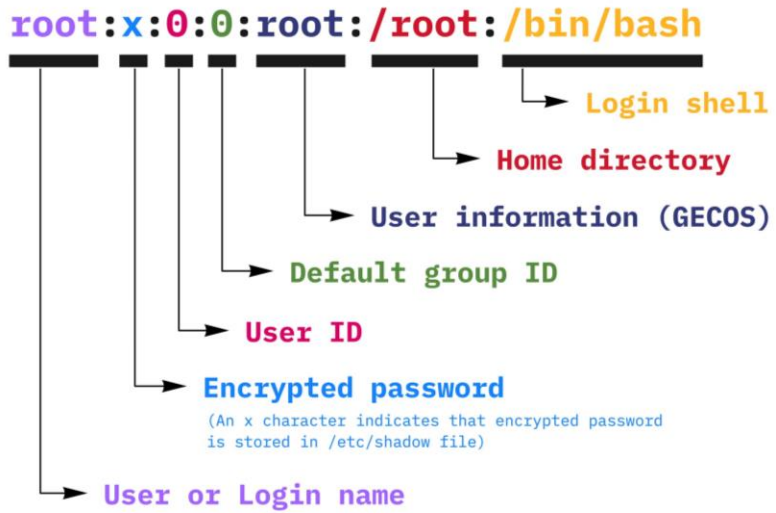
Se puede observar que los archivos:

/etc/passwd tiene todos los usuarios registrados en el sistema.

/etc/group tiene la definición de los grupos

/etc/shadow las contraseñas cifradas de los usuarios y el sistema de cifrado utilizado

login:contraseña:UID:GID:comentario: directorio-personal:Shell-del-usuario



SEGURIDAD ACTIVA: SISTEMA OPERATIVO Y APLICACIONES

ACTIVIDAD

1. Para el archivo passwd extraído de una máquina Linux, crea una tabla en la que se muestre para cada usuario que pueda iniciar sesión:
   - Nombre de usuario
   - Directorio de usuario
   - Shell asignada al usuario

2. Investiga cómo crear una cuenta de usuario, sin permisos de administrador, tanto en Linux como en Windows.

   ✓ Crea un nuevo usuario sin privilegios en dos de tus máquinas virtuales (de ambos SS.OO) e inicia sesión con ellos.

3. Utiliza la herramienta de Nirsoft del enlace para comprobar qué usuarios han iniciado sesión en tu máquina virtual Windows.

   https://www.nirsoft.net/utils/windows_log_on_times_view.html

SEGURIDAD ACTIVA: SISTEMA OPERATIVO Y APLICACIONES

ACTUALIZACIONES

En Windows y Linux existen diferentes gestores para actualizaciones:

- Repositorios de Linux, según la distribución.
  - Apt-get update
  - Apt-get upgrade

- Windows Update. Actualiza:
  - El propio sistema operativo
  - Aplicaciones y servicios
  - Algunos controladores de dispositivos

- El comando **Winget** en Windows permite:
  - Buscar software para su instalación
  - Instalar software
  - Comprobar el software instalado
  - Actualizar software a la última versión

SEGURIDAD ACTIVA: SISTEMA OPERATIVO Y APLICACIONES

ACTUALIZACIONES

Las actualizaciones a menudo introducen mejoras, pero sobre todo, corrigen defectos.

Los parches son actualizaciones que se utilizan específicamente solo para corregir defectos y suelen necesitar que el usuario lo descargue y lo instale.

En Windows podemos gestionar las aplicaciones instaladas y sus versiones utilizando el comando winget.

También existen aplicaciones de terceros:

- Chocolatey
- SUMO
- Patch My PC

SEGURIDAD ACTIVA: SISTEMA OPERATIVO Y APLICACIONES

ACTIVIDAD

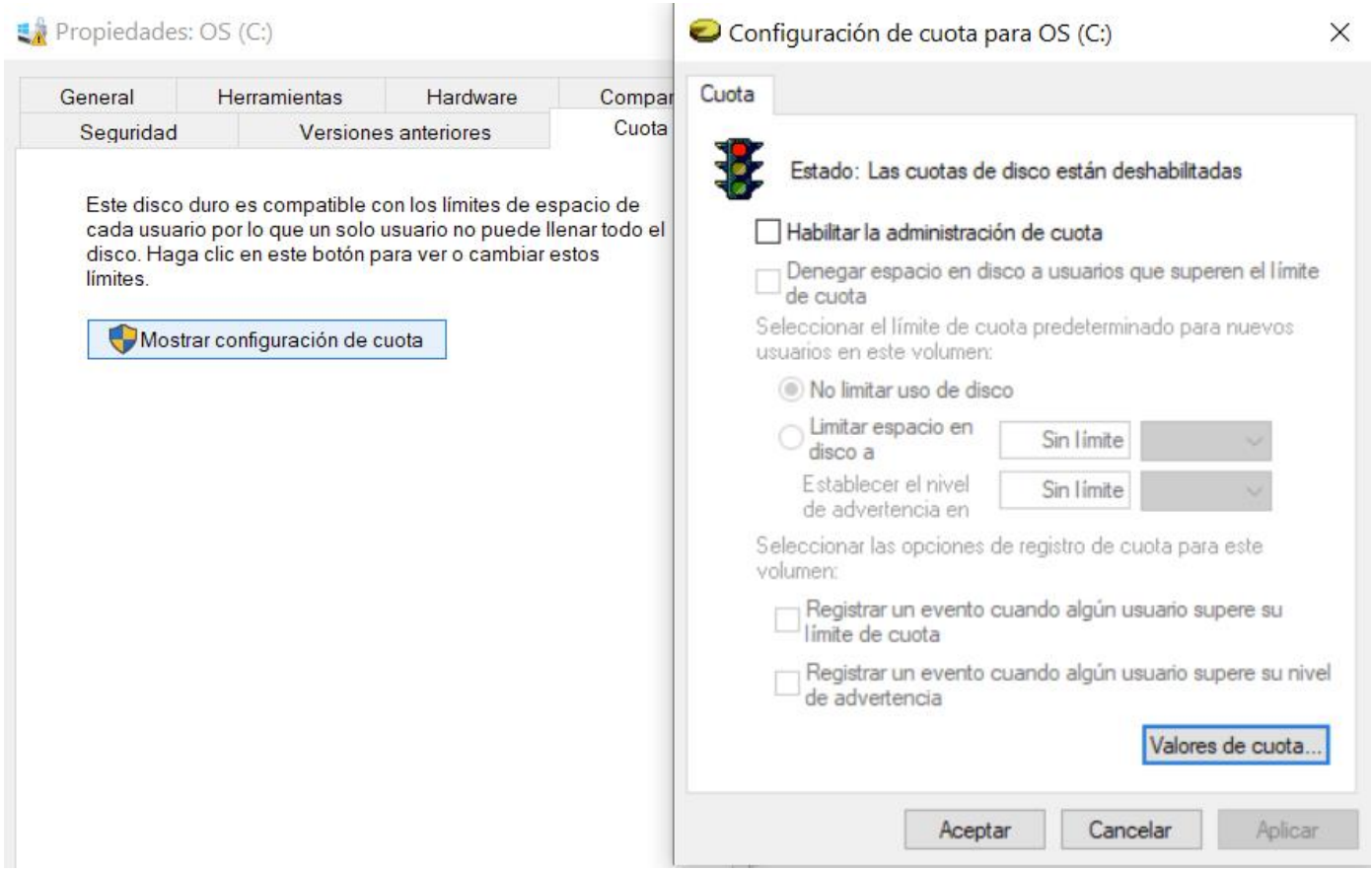
- Utiliza winget en tu máquina virtual de Windows para obtener la lista de aplicaciones instaladas
- Comprueba qué aplicaciones tienes sin actualizar y las versiones que tienes en el equipo
- Encuentra al menos una vulnerabilidad por causa de las versiones de software antiguas que tengas en el sistema. Para ello, busca las versiones de software encontradas en la base de datos de Exploit-db y en buscadores como Google o Duckduckgo
- Lleva a cabo la actualización de uno de los paquetes de software desactualizados
- Busca en winget el reproductor VLC
- Indica cuál de los repositorios instalarías y por qué. Después lleva a cabo la instalación

SEGURIDAD ACTIVA: SISTEMA OPERATIVO Y APLICACIONES

CUOTAS

La asignación de cuotas permiten que un sistema compartido tenga un uso controlado de los recursos.

Es muy habitual asignar cuota de disco a los usuarios, permitiendo usar sólo determinada cantidad de espacio



SEGURIDAD ACTIVA: SISTEMA OPERATIVO Y APLICACIONES

MONITORIZACIÓN Y ANÁLISIS DEL SISTEMA

Permite obtener información sobre **qué está ocurrien**do en el ordenador o en el sistema.

Se debe llevar a cabo periódicamente y ante situaciones anómalas: ralentización del sistema, comportamientos extraños de programas o procesos, avisos del propio sistema operativo o antivirus...

Ante una comprobación del sistema, algunas tareas que podemos llevar a cabo son:

- Comprobar los procesos en ejecución
- Comprobar el estado del sistema
- Comprobar los servicios que se ejecutan
- Comprobar las tareas programadas

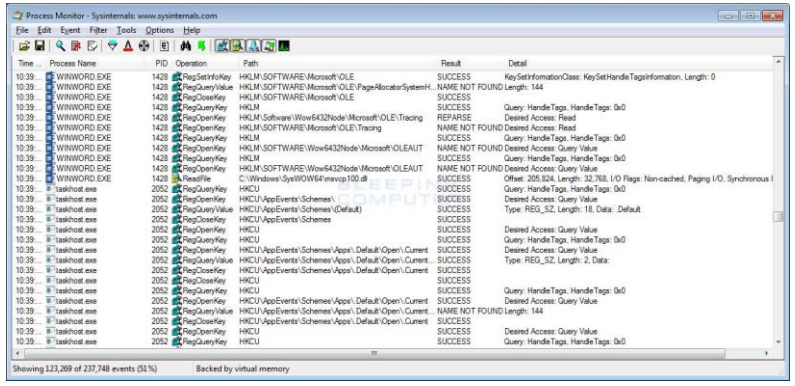
SEGURIDAD ACTIVA: SISTEMA OPERATIVO Y APLICACIONES

MONITORIZACIÓN Y ANÁLISIS DEL SISTEMA

- Comprobar los procesos en ejecución

Conviene conocer bien los procesos que se ejecutan en el sistema
En Windows podemos utilizar herramientas como:

- Taskmanager : propia de Windows
- Process Explorer: de Sysinternals. Aporta buena información sobre los procesos en ejecución
- Procmon: de Sysinternals. Informa sobre qué hace cada proceso en ejecución



Nombre	PID	Estado	Nombre de usuario	CPU	Memoria (e...
dwm.exe	1332	En ejecución	DWM-1	01	72.752 K
svchost.exe	1088	En ejecución	Servicio de red	01	8.660 K
svchost.exe	2012	En ejecución	Servicio de red	00	4.460 K
svchost.exe	2044	En ejecución	Servicio de red	00	2.448 K
svchost.exe	856	En ejecución	Servicio de red	00	764 K
svchost.exe	4516	En ejecución	Servicio de red	00	2.604 K
svchost.exe	5336	En ejecución	Servicio de red	00	544 K
svchost.exe	6704	En ejecución	Servicio de red	00	968 K
svchost.exe	9876	En ejecución	Servicio de red	00	3.124 K
WmiPrvSE.exe	12400	En ejecución	Servicio de red	00	1.792 K
WUDFHost.exe	1028	En ejecución	SERVICIO LOCAL	00	844 K

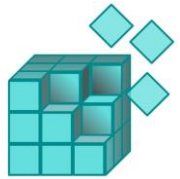
Información sobre algunos procesos habituales en Windows

SEGURIDAD ACTIVA: SISTEMA OPERATIVO Y APLICACIONES

MONITORIZACIÓN Y ANÁLISIS DEL SISTEMA

Comprobar el estado del sistema es una tarea amplia y que debe abordar varios aspectos. Por ejemplo:

- Comprobar estadísticas de uso y rendimiento en busca de anomalías.
  - eventvwr.msc (Visor de eventos)

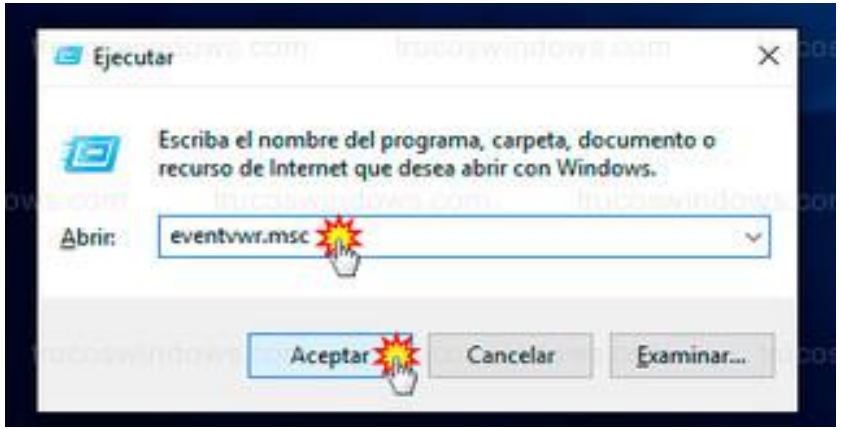


- Comprobar arranque:
  - Msconfig
  - Registro de Windows

- Comprobar tareas programada
  - Taskmanager

SEGURIDAD ACTIVA: SISTEMA OPERATIVO Y APLICACIONES

MONITORIZACIÓN



Visor de eventos:

Nos informa de varios sucesos ocurridos en el sistema.

Por ejemplo, podemos saber cuándo se arrancó, apagó o suspendió el equipo. Para a ello simplemente debemos filtrar por id de evento:

- El evento 13 con origen Kernel-General, registra fecha y hora en la que apagamos el equipo
- El evento 12 con origen Kernel-General, registra fecha y hora en la que se inició el equipo
- El evento 42 con origen Kernel-Power, registra la fecha y hora en la que entra en suspensión/hibernación el equipo
- El evento 1 con origen Kernel-General, registra fecha y hora en la que el equipo sale de un estado de suspensión

SEGURIDAD ACTIVA: SISTEMA OPERATIVO Y APLICACIONES

MONITORIZACIÓN Y ANÁLISIS DEL SISTEMA

Visor de eventos:

Cuando trabajamos con el visor de eventos debemos tener presente que no todos los eventos son errores, por lo cual debemos conocer los diversos tipos de señales del visor de eventos, estas son:

- Error Hace referencia a un problema dentro del equipo ya sea a nivel de hardware o de software.
- Advertencia: No es necesariamente un error grave del sistema, pero es una señal que debemos tomar cartas en el asunto y corregir algún error para que no sea más grave.
- Información: Mediante este mensaje se indica que un programa o aplicación está funcionando de la forma correcta y deseada.

SEGURIDAD ACTIVA: SISTEMA OPERATIVO Y APLICACIONES

MONITORIZACIÓN Y ANÁLISIS DEL SISTEMA

Visor de eventos:

Algunos de los IDs más importantes que podemos tener en cuenta son:

4624 Inicio correcto de sesión.
4625 Fallo en el inicio de sesión (nombre o contraseña incorrectos)
4634 El proceso de cierre de sesión se completó para un usuario.
4800 El equipo ha sido bloqueado.
4801 El equipo ha sido desbloqueado.

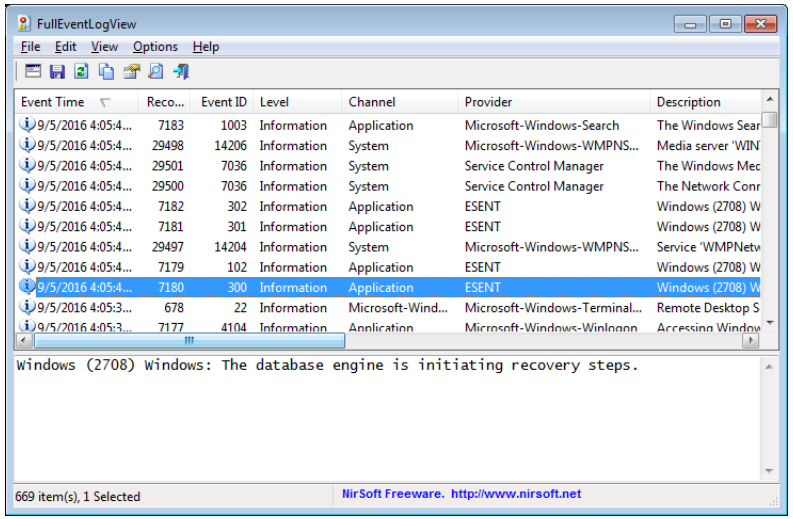
4616 La hora del sistema ha sido modificada.
5024 El servicio de Firewall ha iniciado correctamente.
5025 El servicio de Firewall ha sido detenido.
4698 - 106 Se ha creado una tarea.

SEGURIDAD ACTIVA: SISTEMA OPERATIVO Y APLICACIONES

MONITORIZACIÓN Y ANÁLISIS DEL SISTEMA

Visor de eventos:

Existen otras herramientas que simlifican la vision de eventos del sistema como FullEventLogView
https://www.nirsoft.net/utils/full_event_log_view.html

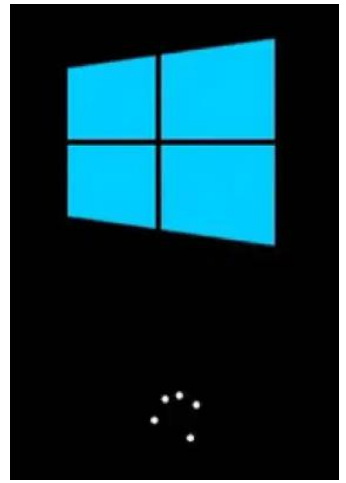


SEGURIDAD ACTIVA: SISTEMA OPERATIVO Y APLICACIONES

MONITORIZACIÓN Y ANÁLISIS DEL SISTEMA

Comprobar el arranque

Para comprobar los procesos que se arrancan al inicio podemos verlo de varias formas:



- En el Administrador de Tareas. Desde W8 tiene una pestaña llamada Inicio donde habilitar/deshabilitar el arranque de programas
- Con aplicaciones externas
- Editando el registro. Observando las siguientes rutas:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

SEGURIDAD ACTIVA: SISTEMA OPERATIVO Y APLICACIONES

ACTIVIDADES

1. Ejecuta en tu máquina Windows el archivo KVRT.exe (no hace falta usarlo, solo arrancarlo)

Comprueba su comportamiento y deduce si es o no un virus utilizando las siguientes herramientas:

1. Administrador de tareas
2. ProccessExplorer
3. Monitor de recursos
4. ProcMon

Debes comprobar (uso de hardware, conexiones TCP/IP, a quién pertenecen las IP a las que se conecta, accesos a archivos del disco duro, accesos y modificaciones en el registro, posibles tareas programadas creadas, si se automatiza su inicio con el arranque...)

2. Realiza las siguientes acciones en tu ordenador Windows:

1. Intenta iniciar sesión con un usuario válido pero con una contraseña incorrecta
2. Inicia sesión correctamente
3. Bloquea el equipo (Windows + L)
4. Desbloquea el equipo
5. Modifica la hora del sistema
6. Detén el servicio de Firewall
7. Arranca de nuevo el Firewall
8. Crea una tarea programada que abra el “Bloc de notas” a una hora determinada

Comprueba cuáles de estas acciones se han registrado en el visor de eventos utilizando FullEventLogView.

SEGURIDAD ACTIVA: SISTEMA OPERATIVO Y APLICACIONES

ANTIVIRUS

El antivirus es un programa que detecta la **presencia de virus informáticos** (malware que altera el funcionamiento normal del ordenador sin que el usuario lo sepa o consienta) y los elimina o repara.

El Firewall es un elemento que permite filtrar las conexiones de red permitiendo o bloqueando las conexiones a distintos niveles de red (filtrando por MAC, por IP o configuración de red, por Puerto, por protocolo utilizado...)

Algunas preguntas que suelen surgir sobre los Antivirus:

- ¿Qué antivirus existen y cuál es mejor?
- ¿Por qué es necesario usar Antivirus?
- ¿Cómo funciona un Antivirus?

SEGURIDAD ACTIVA: SISTEMA OPERATIVO Y APLICACIONES

ANTIVIRUS

Otras herramientas de análisis de Malware interesantes:

- VirusTotal (y otras similares como filescan.io o https://virusscan.jotti.org/)
- Any.Run
- https://www.osi.es/es/herramientas-gratuitas/antivirus-y-cleaners
- Herramientas específicas para tareas concretas:
  - Kaspersky
    - https://www.kaspersky.com/downloads/thank-you/free-virus-removal-tool
    - https://usa.kaspersky.com/downloads/tdsskiller
  - Emsisoft
    - https://www.emsisoft.com/en/home/emergencykit/
  - ...

SEGURIDAD ACTIVA: SISTEMA OPERATIVO Y APLICACIONES

ACTIVIDAD

Descarga en una máquina virtual los archivos adjuntos. En el archivo Tools.rar

No ejecutes los programas que aparecen dentro

Ejecuta un análisis de virus en dicha máquina virtual utilizando alguna de estas herramientas :

- Con Microsoft Safety Scanner
- Con Norton Power Eraser

Analiza los archivos con las siguientes herramientas:

- Virustotal
- Filescan.io
- Any.run

SEGURIDAD ACTIVA: SISTEMA OPERATIVO Y APLICACIONES

PLAN DE CONTINGENCIA

Dentro de la seguridad informática se denomina **plan de contingencia** (también de recuperación de desastres o de continuación de negocios), a la definición de acciones a realizar, recursos a utilizar y personal a emplear en caso de producirse un acontecimiento intencionado o accidental que inutilice o degrade los recursos informáticos o de transmisión de datos de una organización.

Debe considerar todos los componentes del sistema:

- Datos críticos
- Equipo lógico de base
- Aplicaciones
- Equipos físicos y de comunicaciones
- Documentación
- Personal.
- Todos los recursos auxiliares: suministro de potencia; sistemas de climatización; instalaciones; etc.

Plan de contingencia

Etapas fundamentales de un Plan de Contingencia.

- **Definición general** del plan: qué va a incluir, quién lo hará, cuándo...
- Determinación de **vulnerabilidades**: conocer las consecuencias que tendría la ocurrencia de un siniestro.
  - Identificación de aplicaciones y sistemas críticos.
  - Período máximo de recuperación.
- Selección de los **recursos alternativos**: analizar y determinar las alternativas más convenientes en términos de costo-rendimiento
- **Preparación detallada** del plan: acciones a tomar, los actores a involucrar, los recursos a emplear, procedimientos a seguir, etc.
- **Pruebas y mantenimiento**

SEGURIDAD ACTIVA: SISTEMA OPERATIVO Y APLICACIONES

PRÁCTICA

Como jefe/a del departamento de seguridad del instituto debes diseñar un plan de contingencia para esta clase. Debe incluir:

Listado **completo** de todos los componentes críticos indicando el tipo de componente (Datos, aplicaciones, equipos físicos, equipos lógicos, dispositivos de comunicaciones, documentación y personal)

Por cada componente:

- **Valoración** de consecuencias ante un siniestro
- **Alternativas** en caso de fallo en la disponibilidad
- **Acciones** necesarias para que funcione el plan añadiendo una pequeña descripción y cuándo debe llevarse a cabo

Referencias

Seguridad informática. **José Fabián Roa Buendía**. **McGraw-Hill** España, 2013.

Seguridad informática (Edición 2020) **POSTIGO PALACIOS**, **ANTONIO**. Ediciones Paraninfo, S.A., May 19, 2020