

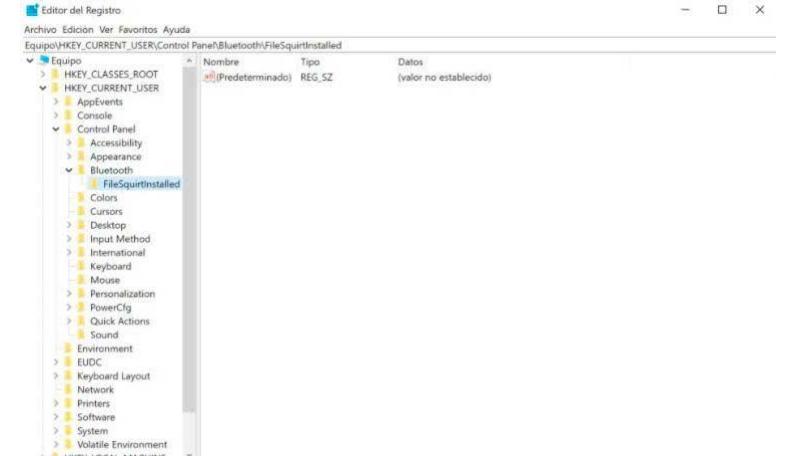
# SISTEMA REGISTRO

# Factores

- 1. Determinación del nivel de registros necesarios, los períodos de retención y las necesidades de almacenamiento.
- 2. Análisis de los requerimientos legales en referencia al registro.
- 3. Selección de medidas de salvaguarda para cubrir los requerimientos de seguridad del sistema de registros.
- 4. Asignación de responsabilidades para la gestión del riesgo.
- 5. Alternativas de almacenamiento para los registros del sistema y sus características de rendimiento, escalabilidad, confidencialidad, integridad y disponibilidad.
- 6. Guía para la selección del sistema de almacenamiento y custodia de los registros.

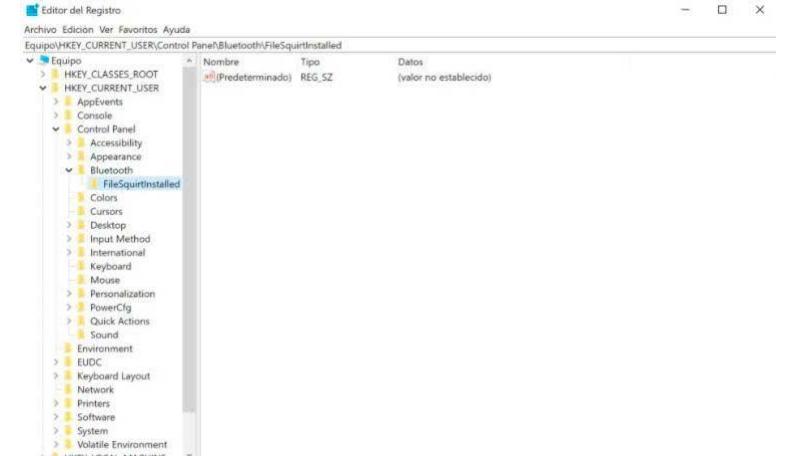
# Elementos de registro en WINDOWS: Editor de Registro

- El Editor de Registro es una herramienta o utilidad gráfica que viene incluida dentro del sistema Microsoft Windows. Esta utilidad nos permite realizar modificaciones en el Registro del Sistema de una forma visual y sencilla.
- Aunque la interface sea sencilla y muy visual hay que ir con cuidado. Una mala modificación del Registro del Sistema podría volverlo inestable. Es por este motivo, que siempre recomendamos realizar una copia de seguridad antes de realizar cualquier cambio.



# Elementos de registro en WINDOWS: Editor de Registro

- El registro del sistema no es más que una base de datos que se encarga de guardar los diferentes ajustes y configuraciones de Windows.
- Este registro es usado para salvaguardar ajustes de los distintos programas, así como de los dispositivos hardware, las preferencias de los usuarios y la configuración del sistema operativo.
- Cada vez que se instala un nuevo programa el entorno Windows se añade en el Registro de Windows un nuevo conjunto de instrucciones específicas para ese programa.



## Editor del Registro

The screenshot shows the Windows Registry Editor window. On the left is a tree view of registry keys under 'Equipo\HKEY\_CURRENT\_USER'. A green arrow labeled 'Rama' points to the 'Console' key. Another green arrow labeled 'Clave' points to the 'FontSize' value under 'Console'. The right pane lists the values of the 'Console' key in a table format. A green arrow labeled 'Valores' points to the 'FontSize' value in the table.

Nombre	Tipo
EnableColorSelection	REG_DWORD
ExtendedEditKey	REG_DWORD
ExtendedEditKeyCustom	REG_DWORD
FontFamily	REG_DWORD
FontSize	REG_DWORD
FontWeight	REG_DWORD
FullScreen	REG_DWORD
HistoryBufferSize	REG_DWORD
HistoryNoDup	REG_DWORD
InsertMode	REG_DWORD

Valores

# Claves

- Las claves de registro contienen valores de registro, tal y como carpetas convencionales pueden contener diferentes tipos de documentos. Este tipo de claves también pueden llegar a alojar otras claves de registro conocidas como subclaves.

# Claves

- **HKEY\_LOCAL\_MACHINE**: Aquí encontramos todas las variables importantes del sistema, así como las configuraciones que son imprescindibles para un funcionamiento óptimo de Windows. En esta clave están agrupadas las configuraciones del software y hardware del PC, como la configuración de la tarjeta gráfica, de la tarjeta de red, etc.
- **HKEY\_USERS**: Esta clave contiene las preferencias de todos los usuarios. La clave **HKEY\_CURRENT\_USER** hace parte de ella.
- **HKEY\_CURRENT\_CONFIG**: Esta clave contiene información sobre la configuración actual del hardware.

# Claves (II)

- **HKEY\_CURRENT\_USER**: En esta clave se almacenan las preferencias del usuario actual, como el fondo de pantalla, el salvapantallas, etc. Allí encontramos otras claves importantes:
- AppEvents (asociaciones de sonidos a los diferentes eventos del sistema)
- Control Panel (configuración del Panel de control específico al usuario)
- Environment (variables del usuario como TEMP y TMP)
- Network (Protocolos, servicios y vínculos de red)
- KBoard Layout (variables regionales del teclado)
- Printers (configuración de las impresoras)
- RemoteAccess (acceso remoto a la red)
- Software (configuración y opciones de los programas instalados)

# Claves (III)

- **HKEY\_CURRENT\_ROOT:** También la encontramos bajo HKEY\_LOCAL\_MACHINE\Software\). Ella contiene los enlaces entre los diferentes tipos de archivo y las aplicaciones que se encuentran allí (por ejemplo "\*.doc=Win word", "\*.xls=Excel" ...). Todos los tipos de archivos del sistema están referenciados allí, así como las rutinas de arrastrar/mover.

- Si el Administrador de tareas está desactivado, por ejemplo por un virus, puede volver a activarlo modificando la clave de registro `DisableTaskMgr` que puede encontrar en `HKEY_CURRENT_USER\Software\ Microsoft\Windows\Current Version\Policies\System`.

# LOGS DE EVENTOS

- El administrador puede designar ubicaciones para registros individuales dentro de las siguientes llaves del registro de Windows.
- HKLM\SYSTEM\CurrentControlSet\Services\EventLog\Application
- HKLM\SYSTEM\CurrentControlSet\Services\EventLog\System
- HKLM\SYSTEM\CurrentControlSet\Services\EventLog\Security

- De forma predeterminada, Visor de eventos archivos de registro usan la extensión .evt y se encuentran en la carpeta %SystemRoot%\System32\winevt\Logs.
- El nombre del archivo de registro y la información de ubicación se almacenan en el Registro.

# Registro eventos en los registros

- **Registro de aplicación**
- El registro de aplicación contiene eventos que registran los programas. Los eventos que se escriben en el registro de aplicaciones los determinan los desarrolladores del programa de software.
- **Registro de seguridad**
- El registro de seguridad contiene eventos como intentos de inicio de sesión válidos y no válidos. También contiene eventos relacionados con el uso de recursos, por ejemplo, al crear, abrir o eliminar archivos. Debe iniciar sesión como administrador o como miembro del grupo Administradores para activar, usar y especificar qué eventos se registran en el registro de seguridad.
- **Registro del sistema**
- El registro del sistema contiene eventos que registran los componentes del sistema de Windows. Estos eventos están predeterminados por Windows.

# Registro eventos en los registros (SERVER)

- **Registro del servicio de directorio**
- El registro del servicio de directorio contiene eventos relacionados con Active Directory. Este registro solo está disponible en controladores de dominio.
- **Registro del servidor DNS**
- El registro del servidor DNS contiene eventos relacionados con la resolución de nombres DNS hacia o desde direcciones de protocolo de Internet (IP). Este registro solo está disponible en servidores DNS.
- **Registro del servicio de replicación de archivos**
- El registro del servicio de replicación de archivos contiene eventos que se registran durante el proceso de replicación entre controladores de dominio. Este registro solo está disponible en controladores de dominio.

# LOGS DE EVENTOS A SUPERVISAR

- Para ejecutar el Visor de eventos, desde el menú **Inicio**, teclee **eventvwr.msc**
- **Auditar eventos de inicio de sesión**
- <https://learn.microsoft.com/es-es/windows/security/threat-protection/auditing/basic-audit-logon-events>
- **Eventos para supervisar**
- <https://learn.microsoft.com/es-es/windows-server/identity/ad-ds/plan/appendix-l--events-to-monitor>

# Registro de linux

- `cd /var/log`

# Eliminación de huellas tras una intrusión

- Lo primero que debemos tener presente es qué metodología de intrusión hemos realizado, qué puertos y servicios han vulnerado.
- Durante una intrusión se hace uso de gran cantidad de herramientas:
- troyanos, puertas traseras, sniffers para capturar tráfico de red, servicios del propio sistema víctima, etc.

# Empleando “Wevtutil”

- copiar en un
- archivo el listado de los distintos eventos acontecidos en el sistema,
- para posteriormente poder buscar la palabra “security”, y localizar de
- esta manera aquellos eventos relacionados con la seguridad del
- sistema que tengamos que eliminar.
- • C:\>wevtutil el > logs.txt
- • C:\> type logs.txt | find /i “security”

- Con la opción “gl” se muestra la información de configuración del “log” determinado, lo cual incluye si el “log” está habilitado o no, el límite máximo correspondiente al tamaño del archivo “log”, y la ruta al archivo donde se almacena el archivo de registro.
- C:\> wevtutil gl Security
- Mediante la opción “gli” se muestra la información sobre el estado del log especificado.
- C:\> wevtutil gli Security

- • C:\> wevtutil gl Security
- Mediante la opción “gli” se muestra la información sobre el estado del log especificado.
- • C:\> wevtutil gli Security
- Una vez hayamos identificado el nombre del log que queremos eliminar, se procede al borrado de la totalidad del archivo de registro de eventos “Security”. Evidentemente se podrá eliminar cualquier archivo de registro de eventos. A continuación lanzamos el comando para la eliminación completa del archivo seleccionado.
- • C:\> wevtutil cl Security
- A partir de este momento los eventos de seguridad quedan eliminados.
- Si procedemos a visualizar contenido del archivo log “Security” con el Visor de Eventos de Windows, veremos que se registra únicamente la existencia de un solo evento.

## b) Empleando “PowerShell”

- PS C:\>Clear-Eventlog -Log Application, System
- • PS C:\>Get-WinEvent -ListLog Application,Setup,Security -Force
- | % { Wevtutil.exe cl \$\_.Logname }
- Debemos saber que mediante estas acciones de limpieza no se realiza, sin embargo, un borrado seguro del directorio donde residía el archivo.
- Es por ello que tras un análisis forense podría posiblemente recuperarse (total o parcialmente) el archivo log, y por ende los eventos que éste contenía

# Empleando “Metasploit”

- Si la intrusión la hemos realizado obteniendo una “Shell meterpreter”,
- también podemos hacer uso de las propias herramientas de Metasploit
- para llevar a cabo el borrado de huellas. Para ello deberemos cargar el
- módulo “incógnito” y posteriormente llamar al comando “clearev”:
  - meterpreter> load incognito
  - meterpreter> clearev
  - [\*] Wiping 102 records from Application...
  - [\*] Wiping 236 records from System...
  - [\*] Wiping 48 records from Security...

# Empleando “Clearlogs”

- Se trata de
- “Clearlogs”. Su uso es muy simple, basta con lanzar el comando
- “clearlogs.exe -sec”. Podemos descargar la herramienta en el siguiente
- enlace:
- <https://sourceforge.net/projects/clearlogs/>

- /var/log/message: registro de mensajes generales del sistema
- /var/log/auth.log: log de autenticación
- /var/log/kern.log: registro del kernel
- /var/log/cron.log: registro de crond
- /var/log/maillog: registro del servidor de mails
- /var/log/qmail/ : registro de Qmail
- /var/log/httpd/: registro de errores y accesos a Apache
- /var/log/lighttpd: registro de errores y accesos a Lighttpd
- /var/log/boot.log : registro de inicio del sistema
- /var/log/mysqld.log: registro de la base de datos MySQL
- /var/log/secure: log de autenticación
- /var/log/utmp or /var/log/wtmp : registro de logins

# Eliminación de huellas tras una intrusión LINUX

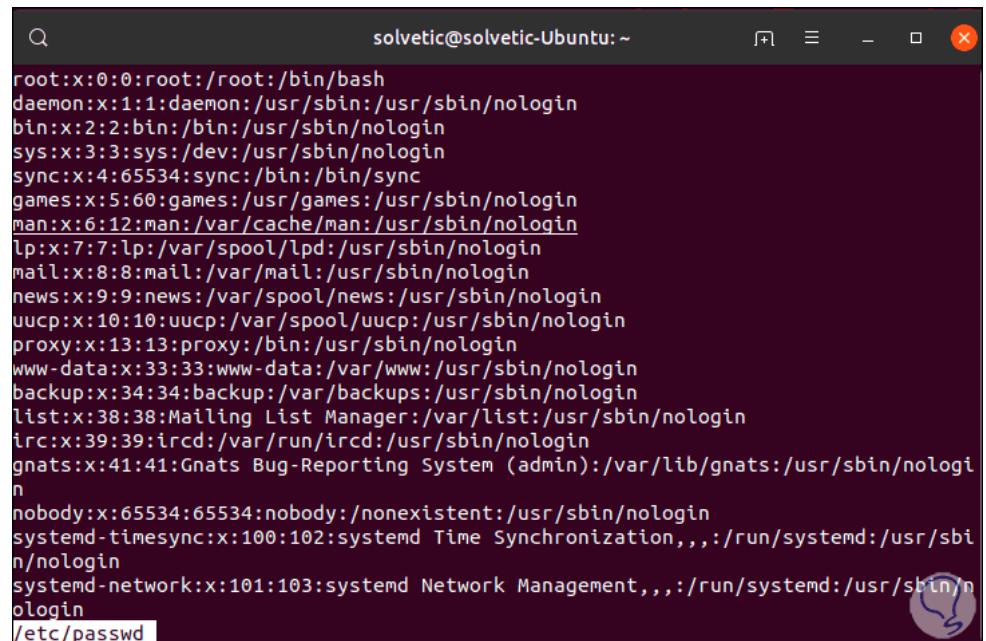
- Un buen método para llevar a cabo la eliminación de estos “logs”, es
- mediante el empleo de la herramienta “Shred” (comando “shred -zu
- ‘\*.log’ ”) . Se trata de una herramienta que destruye y hace
- prácticamente imposible la recuperación de aquella información
- almacenada en disco.

# Inhabilitar el sistema de la víctima

- La forma más común consiste en
- inhabilitar la entrada al sistema (el login), y causar un destrozo del
- sistema por dentro, de forma que no pueda recuperarse sin antes
- formatear el sistema.
- Se presentan algunos archivos de interés:
- /etc/passwd
- /etc/shadow
- /bin/login
- /etc/inetd.conf

# Lista usuarios Linux

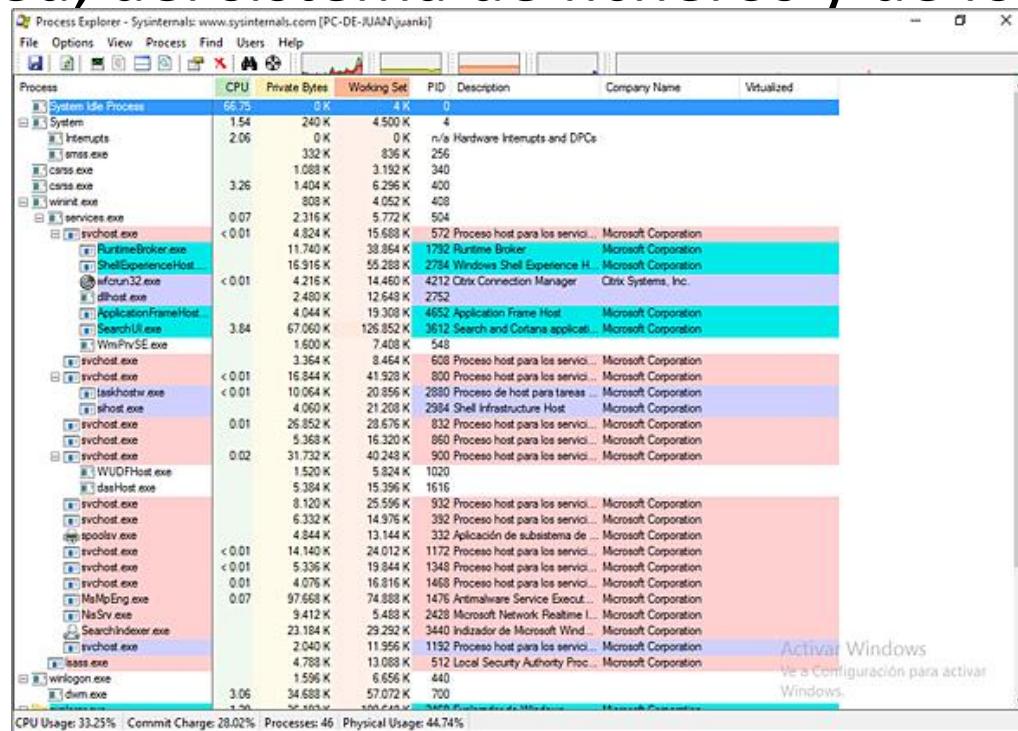
- /etc/passwd
- Nombre de usuario actual
- Contraseña cifrada (la letra x indica que la contraseña es alojada en el archivo /etc/shadow)
- Número de identificación de usuario (UID)
- Número de identificación del grupo del usuario (GID)
- Nombre completo del usuario (GECOS)
- Directorio de inicio de usuario
- Shell de inicio de sesión (por defecto en /bin/bash)
- Otra opción: getent passwd



```
Q solvetic@solvetic-Ubuntu:~ Q
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
/etc/passwd
```

# Sysinternals Suite

- La suite Sysinternals está compuesta por numerosas utilidades para la gestión de la seguridad, de la red, del sistema de ficheros y de los discos, así como del sistema



<https://technet.microsoft.com/es-es/sysinternals/bb842062>