Configuración de Usuarios

Transcribed on August 3, 2025 at 1:10 PM by Minutes AI

Speaker 1 (00:03)

Bienvenidos a una nueva sesión.

En esta sesión vamos a hablar de la configuración de usuarios locales, vamos a hablar sobre los perfiles de usuarios, cómo podemos configurarlos y cómo tenemos que administrarlos y luego hablaremos también del proceso de inicio de sistema que está muy relacionado con el perfil del usuario.

Una de las bases de la seguridad informática es la ley del mínimo privilegio.

Desde Windows Vista el usuario administrador viene por defecto deshabilitado.

Lo ideal es tener un usuario con privilegios de administrador y otro, que es el que vamos a utilizar habitualmente, que sea un usuario sin privilegios.

Los usuarios de un equipo tendrá un directorio para su documentación denominado users, donde solo puede acceder ese usuario.

En un entorno de dominio los usuarios son identidades del dominio, no son identidades del equipo, entonces generalmente se van a gestionar de forma segura desde el controlador de dominio y se van a almacenar en la base de datos del controlador de dominio.

Además se puede redirigir el directorio de los usuarios a un servidor central para fortificar la seguridad y tener una administración centralizada.

En los entornos locales es bueno almacenar los datos del usuario en un volumen separado del sistema.

Esto nos va a permitir administrar los permisos, las cuotas de disco y también los procesos de respaldo y restauración de datos.

Los perfiles de usuario se almacenan junto con su identificador de seguridad en la ruta del registro que tenéis en la diapositiva dentro de Local Machine.

Software Microsoft Windows NT Current Version Profit Lights Para modificar la ruta del perfil podemos hacerlo de varias maneras.

Podemos modificar el valor de Profil Image Page Path para cada usuario o podemos modificar la ruta base a partir de la cual se crean los perfiles configurando una variable.

Es importante copiar la carpeta Default User y allusers respetando los permisos originales para que Windows busque el perfil modelo para aplicarlo a los nuevos usuarios.

Los nuevos usuarios se van a alojar en esa ruta y el valor de la variable de entorno UserProfile será la nueva carpeta con el nombre de usuario.

Los usuarios existentes pueden cambiar de ubicación con el comando xcopy.

Después habrá que realizar los cambios en el registro de forma manual para esas claves de registro.

Vamos a ver cómo podemos trabajar con la creación de usuarios.

Nos vamos a la máquina virtual y tenemos en Windows varias maneras de trabajar con los usuarios.

Si nos vamos a la parte de botón de Inicio, Configuración, Seleccionamos el usuario y vemos que estamos utilizando un usuario local.

En este caso esto quiere decir que nosotros vamos a tener el usuario almacenado con sus secretos y sus credenciales en el disco del dispositivo.

Y también tenemos que tener en cuenta que algunas características o algunas funciones no van a estar habilitadas porque necesitaríamos utilizar un usuario tipo usuario online, un usuario de Microsoft 365, de Office 365 o un usuario tipo Hotmail o tipo upload.

Bueno, aquí tendríamos las diferentes opciones relacionadas con el usuario.

Si nos vamos por ejemplo a la parte de correos y cuentas, pues evidentemente lo que nos va a decir es que necesitamos utilizar un usuario que esté conectado con la nube para poder recibir el correo.

Entonces tendríamos que añadir aquí las cuentas y podríamos iniciar sesión con ese usuario.

En las opciones de inicio de sesión nos va a pasar un poco lo mismo.

Para ir a la parte de opciones de inicio de sesión, pues tendríamos aquí las diferentes características con los que nosotros podríamos iniciar sesión y algunas configuraciones que tendríamos aquí disponibles.

Pero todas estas características o la mayor parte de estas características van a requerir también que utilicemos una cuenta de usuario tipo Microsoft 365.

Tendríamos aquí la posibilidad también de acceder a la parte del backup y dentro de la parte de backup vamos a tener también las opciones de sincronización.

Pero igual que nos pasa con otras características, necesitamos una cuenta de Microsoft.

Los equipos son compatibles con cuentas tipo Google para algunas características no necesariamente tiene que ser una cuenta de Microsoft, pero hay ciertas características que vamos a necesitar que sea una cuenta tipo Microsoft 365 o que sea una cuenta tipo Office 365 para poder sincronizarse, por ejemplo con un servicio de OneDrive de almacenamiento que nosotros tengamos en la nube.

Si nos vamos a la parte de otras cuentas, desde aquí nosotros vamos a poder añadir otras cuentas de usuario.

Nos va a aparecer un asistente que nos va a guiar en el proceso de instalación.

Este asistente nos va a indicar aquí que pongamos el nombre, la contraseña y después nos va a pedir una serie de preguntas de seguridad.

Mucho ojo con las preguntas de seguridad de este tipo porque pueden ser un agujero de seguridad importante.

Lo recomendable es que nosotros pongamos aquí valores que no sean verdaderos porque si no alguien mediante ataques de ingeniería social podría acceder a estos datos y después podría utilizar estas preguntas para acceder a una cuenta de la que no se conoce la contraseña.

Entonces mucho ojo con este tipo de cuestionarios.

Daríamos a siguiente y nosotros ya tendríamos aquí esta cuenta de usuario local.

Una vez que nosotros tenemos la cuenta vamos a poder venir aquí y vamos a poder cambiar el tipo de cuenta, que veis que por defecto es un usuario estándar, pero nosotros podríamos también crear o convertir esta cuenta en un usuario administrado.

Otras maneras que tenemos de trabajar con las cuentas de usuario es también a través de la administración de dispositivos.

Si nos vamos a la parte de administrador de equipo vemos que tenemos aquí usuarios y grupos y dentro de la parte de usuarios y grupos, en la parte de usuarios podemos generar un nuevo usuario, nos va a aparecer también o asistente.

Vemos que una vez que tenemos el usuario vamos a tener la posibilidad de cambiarle el password y también en la parte de propiedades vamos a tener la posibilidad de seleccionar si este usuario que por defecto pertenece al grupo de usuarios, queremos que pertenezca por ejemplo al grupo de administradores.

También nos va a permitir trabajar con el perfil del usuario, nosotros podemos redirigir el perfil del usuario bien a una ruta local o bien a una ruta en un servidor.

Esto podemos hacerlo a la hora de crear el usuario, aunque en entornos por ejemplo empresariales, en entornos de dominio, pues normalmente lo vamos a hacer a través de directivas de un.

Tenemos una tercera forma de trabajar con la parte de los usuarios que sería a través del panel de control.

Si nos vamos a la parte del panel de control, en la parte del panel de control nos vamos a la parte de usuarios y dentro de la parte de los usuarios podemos nuevamente administrar otra cuenta y desde aquí podríamos crear otro usuario, vemos que nos redirige a la parte de configuración y crearíamos desde aquí otro usuario con las mismas condiciones de estos usuarios que nosotros hemos creado.

Si seleccionamos cualquiera de estos usuarios desde aquí podemos cambiar el nombre del usuario, podemos cambiarle el password, podemos cambiar el tipo de cuenta, podemos borrar esa cuenta o ir a la administración de otra cuenta diferente.

El proceso de arranque del sistema va a implicar la ejecución de multitud de programas, algunos se ejecutan de forma general para todos los usuarios del equipo y otros se van a ejecutar para un usuario específico que inicia sesión.

El malware puede tratar de alojarse en un punto de ejecución durante el proceso de arranque para mantenerse en el sistema después de la infección y pasar desapercibido.

De esta manera se va a cargar en cada inicio de sesión de ese usuario o en cada arranque de ese dispositivo.

Normalmente los lugares del registro suelen ser Local Machine o currentuser y los últimos sistemas de Windows.

El usuario tiene menos privilegios, no puede escribir en la rama global, por lo que es más frecuente el contexto de usuario actual.

¿Cómo funciona el proceso de arranque de Windows?

Bueno pues primero sesión manager que es SMSS, va a levantar el modo usuario.

Antes de ese punto se ejecutan algunos programas como el que comprueba la integridad del disco, por ejemplo autocheck alojado en la rama de registro que tenéis en la diapositiva.

En la rama de registro de Session Manager del directorio System se va a ejecutar el bus de Secund.

Luego se van a ejecutar los servicios en modo automático, la pantalla de usuario y contraseña y se va a cargar la interfaz gráfica del usuario.

GINA es una librería dinámica que recoge los datos de WinLogo y lanza el proceso de Explorer.

Exe y crea User Init que creará el entorno del usuario.

Explorer.

Exec maneja el escritorio y la barra de herramientas creando un token y permisos del usuario, el resto del proceso se le dan los permisos de éste.

Finalmente se ejecutan los diferentes Run y los programas de la carpeta de NI.

Aquí tendríais un poco lo que sería el ejemplo de la rama del registro donde tenemos winlogo y los diferentes elementos que tendríamos disponibles.

Existen otros puntos de ejecución que pueden hacer que un software se lance de forma automatizada.

En algunos casos el malware va a tratar de utilizar estos puntos de ejecución.

Tenemos una herramienta muy interesante sysinternal que es Start To que nos va a permitir el poder verificar los diferentes programas de inicio o las diferentes ejecuciones que tenemos en los diferentes puntos de ejecución.

Entre ellos estaría Load que es una clave heredada que todavía puede ser usada para lanzar programas.

Notify utilizada para especificar un programa que se ejecuta con ciertos eventos.

App Initll que esta rama especifica las librerías DLL que pueden ser cargadas junto a los procesos del sistema y cada proceso cargado por User DLL va a cargar las librerías de esta rama del registro.

A partir de Windows Vista viene deshabilitado por defecto porque existían ciertos ataques conocidos sobre esta rama específica del registro.

Msconfig nos permite manejar de forma gráfica algunos elementos del arranque de Windows y además permite modificar los archivos Bootini, Winini y Systemini.

Puede filtrar servicios que pertenecen a Windows, lo cual es un elemento muy útil que nos va a permitir verificar que vamos a tener disponible en el arraigo.

Msconfig también sirve para lanzar algunas herramientas de recuperación.

Vamos a ver cómo es msconfig.

Nos vamos a la máquina virtual, lanzamos msconfig y aquí vamos a tener disponible la herramienta.

Vemos que tenemos la capacidad de modificar el proceso de inicio del sistema, donde podemos seleccionar diferentes elementos y podemos seleccionar cómo queremos que se cargue diferentes elementos del sistema operativo.

Tendríamos la parte debut, donde también nosotros aquí vamos a poder hacer configuraciones en la parte de arranque del equipo y en las opciones avanzadas tendríamos más posibilidades de configurar esto en función de la necesidad específica que nosotros tengamos para recuperarnos de un error o para hacer un determinado análisis de malware o para investigar qué es lo que está sucediendo en el arranque del dispositivo.

Tendríamos aquí la parte de servicios, donde además podemos ocultar aquellos servicios que están relacionados con Microsoft.

Vemos que en esta máquina, si nosotros hacemos eso, lo único que vamos a tener es el servicio de VirtualBox.

Y luego tendríamos aquí la parte de Startup.

Dentro de la parte de startup de inicio, en las últimas versiones de Windows se ha derivado esta funcionalidad al administrador de tareas, de tal forma que si nosotros lanzamos desde aquí el administrador de tareas, nos va a ir a la parte de herramientas que se van a lanzar en el inicio y podemos hacer un análisis de aquellos elementos que arrancan junto al equipo y qué impacto tienen esos elementos en el arranque del dispositivo.

Finalmente con msconfig vamos a tener aquí una serie de herramientas que nosotros podemos lanzar desde aquí el control de cuentas de usuario, el administrador de equipos, información sobre el sistema.

De tal forma que si nosotros lanzamos cualquier herramienta vamos a tener aquí la posibilidad de lanzarla desde msconfig.

Entonces tenemos un conjunto de herramientas que podemos verificar y que nos van a servir para poder trabajar o para poder solucionar problemas dentro del dispositivo.

Como conclusión, la administración de identidades es uno de los puntos clave de la seguridad actual.

Una política adecuada de uso y administración de usuarios va a ayudar a mitigar los efectos de malware y reducir la capacidad de actuación de software malicioso y otro tipo de ataques.

El inicio o arranque del sistema es un elemento clave para evitar que los programas no autorizados permanezcan instalados en el dispositivo o se puedan ejecutar en cada inicio de sesión o arranque del equipo.

Tenemos una propuesta de ejercicio que es que creéis dos usuarios locales del equipo en la máquina virtual que no tengan privilegios, que sean usuarios normales y que esos usuarios para crearlos utilicemos dos consolas diferentes de creación o administración de usuarios.

Después podemos revisar también las diferentes configuraciones, las diferentes opciones de configuración de los usuarios locales.

Llegamos al final de la sesión, os esperamos en el siguiente vídeo.