

Unidad 3: Seguridad Lógica

Resultados de Aprendizaje a trabajar en esta Unidad:
RA1: Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo. **RA2:** Implanta mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante amenazas o ataques al sistema.
Contenidos a trabajar en esta Unidad:
• Principios de seguridad lógica • Control de acceso lógico • Política de contraseñas • Control de acceso en BIOS y gestor de arranque • Control de acceso al sistema operativo • Política de usuarios y grupos

Contenidos de la Unidad

1. PRINCIPIOS DE LA SEGURIDAD LÓGICA 2
2. CONTROL DE ACCESO LÓGICO 4
3. POLÍTICA DE USUARIOS Y GRUPOS 12
4. BIBLIOGRAFÍA 14

1. PRINCIPIOS DE LA SEGURIDAD LÓGICA

La **seguridad lógica** es el conjunto de medidas, normas y herramientas de software destinadas a proteger los datos, los procesos, los programas y el acceso de los usuarios a los sistemas informáticos. Es decir, consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas.

Algunas de las principales amenazas que tendrán que contrarrestar los administradores de sistemas son precisamente el acceso y modificación no autorizada a datos y aplicaciones.

Este tipo de seguridad se basa fundamentalmente en la efectiva administración de permisos, y en medidas de control de acceso basadas en la identificación, autenticación y autorización de accesos en un sistema informático.

1.1. Ciberataques

Un **ciberataque** es un intento deliberado y malicioso de acceder sin autorización, alterar, robar, destruir o interrumpir sistemas informáticos, redes, dispositivos o datos digitales. Generalmente, se llevan a cabo atacando la seguridad lógica de una empresa u organización.

Un ciberataque está compuesto por una serie de fases, o eslabones de una cadena. El modelo que describe las fases de un ciberataque se conoce como la **Cyber Kill Chain (o cadena de ciberataques)** y está formado por siete fases, cada una de las cuales supone una etapa del ataque. Su principal utilidad es permitir a los equipos de seguridad es detectar, contener o interrumpir un ataque en cualquiera de sus etapas antes de que logre su objetivo final.

Las fases o eslabones de la cadena son:

1) **Reconocimiento**: el ciberdelincuente recopila información sobre su objetivo.
2) **Preparación**: prepara el ataque de forma específica para su objetivo, utilizando la información recopilada en la fase anterior.
3) **Distribución**: se produce la transmisión del ataque.
4) **Explotación**: implica la "detonación" del ataque, comprometiendo al equipo infectado y a la red a la que pertenezca.
5) **Instalación**: el atacante instala el malware a la víctima.
6) **Comando y control:** el atacante tiene el control del sistema de la víctima, en el que podrá realizar o lanzar acciones maliciosas.
7) **Acciones sobre los objetivos**: el atacante se hace con los datos de sus objetivos, e intenta expandir su acción maliciosa hacia más objetivos.

1.2. Medidas de seguridad lógica

El éxito de un ataque dependerá en gran parte de que el sistema tenga implantadas más o menos medidas de protección.

Las principales medidas de seguridad lógica que podemos adoptar en un sistema son:

- **Política de contraseñas**: establecer requisitos para crear y gestionar contraseñas seguras, así como evitar su reutilización y protegerlas frente a accesos no autorizados.
- **Listas de control de acceso (ACL):** definir qué usuarios o grupos pueden acceder a los recursos del sistema y qué operaciones pueden realizar sobre ellos, aplicando el principio de mínimo privilegio.
- **Criptografía**: utilizar técnicas como el cifrado, las funciones hash y las firmas digitales para proteger la confidencialidad e integridad de los datos, verificar su autenticidad y facilitar el no repudio.
- **Política de almacenamiento**: organizar y gestionar el almacenamiento de los datos teniendo en cuenta el rendimiento, la capacidad, la disponibilidad y la accesibilidad, con el objetivo de evitar interrupciones del servicio y pérdidas de información.
- **Política de copias de seguridad:** establecer procedimientos para realizar copias de seguridad de forma periódica, definiendo qué información se copia, dónde se almacena, durante cuánto tiempo se conserva y cómo se recupera en caso de pérdida o incidente.
- **Protección frente al malware:** utilizar herramientas y medidas de prevención, detección y eliminación de programas maliciosos, como antivirus y sistemas de protección de los equipos.
- **Securización del software (hardening):** mantener los sistemas operativos y las aplicaciones actualizados, eliminar servicios y componentes innecesarios y aplicar configuraciones seguras para reducir las posibles vulnerabilidades.
- **Seguridad perimetral**: controlar y filtrar las comunicaciones entre redes y sistemas mediante mecanismos como cortafuegos (firewalls), servidores proxy y segmentación de redes mediante VLAN.
- **Alta disponibilidad**: implantar mecanismos de redundancia, como servidores, conexiones o sistemas de almacenamiento alternativos, para mantener los servicios operativos ante fallos de componentes o equipos.

2. CONTROL DE ACCESO LÓGICO

El control de acceso lógico es la principal línea de defensa en la mayor parte de los sistemas.

Para controlar el acceso, habitualmente se usan dos procesos:

- **Identificación**: es el momento en el que el usuario se da a conocer al sistema (teclea su nombre de usuario, por ejemplo).
- **Autenticación**: es la verificación que realiza el sistema para validar al usuario.

Por eficacia, los usuarios de un sistema deberían identificare y autenticarse una única vez, pudiendo entonces acceder a todos los recursos que el sistema permita a ese usuario. Esto se llama Single Sign-On (SSO) o sincronización de passwords. Un ejemplo de esto puede ser nuestra cuenta de Oficce365 en la que tras iniciar sesión, podemos utilizar las diferentes aplicaciones que pone a nuestra disposición (Outlook, Teams, OneDrive, etc.) sin necesidad de iniciar sesión de nuevo.

Para llevar a cabo esta técnica, se usan servidores de autenticación, encargados de verificar la identidad del usuario como servicio para otros sistemas de la organización.

Los sistemas de control de acceso protegidos por contraseña son un punto crítico para la seguridad de los sistemas, por lo que suelen ser objeto de ataques de diferentes tipos:

- **Ataques de fuerza bruta**: intentan "averiguar" claves probando todas las combinaciones posibles hasta encontrar la que permita el acceso.
- **Ataques de diccionario**: prueban combinaciones partiendo de una lista de contraseñas frecuentes (diccionario). Suelen ser ataques más eficaces que los de fuerza bruta.



Una forma de proteger los sistemas frente a los ataques de prueba y error realizados por máquinas es mediante el establecimiento de un número máximo de intentos fallidos, tras los cuales, se bloquea durante un tiempo el acceso al sistema con ese nombre de usuario. El bloqueo se puede desactivar tras un tiempo, mediante una clave de desbloqueo, o incluso necesitando alguna acción por parte de los administradores del sistema. Este es, por ejemplo, el sistema utilizado por las claves PIN de las tarjetas SIM de teléfono.

2.1. Política de contraseñas

La contraseña es la llave que nos identifica en el sistema y, al igual que no debemos dejar la llave de nuestra casa debajo del felpudo, no debemos utilizar contraseñas sencillas de averiguar, ni dejarla anotada en un post-it cerca de nuestro dispositivo.

Existen diferentes parámetros en los que podemos actuar para garantizar que las contraseñas de acceso al sistema cumplan unos mínimos de fortaleza frente a pruebas para averiguarla o descifrarla.

Para que una clave sea segura se recomienda:

- Que se requiera una longitud mínima. Se estima que 8 caracteres es el menor número que debería tener. A mayor longitud, mayor seguridad ante ataques de fuerza bruta.
- Que tenga una combinación de varios tipos de caracteres (letras, símbolos, números, mayúsculas, minúsculas). Cuanto más variada sea la contraseña, más difícil será de averiguar.

Otros consejos de seguridad básica respecto a contraseñas:

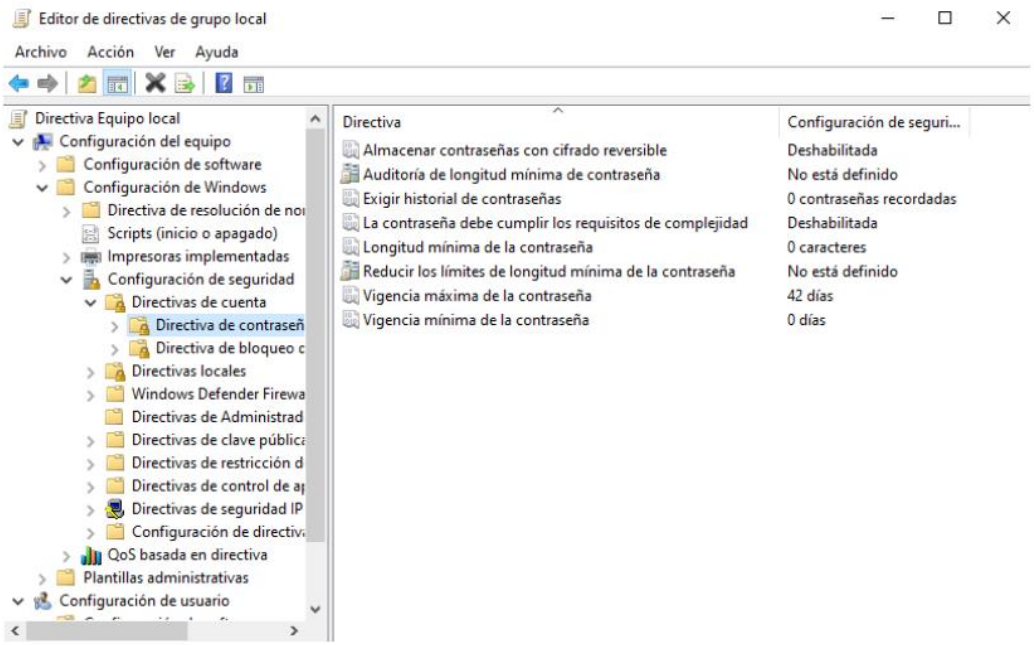
- No utilizar caracteres repetidos.
- No usar el nombre de inicio de sesión.
- No utilizar una única palabra, especialmente si aparece en el diccionario.
- No utilizar fechas importantes y fácilmente relacionables con nosotros (cumpleaños, aniversarios…).
- Tener diferentes contraseñas para diferentes entornos.
- No revelar la contraseña a nadie, ni escribirla en notas.
- Cambiar las contraseñas con regularidad.

2.2. Contraseñas seguras en Windows 10

En Windows 10, las políticas de contraseñas permiten establecer requisitos de seguridad para las cuentas de usuario, como la longitud mínima de las contraseñas, su complejidad o su periodo de validez. En Windows 11, el procedimiento para configurar las políticas de contraseñas es prácticamente el mismo

La configuración se realiza mediante las directivas de seguridad local, a las que se puede acceder de las siguientes formas:

- Mediante `secpol.msc`: abrir el cuadro Ejecutar (Windows + R), escribir secpol.msc y pulsar Enter. Se abrirá directamente la herramienta Directiva de seguridad local.
- Mediante `gpedit.msc`: abrir el cuadro Ejecutar (Windows + R), escribir gpedit.msc y navegar por la siguiente ruta: Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas de cuenta → Directiva de contraseñas.
- Desde el Panel de control: acceder a Herramientas administrativas y abrir Directiva de seguridad local. Después, seguir la misma ruta indicada anteriormente hasta llegar a Directiva de contraseñas.



Estas herramientas pueden no estar disponibles en todas las ediciones de Windows 10. Por ejemplo, el Editor de directivas de grupo local (gpedit.msc) y la herramienta de directivas de seguridad local (secpol.msc) no están disponibles de forma habitual en la edición Home.

Una vez dentro de esta sección de directivas de contraseña, podemos encontrar opciones como:

- Almacenar contraseña usando cifrado reversible. Obviamente no es recomendable tener activa esta directiva.
- Forzar historial de contraseñas: establece el número de contraseñas a recordar, y no permite repetir esas contraseñas.

- Las contraseñas deben cumplir requisitos de complejidad: fuerza a que las contraseñas cumplan unos mínimos de longitud, tipo de caracteres, no contener parte del nombre de usuario...
- Longitud mínima de las contraseñas.
- Vigencia máxima y mínima: días que la contraseña puede estar activa.

En las directivas de bloqueo de cuentas podemos encontrar:

- Duración del bloqueo de cuentas: esta configuración de seguridad determina el número de minutos que permanece bloqueada la cuenta antes de que se desbloquee automáticamente. Si se define la duración del bloqueo de la cuenta como 0, la cuenta quedará bloqueada hasta que un administrador la desbloquee.
- Reestablecer la cuenta de bloqueos después de ... : determina los minutos que deben transcurrir después de un intento de inicio de sesión erróneo para que el contador correspondiente restablezca a 0 los intentos de inicio de sesión erróneos.
- Umbral de bloqueos de cuenta: determina el número de intentos de inicio de sesión erróneos necesarios para que se bloquee una cuenta de usuario.

Por norma general, es recomendable configurar una política de contraseñas que:

- Requiera claves de al menos 12 caracteres.
- Que cumplan características de complejidad.
- Que haya que renovarlas cada X meses.
- Bloquear el acceso a la cuenta durante 15 minutos tras el tercer intento de inicio de sesión erróneo.

Para más información, se puede consultar la documentación oficial.

2.3. Contraseñas seguras en Linux

En los sistemas Linux/Unix, la autenticación de los usuarios en diferentes aplicaciones y servicios se gestiona, entre otros mecanismos, mediante PAM (Pluggable Authentication Modules), un sistema que permite configurar de forma flexible los métodos de autenticación.

PAM está formado por un conjunto de bibliotecas compartidas que las aplicaciones utilizan para comprobar la identidad de los usuarios. De esta forma, las aplicaciones delegan el proceso de autenticación en PAM, en lugar de implementar sus propios mecanismos.

Una de sus principales ventajas es que permite al administrador elegir y configurar los métodos de autenticación sin necesidad de modificar las aplicaciones. Según la configuración y los módulos disponibles, se pueden utilizar contraseñas, tarjetas inteligentes, mecanismos biométricos u otros métodos de verificación.

Por ejemplo, el inicio de sesión en una terminal, el acceso mediante SSH o el uso de determinados servicios del sistema pueden recurrir a PAM para autenticar a los usuarios.

En Linux, la configuración de PAM se encuentra habitualmente en el directorio /etc/pam.d/, donde existen archivos que definen las reglas de autenticación de diferentes servicios. Además, algunos módulos permiten aplicar políticas de contraseñas, como establecer requisitos de complejidad o limitar los intentos de autenticación.

Sus ventajas más importantes se pueden resumir en:

- Ofrece un esquema de autenticación común y centralizado.
- Permite a los desarrolladores abstraerse de las labores de autenticación.
- Facilita el mantenimiento de las aplicaciones.

Hay cuatro tipos de módulos PAM que se utilizan para controlar el acceso a los servicios:

- Account: en este grupo se engloban tareas que no están relacionadas directamente con la autenticación como, por ejemplo, permitir/denegar el acceso en función de la hora.
- Authentication: tareas encaminadas a comprobar que el usuario es quien dice ser.
- Password: se encarga de mantener actualizado el elemento de autenticación asociado a cada usuario como, por ejemplo, su contraseña. Acciones como comprobar la fortaleza de una clave son típicas de este grupo.
- Session: en este grupo se engloban tareas que se deben llevar a cabo antes de iniciarse el servicio y después de que este finalice. Útil para, por ejemplo, mantener registros de acceso.

En PAM, el módulo pam_cracklib es el encargado de comprobar los criterios de complejidad de las contraseñas. Se instala con la orden:

```
sudo apt-get install libpam-cracklib
```

Una vez instalado el módulo, podemos comprobar cómo han cambiado los criterios de complejidad de las contraseñas. Podemos comprobar el registro de identificaciones de usuario en el sistema (en diferentes situaciones) examinando el contenido del archivo /var/log/auth.log

2.4. Niveles de identificación de usuario

En los sistemas informáticos existen controles de identificación a diferentes niveles:

- Primer nivel: contraseña de arranque del equipo y configuración de la BIOS.
- Segundo nivel: contraseña de entradas en el gestor de arranque del equipo.

- Tercer nivel: identificación de usuario en el inicio de sesión del sistema operativo.
- Cuarto nivel: contraseña y cifrado en el acceso a datos, archivos, sitios web, etc.

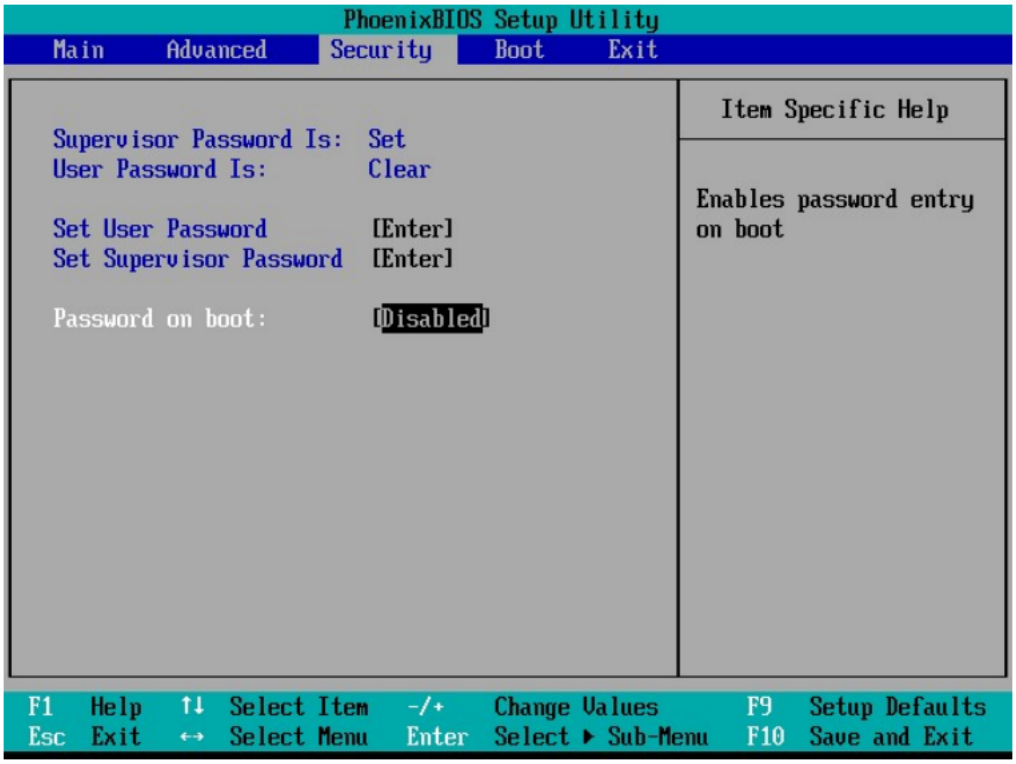
2.5. Control de acceso en la BIOS

El BIOS (Basic Input Output System) es el software de más bajo nivel que se ejecuta en el equipo. Lo componen las rutinas de gestión del hardware.

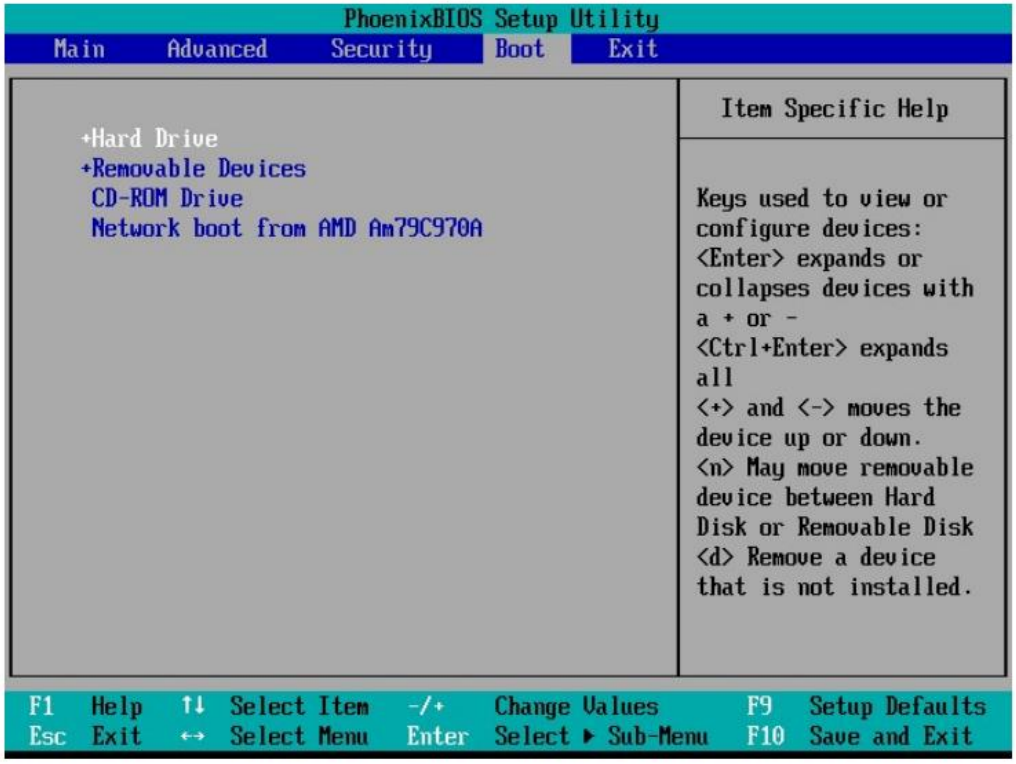
En la BIOS podemos configurar parámetros hardware de la máquina, como el reloj interno, el dispositivo de arranque, comprobaciones de memoria, configuración de caché, etc.

Debemos proteger el acceso a la configuración de la BIOS mediante contraseña para evitar accesos indebidos a la configuración del equipo. Según la marca y versión de la BIOS, podremos configurar la seguridad de acceso de diferentes formas:

- Seguridad del sistema: estableciendo una contraseña de usuario, que se pedirá cada vez que se inicie la máquina. Protege el inicio del equipo.
- Seguridad de configuración de BIOS: asignando una password de administración, de forma que no se pueda configurar la BIOS sin conocer esa contraseña. Protege la configuración del equipo.



En esta otra imagen de la BIOS se puede configurar el orden en que se comprobarán los dispositivos para realizar el arranque. Una medida de seguridad es poner el disco duro el primero, para evitar así el arranque desde dispositivos extraíbles.



Cualquier soporte extraíble que permita iniciar el equipo sin el control del sistema operativo instalado es una brecha de seguridad. Por eso es importante configurar la BIOS para impedir que el equipo inicie la ejecución de cualquier sistema operativo diferente al instalado.

Las distribuciones Live son sistemas operativos almacenados en un medio extraíble (CD, DVD, USB…) que puede ejecutarse directamente en un PC.

Iniciando el equipo desde otro soporte diferente al disco principal, es posible acceder al sistema de ficheros del equipo sin control del sistema operativo, con lo que ello supone.

Este es uno de los métodos más habituales para intentar accesos no autorizados a sistemas o al sistema de fichero de los mismos.

2.6. Recuperación de contraseñas

En función de la calidad de la contraseña, en ocasiones no será posible recuperarlas en caso de olvido.

- **Ophcrack**

Es una herramienta de recuperación de contraseñas de Windows basada en las tablas Rainbow. Es una implementación muy eficiente de las Tablas Rainbow hecha por los inventores de este método.

Al arrancar el programa intentará encontrar la contraseña de nuestro usuario mediante fuerza bruta. Lo más normal es que esto falle y es entonces cuando se cargan y utilizan las tablas Rainbow.

Las tablas rainbow o tablas arcoíris son tablas precalculadas que almacenan cadenas de valores hash obtenidos a partir de posibles contraseñas y permiten relacionar determinados hashes con contraseñas candidatas. Se utilizan para intentar recuperar contraseñas a partir de sus hashes sin tener que calcular todas las combinaciones desde cero en cada intento.

- **John the Ripper**

En las distribuciones actuales de Linux, el archivo que contiene la lista de usuarios y contraseñas es /etc/shadow, visible solo por el usuario root, a diferencia del /etc/passwd en que antes se almacenaban las contraseñas cifradas. Sin embargo, si conseguimos arrancar el equipo con un Live, podremos acceder al contenido de ese archivo.

La estructura del /etc/shadow es una línea por cada usuario del equipo, con diferentes campos separados por ":", siendo el segundo campo la contraseña cifrada:

```
techblog1:$6$Z8.HiXCD$sAqhFl4B6Kfmfp0iWEMYD8aVmJMtg2fFGNbSmk.RNKLI/C0Zx/PLPo30ZY
IVM9c3/wCl6HHvGZGPvJkVWLiuz1:14642:0:99999:7:::
techblog2:$6$5vb5UgV7$r6mPm4BOVnQdghrNl7MqgErPxuflAMsnywSjdg3ZcAWyeAWewvDiL6z02d
QlbtmQIPuICjrurtvSq0cwXBCVZ1:14642:0:99999:7:::
techblog3:$6$KtX56/ED$uq4arCzOD7rEzO7PrNgZW25VP1srTfy3LNeCUySYXY6gkrzPZAdtcJqav6
3d5Qv4ZdtyiVuluNE8bU3XooJ5I1:14642:0:99999:7:::
```

Mediante el programa "John the Ripper" podremos efectuar distintos tipos de ataques de fuerza bruta contra el archivo para intentar obtener la password de los usuarios del sistema, incluido el root.

2.7. Modificación de contraseñas

Existen herramientas tanto para Linux como para Windows que nos permiten volver a establecer la contraseña de un usuario. Si podemos reestablecer la contraseña de un administrador, tendremos una gran brecha de seguridad.

- **Windows**

La distribución UBCD (Ultimate Boot CD) para Windows, nos permite asignar una nueva contraseña a un usuario, o bien cambiar el tipo de usuario (de limitado a administrador), o incluso crear un nuevo usuario administrador.

- **Linux**

Partiendo de una distribución Live para arrancar el equipo, una vez iniciado el sistema, se puede montar el sistema de ficheros de la partición de disco, pudiendo añadir las

entradas deseadas en los archivos /etc/passwd, /etc/shadow y /etc/Group, con lo que podemos dar de alta a un usuario administrador muy fácilmente.

3. POLÍTICA DE USUARIOS Y GRUPOS

Uno de los aspectos fundamentales de la seguridad en sistemas operativos multiusuario es la definición de cuentas de usuario y su asignación a los perfiles correspondientes.

Este proceso conlleva cuatro pasos:

- Definición de puestos: separación de funciones y asignación de permisos para cada tarea.
- Identificar la sensibilidad del puesto: determinar si una función requiere permisos críticos o no.
- Elección de la persona para cada puesto: se debe considerar experiencia, perfil técnico, etc.
- Formación inicial y continua del usuario: en aspectos de seguridad del sistema.

La definición de permisos de acceso requiere determinar el nivel de seguridad necesario sobre los datos, resultando imprescindible clasificar la información y determinar el riesgo de su exposición a usuarios no autorizados.

Conviene comenzar definiendo las medidas de seguridad sobre la información sensible y aplicaciones críticas, e ir descendiendo y estableciendo las medidas de seguridad en orden de prioridad.

3.1. Control de acceso a datos

En sistemas multiusuario, en sistemas en red o en sistemas gestionados por directorio (por ejemplo, Active Directory), nos encontramos con que la seguridad de objetos del sistema (carpetas, archivos, procesos, recursos, etc.) se administra mediante el control y asignación de permisos.

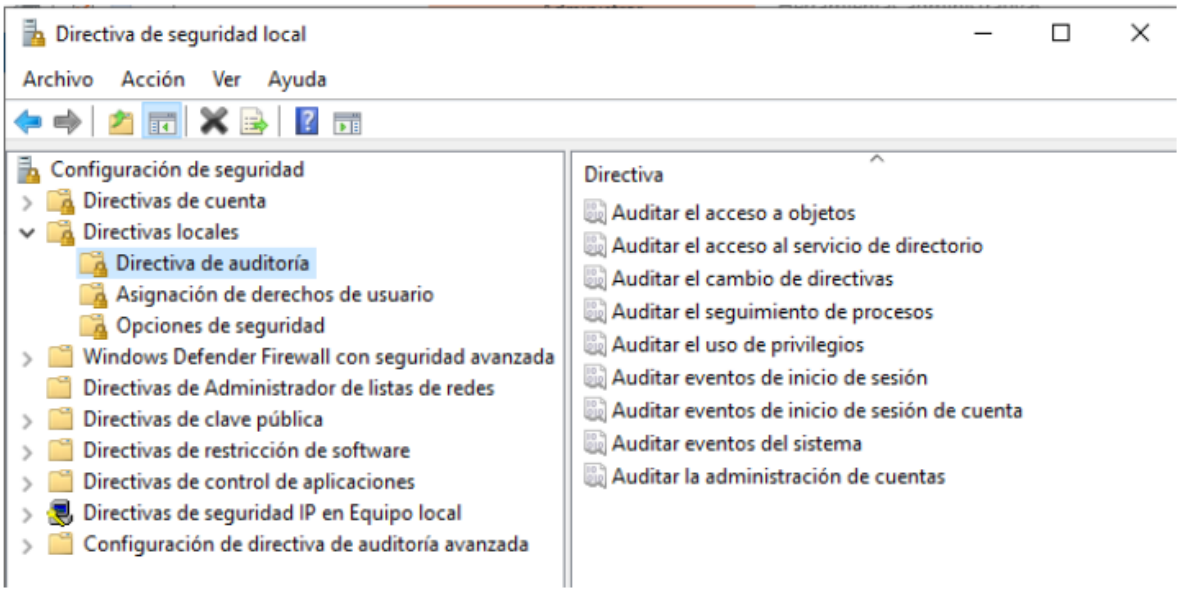
En objetos del sistema de archivos es posible establecer listas de control de acceso (ACL, Access Control List) que permiten establecer permisos de forma individual o a grupos de usuarios.

- **Windows**

Para modificar la configuración de seguridad local en sistemas Windows, se deben establecer directivas de seguridad local accediendo desde Panel de Control / Herramientas Administrativas / Directiva de seguridad local.

En este apartado podremos encontrar:

- Directivas de auditoría: establece qué sucesos de seguridad quedan registrados. Se examinan con el visor de sucesos.
- Asignación de derechos de usuario: configura qué usuarios tienen derechos de inicio de sesión, privilegios de administración...
- Opciones de seguridad: activa/desactiva las configuraciones de seguridad del equipo como firma digital de datos, acceso a unidades extraíbles, instalación de controladores, solicitud de inicio de sesión, etc.



A nivel de acceso a ficheros y directorios, la herramienta cacls permite establecer listas de control de acceso.

- **Linux / Unix**

Los permisos sobre ficheros en sistemas operativos Linux / Unix se asignan mediante la orden chmod.

Cada objeto del sistema de ficheros de Unix tiene tres grupos de permisos, para el propietario, para el grupo del propietario y para otros usuarios.

Los permisos pueden ser rwx, es decir: de lectura, escritura y ejecución.

Para asignar derechos sobre los archivos con el comando chmod entendemos cada grupo de permisos como un valor binario de tres bits, por lo que podemos asignar los permisos de forma numérica o por parámetros.

A continuación hay algunos ejemplos:

- Asignar permiso de ejecución en el archivo salida.sh para todos los usuarios.
  - chmod +x salida.sh
- Agregar permiso de ejecución sólo para el propietario del archivo
  - chmod u+x salida.sh

- Asignar en formato numérico los permisos de ejecución, lectura y escritura para el propietario, y ejecución y lectura para el resto de usuarios.
    - chmod 755 salida.sh

El comando para cambiar un archivo de grupo es chgrp, y para cambiar el propietario, chown.

Para más información, se puede consultar este tutorial.

4. BIBLIOGRAFÍA

Las 7 fases de un ciberataque. Incibe. Disponible en: https://www.incibe.es/empresas/blog/las-7-fases-ciberataque-las-conoces

Ciberataques. IBM. Disponible en: https://www.ibm.com/es-es/think/topics/cyber-attack

Documentación Windows – Cacls. Disponible en: https://learn.microsoft.com/es-es/windows-server/administration/windows-commands/cacls

Documentación Windows - Configuración de directivas de seguridad. Disponible en: https://learn.microsoft.com/es-es/previous-versions/windows/it-pro/windows-10/security/threat-protection/security-policy-settings/how-to-configure-security-policy-settings

Tablas Rainbow. Wikipedia. Disponible en: https://es.wikipedia.org/wiki/Tabla_arco%C3%ADris

Tutorial comando chmod. Desarrollo Web. Disponible en: https://desarrolloweb.com/articulos/tutorial-comando-chmod.html

Seguridad Informática. Alfonso García-Cervigón, María del Pilar Alegre. Paraninfo.

Seguridad Informática. José Fabián Roa Buendía. McGraw Hill.

Seguridad y alta disponibilidad. Ignacio Triviño Mosquera. Síntesis.