SAD - U3.3. Password Policy

Descargar estos apuntes

Índice

1. Almacenamiento de contraseñas

Ya hemos visto que, para acceder a la información almacenada en un sistema informático en primer lugar hay que superar las **barreras físicas** de acceso. Una vez superadas estas barreras, el siguiente paso en materia de seguridad será establecer unas **barreras lógicas** que impidan el acceso a nuestros datos.

La primera barrera lógica que se puede establecer es la creación de mecanismos de control de acceso a la información. Para ello, en vez de que al encender los equipos se pueda acceder directamente a todos los datos almacenados en los mismos, una primera medida sería la **creación de usuarios** para organizar la información, de forma que cada usuario únicamente pudiera acceder a la información de la cuenta para la que dispone de autorización.

Las cuentas de usuario permiten asignar a cada uno de ellos unos derechos y privilegios que restringirán las operaciones que este va a poder realizar dentro de un sistema informático, así como la posibilidad de rastrear dichas operaciones. Como sistema de verificación de la identidad de cada uno de los usuarios se suele establecer la combinación entre un nombre identificativo (usuario, user, etc.), con la de una contraseña o password.

Además, los equipos tienen instaladas distintas aplicaciones, respecto de las que se puede establecer un control de usuarios integrado con el del sistema operativo o independiente del mismo. En este caso, el acceso a las aplicaciones se realizará mediante un usuario y contraseña, que se verificarán en el sistema de autenticación de la aplicación.

Si se trabaja en un entorno de red, es posible que, para acceder a algún recurso de la misma, se exijan unas credenciales determinadas, establecidas a través de las **listas de control de acceso (ACL, Access Control List)**. Además, en las redes, los dispositivos de red, como los routers, pueden servir de barrera lógica impidiendo el acceso a determinadas zonas de la red para algunos usuarios (asignándoles un rango restrictivo de direcciones IP).

1.1. Políticas de seguridad de contraseñas

Con el fin de evitar que las amenazas a las contraseñas sean efectivas y que un usuario malintencionado pueda acceder a los datos de un sistema informático, es esencial que los usuarios y empresas establezcan unas políticas de seguridad relativas a las contraseñas.

Una política correcta de seguridad prestará atención en fijar unas normas para la elección de contraseñas que dificulten los ataques por diccionario o por fuerza bruta.

Para ello, las normas básicas son las siguientes:

- No deben ser o contener **palabras usuales** ni relacionadas con el entorno del usuario, como por ejemplo: nombres de mascotas, fechas de cumpleaños, número del DNI, etc.
- No deben ser **palabras con significado**, por ejemplo, alimento. La contraseña debería ser una combinación de mayúsculas, minúsculas, números y otros caracteres, por ejemplo: aX4t$5#. A mayor variedad de símbolos utilizada, mayor dificultad para averiguar la contraseña.
- La **longitud** de la contraseña debería ser de ocho caracteres como mínimo.
  – Hay que **evitar que el usuario utilice la misma contraseña** en varios sitios, por ejemplo, que se utilice la misma contraseña para entrar a las aplicaciones de la empresa, al correo y a redes sociales.
  – Se deben **cambiar las contraseñas proporcionadas por defecto** al registrarse por Internet en cualquier servicio.

> ⚠ **Papel del administrador del sistema**
>
> En todo caso, como administradores de sistemas, si bien hay que prestar especial atención en la formación al usuario para que cumpla todas las normas propuestas, habrá que tomar medidas adicionales para el caso de que estos no cumplan dichas normas, “forzándoles” a tomar ciertas medidas de seguridad:
>
> - Estableciendo un número máximo de intentos para acceder al sistema.
>   Por ejemplo, si el usuario introduce tres veces seguidas una contraseña incorrecta, se bloquea el acceso y solo puede ser desbloqueado por el administrador.
> - Obligando al usuario a que establezca contraseñas con un mínimo de ocho caracteres alfanuméricos que combinen, al menos, una mayúscula,una minúscula, un número y un signo de puntuación.
> - Obligando al usuario a cambiar la contraseña cada cierto tiempo (por ejemplo, cada tres meses).
> - Impidiendo al usuario repetir las tres últimas contraseñas utilizadas.

1.2. Políticas de contraseñas en Windows

Las políticas relacionadas con las contraseñas se gestionan, en los sistemas Windows, desde la **consola de Directivas de seguridad local**, que es una herramienta muy valiosa desde el punto de vista de la seguridad, ya que afina al máximo los privilegios de los usuarios y diversas directivas relacionadas con la seguridad.

En Windows tenemos dos herramientas para establecer las políticas de contraseñas:

- **Directiva de seguridad local (secpol.msc)**: es una herramienta de administración de seguridad que permite a los administradores locales establecer políticas de seguridad locales para todas las computadoras de un grupo de trabajo o para un equipo autónomo.
  Podemos abrirlo ejecutando `secpol.msc` y accediendo a la sección `Directivas de cuenta` y `Directivas de contraseña` y `Directivas de bloqueo de cuenta`. Esta herramienta nos muestra un subconjunto de las directivas de grupo que se aplican a la cuenta de usuario actual.
- **Directiva de grupo**: es una herramienta de administración de seguridad que permite a los administradores de red establecer políticas de seguridad para los equipos de un dominio de Active Directory.
  Podemos abrirlo ejecutando `gpedit.msc` y accediendo a la sección `Configuración del equipo` y `Configuración de Windows` y `Configuración de seguridad` y `Directivas de cuenta` y `Directivas de contraseña` y `Directivas de bloqueo de cuenta`.

Las opciones que permiten establecer las políticas de contraseñas en Windows son las siguientes:

- **Historial de contraseñas**: se establece el número de contraseñas que se deben recordar antes de poder volver a utilizarlas. Por defecto, en Windows 10, es de 24 contraseñas.
- Cumplir con los requisitos de complejidad de la contraseña: se establece si la contraseña debe cumplir con los requisitos de complejidad. Por defecto, en Windows 10, es de 3 de los 4 tipos de caracteres siguientes: mayúsculas, minúsculas, números y caracteres especiales.
- **Longitud mínima de la contraseña**: se establece la longitud mínima de la contraseña. Por defecto, en Windows 10, es de 7 caracteres.
- **Días que deben pasar antes de que la contraseña caduque**: se establece el número de días que deben pasar antes de que la contraseña caduque. Por defecto, en Windows 10, es de 30 días.
- **Días que deben pasar antes de que el usuario deba cambiar la contraseña**: se establece el número de días que deben pasar antes de que el usuario deba cambiar la contraseña. Por defecto, en Windows 10, es de 42 días.

Además, en Windows 10, se puede establecer una **directiva de bloqueo de cuenta** que permite establecer:

- **Duración de la cuenta bloqueada**: se establece el número de minutos que la cuenta debe estar bloqueada antes de que se pueda desbloquear. Por defecto, en Windows 10, es de 30 minutos.
- **Restablecer el contador de bloqueo de cuenta después de**: se establece el número de minutos que deben pasar antes de que se restablezca el contador de bloqueo de cuenta. Por defecto, en Windows 10, es de 30 minutos.
- **Número de intentos de inicio de sesión**: se establece el número de intentos de inicio de sesión fallidos antes de que se bloquee la cuenta. Por defecto, en Windows 10, es de 5 intentos.

1.3. Políticas de contraseñas en Linux

En Linux también podemos definir directivas de seguridad a la hora de asignar contraseñas a los usuarios. Para ello, se utilizan las librerías `libpam` (Pluggable Authentication Modules) que permiten establecer políticas de contraseñas en el sistema.

El `sistema PAM` es un sistema de autenticación flexible que permite a los administradores de sistemas establecer políticas de contraseñas, de bloqueo de cuentas, de caducidad de contraseñas, etc.

> **libpam-pam_cracklib**
>
> En versiones antiguas de Linux, la librería que se utiliza para establecer las políticas de contraseñas es `libpam-cracklib`.
> La configuración de las políticas de contraseñas se realiza en el archivo `/etc/pam.d/common-password` usando directivas similares a las que veremos a continuación.

En las últimas versiones de los sistemas GNU/Linux, entre ellas Debian, y las últimas versiones de `Kali`, se utiliza la librería `libpam-pwquality`.

Para instalar la librería `libpam-pwquality` en Debian, debemos de ejecutar el siguiente comando:

```
sudo apt install libpam-pwquality
```

Una vez instalado, debemos de modificar el archivo `/etc/security/pwquality.conf` para establecer las políticas de contraseñas. Las opciones que podemos configurar son:

Opciones para definir las políticas:

- **difok**: Número de caracteres en una nueva contraseña que no deben estar presentes en la contraseña anterior.
- **minlen**: Tamaño mínimo aceptable para la nueva contraseña.
- **dcredit**: Crédito máximo por tener dígitos en la nueva contraseña.
- **ucredit**: Crédito máximo por tener letras mayúsculas en la nueva contraseña.
- **lcredit**: Crédito máximo por tener letras minúsculas en la nueva contraseña.
- **ocredit**: Crédito máximo por tener otros caracteres en la nueva contraseña.
- **minclass**: Número mínimo de clases de caracteres requeridas para la nueva contraseña
- **maxrepeat**: Número máximo de caracteres repetidos.
- **maxclassrepeat**: Número máximo de caracteres consecutivos en la misma clase.
- **gecoscheck**: Verifica si las palabras individuales de más de 3 caracteres del campo passwd GECOS (campo de comentarios) del usuario - están contenidas en la nueva contraseña.
- **dictpath**: Ruta a los diccionarios de clacklib.
- **badwords**: Lista de palabras separadas por espacios que no deben incluirse en la contraseña.

Sistema de créditos, valores negativos y clases en pwquality

Créditos
Para definir la calidad y complejidad de las contraseñas se utiliza un sistema de créditos. Esto es muy interesante, básicamente se obtienen créditos por la complejidad. Una contraseña más corta podría ser aceptable si es más compleja en otras formas.

Por ejemplo una contraseña "ahwouwtdye" podría pasar una prueba minlen = 10. Si dcredit se establece en 2, una contraseña "ahwouw12" pasaría la prueba por que obtendríamos 2 créditos por cada dígito, entonces 8 caracteres más 2 créditos se valoran como 10 caracteres. Esto dependerá de como se establezcan los parámetros ucredit, lcredit, dcredit y ocredit.

Valores negativos
Establecer valores de créditos negativos significa que debe tener al menos ese tipo de carácter. Por ejemplo, establecer dcredit a -1 significaría que debe incluir al menos un dígito para que se acepte una contraseña. Es decir, no se trata de una suma de créditos sino de un requerimiento obligatorio.

Clases (minclass)
Otra configuración interesante es minclass. Determina cuántas clases diferentes de caracteres se deben usar para que una contraseña sea aceptable. Hay 4 tipos de clases: minúsculas, mayúsculas, dígitos, caracteres especiales (símbolos o signos).
Por ejemplo, un minclass = 2 exige que una contraseña contenga la combinación de dos tipos de clases. Ya sean mayúsculas o minúsculas, mayúsculas y caracteres especiales, minúsculas y dígitos, etc. Lo mismo pasaría si se establece a minclass = 4, la contraseña debería contener al menos un carácter de cada clase.

También se puede establecer un límite al número máximo de caracteres de cualquier tipo de clase. Por ejemplo, con el parámetro maxclassrepeat = 4 indicamos que las contraseñas no pueden contener más de 4 minúsculas, mayúsculas, dígitos y otros caracteres especiales.

Más información sobre el uso de directivas del fichero de pwquality: https://linux.die.net/man/8/pam_pwquality

También se pueden configurar estos parámetros, usando las directivas anteriores, en el archivo `/etc/pam.d/common-password`. Las configuraciones que se hacen en common-password prevalecen sobre las que se establecen en pwquality.conf.

```
password   requisite pam_pwquality.so retry=3 minlen=9 ucredit=-1 ocredit=-1 dcredit=-2
```

Hay varias herramientas para comprobar la validez de las contraseñas en Linux. Podemos citar algunas como `cracklib-check`, pwquality (libpwquality-tools) dispone de una herramienta llamada `pwscore` que podemos usar para comprobar la complejidad de una contraseña en base a los criterios establecidos en pwquality. Algunos ejemplos de uso.

```
# echo 123 | pwscore
Falló la comprobación de calidad de la contraseña:
 La contraseña tiene menos de 8 caracteres

# echo abc123.. | pwscore
Falló la comprobación de calidad de la contraseña:

 La contraseña no supera la verificación de diccionario - Es demasiado simple/sistemática.

# echo L3h5as/2a$-ls=72 | pwscore
100

#cracklib-check
1234
1234: it is too short
```

Caducidad y bloqueo de cuentas en Linux

Ya vimos que en el formato del archivo `/etc/shadow` se almacena la información de las contraseñas de los usuarios. En este archivo se almacena la información de los tiempos y plazos de caducidad de las contraseñas de los usuarios.

Los valores por defecto para estos parámetros se establecen en el archivo `/etc/login.defs`. En el archivo se definen las políticas de gestión de contraseñas para la creación de **nuevos usuarios**. También podemos establecer otros directivas como el valor umask por defecto, si el usuario tendrá un home para el si no se le especifica en su creación (useradd -m), cambiar la secuencia de ID (por defecto suelen ser 1000 y algo para usuarios normales), mensaje de bienvenida del inicio de sesión del usuario (motd_file), etc.

Algunas de las directivas más comunes que podemos establecer:

- PASS_MAX_DAYS: Número máximo de días que se puede usar una contraseña.
- PASS_MIN_DAYS: Número mínimo de días permitido entre cambios de contraseña.
- PASS_WARN_AGE: Número de días de advertencia antes de que caduque una contraseña.
- PASS_MIN_LEN y PASS_MAX_LEN: Número mínimo y máximo de caracteres que debe tener la contraseña.
- PASS_ALWAYS_WARN: Advierte sobre contraseñas débiles.
- PASS_CHANGE_TRIES: Número máximo de intentos de cambiar la contraseña si se rechaza por que es demasiado "fácil".
- ENCRYPT_METHOD: Tipo de cifrado que tendrá la contraseña (SHA256 5 o SHA512 6).
- LOGIN_RETRIES: Número máximo de reintentos de inicio de sesión en el caso de que la contraseña sea incorrecta.
- LOGIN_TIMEOUT: Tiempo máximo en segundos para iniciar sesión

Más información sobre login.defs: https://linux.die.net/man/5/login.defs

```
PASS_MAX_DAYS 90
PASS_MIN_DAYS 0
PASS_WARN_AGE 7
```

Los valores anteriores indicarían que la contraseña caduca cada 90 días, que se puede cambiar en cualquier momento y que se avisa al usuario 7 días antes de que caduque la contraseña y son los que se añadirán en la configuración del usuario en el archivo `/etc/shadow`.

Por último, si queremos modificar la configuración de la caducidad de las contraseñas de un usuario en concreto, podemos hacerlo con el comando `chage`. Con el comando **chage (change age)** podemos establecer la caducidad de contraseñas y cuentas de usuario. Esto no afecta a los nuevos usuarios, se establece de forma nominal a usuarios existentes.

Opciones del comando chage:

- -d, --lastday: Establece el día del último cambio de la contraseña.
- -E, --expiredate: Establece la fecha de caducidad.
- -I, --inactive: Deshabilita la cuenta después inactividad de días de la fecha de caducidad.
- -l, --list: Muestra la información de la edad de la cuenta.
- -m, --mindays: Establece el número mínimo de días antes de cambiar la contraseña.
- -M, --maxdays: Establece el número máximo de días antes de cambiar la contraseña.
- -R, --root: Directorio en el que hacer chroot.
- -W, --warndays: Establece los días de aviso de expiración.

Con el parámetro -l podemos ver información sobre las cuentas.

```
# chage -l usuario
Last password change                                    : Apr 18, 2024
Password expires                                        : never
Password inactive                                       : never
Account expires                                         : never
Minimum number of days between password change          : 0
Maximum number of days between password change          : 90
Number of days of warning before password expires       : 7
```

Registro de intentos de autenticación

El registro de intentos de autenticación es un mecanismo esencial para rastrear y auditar los intentos de inicio de sesión en el sistema.

Los eventos de autenticación, como intentos de inicio de sesión exitosos o fallidos, se registran en archivos de registro específicos, como el archivo `/var/log/auth.log` en sistemas Linux o en el `visor de eventos de Windows`. Estos registros proporcionan información valiosa para identificar posibles intentos de acceso no autorizados o actividades sospechosas.