TEMA 3. SEGURIDADE LÓXICA

Neste primeiro tema de seguridade lóxica, estudaremos a privación do acceso lóxico aos sistemas, revisando políticas de contrasinais.

.

1. Principios de la seguridad lógica

El activo más importante que se poseen las organizaciones es la **información**, y por lo tanto deben existir técnicas más allá de la seguridad física que la aseguren, estas técnicas las brinda la seguridad lógica.

La seguridad lógica consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y solo se permita acceder a ellos a las personas autorizadas para hacerlo. A lo largo de los temas 3 (seguridad en el acceso lógico a sistemas), 4 (software antimalware), y 5 (criptografía), veremos algunos de los métodos fundamentales.

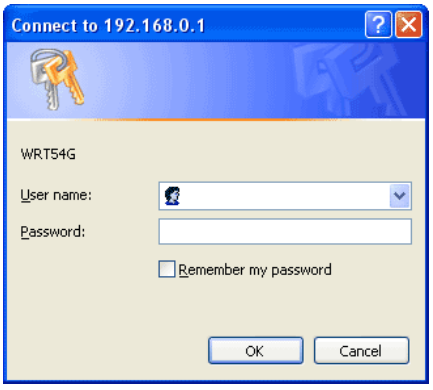
Algunas de las principales amenazas que tendrán que combatir los administradores de sistemas son el acceso y modificaciones no autorizadas a datos y aplicaciones.

La seguridad lógica se basa, en gran medida, en la efectiva administración de los permisos y el control de acceso a los recursos informáticos, basados en identificación, autenticación y autorización de accesos.

Como principio básico de seguridad lógica en la configuración de sistemas: todo lo que no está permitido debe estar prohibido.

2. Control de acceso lógico

El control de acceso lógico es la principal línea de defensa para la mayoría de los sistemas, permitiendo prevenir el ingreso de personas no autorizadas a la información de los mismos.



Para realizar la tarea de controlar el acceso se emplean 2 procesos normalmente: **identificación** y **autenticación**. Se denomina identificación al momento en que el usuario se da a conocer en el sistema; y autenticación a la verificación que realiza el sistema sobre esta identificación.

Desde el punto de vista de la eficiencia, es conveniente que los usuarios sean identificados y autenticados solamente una vez, pudiendo acceder a partir de ahí a todas las aplicaciones y datos a los que su perfil les permita, tanto en sistemas locales como en sistemas a los que deba acceder en forma remota. Esto se denomina **single login** o **sincronización de passwords**.

Una de las posibles técnicas para implementar esta única identificación de usuarios sería la utilización de un **servidor de autenticaciones** sobre el cual los usuarios se identifican y que se encarga luego de autenticar al usuario sobre los restantes equipos a los que éste pueda acceder.

Este servidor de autenticaciones no debe ser necesariamente un equipo independiente y puede tener sus funciones distribuidas tanto geográfica como lógicamente, de acuerdo con los requerimientos de carga de tareas. Es el caso de servidores LDAP en GNU/Linux y Active Directory sobre Windows Server.

Los sistemas de control de acceso protegidos con contraseña, suelen ser un punto crítico de la seguridad y por ello suelen recibir distintos tipos de ataques, los más comunes son:

- **Ataque de fuerza bruta**: se intenta recuperar una clave probando todas las combinaciones posibles hasta encontrar aquella que permite el acceso. Cuanto más corta, más sencilla de obtener probando combinaciones.
- **Ataque de diccionario**: intentar averiguar una clave probando todas las palabras de un diccionario o conjunto de palabras comunes. Este tipo de ataque suele ser más eficiente que un ataque de fuerza bruta, ya que muchos usuarios suelen utilizar una palabra existente en su lengua como contraseña para que la clave sea fácil de recordar, lo cual no es una práctica recomendable.

Una forma sencilla de proteger un sistema contra los ataques de fuerza bruta o los ataques de diccionario es establecer un número máximo de tentativas, de esta forma se bloquea el sistema automáticamente después de un número de intentos infructuosos predeterminado. Un ejemplo de este tipo de sistema de protección es el mecanismo empleado en las tarjetas SIM que se bloquean automáticamente tras tres intentos fallidos al introducir el código PIN.

A continuación veremos criterios para establecer políticas seguras de contraseñas.

Política de contraseñas

Las contraseñas son las claves que se utilizan para obtener acceso a información personal que se ha almacenado en el equipo y aplicaciones, como en los entornos web (mail, banca online, redes sociales, etc.). Para que una contraseña sea segura se recomienda:

- **Longitud mínima**: cada carácter en una contraseña aumenta exponencialmente el grado de protección que ésta ofrece. Las contraseñas a ser posible deben contener un mínimo de 8 caracteres, lo ideal es que tenga 14 caracteres o más.
- **Combinación de caracteres** (letras minúsculas y mayúsculas, números y símbolos especiales): cuanto más diversos sean los tipos de caracteres de la contraseña más difícil será adivinarla.

Para un ataque de fuerza bruta que intenta encontrar contraseñas generando todas las combinaciones posibles, si empleamos una contraseña de 5 caracteres en minúscula para el idioma español que posee 27 caracteres diferentes, tendría que probar 275 = 14 348 907 combinaciones a probar.

En caso de emplear mayúsculas y minúsculas el número de combinaciones se multiplicaría siendo (27 x 2)5 = 525 = 380 204 032 combinaciones a probar.

Algunos métodos que suelen emplearse para crear contraseñas resultan fáciles de adivinar, a fin de evitar contraseñas poco seguras, se recomienda:

- No incluir secuencias ni caracteres repetidos. Como "12345678", "222222", "abcdefg".
- No utilizar el nombre de inicio de sesión.
- No utilizar palabras de diccionario de ningún idioma.
- Utilizar varias contraseñas para distintos entornos.
- Evitar la opción de contraseña en blanco.
- No revelar la contraseña a nadie y no escribirla en equipos que no controlas.
- Cambiar las contraseñas con regularidad.

A continuación realizaremos un análisis en profundidad a distintos niveles, de los mecanismos de control de acceso a los sistemas mediante contraseña:

- **1° nivel:** control con contraseña del arranque y de su propia configuración proporcionado por la BIOS.
- **2º nivel:** control mediante contraseña del arranque y de la edición de las opciones proporcionadas por los gestores de arranque.
- **3º nivel:** control mediante usuario y contraseña por parte de los sistemas operativos. El sistema operativo permite el control de acceso a datos y aplicaciones mediante la configuración de privilegios a los distintos perfiles de usuario o individualmente a estos.
- **4º nivel:** contraseña y cifrado de acceso a datos y aplicaciones, entre otros los archivos ofimáticos, comprimidos, sitios web (mail, banca online), etc.

Control de acceso en la BIOS y gestor de arranque

BIOS (Basic Input/Output System): es el nivel más bajo de software que configura o manipula el hardware de un ordenador de manera que cada vez que iniciamos el ordenador este se encarga de reconocer todo el hardware que contiene el ordenador y controlar el estado de los mismos.

En la BIOS podemos configurar cualquier parámetro referente al hardware, de qué dispositivo arrancará en primer lugar o parámetros más comprometidos como el voltaje que se le suministra al núcleo del microprocesador.

Por este motivo tendremos que proteger nuestra BIOS de manera que solo un Administrador o un usuario responsable puedan cambiar los valores de la configuración.

Según la versión y la marca de la BIOS podemos configurar la seguridad del mismo de distintas formas. Estableceremos una clasificación sobre los niveles de seguridad que suele tener:

- **Seguridad del sistema** (system): en cada arranque de la máquina nos pedirá que introduzcamos una contraseña que previamente se ha configurado en el BIOS. En caso de no introducirla o introducirla incorrectamente, el sistema no arrancará.

- **Seguridad de configuración de la BIOS** (setup): en este apartado se suelen distinguir dos roles aplicables: Usuario (solo lectura) y Administrador (lectura/modificaciones).

Control de acceso en el sistema operativo

Existen métodos de acceso al sistema operativo muy seguros como por ejemplo mediante huella dactilar, pero el más utilizado sigue siendo a través de una contraseña asociada a una cuenta de usuario.

Como hemos visto anteriormente existen métodos para poder acceder a los sistemas operativos sin control de contraseña, en el caso de GNU/Linux mediante el modo de recuperación. En el caso de Windows para versiones como XP mediante el modo prueba de fallos o pulsando 2 veces en la ventana de inicio de usuarios Ctrl + Alt + Supr e intentando acceder a la cuenta del usuario Administrador sin contraseña, ya que en la instalación no se le asigna ninguna, por tanto por defecto suele estar vacía.

Pero existen otros métodos, normalmente asociados a poder arrancar con una distribución Live para poder recuperar o conocer las contraseñas de cualquier usuario, así como borrarlas o modificarlas.

Como recomendación, estas herramientas empleadas nos servirán para **auditar nuestros sistemas** de credenciales de acceso a sistemas operativos y ver el nivel de fortaleza de las mismas, ya que dependiendo del nivel de nuestras contraseñas no siempre será posible recuperarlas.

3. Política de usuarios y grupos

La definición de cuentas de usuario y su asignación a perfiles determinados, grupos o roles, así como la asignación de privilegios sobre los objetos del sistema es uno de los aspectos fundamentales de la seguridad, y una de las tareas fundamentales del administrador de sistemas. Este proceso lleva generalmente cuatro pasos:

- **Definición de puestos**: separación de funciones posibles y el otorgamiento de los mínimos permisos de acceso requeridos por cada puesto para la ejecución de las tareas asignadas.
- **Determinación de la sensibilidad del puesto**: determinar si una función requiere permisos críticos que le permitan alterar procesos, visualizar información confidencial, etc.
- **Elección de la persona para cada puesto**: requiere considerar los requerimientos de experiencia y conocimientos técnicos necesarios para cada puesto.
- **Formación inicial y continua de los usuarios**: deben conocer las pautas organizacionales, su responsabilidad en cuanto a la seguridad informática y lo que se espera de él. Debe estar orientada a incrementar la conciencia de la necesidad de proteger los recursos informáticos.

La definición de los permisos de acceso requiere determinar cuál será el nivel de seguridad necesario sobre los datos, por lo que es imprescindible clasificar la información, determinando el riesgo que produciría una eventual exposición de la misma a usuarios no autorizados. Así los diversos niveles de la información requerirán diferentes medidas y niveles de seguridad.

Para empezar la implementación es conveniente comenzar definiendo las medidas de seguridad sobre la información más sensible o las aplicaciones más críticas, y avanzar de acuerdo a un orden

de prioridad descendiente, establecido alrededor de las aplicaciones. Una vez clasificados los datos, deberán establecerse las medidas de seguridad para cada uno de los niveles.

0. Índice