

Elección de Claves de Acceso (Passwords)

Julio Ardita
CYBSEC S.A.
jardita@cybsec.com

Fecha: 3 de septiembre de 1996

1. Introducción

Las claves de acceso son la barrera mas común en contra de accesos no autorizados a un sistema, y prácticamente hoy en día son la única barrera; es por eso que hay que poner especial atención en el tema de la elección de las claves de acceso.

Varios estudios que he leído en diferentes libros, demuestran que la vulnerabilidad de un sistema esta dada en gran parte por la fortaleza de sus claves de acceso. ¿Que quiero decir con fortaleza?. Si una persona que posee un nombre de acceso: Juan, pone de clave de acceso al sistema: Juan, toda la fortaleza del sistema de seguridad del sistema se cae.

2. Casos reales

Muchos dirán que es imposible que una persona ponga de clave de acceso su mismo nombre, pero esto no es así; en mis estudios, de un 100% de los casos analizados, el 3% utiliza de clave de acceso su mismo nombre, otro 7% utiliza de clave de acceso palabras relacionadas con su nombre o su apellido, y otro 30% utiliza palabras fácilmente encontradas en un diccionario común.

Un gran problema real con claves de acceso, lo poseen los sistemas operativos Irix de Silicon Graphics y últimamente las maquinas Netra de Sun Corp. Las maquinas con sistema operativo Irix, venían de fabrica, con varios nombre de acceso sin claves, por ejemplo: guest; entonces el intruso lo único que tenia que hacer era conectarse a un sistema Irix y cuando pedía el nombre de usuario, tipeaba: guest (que quiere decir invitado) y accedía al sistema. Otro error mas grave los poseen los sistemas Netra de Sun, las nuevas maquinas que ofrece Sun para conexión con internet, vienen por defecto de fabrica, con el nombre de usuario: setup y la clave que posee es: setup.

3. Peligros

Sumando los porcentajes, un 40% de las claves analizadas fueron descubiertas, quedando un 60% solo a salvo. Esto nos abre una gran brecha de seguridad en nuestro sistema. Si un intruso ingresa a nuestro sistema, podrá contar con el 40% de las claves para volver a ingresar. Si poseemos 200 usuarios en el sistema, el intruso poseerá 80 nombres con claves de acceso para volver a entrar al sistema.

Cuando un intruso entra en un sistema, lo considera propiedad de él; siempre el intruso va a tratar de conseguir mayores privilegios dentro del sistema hasta lograr los privilegios del administrador de sistemas.

El otro objetivo del intruso es mantenerse en el sistema el mayor tiempo posible, y para realizar esto, el intruso se vale de varias herramientas, una de las más usadas y principales es el cracker de passwords, traducido al castellano sería "reventador de claves de acceso".

Si nos diéramos cuenta de que un intruso ha logrado entrar al sistema, tendríamos que cambiar todas las claves de acceso para que el intruso no pueda ingresar más a nuestro sistema; lo que nos tomaría a nosotros mucha pérdida de tiempo, el sistema se debería mantener abajo por unas horas, mientras se cambian las claves de acceso, y esto acarrearía numerosos problemas de índole personal con los usuarios del sistema, ya que deberían volver a cambiar sus claves de acceso.

Cuando un intruso ha ingresado al sistema, y posee nuestro archivo de claves (1), la única forma de estar seguros que no volverá a entrar, es cambiando todas las claves de acceso al sistema, ya que si dejamos algunas sin cambiar, esas pueden ser la futura puerta de acceso del intruso.

4. Cracker de Passwords

El cracker de passwords, o "reventador de claves de acceso"; es una herramienta muy usada por los intrusos y a la vez muy útil. Una vez que el intruso ha logrado conseguir el archivo de claves, el intruso pone a funcionar el cracker con ese archivo. Este cracker, es un programa que se dedica a comparar las claves encriptadas en contra de un diccionario.

La forma de funcionamiento es muy sencilla: utilizando el DES(2), toma cada palabra del diccionario y la encripta 4096 veces y a su vez la va comparando contra las claves encriptadas del archivo de claves del sistema al cual accedió; cuando encuentra una que coincide ya encontró una clave de acceso.

Un ejemplo podría ser utilizando el sistema Unix. El archivo de claves en forma reducida, podría presentarse como:

prueba:Gp4hp6YLRYYk:

Esto es el usuario prueba, posee una clave encriptada que, en este caso, es también la palabra prueba. Cada palabra puede ser encriptada de 4096 formas diferentes. En una de las formas es como figura en el archivo de claves.

5. Políticas de claves de seguridad

Para poder utilizar bien las claves de seguridad, la empresa debe plantearse una política de claves de acceso, la cual estará incluida dentro de la política de seguridad de la empresa.

Una política en el tema de claves de acceso, podría ser:

- 1) No colocar como clave de acceso su nombre, apellido o algún otro dato personal o familiar.
- 2) No utilizar palabras simples, que puedan ser encontradas en un diccionario.
- 3) No utilizar palabras de otros idiomas.
- 4) Utilizar combinaciones de letras y números en la clave de acceso.
- 5) No comentar a nadie su clave de acceso al sistema.

5.1. Claves que se proponen

Agregándose a la política de seguridad se podrían proponer formas de claves de acceso. Por ejemplo:

- 1) La clave debe poseer tres letras, seguidas de dos números y luego otras tres letras.
- 2) La clave debe estar compuesta de 2 números, cuatro letras y luego dos números.
- 3) La clave debe poseer 2 números y luego 6 letras.

Y así se podría continuar, lo importante es que cada empresa tenga su propia política de seguridad.

5.2. Charlas de toma de conciencia

Otra gran ayuda, es una breve charla introductoria sobre:

- La seguridad básica.

- La elección de la clave de acceso.
- Que la clave de acceso no se debe anotar, sino memorizar.
- No se debe mencionar la clave de acceso a ningún compañero.

Una charla de este tipo, no tomaría mas de 30 minutos y puede preparar a los usuarios del sistema sobre la seguridad.

Un tema a tratar es la represaria; si alguno revela su clave de seguridad, le podría causar hasta un despido.

5.3. Cambio de claves mensual

Otra buena medida a adoptar, es el cambio mensual de claves de acceso, utilizando el mismo sistema como base, se podría diseñar un programa que mensualmente pidiera el cambio de claves de acceso y chequeara que no se utilizaran claves viejas o ya usadas.

Con esta medida, el tema claves de acceso esta en muy alto porcentaje de seguridad.

6. Monitoreo del sistema y chequeo de claves propias del sistema

Por mas que el tema de las claves de acceso este solucionado, no hay que olvidar el chequeo de seguridad que debe hacerse al sistema semanalmente, para testear si hay presencia de algún intruso o ocurre algo anormal.

También, la tarea del gerente de seguridad del sistema, es analizar y utilizar las herramientas que utilizan los intrusos para tratar de ingresar al sistema y protegerlo adecuadamente.

Esto se realiza utilizando las mismas herramientas que utilizan los intrusos. Un buen gerente de seguridad, debe poseer un cracker de claves de acceso, y periódicamente correrlo en el propio sistema para chequear la seguridad de las claves de acceso.

7. Futuro

Utilizando las medidas mencionadas en este articulo, se reduce considerablemente el riesgo de sufrir ataques por vía de claves de acceso olvidadas o claves de acceso muy sencillas.

Esto no debe tomarse como única medida para la protección de un sistema, esta es una parte de las medidas a tomar.

Referencias

- (1) En este caso específico me refiero a un archivo de claves del tipo Unix.
- (2) El DES es el sistema criptográfico que utiliza el Unix para encriptar las claves de acceso.