CONTRASEÑAS. CUESTIÓN DE CONCIENCIA

[Paper publicado en http://www.mipistus.blogspot.com]

Jorge Alejandro Mieres
jamieres@gmail.com

La primera línea de defensa que posee un sistema informático para evitar que personas no autorizadas accedan al él, es determinar mediante un método de autenticación, denominado logín o logon, quién o qué está accediendo al sistema. Una de las piezas más criticas de este proceso de autenticación la constituyen las contraseñas.

Esta principal barreras de protección está formada por caracteres (letras, números, símbolos) cuya cantidad y combinación que utilicemos para formar nuestras contraseñas nos dará el grado de robustez de la misma. Evidentemente, cuanto más larga y más caracteres posee, aumentará exponencialmente el grado de protección y, por ende, será menor la probabilidad de ser descubiertas.

A modo didáctico y para clarificar la importancia que tienen las contraseñas, nos remitiremos a uno de los principales personajes de la famosa película MATRIX RELOADED, el "hacedor de llaves". Este personaje es muy importante porque es el encargado de fabricar y mantener las llaves que dan acceso a las diferentes zonas de MATRIX. MATRIX representa un mundo generado por computadoras y las llaves que dan acceso a las diferentes zonas son contraseñas. Entonces se podría decir que las contraseñas son las llaves con las que se controlan los accesos. Es decir, controlan el acceso a la información (contraseñas en documentos), restringen el acceso a los recursos (contraseñas en páginas web) o implementan autenticación (demostrando que eres quien dices ser).

Evidentemente, uno de los problemas más comunes en seguridad informática no tiene que ver con malas implementaciones o problemas de ataques, sino que proviene de contraseñas inseguras o fáciles de adivinar, lo cual es muy fácil de solucionar con sólo cambiar la contraseña. Lo que resulta realmente difícil es concientizar a los usuarios para que utilicen contraseñas complejas.

Si bien resulta muy difícil, aunque no imposible, que un atacante externo a nuestra red pueda "descubrir nuestras contraseñas", no se tiene el mismo criterio cuando existe la posibilidad de que el ataque provenga desde nuestra propia red, y si el atacante conoce algo de la víctima el riesgo se incrementa ya que podrá probar palabras relacionadas a él. Es muy común que este intento de intrusión ocurra, para muchos usuarios es muy tentador intentar "descubrir" la contraseña de administrador o las del correo electrónico de algún compañero para jugarle alguna broma.

Hoy en día, existen herramientas específicas y automatizadas que pueden ser utilizadas para violar la seguridad de los sistemas informáticos recurriendo a ataques por fuerza bruta o ataques por diccionarios de contraseñas (wordlist) para intentar “romperlas” y así ingresar al sistema. Por ello siempre es recomendable limitar el tiempo de vida de las contraseñas evitando tenerlas el tiempo suficiente para que sean deducibles por cualquiera de los ataques mencionados.

También es muy común encontrarse con personas que utilizan como usuario/contraseña la misma palabra y muchas veces relacionadas a él, por ejemplo el nombre, apellido, el nombre del hijo, el numero de teléfono, número de documento, direcciones, claves muy sencillas como "1234" (muchas veces es mas

seguro la ausencia de contraseña que una como "1234"); o para evitar olvidarlas las anotan y la dejan sobre el escritorio, en un pizarrón y hasta bien grande en una hoja A4 pegada al costado del monitor sin darse cuenta que lo único que se logra con ello es aumentar la probabilidad de que un atacante averigüe alguna contraseña y pueda escalar privilegios hasta alcanzar el de administrador.

Esto se debe a que, salvo raras excepciones, el usuario no tiene conciencia de la seguridad. Para ellos, muchas de las medidas de seguridad que se implementan, como puede ser la autenticación mediante una simple contraseña, son vistas como un contratiempo, como una exigencia sin consentimiento que lleva a cabo la gente de sistemas para justificar su trabajo y que no aporta ninguna ventaja, lo toman como una agresión o intromisión a su forma de trabajar y al final, y dentro de su lógica, terminan buscando la comodidad (dejarlas anotadas para no ser olvidadas) siendo peor el remedio que la enfermedad.

Se cree erróneamente que la responsabilidad de las medidas de protección de acceso recae solamente en el o los administradores de la red y por ello no se tiene conciencia de la vulnerabilidad que implica un olvido de contraseña o anotarlas en algún lugar visible por cualquier persona. Hay que tener presente que la protección de la contraseña también recae en los usuarios ya que al comprometer una cuenta se puede estar comprometiendo todo el sistema.

Por lo tanto, el fortalecer las contraseñas y el cambio frecuente de las mismas, son las principales herramientas con las que disponemos como usuarios para aumentar la seguridad y fortalecer no solo la integridad de los sistemas informáticos sino que también nuestra propia información confidencial. Una contraseña robusta es aquella que:

- No puede encontrarse en un diccionario.
- Contiene números, letras y símbolos.
- Contiene letras mayúsculas y minúsculas.
- Cuanto más larga, mas robusta es.

Por otro lado, cabe mencionar la importancia de definir una política de contraseñas. En general, se puede definir la longitud máxima y mínima, el período máximo en que estará activa (pasado ese período deberá ser cambiada), el período mínimo en que estará activa (el tiempo que debe transcurrir antes que un usuario esté habilitado para cambiar su contraseña), un control de complejidad (para evitar contraseñas triviales), un control de historial (para evitar que se repitan las contraseñas), etc. Los siguientes valores se pueden considerar seguros para una política de contraseñas:

- Longitud mínima: 8 caracteres.
- Longitud máxima: Entre 12 y 14 caracteres.
- Período máximo: 30 días.
- Período mínimo: 1 día
- Control de complejidad: Habilitado
- Historial de contraseñas: Habilitado
- Cantidad de contraseñas en el historial: 12

Estrategias para la elección de contraseñas.

Algunos métodos que suelen emplearse para crear contraseñas pueden resultar fáciles de adivinar para un atacante. A fin de evitar contraseñas poco seguras y fáciles de averiguar, se mencionarán a continuación algunas recomendaciones a tener en cuenta a la hora de elegirlas:

- No utilice contraseñas que sean palabras que puedan ser encontradas en diccionarios, aunque sean en otro idioma, ni nombres como el del usuario, familiares o mascotas.
- Tampoco utilice contraseñas totalmente numéricas con algún significado como números telefónicos, DNI, fecha de nacimiento, etc.
- Trate de elegir una contraseña que mezcle caracteres alfanuméricos con mayúsculas y minúsculas.
- Procure que, como mínimo, la contraseña tenga ocho (8) caracteres.
- Deben ser fáciles de recordar para evitar verse obligado a escribirlas.

Algunos ejemplos podrían ser:

- Combinar palabras cortas con números o caracteres de puntuación: Soy2_Yo3.
- Usar acrónimos, por ejemplo de alguna frase fácil de recordar: En casa De Herrero Cuchillo de palo: EcDHCdp, y hasta añadir algún número para mayor seguridad: EcDHCdp12 .
- Incluso es mejor si la frase no es conocida: Hasta ahora No He olvidado Mi Contraseña: HaNHoMC.

Consejos para proteger las contraseñas.

Muchas vulnerabilidades están dadas por el descuido del propio usuario. Algunas medidas básicas de protección podrían ser las siguientes:

- Nunca comparta las contraseñas, y si lo hace cámbielas inmediatamente.
- No anote la contraseña en ningún sitio ni la escriba si alguien esta observando, es una norma tácita de buen usuario no mirar el teclado mientras alguien teclea su contraseña.
- No las envíe por correo electrónico ni la mencione en una conversación.
- No mantenga una contraseña indefinidamente, se recomienda cambiarla en forma periódica.
- Cuanto menos tipos de caracteres haya en la contraseña, más larga deberá ser ésta.

Conclusión.

Después de lo mencionado podrán darse cuenta que la existencia de contraseñas débiles puede derivar en un riesgo muy importante para la seguridad de nuestro sistema informático y que su seguridad esta dada en gran parte por la fortaleza de nuestras contraseñas.

Una parte fundamental de nuestro trabajo depende de la implementación de buenas contraseñas, es decir, de su complejidad. A su vez, esta implementación depende de la educación que cada usuario recibe, de las Políticas de Seguridad aplicadas y de auditorias permanentes; por ello es muy importante contar con una política de contraseñas que, de forma sencilla y comprensible, nos brinde los lineamientos necesarios para cubrir el punto en cuestión.

RECUERDE: “Una contraseña debe ser como un cepillo de dientes. Úselo todos los días; cámbielo regularmente y no lo comparta con sus amigos”

Bibliografía:

Guideline on Network Security Testing. National Institute of Standards and Technology (NIST)
Password. HHS. Institute for Security and Open Methodologies (ISECOM)
Seguridad Informática: sus implicancias e implementación. Lic. Cristian Borghello