Laboratorio: Crear y almacenar contraseñas seguras

Objetivos

Comprender los conceptos correspondientes a una contraseña segura.

Parte 1: Explore los conceptos relacionados con la creación de una contraseña segura.

Parte 2: ¿Desea explorar los conceptos relacionados con el almacenamiento seguro de sus contraseñas?

Aspectos básicos/situación

Las contraseñas se usan mucho para reforzar el acceso a los recursos. Los atacantes usarán muchas técnicas para descubrir las contraseñas de los usuarios y conseguir acceso no autorizado a recursos o datos.

Para protegerse mejor, es importante que entienda en qué consiste una contraseña segura y cómo almacenarla en forma segura.

Recursos necesarios

- Computadora o dispositivo móvil con acceso a Internet

Parte 1: Creación de una contraseña segura

Las contraseñas seguras tienen cuatro requisitos principales que se detallan a continuación por orden de importancia:

1) El usuario debe poder recordar la contraseña fácilmente.
2) Otra persona no debe poder adivinar la contraseña.
3) Un programa no debe poder adivinar ni descubrir la contraseña.
4) Debe ser compleja, incluyendo números, símbolos y una combinación de letras mayúsculas y minúsculas.

Basándose en la lista anterior, el primer requisito, probablemente, sea el más importante porque usted debe poder recordar su contraseña. Por ejemplo, la contraseña **#4sFrX^-aartPOknx25_70!xAdk<d!** se considera una contraseña segura porque satisface los tres últimos requisitos, pero es muy difícil de recordar.

Muchas organizaciones requieren contraseñas que contengan una combinación de números, símbolos y letras mayúsculas y minúsculas. Las contraseñas que cumplen con esta política están bien siempre y cuando los usuarios puedan recordarlas. Abajo hay un ejemplo de un conjunto de directivas de contraseña en una organización típica:

- La contraseña debe tener una longitud de, al menos, 8 caracteres.
- La contraseña debe contener letras mayúsculas y minúsculas.
- La contraseña debe contener un número.
- La contraseña debe contener un carácter especial.

Tómese un momento para analizar las características de una contraseña segura y el conjunto común de directivas de contraseña antes mencionado. ¿Por qué el conjunto de políticas deja de lado los dos primeros puntos? Explique.

Una excelente forma de crear contraseñas seguras es elegir cuatro o más palabras al azar y concatenarlas. La contraseña **televisionranabotasiglesia** es más segura que **J0n@que#81**. Observe que, si bien la segunda contraseña cumple con las políticas antes descritas, los programas descifradores de contraseñas (cracks) son muy eficientes para detectar este tipo de contraseña. Aunque muchos conjuntos de directivas de contraseña no aceptarán la primera contraseña, **televisionranabotasiglesia**, esta es mucho más segura que la segunda. Es mucho más fácil de recordar para el usuario (especialmente, si está asociada con una imagen), es muy larga y su factor aleatorio hace que sea más difícil de adivinar para los programas descifradores de contraseñas.

Con una herramienta de creación de contraseñas en línea, cree contraseñas basadas en el conjunto común de directivas de contraseña para empresas antes descrito.

a. Abra un navegador web y vaya a http://passwordsgenerator.net.

b. Seleccione las opciones para cumplir con el conjunto de directivas de contraseña.

c. Genere la contraseña.

   ¿La contraseña generada es fácil de recordar?

   Mediante una herramienta de creación de contraseñas en línea, cree contraseñas basadas en palabras al azar. Tenga en cuenta que, como las palabras se escriben unidas, no se consideran como palabras del diccionario.

d. Abra un navegador web y vaya a http://preshing.com/20110811/xkcd-password-generator/.

e. Genere una contraseña de palabras al azar haciendo clic en **Generate Another!** en la parte superior de la página web.

f. ¿La contraseña generada es fácil de recordar?

Parte 2: Almacenamiento seguro de contraseñas

Si el usuario elige usar un administrador de contraseñas, la primera característica de una contraseña segura puede ignorarse porque el usuario tiene acceso al administrador de contraseñas en todo momento. Tenga presente que algunos usuarios solo confían en su propia memoria para guardar sus contraseñas. Los administradores de contraseñas, tanto locales como remotos, deben tener un almacén de contraseñas, que podría verse comprometido.

El almacén de contraseñas del administrador de contraseñas debe tener un cifrado seguro y el acceso a este debe controlarse estrictamente. Gracias a aplicaciones de teléfonos móviles e interfaces web, los administradores de contraseñas basados en la nube ofrecen acceso ininterrumpido y en cualquier momento a los usuarios.

Un administrador de contraseñas popular es LastPass.

Cree una cuenta de LastPass de prueba:

a. Abra un navegador web y vaya a https://lastpass.com/.

b. Haga clic en **Start Trial** para crear una cuenta de prueba.

c. Complete los campos, según las instrucciones.

d. Establezca una contraseña maestra. Esta contraseña le da acceso a su cuenta de LastPass.

e. Descargue e instale el cliente LastPass para su sistema operativo.

f. Abra el cliente e inicie sesión con su contraseña maestra de LastPass.

g. Explore el administrador de contraseñas de LastPass.

A medida que agrega contraseñas a LastPass, ¿en dónde se almacenan las contraseñas?

Además de usted, al menos una entidad más tiene acceso a sus contraseñas. ¿Cuál es esa entidad?

Si bien puede ser conveniente tener todas sus contraseñas almacenadas en el mismo lugar, también tiene desventajas. ¿Puede pensar en algunas?

Parte 3: Entonces, ¿qué es una contraseña segura?

Teniendo presentes las características de contraseña segura provistas al inicio de este laboratorio, elija una contraseña que sea fácil de recordar pero difícil de adivinar. Está bien usar contraseñas complejas siempre que no afecten requisitos más importantes como la capacidad para recordarlas fácilmente.

Si se usa un administrador de contraseñas, la necesidad de que puedan recordarse fácilmente puede omitirse.

A continuación, se proporciona un resumen rápido:

Elija una contraseña que pueda recordar.

Elija una contraseña que otra persona no pueda asociar con usted.

Elija contraseñas diferentes y nunca use la misma contraseña para servicios diferentes.

Está bien usar contraseñas complejas siempre que esto no las haga difíciles de recordar.