Gerardo Acevedo Arzola
Seguridad Informática

Laboratorios Capítulo 3

3.1.1.5 Lab Create and Store String Password

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.
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.

1.- ¿Por qué el conjunto de políticas deja de lado los dos primeros puntos?

R. No se menciona "El usuario debe poder recordar la contraseña", porque es intuitivo que las contraseñas las tienes que tener en la memoria y si la haces compleja para recordar no sería posible acceder a los datos o en el peor de los casos al usuario se le olvida su contraseña.

No se menciona "Otra persona no debe poder adivinar la contraseña", ya que las contraseñas deben ser complejas y no obvias, además la normativa de agregar más caracteres especiales no hace más fácil la contraseña.

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

Contraseña generada: **8aL\{e+9eb**

¿La contraseña generada es fácil de recordar? **Sí**

3.- 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.

Contraseña generada: **marriedcampreporthalfway**

¿La contraseña generada es fácil de recordar? Sí

4.-

a) A medida que agrega contraseñas a LastPass, ¿en dónde se almacenan las contraseñas**?**
R. En su bodega

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

c) Si bien puede ser conveniente tener todas sus contraseñas almacenadas en el mismo lugar, también tiene desventajas
R. Como el curso mencionó, años atrás LastPass se puso en riesgo, aunque no pasó nada puedo ser peor. Si los hackers entrarán a mi cuenta sabrían todas las contraseñas de todas las páginas web que visito.

3.1.2.3 Lab Backup Data to External Storage

1.- ¿Por qué elegiría respaldos a las 3:00?

R. Para guardar el respaldo cuando estamos descansando y así guardar lo hecho en todo el día

2.-

a) Enumere algunos servicios de respaldo basados en la nube
DropBox
Google Drive
GitHub
Mega
Carbonite
iCloud
SkyDrive

b) Investigue los servicios que detalló anteriormente. ¿Son gratuitos?
R. Sí, pero tiene una capacidad de almacenamiento es su versión gratis, en pago esa capacidad aumenta.

c) ¿Los servicios que detalló dependen de una plataforma específica?
No

d) ¿Puede acceder a sus datos desde todos los dispositivos que posee (equipo de escritorio, portátil, tableta y teléfono)?
Sí

3.- ***Reflexión***

a) ¿Cuáles son las ventajas de realizar respaldos de los datos en un disco externo local? **R. Que solo nosotros tenemos control del acceso a este medio**

b)

c) . ¿Cuáles son las desventajas de realizar respaldos de los datos en un disco externo local?
R. Que somos responsables de los daños físicos virtuales, así como perdidas del equipo

d) ¿Cuáles son las ventajas de realizar respaldos de datos en un disco basado en la nube?
R. Accesibilidad de los datos donde sea y cuando sea,si el dispositivo se daña los archivos quedan intactos
. ¿Cuáles son las desventajas de realizar respaldos de datos en un disco basado en la nube?
R. Almacenamiento limitado, amenazas por inseguridad los servicios de almacenamiento.

3.1.2.5 Lab Who Owns Your Data

1.-

a) ¿ Tiene una cuenta con un proveedor de servicios en línea? **Si** ¿Ha leído el acuerdo de los términos de servicio?
No

(Investigación de acuerdo a los términos de uso y privacidad de la plataforma Facebook)

b) ¿Cuál es la política de uso de datos?
- **Proporcionar, personalizar y mejorar nuestros Productos.**
- **Información relacionada con la ubicación**
- **Información entre dispositivos y Productos de Facebook**
- **Investigación y desarrollo de productos**
- **Anuncios y otro contenido patrocinado**

c) ¿Cuáles son las configuraciones de privacidad? Esta destinada por subtemas:
R. Publicaciones, Eliminación de publicaciones, Perfil, Lista de Amigos, Reacciones y comentarios, Comentarios y reacciones de otras personas, Etiquetas, Eliminación de etiquetas, Biografía, Búsqueda, Sección de noticias y Ubicación.

d) ¿Cuál es la política de seguridad?
R. Manejo de información, Información que se comparte, Información que se comparte a terceros, Uso de información, Protección de información

e) ¿Cuáles son sus derechos en relación con sus datos?
- **Como propietario de derechos de autor, la ley te otorga ciertos derechos para impedir que otras personas puedan copiar o distribuir tu obra, o crear obras nuevas basadas en la tuya.**
- **Cuando publicas contenido o información con la configuración "Público", significa que permites que todos, incluidas las personas que son ajenas a Facebook, accedan y usen dicha información y la asocien a ti (es decir, tu nombre y foto del perfil).**
- **Siempre valoramos tus comentarios o sugerencias acerca de Facebook, pero debes entender que podríamos utilizarlos sin obligación de compensarte por ello (del mismo modo que tú no tienes obligación de ofrecerlos).**
- **Cuando utilizas una aplicación, esta puede solicitarte permiso para acceder a tu contenido e información y al contenido y la información que otros han compartido contigo. Exigimos que las aplicaciones respeten tu privacidad**

¿Puede solicitar una copia de sus datos?
Sí

f) ¿Qué puede hacer el proveedor con los datos que usted carga?
R. Hacerlos públicos personas que utilizan las página o que son ajenas, personalizar anuncios, mostrar publicaciones a mis gustos, mostrar publicaciones con origen en una ubicación cercana al a mía.

g) ¿Qué sucede con sus datos cuando cierra su cuenta?
R. Al eliminar la cuenta todo tu contenido se volverá inaccesible al instante, aunque la empresa tardará 90 días en eliminar tus datos. Mensajes privados permanecerán, así como copias de algunos materiales permanezcan en nuestra base de datos, pero se disocien de identificadores personales.

2.-

a) ¿Qué puede hacer para protegerse?
R. Leer términos y condiciones antes de proporcionar datos personales a servicios, casi también informarse sobre como las aplicaciones que ya estoy de alta manejan mis datos en la plataforma y a quienes se le está dando mi información.
También sería bueno limitar la información que estoy proporcionando y no publicar cosas que puedan ser valioso para mis privacidad.

b) ¿Qué puede hacer para proteger su cuenta y proteger sus datos?
No dar información que no quiera que sean difundidos y utilizados sin su consentimiento.

3.2.2.3 Lab Discover Your Own Risky Online Behavior

(De acuerdo a la encuesta *Explore los términos de la política de servicio* dada en el laboratorio)

Puntuación: 10 ptos.

Resultados

0: usted es muy seguro en línea.

0 – 3: usted es medianamente seguro en línea pero aún debe cambiar su comportamiento para que sea totalmente seguro.

3 – 17: tiene un comportamiento poco seguro en línea y un alto riesgo de ser comprometido.

18 o más: es muy poco seguro en línea y será comprometido

Reflexión

Después de analizar su comportamiento en línea, ¿qué cambios implementaría para protegerse en línea? Siempre al navegar por internet asegurar que los sitios web que visito son seguros, así como asegurar que cualquier entrada a mi dispositivo no lo comprometa a ataques. No conectarme a redes que no tenga la confianza de ser seguros, y analizar cualquier dispositivo que conecte a mi computadora.