Actividad 09. Generar contraseñas seguras

CONTRASEÑAS SEGURAS

La protección con contraseña es una técnica de control de acceso que ayuda a mantener datos importantes protegidos de hackers garantizando que solo se puede acceder con las credenciales correctas.

La protección con contraseña es una de las herramientas de seguridad de datos más común disponible para los usuarios, pero se pueden traspasar fácilmente si no se crearon teniendo en cuenta a los hackers. Las organizaciones pueden facilitar una mejor administración de contraseñas mediante la implementación de una solución de protección de contraseñas diseñada para bloquear las contraseñas débiles, las variantes repetitivas y cualquier término que podría ser fácil de adivinar.

¿Por qué es importante la protección con contraseña?

Las contraseñas son la primera línea de defensa contra el acceso no autorizado de archivos, dispositivos y cuentas en línea. Las contraseñas seguras ayudan a proteger los datos de usuarios y software malintencionados. Cuanto más segura sea la contraseña, más protegida estará la información. El uso de contraseñas no seguras se parece mucho a dejar abierta la puerta del coche o tu casa: simplemente no es seguro.

Consecuencias de las contraseñas no seguras

Si una persona promedio tiene más de 150 cuentas en línea, la fatiga de las contraseñas es una realidad. Es tentador utilizar contraseñas simples o la misma contraseña para varias cuentas, en lugar de crear contraseñas exclusivas para cada una. No obstante, la complacencia de las contraseñas puede tener consecuencias devastadoras para las empresas y los usuarios individuales.

Para las personas, la pérdida de valiosa información personal, financiera y médica puede tener repercusiones económicas y reputacionales duraderas. Es posible que las víctimas no puedan comprar un coche, alquilar un piso o conseguir una hipoteca; e incluso pueden llegar a denegarles servicios médicos críticos. Para muchos, restaurar su reputación y volver a tener una vida normal tendrá un coste de tiempo y dinero.

Cuando los ciberdelincuentes obtienen acceso no autorizado a los datos de una organización, las consecuencias pueden ser graves. Las empresas pueden experimentar una pérdida significativa de ingresos y propiedad intelectual e industrial, así como una interrupción de las operaciones. También pueden incurrir en multas reglamentarias y sufrir daños en su reputación.

Los hackers utilizan técnicas cada vez más sofisticadas para robar contraseñas.

¿Cómo se piratean las contraseñas?

Los usuarios malintencionados utilizan una amplia variedad de tácticas para robar contraseñas, por ejemplo:

- Ataques por fuerza bruta, un método que utiliza un sistema de prueba y error para descifrar contraseñas y credenciales de inicio de sesión, para obtener acceso no autorizado a cuentas y sistemas.
- Relleno de credenciales, el uso automatizado de nombres de usuario y contraseñas robados para obtener acceso no autorizado a cuentas en línea.
- Ataques de diccionario, que intentan descifrar una contraseña introduciendo todas las palabras del diccionario, utilizando derivaciones de dichas palabras con sustituciones de caracteres alfabéticos y alfanuméricos, y empleando contraseñas y frases clave filtradas.
- Registro de pulsaciones de teclas, el uso de un programa de software para realizar un seguimiento de las pulsaciones de teclas de un usuario para robar PIN, números de tarjeta de crédito, nombres de usuario, contraseñas, etc.

- Malware, un software malintencionado diseñado para dañar o explotar los sistemas y, en muchos casos, robar contraseñas.
- Difusión de contraseña, el uso de una contraseña individual en muchas cuentas para evitar los bloqueos de cuentas y permanecer desapercibidos.
- Phishing, que engaña a los usuarios para que compartan sus credenciales con hackers que suplantan a instituciones y proveedores legítimos.

La mejor forma de protegerse contra hackers de contraseñas es:

- Utilizar contraseñas seguras en todos los dispositivos y cuentas.
- Desconfiar de los enlaces y los archivos adjuntos.
- Proteger de la vista los documentos en papel, las pantallas de los dispositivos y los teclados, para que los delincuentes no puedan robar contraseñas mirando por encima del hombro del objetivo.
- Evitar acceder a datos personales y financieros con una Wi-Fi pública.
- Instalar software antivirus y antimalware en todos los dispositivos.

Cómo crear una contraseña segura

Las contraseñas seguras son útiles para defenderte de ciberataques y reducir el riesgo de una vulneración de seguridad. Normalmente, son largas (12 caracteres como mínimo) e incluyen letras mayúsculas, letras minúsculas, números y caracteres especiales. Las contraseñas seguras no deben incluir información personal. Sigue estas directrices para crear contraseñas seguras:

- Utiliza al menos de ocho a doce caracteres.
- Utiliza una combinación de letras, números y símbolos.
- Utiliza al menos una letra mayúscula.
- Utiliza una contraseña diferente para cada una de tus cuentas.

- Utiliza palabras inusuales y poco comunes. Recurre a letras de canciones, citas o frases populares para que la contraseña sea más fácil de recordar. Por ejemplo, utilizar las dos primeras letras de cada palabra de la frase “Casa Tomás era mi restaurante favorito del Portezuelo” podría generar la contraseña: `CaToermirefadePo97`

Algunos ejemplos de contraseñas seguras son:

```
Cook-Shark-33-Syrup-Elf
Tbontbtitq31!
Seat_Cloud_17_Blimey
```

Las contraseñas no seguras a menudo contienen información personal o siguen patrones de teclado. Algunos ejemplos de contraseñas no seguras son:

```
1234567.
1111111.
Qwerty.
Qwerty123.
Contraseña.
Contraseña1.
1q2w3e.
Abc123.
```

En los siguientes artículos se habla de cómo generar contraseñas seguras y herramientas para descifrarlas:

- Cómo crear una contraseña segura y tener una cuenta más protegida
- Gestión de contraseñas seguras
- Cinco ideas de contraseñas seguras para aumentar tu seguridad
- Cómo crear y gestionar contraseñas seguras
- Las mejores herramientas para crackear contraseñas

Herramientas para descifrar contraseñas

- **John the Ripper**: una herramienta gratuita y de código abierto para descifrar contraseñas para auditoría y recuperación. John the Ripper admite cientos de tipos de cifrado y hash, incluidos Unix, Windows, macOS, WordPress, servidores de bases de datos, sistemas de archivos, archivos y más.
- **Hashcat:** una herramienta avanzada de recuperación de contraseñas gratuita y de código abierto. Hashcat se autodenomina «el descifrador de contraseñas más rápido del mundo» y proporciona funciones avanzadas como redes de descifrado distribuido.
- **Caín y Abel:** una herramienta gratuita de recuperación de contraseñas para computadoras con Windows. Caín y Abel utilizan técnicas como ataques de contraseña de fuerza bruta, diccionario y criptoanálisis.
- **RainbowCrack**: una herramienta gratuita y de código abierto para descifrar hash que utiliza tablas Rainbow. RainbowCrack está disponible para Windows y Linux y admite la aceleración de GPU mediante GPU NVIDIA y AMD.
- **Aircrack-ng:** un conjunto gratuito y de código abierto de herramientas de seguridad de redes Wi-Fi. Aircrack-ng incluye utilidades para monitorear, capturar paquetes, atacar, probar y descifrar contraseñas de Wi-Fi.
- **Hydra**: una herramienta gratuita y de código abierto para descifrar el inicio de sesión en red en paralelo. Hydra puede descifrar docenas de protocolos, incluidos Cisco, HTTP(S), ICQ, IMAP, MySQL, Oracle, SMTP y más.
- **THC Hydra:** una herramienta gratuita y de código abierto para descifrar contraseñas como "prueba de concepto". THC Hydra está disponible para Windows, macOS y Linux y admite protocolos como FTP, SMTP y HTTP-GET.
- **Medusa:** una herramienta gratuita, de código abierto, rápida y masivamente paralela para descifrar contraseñas. Medusa puede realizar pruebas de contraseñas de fuerza bruta contra múltiples hosts o usuarios simultáneamente.

Se pide:

1. Indica los factores que hay que tener en cuenta para elaborar contraseñas seguras.
2. Elaborar una herramienta (programa, hoja de cálculo…) para generar contraseñas seguras de forma aleatoria.
3. Indica sitios web donde generar contraseñas seguras.
4. Instala, utiliza y describe una de las herramientas para descifrar contraseñas indicadas