Sistemas Informáticos

UD5. Actividad 1

Programación de tareas Linux

INDICE

INDICE IMÁGENES

INTRODUCCIÓN

Las contraseñas son esenciales para proteger nuestra información en internet. Sin embargo, muchas personas usan combinaciones fáciles de adivinar o las repiten en varias cuentas, lo que facilita que los atacantes accedan a sus datos. Para evitar esto, se utilizan algoritmos especiales que hacen que las contraseñas sean más seguras y difíciles de descifrar.

Estos algoritmos convierten las contraseñas en códigos cifrados que no pueden leerse directamente. Algunos de los más utilizados son bcrypt, Argon2 y SHA-256, que hacen que incluso si alguien roba los datos, no pueda recuperar la contraseña original fácilmente. Además, se utilizan técnicas como los salts y pepper, que añaden seguridad extra para evitar ataques como la fuerza bruta o las tablas rainbow.

En este trabajo, explore los algoritmos más importantes para proteger contraseñas y por qué son necesarios. También hablaremos de las mejores prácticas para crear contraseñas seguras, como el uso de gestores de contraseñas y la autenticación en dos pasos. Conocer estos métodos nos ayuda a mejorar nuestra seguridad en línea y a evitar que nuestra información caiga en manos equivocadas.

Fig1.1

¿Por qué es importante proteger las cuentas de usuario?

Proteger las cuentas de usuario es fundamental en la era digital, ya que contienen información personal, financiera y profesional que puede ser utilizada de forma maliciosa por ciberdelincuentes. Muchas veces, las cuentas están vinculadas a servicios bancarios, redes sociales, correos electrónicos y archivos personales. Si una cuenta es comprometida, el atacante puede robar dinero, acceder a información sensible o incluso suplantar la identidad del usuario para cometer fraudes.

Uno de los mayores riesgos es el reutilizar contraseñas en diferentes plataformas. Si un sitio web sufre una filtración de datos, los atacantes pueden usar esas credenciales en otros servicios para intentar acceder a más cuentas. Además, en el caso de empresas, un ataque a las credenciales de un empleado puede poner en peligro datos confidenciales y afectar la reputación de la organización.

Por estos motivos, es esencial emplear contraseñas seguras, utilizar gestores de contraseñas y activar mecanismos de seguridad adicionales como la autenticación en dos pasos (2FA).

Fig1.2

Principales ataques para robar contraseñas

Los ciberdelincuentes utilizan diversas estrategias para robar contraseñas y obtener acceso no autorizado a cuentas. Los ataques más comunes incluyen:

1. Ataques de fuerza bruta

Este método consiste en probar diferentes combinaciones de contraseñas hasta encontrar la correcta. Los atacantes usan programas automáticos que pueden generar millones de combinaciones en poco tiempo. Cuanto más corta y simple sea la contraseña, más fácil será descifrarla con este tipo de ataque.

Cómo prevenirlo:

Usar contraseñas largas de al menos 12-16 caracteres.

Evitar contraseñas predecibles o basadas en palabras comunes.

2. Ataques de diccionario

En este caso, los atacantes utilizan bases de datos con listas de contraseñas comunes y palabras del diccionario para intentar acceder a cuentas. Muchas personas usan contraseñas como "123456", "password" o "qwerty", que pueden ser descifradas en segundos.

Cómo prevenirlo:

Usar una combinación de letras mayúsculas y minúsculas, números y símbolos.

Evitar palabras del diccionario o frases fácilmente adivinables.

3. Phishing

El phishing es uno de los métodos más efectivos para robar credenciales. Consiste en engañar a la víctima para que revele su contraseña a través de un sitio web falso o un correo electrónico fraudulento.

Fig1.3

Cómo prevenirlo:

No hacer clic en enlaces sospechosos en correos electrónicos o mensajes.

Verificar siempre la URL del sitio web antes de ingresar credenciales.

Activar 2FA para que, aunque alguien robe la contraseña, no pueda acceder a la cuenta.

4. Malware y keyloggers

El malware es un software malicioso que puede instalarse en un dispositivo sin que el usuario lo note. Algunos tipos, llamados keyloggers, registran las pulsaciones del teclado para capturar contraseñas y otra información sensible.

Fig1.4

Cómo prevenirlo:

Mantener el sistema operativo y los programas actualizados.

No descargar archivos ni programas de fuentes desconocidas.

Usar un antivirus y realizar análisis periódicos del dispositivo.

5. Ataques con tablas rainbow

Estos ataques se usan para descifrar contraseñas almacenadas en bases de datos con un hash débil o sin medidas de seguridad adicionales. Se basan en bases de datos precalculadas de valores hash y sus contraseñas correspondientes.

Cómo prevenirlo:

Usar algoritmos de hashing seguros como bcrypt o Argon2.

Aplicar salts aleatorios para hacer que cada contraseña cifrada sea única.

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

Fig1.5

CREA CONTRASEÑAS ROBUSTAS

Una contraseña robusta es aquella que es difícil de adivinar y resistente a los ataques mencionados. Para lograrlo, se recomienda seguir estos principios:

- Longitud mínima de 12-16 caracteres (más es mejor).
- Usar una combinación de letras mayúsculas y minúsculas, números y símbolos.
- Evitar información personal, como nombres, fechas de nacimiento o palabras comunes.
- No reutilizar contraseñas en diferentes sitios.
- Usar frases de contraseña, que son más fáciles de recordar y más seguras (ejemplo: Sol&MarC4min@r3s).

Ejemplo de una mala contraseña: 12345678
Ejemplo de una buena contraseña: #p4t0N3gr0!C0m3Ques0

Una alternativa segura es utilizar un gestor de contraseñas, que genera y almacena contraseñas complejas sin necesidad de recordarlas.

GESTORES DE CONTRASEÑA

Los gestores de contraseñas son herramientas que permiten almacenar, generar y gestionar credenciales de manera segura. Estos programas utilizan cifrado fuerte para proteger la información y solo requieren recordar una contraseña maestra.

Ventajas de usar un gestor de contraseñas:
Evita el uso de contraseñas débiles o repetidas.
Facilita la creación de contraseñas seguras y aleatorias.
Protege las contraseñas con cifrado avanzado.

Fig1.6

Algunas opciones recomendadas:

Bitwarden (gratis y de código abierto).

LastPass (opción gratuita y premium).

1Password (muy usado en empresas).

Dashlane (enfocado en seguridad y facilidad de uso).

ACTIVA LA AUTENTIFICACIÓN DE DOS FACTORES (2FA)

La autenticación en dos factores (2FA) agrega una capa extra de seguridad al requerir un segundo método de verificación, además de la contraseña.

Ejemplos de 2FA:

- Códigos enviados por SMS o correo electrónico.
- Aplicaciones de autenticación como Google Authenticator, Authy o Microsoft Authenticator.
- Llaves de seguridad físicas como YubiKey.

¿Por qué es importante activar el 2FA?

Dificulta el acceso a las cuentas incluso si alguien roba la contraseña.

Protege cuentas sensibles como correos electrónicos, bancos y redes sociales.

Evita accesos no autorizados incluso si se reutiliza una contraseña filtrada.

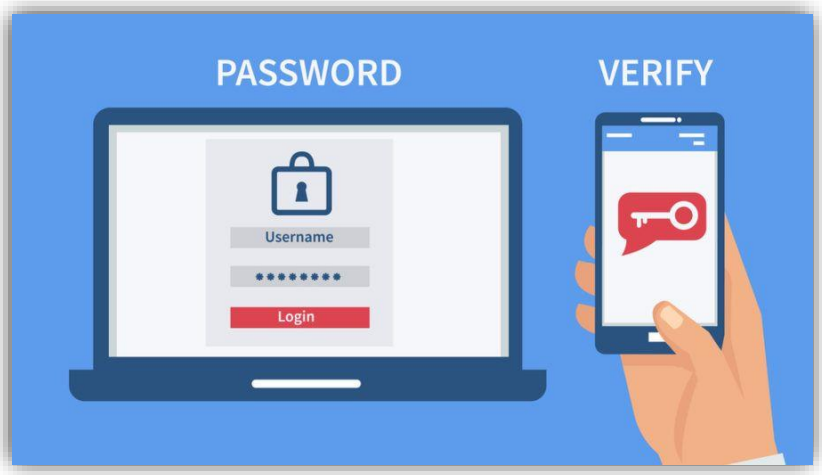

Fig1.7

Cómo activarlo:

Ingresar a la configuración de seguridad de la cuenta.

Buscar la opción de autenticación en dos pasos o 2FA.

Elegir el método preferido (SMS, aplicación de autenticación o llave física).

La autenticación en dos pasos es una de las formas más efectivas para proteger cuentas y evitar accesos no autorizados.

ALGORITMOS PARA ENCRIPTAR CONTRASEÑAS

Cuando se almacenan contraseñas, no deben guardarse en texto plano, ya que esto permitiría que cualquier persona con acceso a la base de datos pueda leerlas. Para evitarlo, se utilizan algoritmos criptográficos, que convierten las contraseñas en códigos cifrados.

Existen dos tipos principales de algoritmos para proteger contraseñas:

- Algoritmos de hashing: Transforman la contraseña en un código irreversible. Se usan principalmente para almacenar contraseñas de manera segura.
- Algoritmos de cifrado: Protegen la información convirtiéndola en datos ilegibles, pero permiten descifrarla con una clave adecuada. Se utilizan cuando es necesario recuperar la contraseña original.

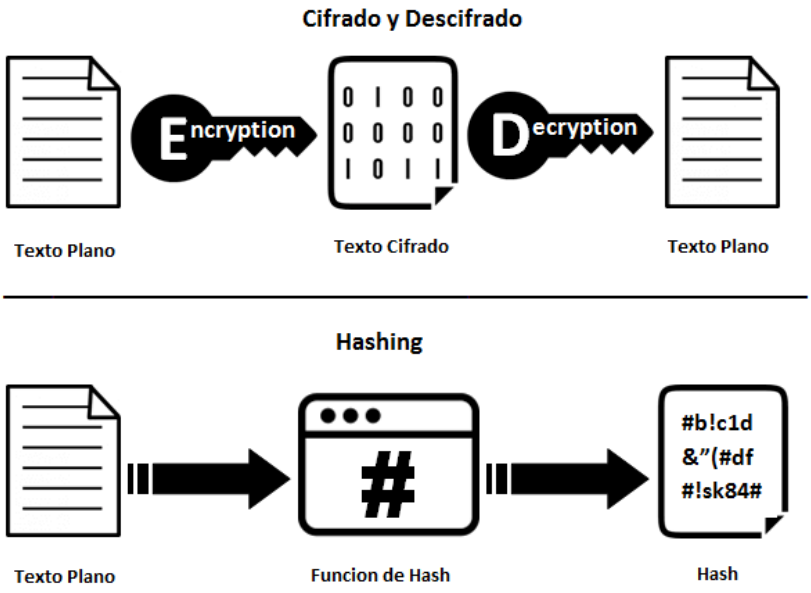

Fig1.8

1. MD5 (Message Digest 5)

Fue uno de los primeros algoritmos de hashing, generando un código de 128 bits. Aunque rápido y eficiente, hoy en día es inseguro porque permite ataques de colisión y fuerza bruta con facilidad.

- No es adecuado para contraseñas, pero aún se usa para verificar la integridad de archivos.

2. SHA-1 (Secure Hash Algorithm 1)

Mejora de MD5 que genera un hash de 160 bits. Aunque más seguro, ya no se recomienda porque en 2017 se demostró que puede ser vulnerado con suficiente poder computacional.

- Uso recomendado: No es seguro para contraseñas, pero aún se emplea en algunos sistemas heredados.

3. SHA-2 (SHA-256, SHA-512)

Evolución de SHA-1 que ofrece mayor seguridad y resistencia a ataques de colisión. Sus variantes más comunes son SHA-256 y SHA-512, utilizadas en blockchain y certificados digitales.

- Uso recomendado: Es seguro, pero al ser un algoritmo rápido, no es ideal para contraseñas sin medidas adicionales como salts y múltiples iteraciones.

4. AES (Advanced Encryption Standard)

A diferencia de los anteriores, AES es un algoritmo de cifrado que permite proteger datos confidenciales mediante claves de 128, 192 o 256 bits. Es altamente seguro y se usa en comunicaciones encriptadas, pero no es ideal para contraseñas, ya que requiere una clave para desencriptar los datos.

- Uso recomendado: Protección de archivos y datos sensibles, pero no para almacenamiento de contraseñas.

5. Argon2 (El más seguro para contraseñas)

Ganador de la Password Hashing Competition en 2015, Argon2 es actualmente el algoritmo más recomendado para almacenar contraseñas. Su versión Argon2id combina seguridad contra ataques de hardware avanzado y fuerza bruta, permitiendo ajustar el uso de memoria y procesamiento para hacerlo más resistente.

- Uso recomendado: Es la mejor opción para el almacenamiento seguro de contraseñas en sistemas modernos.

Conclusión

Proteger nuestras cuentas de usuario es fundamental para evitar robos de información y fraudes en línea. Los atacantes utilizan diversos métodos para obtener credenciales, como ataques de fuerza bruta, phishing y malware. Para mitigar estos riesgos, es clave usar contraseñas seguras, no reutilizarlas y complementar la seguridad con gestores de contraseñas y autenticación en dos factores.

Siguiendo estas buenas prácticas, podemos reducir significativamente el riesgo de que nuestras cuentas sean comprometidas y mantener nuestra información segura en el mundo digital.

Bibliografía

Incibe_

MetaCompliance

Programacion.net

wikipedia