Gestión de contraseñas y autenticación de dos factores

Nombre: _____

Fecha: _____

Puntaje: _____

1.

¿Qué es un gestor de contraseñas?

1. Un programa que almacena y cifra las contraseñas de manera segura.
2. Un tipo de virus que roba contraseñas.
3. Una extensión del navegador que solo guarda marcadores.

Respuesta correcta:
A.

Un programa que almacena y cifra las contraseñas de manera segura.

2.

¿Cuál es el término en español para la contraseña principal que desbloquea un gestor de contraseñas?

Respuesta: _____

Respuesta correcta:

3.

Dentro de los factores de autenticación, ¿cuál de los siguientes corresponde a 'algo que eres'?

1. Contraseña
2. Código SMS
3. Huella dactilar
4. Llave de seguridad física

Respuesta correcta:
C.

Huella dactilar

4.

¿Qué es un ataque de 'phishing'?

1. Un programa malicioso que se instala en el sistema.
2. Un intento de engaño para obtener información confidencial haciéndose pasar por una entidad legítima.
3. Un método de fuerza bruta para adivinar contraseñas.

Respuesta correcta:
B.

Un intento de engaño para obtener información confidencial haciéndose pasar por una entidad legítima.

5.

¿Cuál es la abreviatura de Time-based One-Time Password (contraseña de un solo uso basada en tiempo)?

Respuesta: _____

Respuesta correcta:

TOTP

6.

¿Por qué es peligroso reutilizar la misma contraseña en diferentes sitios web?

1. Porque es más difícil de recordar.
2. Porque es una práctica recomendada por seguridad.
3. Porque si un sitio sufre una violación de datos, el atacante puede acceder a otras cuentas.
4. Porque los sitios web pueden compartir contraseñas entre ellos.

Respuesta correcta:
C.

Porque si un sitio sufre una violación de datos, el atacante puede acceder a otras cuentas.

7.

¿Qué es una 'llave de seguridad' o 'security key' en el contexto de 2FA?

1. Un dispositivo físico que genera códigos de autenticación o se conecta por USB/NFC.
2. Una aplicación móvil que guarda contraseñas.
3. Un código impreso en papel para recuperar la cuenta.
4. Un mensaje SMS que envía un código temporal.

Respuesta correcta:
A.

Un dispositivo físico que genera códigos de autenticación o se conecta por USB/NFC.

8.

¿Cómo se llama el proceso de convertir una contraseña en texto plano en una cadena de caracteres de longitud fija (irreversible) para almacenarla de forma segura?

Respuesta: _____

Respuesta correcta:

hashing

9.

¿En qué consiste un ataque de 'fuerza bruta'?

1. Probar sistemáticamente todas las combinaciones posibles de caracteres hasta encontrar la contraseña correcta.
2. Engañar al usuario para que revele su contraseña.
3. Interceptar el tráfico de red para capturar contraseñas.

Respuesta correcta:
A.

Probar sistemáticamente todas las combinaciones posibles de caracteres hasta encontrar la contraseña correcta.

10.

¿Qué es el 'salting' en el almacenamiento de contraseñas?

1. Agregar una cadena aleatoria única a cada contraseña antes de aplicar el hash.
2. Encriptar la contraseña con una clave secreta.
3. Guardar la contraseña en texto plano pero en un archivo oculto.
4. Usar una contraseña maestra para todas las cuentas.

Respuesta correcta:
A.

Agregar una cadena aleatoria única a cada contraseña antes de aplicar el hash.

11.

¿Qué significan las siglas 2FA en español?

Respuesta: _____

Respuesta correcta:

12.

Entre SMS y una aplicación de autenticación basada en TOTP (como Google Authenticator), ¿cuál ofrece mayor seguridad para 2FA y por qué?

1. SMS, porque es más fácil de usar.
2. La aplicación TOTP, porque no es vulnerable a la interceptación de mensajes ni al SIM swapping.
3. Ambos tienen la misma seguridad.
4. Ninguno es seguro; solo las llaves físicas son seguras.

Respuesta correcta:
B.

La aplicación TOTP, porque no es vulnerable a la interceptación de mensajes ni al SIM swapping.

13.

¿Qué es una 'violación de datos' o 'data breach'?

1. Un acceso no autorizado a información personal almacenada por una organización.
2. Una actualización de software que corrige errores.
3. Un correo electrónico falso que solicita datos bancarios.

Respuesta correcta:
A.

Un acceso no autorizado a información personal almacenada por una organización.

14.

¿Cómo se llama el ataque que utiliza una lista predefinida de palabras comunes para intentar adivinar una contraseña?

Respuesta: _____

Respuesta correcta:

ataque de diccionario

15.

¿Cuál es la función principal de una 'bóveda de contraseñas' o 'password vault'?

1. Generar contraseñas aleatorias.
2. Almacenar y cifrar todas las contraseñas del usuario en un solo lugar.
3. Compartir contraseñas con otros usuarios automáticamente.
4. Recuperar contraseñas olvidadas sin intervención del usuario.

Respuesta correcta:
B.

Almacenar y cifrar todas las contraseñas del usuario en un solo lugar.

16.

¿Cuál de los siguientes NO se considera un factor de autenticación independiente en 2FA?

1. Contraseña + código SMS.
2. Contraseña + huella dactilar.
3. Contraseña + pregunta secreta de seguridad.
4. Contraseña + llave de seguridad física.

Respuesta correcta:
C.

Contraseña + pregunta secreta de seguridad.

17.

¿Cuál es el término general para una pieza de información utilizada para verificar la identidad de un usuario (como una contraseña, una huella o un token)?

Respuesta: _____

Respuesta correcta:

factor de autenticación

18.

¿Para qué sirve la técnica de 'key stretching' (estiramiento de clave) en la seguridad de contraseñas?

1. Para hacer que las contraseñas sean más largas de lo que el usuario las escribe.
2. Para aumentar el tiempo y recursos necesarios para probar cada intento de descifrado del hash.
3. Para reducir la fortaleza de la contraseña y hacerla más fácil de recordar.

Respuesta correcta:
B.

Para aumentar el tiempo y recursos necesarios para probar cada intento de descifrado del hash.

19.

¿Cuál de las siguientes es una ventaja de utilizar un gestor de contraseñas?

1. Solo necesitas recordar una contraseña fuerte.
2. Rellena automáticamente las contraseñas en los sitios web.
3. Cifra toda tu información almacenada.
4. Todas las anteriores.

Respuesta correcta:
D.

Todas las anteriores.

20.

¿Qué significan las siglas MFA en seguridad informática?

Respuesta: _____

Respuesta correcta:

Respuestas

1. **A.**

   Un programa que almacena y cifra las contraseñas de manera segura.

3. **C.**

   Huella dactilar

4. **B.**

   Un intento de engaño para obtener información confidencial haciéndose pasar por una entidad legítima.

5. TOTP

6. **C.**

   Porque si un sitio sufre una violación de datos, el atacante puede acceder a otras cuentas.

7. **A.**

   Un dispositivo físico que genera códigos de autenticación o se conecta por USB/NFC.

8. hashing

9. **A.**

   Probar sistemáticamente todas las combinaciones posibles de caracteres hasta encontrar la contraseña correcta.

10. **A.**

    Agregar una cadena aleatoria única a cada contraseña antes de aplicar el hash.

12. **B.**

    La aplicación TOTP, porque no es vulnerable a la interceptación de mensajes ni al SIM swapping.

13. **A.**

    Un acceso no autorizado a información personal almacenada por una organización.

14. ataque de diccionario

15. **B.**

Almacenar y cifrar todas las contraseñas del usuario en un solo lugar.

16. **C.**

    Contraseña + pregunta secreta de seguridad.

17. factor de autenticación

18. **B.**

    Para aumentar el tiempo y recursos necesarios para probar cada intento de descifrado del hash.

19. **D.**

    Todas las anteriores.

20.