# Ciberseguridad. Amenazas II.

1. ¿Qué es un ataque de fuerza bruta?

a) Una táctica para compartir contraseñas con amigos.

b) Una técnica para descifrar contraseñas mediante la prueba sistemática de todas las combinaciones posibles.

c) Una estrategia para proteger contraseñas.

d) Un método para crear contraseñas seguras.

1. ¿Cómo funciona un ataque de fuerza bruta?

a) Adivinando aleatoriamente las contraseñas de un usuario al probar pocas combinaciones.

b) Solicitando la contraseña al usuario directamente.

c) Probando múltiples combinaciones de contraseñas hasta encontrar la correcta.

d) Utilizando programas informáticos para eliminar contraseñas.

1. ¿Qué tipo de cuentas pueden ser objetivo de un ataque de fuerza bruta?

a) Cuentas de videojuegos.

b) Cuentas en línea como correos electrónicos o cuentas bancarias.

c) Cuentas de películas en línea.

d) Cuentas de redes sociales.

1. ¿Cómo pueden los ciberdelincuentes probar miles o incluso millones de combinaciones de contraseñas en poco tiempo?

a) Enviando correos electrónicos a las personas solicitando sus contraseñas.

b) Haciendo llamadas telefónicas para solicitar contraseñas.

c) Adivinando manualmente cada contraseña.

d) Utilizando programas informáticos especializados.

1. ¿Por qué los ciberdelincuentes pueden utilizar un ataque de fuerza bruta en redes Wi-Fi?

a) Para intentar descifrar la clave de seguridad de la red.

b) Para mejorar la velocidad de conexión.

c) Para enviar mensajes a través de la red de forma segura.

d) Para compartir la conexión con más personas.

1. ¿Qué pueden obtener los ciberdelincuentes si tienen éxito en un ataque de fuerza bruta a una cuenta en línea?

a) Publicidad gratuita para la cuenta.

b) Recompensas monetarias.

c) Mejoras en la seguridad de la cuenta.

d) Acceso no autorizado a la cuenta.

1. ¿Por qué es importante utilizar contraseñas seguras frente a un ataque de fuerza bruta?

a) Porque reduce la velocidad de conexión a Internet.

b) Porque aumenta la dificultad para descifrarlas.

c) Porque hace que las contraseñas sean más fáciles de adivinar.

d) Porque permite compartir las contraseñas con amigos.

1. ¿Cuál es un ejemplo de un sistema que puede ser objetivo de un ataque de fuerza bruta?

a) Redes Wi-Fi.

b) Juegos de video.

c) Tiendas en línea.

d) Aplicaciones de mensajería.

1. ¿Qué pueden hacer los usuarios para protegerse contra un ataque de fuerza bruta?

a) Utilizar contraseñas complejas y únicas.

b) Ignorar cualquier advertencia de seguridad en sus dispositivos.

c) Utilizar la misma contraseña para todas las cuentas en línea.

d) Compartir contraseñas con amigos cercanos.

1. ¿Qué se recomienda para protegerse contra los ataques de fuerza bruta?

a) Utilizar contraseñas fuertes y seguras.

b) Compartir contraseñas con amigos cercanos.

c) Desactivar cualquier medida de seguridad adicional.

d) Utilizar contraseñas cortas y simples.

1. ¿Por qué es importante utilizar la autenticación de dos factores?

a) Proporciona una capa adicional de seguridad.

b) Ralentiza el acceso a las cuentas.

c) Hace que sea más fácil adivinar contraseñas.

d) No tiene ningún efecto en la seguridad de las cuentas.

1. ¿Qué tipo de método adicional de verificación se puede utilizar según el texto?

a) Una contraseña adicional.

b) Un escáner de huellas dactilares.

c) Una pregunta de seguridad.

d) Un código enviado al teléfono móvil.