# Ciberseguridad. Amenazas 2.

1. ¿Qué es un ataque de día cero?

a) Un ataque que afecta solo a algunos sistemas operativos.

b) Un ataque que aprovecha una vulnerabilidad aún no descubierta ni parcheada.

c) Un ataque que ocurre en el primer día del año.

d) Un ataque que solo ocurre durante el día.

1. ¿Cuál NO es un objetivo de un ataque de día cero?

a) Descubrir nuevas vulnerabilidades.

b) Tomar el control de un sistema.

c) Instalar Malware.

d) Robar información confidencial de los usuarios.

1. ¿Qué tipo de acciones maliciosas pueden llevar a cabo los atacantes que descubren una vulnerabilidad de día cero?

a) Ejecutar código malicioso, tomar el control de un sistema, robar información confidencial o instalar malware.

b) Incrementar la velocidad y rendimiento del sistema.

c) Ayudar a los desarrolladores a corregir las vulnerabilidades.

d) Mejorar la seguridad del sistema y protegerlo de futuros ataques.

1. ¿Cuál de los siguientes es un ejemplo de ataque de día cero?

a) Stuxnet.

b) WannaCry.

c) Heartbleed.

d) ILOVEYOU.

1. ¿En qué año ocurrió el ataque de Stuxnet?

a) 2010.0

b) 2008.0

c) 2012.0

d) 2014.0

1. ¿Cuál era el objetivo del ataque Stuxnet?

a) Espiar a los usuarios de dispositivos móviles.

b) Distribuir malware a través de sitios web comprometidos.

c) Cifrar los archivos de los usuarios y exigir un rescate.

d) Alterar el funcionamiento de las centrifugadoras utilizadas en el enriquecimiento de uranio.

1. ¿Cuál de las siguientes afirmaciones es verdadera sobre los ataques de día cero?

a) No se pueden prevenir ni proteger contra ellos.

b) Son corregidos por los fabricantes antes de que sean explotados.

c) Son conocidos por el público en general.

d) Representan una amenaza grave para la seguridad.

1. ¿Cuál de las siguientes medidas es recomendada para protegerse contra los ataques de día cero?

a) Descargar software de fuentes no confiables.

b) Mantener el software y los sistemas operativos desactualizados.

c) Realizar copias de seguridad periódicas de los datos importantes.

d) Abrir correos electrónicos y mensajes de origen desconocido.

1. ¿Qué es recomendado hacer para protegerse contra los ataques de día cero?

a) Mantener el software y los sistemas operativos actualizados con los últimos parches de seguridad.

b) Hacer clic en enlaces y archivos adjuntos de correos electrónicos desconocidos.

c) Descargar software de fuentes desconocidas.

d) Utilizar software obsoleto y sin actualizaciones.

1. ¿Qué software fue descontinuado en 2020 debido a su historial de vulnerabilidades y baja seguridad?

a) Adobe Flash Player.

b) Microsoft Office.

c) Google Chrome.

d) Mozilla Firefox.

1. ¿Cuál es la importancia de parchear las vulnerabilidades y mantener sistemas y software actualizados?

a) Aumenta la probabilidad de ser víctima de un ataque de día cero.

b) Minimiza la posibilidad de sufrir un ataque exitoso.

c) No es necesario parchear las vulnerabilidades, ya que no representan una amenaza.

d) Ayuda a los atacantes a encontrar nuevas vulnerabilidades.

1. ¿Qué tipo de soluciones de seguridad se recomiendan para prevenir los ataques de día cero?

a) Soluciones de seguridad gratuitas sin actualizaciones.

b) Ninguna solución de seguridad es efectiva contra los ataques de día cero.

c) Antivirus y firewalls que incluyan capacidades de detección y prevención de ataques de día cero.

d) Software pirata y sin licencia.

1. ¿Cuál de las siguientes acciones NO ayuda a protegerse contra los ataques de día cero?

a) Ejecutar archivos adjuntos de origen desconocido.

b) Realizar copias de seguridad periódicas de los datos importantes.

c) Utilizar defensas de seguridad confiables.

d) Mantener el software y los sistemas operativos actualizados.

1. ¿Qué significa que un ataque de día cero aproveche una vulnerabilidad en un sistema o aplicación que aún no ha sido descubierta ni parcheada por el fabricante?

a) El fabricante es consciente de la vulnerabilidad, pero no ha desarrollado un parche de seguridad.

b) El ataque se produce después de que se descubra la vulnerabilidad, pero antes de que se instale un parche.

c) El ataque se produce después de que se descubra la vulnerabilidad, pero antes de que se desarrolle un parche.

d) El ataque se produce antes de que se descubra la vulnerabilidad.

1. ¿Cuál de las siguientes afirmaciones resume mejor los ataques de día cero?

a) Son ataques que se originan en países extranjeros y no representan una amenaza local.

b) Son explotaciones de vulnerabilidades desconocidas que aún no han sido corregidas por los fabricantes.

c) Son ataques que solo afectan a sistemas operativos, no a aplicaciones de software.

d) Son ataques que ocurren exclusivamente durante el primer día de cada mes.

1. ¿Qué es un ataque de fuerza bruta?

a) Un programa automatizado que bloquea los intentos de acceso después de varios intentos fallidos.

b) Un código enviado al teléfono móvil para verificar la identidad de un usuario.

c) Un intento de acceder a cuentas en línea mediante contraseñas seguras.

d) Un método utilizado por los ciberdelincuentes para descifrar contraseñas probando todas las combinaciones posibles.

1. ¿Cuál es el objetivo principal de un ataque de fuerza bruta?

a) Acceder a cuentas bancarias en línea.

b) Proteger archivos y comunicaciones encriptadas.

c) Obtener acceso no autorizado a redes Wi-Fi.

d) Descifrar contraseñas o claves de seguridad.

1. ¿Qué son los "crackers" en el contexto de los ataques de fuerza bruta?

a) Actualizaciones de seguridad proporcionadas por los proveedores de software.

b) Programas automatizados utilizados por los ciberdelincuentes.

c) Medidas de seguridad implementadas en sistemas de cifrado.

d) Contraseñas seguras y únicas.

1. ¿En qué casos utilizan los ciberdelincuentes ataques de fuerza bruta?

a) Para intentar acceder a cuentas en línea, sistemas de cifrado y claves de acceso a redes Wi-Fi.

b) Para verificar la seguridad de una contraseña en línea.

c) Para bloquear o limitar los intentos de acceso después de un número determinado de intentos fallidos.

d) Para proteger archivos y comunicaciones encriptadas.

1. ¿Cómo se pueden proteger las cuentas en línea contra los ataques de fuerza bruta?

a) Utilizando autenticación de dos factores (2FA).

b) Configurando sistemas que bloqueen o limiten los intentos de acceso después de varios intentos fallidos.

c) Utilizando contraseñas seguras y únicas.

d) Todas las respuestas son correctas.

1. ¿Cuál es la función de la autenticación de dos factores (2FA)?

a) Proporcionar una capa adicional de seguridad mediante un segundo método de verificación.

b) Descifrar contraseñas y claves de seguridad mediante la prueba de todas las combinaciones posibles.

c) Proteger archivos y comunicaciones encriptadas.

d) Probar diferentes combinaciones de contraseñas en un corto período de tiempo.

1. ¿Por qué es importante utilizar contraseñas seguras y únicas?

a) Para dificultar los ataques de fuerza bruta y que las claves descubiertas sirvan en otros servicios.

b) Para acceder a cuentas bancarias en línea.

c) Para enviar códigos de verificación al teléfono móvil.

d) Para proteger archivos y comunicaciones encriptadas.

1. ¿Cuál es uno de los métodos utilizados en los ataques de fuerza bruta?

a) Prueba exhaustiva y sistemática de todas las combinaciones posibles de contraseñas.

b) Configuración de bloqueos en sistemas de cifrado.

c) Uso de programas especializados para enviar códigos de verificación.

d) Actualización de software con las últimas mejoras de seguridad.

1. ¿Qué pueden intentar los ciberdelincuentes al utilizar ataques de fuerza bruta en redes Wi-Fi?

a) Acceder a cuentas bancarias en línea.

b) Bloquear o limitar los intentos de acceso después de varios intentos fallidos.

c) Enviar códigos de verificación al teléfono móvil.

d) Descifrar la clave de acceso a la red Wi-Fi.

1. ¿Qué deben evitar los usuarios para protegerse de los ataques de fuerza bruta?

a) Utilizar autenticación de dos factores (2FA).

b) Implementar mecanismos de bloqueo que limiten los intentos de acceso.

c) Utilizar contraseñas débiles o predecibles.

d) Mantener el software actualizado con las últimas actualizaciones de seguridad.

1. ¿Qué se busca al utilizar un ataque de fuerza bruta en sistemas de cifrado?

a) Descifrar la clave de cifrado probando todas las posibles combinaciones.

b) Utilizar autenticación de dos factores (2FA) para una mayor seguridad.

c) Acceder a cuentas en línea como correos electrónicos y redes sociales.

d) Implementar mecanismos de bloqueo para proteger contra ataques de fuerza bruta.

1. ¿Cuál es el propósito de las actualizaciones de seguridad y parches proporcionados por los proveedores de software?

a) Descifrar contraseñas y claves de seguridad.

b) Corregir vulnerabilidades conocidas que podrían ser explotadas en ataques de fuerza bruta.

c) Enviar códigos de verificación al teléfono móvil.

d) Proteger archivos y comunicaciones encriptadas.

1. ¿Qué es un ataque man-in-the-middle?

a) Una medida de seguridad para evitar el robo de contraseñas.

b) Una técnica para proteger la información confidencial en línea.

c) Un método utilizado para bloquear el acceso a redes Wi-Fi públicas.

d) Una técnica en la que un atacante intercepta y manipula la comunicación entre dos personas.

1. ¿Qué puede hacer un atacante en un ataque man-in-the-middle?

a) Enviar mensajes de advertencia de seguridad a los usuarios.

b) Leer, modificar o incluso insertar información en los mensajes transmitidos.

c) Proteger la información personal de los usuarios.

d) Establecer conexiones seguras en redes Wi-Fi públicas.

1. ¿Cuál es un ejemplo común de ataque man-in-the-middle?

a) Utilizar contraseñas seguras en transacciones financieras en línea.

b) Interceptar el tráfico de Internet en una red Wi-Fi de una cafetería o biblioteca.

c) Manipular la apariencia de un sitio web para engañar a los usuarios.

d) Descubrir la contraseña de una red Wi-Fi probando en poco tiempo muchas contraseñas posibles.

1. ¿Qué puede hacer un atacante en un ataque man-in-the-middle en una red Wi-Fi pública?

a) Mejorar la velocidad de conexión en la red Wi-Fi pública.

b) Proteger la información personal de los usuarios.

c) Interceptar todo el tráfico de Internet y leer información confidencial.

d) Bloquear el acceso a la red Wi-Fi pública.

1. ¿Qué puede ocurrir en un ataque man-in-the-middle en transacciones financieras en línea?

a) Un atacante puede enviar mensajes de advertencia de seguridad a los usuarios.

b) Un atacante puede bloquear la conexión al sitio web seguro.

c) Un atacante puede interceptar los detalles de la tarjeta de crédito y realizar compras fraudulentas.

d) Un atacante puede proteger la información personal de los usuarios.

1. ¿Cómo actúa un atacante en un ataque man-in-the-middle?

a) Como un experto en criptografía.

b) Como un intermediario silencioso que manipula la información transmitida sin dar señales de ello.

c) Como un proveedor confiable de redes Wi-Fi públicas.

d) Como un intermediario que roba información gracias a una web falsa que simula ser la página web auténtica de un banco.

1. ¿Qué medidas se pueden tomar para protegerse de un ataque man-in-the-middle en redes Wi-Fi?

a) No ingresar información personal en sitios web con conexiones seguras.

b) Utilizar redes Wi-Fi cualquiera, como las proporcionadas en sitios públicos.

c) Utilizar redes Wi-Fi seguras y confiables, como las proporcionadas por las escuelas o los hogares.

d) Utilizar contraseñas fuertes en las redes Wi-Fi.

1. ¿Qué señal puede indicar la presencia de un ataque man-in-the-middle en un sitio web?

a) Mensajes de advertencia de seguridad enviados por el atacante.

b) Un candado en la barra de direcciones del navegador.

c) Cambios inesperados en la apariencia del sitio web.

d) Conexiones lentas en la red Wi-Fi.

1. ¿Qué puede hacer un atacante en un ataque man-in-the-middle en una red Wi-Fi pública?

a) Bloquear el acceso a la red Wi-Fi pública y no permitir su uso.

b) Proteger la información personal de los usuarios.

c) Interceptar todo el tráfico de Internet y leer información confidencial.

d) Mejorar la velocidad de conexión en la red Wi-Fi pública.

1. ¿Qué puede ocurrir en un ataque man-in-the-middle en transacciones financieras en línea?

a) Un atacante puede proteger la información personal de los usuarios.

b) Un atacante puede enviar mensajes de advertencia de seguridad a los usuarios.

c) Un atacante puede interceptar los detalles de la tarjeta de crédito y realizar compras fraudulentas.

d) Un atacante puede bloquear la conexión al sitio web seguro.

1. ¿Cómo actúa un atacante en un ataque man-in-the-middle?

a) Como un proveedor confiable de redes Wi-Fi públicas.

b) Como un defensor de la seguridad cibernética.

c) Como un intermediario silencioso que manipula la información transmitida.

d) Como un experto en criptografía.