

AMENAZAS DE CIBERSEGURIDAD

1. Apropiación de formulario

- 1.1. ¿Qué es la apropiación de formulario y cómo se lleva a cabo?
- 1.2. ¿Cuál es un ejemplo común de apropiación de formulario mencionado en el texto?
- 1.3. ¿Cómo pueden los ciberdelincuentes dirigir a los usuarios a sitios web falsos o aplicaciones fraudulentas?
- 1.4. ¿Por qué es importante que los usuarios verifiquen la autenticidad de los sitios web y las aplicaciones antes de proporcionar información personal?

2. Ataque de abrevadero

- 2.1. ¿Qué es un ataque de abrevadero y cómo se lleva a cabo?
- 2.2. ¿Escribe un ejemplo de cómo los ciberdelincuentes utilizan sitios web falsos en un ataque de abrevadero?
- 2.3. ¿Cómo pueden los atacantes aprovechar una cuenta de correo electrónico comprometida en un ataque de abrevadero?
- 2.4. ¿Qué medidas pueden tomar los usuarios para protegerse contra los ataques de abrevadero?

3. Ataque de día cero

- 3.1. ¿Qué es un ataque de día cero y por qué se le llama así?
- 3.2. ¿Qué ventaja tienen los atacantes en un ataque de día cero en comparación con otros tipos de ciberataques?
- 3.3. ¿Puedes dar un ejemplo de cómo un hacker podría llevar a cabo un ataque de día cero en un sistema operativo popular?
- 3.4. ¿Qué acciones pueden tomar los usuarios para reducir el riesgo de ser víctimas de un ataque de día cero en sus navegadores web?

4. Ataque de fuerza bruta

- 4.1. ¿Qué es un ataque de fuerza bruta y cómo funciona?
- 4.2. ¿Cuál es el objetivo principal de un ataque de fuerza bruta?
- 4.3. ¿Puedes dar un ejemplo de cómo un hacker podría usar un ataque de fuerza bruta para acceder a una cuenta en línea?
- 4.4. ¿Qué medidas pueden tomar los usuarios para protegerse contra los ataques de fuerza bruta en sus contraseñas?

5. Ataque man-in-the-middle

- 5.1. ¿Qué es un ataque man-in-the-middle y cómo funciona?
- 5.2. ¿Cuál es el papel del atacante en un ataque man-in-the-middle?
- 5.3. ¿Puedes dar un ejemplo de cómo un atacante podría llevar a cabo un ataque man-in-the-middle en una red Wi-Fi pública?
- 5.4. ¿Qué medidas pueden tomar los usuarios para protegerse contra los ataques man-in-the-middle en redes públicas?

6. Botnet

- 6.1. ¿Qué es una botnet y cuál es su propósito principal?
- 6.2. ¿Cómo puede un atacante controlar una botnet?
- 6.3. ¿Qué tipo de actividades maliciosas puede llevar a cabo una botnet?
- 6.4. ¿Qué medidas pueden tomar los usuarios para protegerse contra las botnets y evitar que sus dispositivos sean parte de una?

7. Brecha de seguridad

- 7.1. ¿Qué es una brecha de seguridad y qué causa su aparición?
- 7.2. ¿Puedes dar un ejemplo de cómo un ataque de phishing puede resultar en una brecha de seguridad en una empresa?
- 7.3. ¿Cuál es un ejemplo de una brecha de seguridad que puede ocurrir en un entorno escolar, según el texto?
- 7.4. ¿Qué medidas pueden tomar las organizaciones para prevenir las brechas de seguridad y proteger la información confidencial?

8. DNS poisoning

- 8.1. ¿Qué es el DNS poisoning y cuál es su objetivo principal?
- 8.2. ¿Cómo podría un ciberdelincuente llevar a cabo un ataque de DNS poisoning en un servidor DNS?
- 8.3. ¿Qué es el "pharming" y cómo está relacionado con el DNS poisoning?
- 8.4. ¿Qué medidas pueden tomar los usuarios para protegerse contra el DNS poisoning al navegar por internet?

9. DoS (Ataque de Denegación de Servicio)

- 9.1. ¿Qué es un ataque de denegación de servicio (DoS) y cuál es su objetivo principal?
- 9.2. ¿Puedes describir el "ataque de inundación de paquetes" y cómo se relaciona con un ataque DoS?
- 9.3. ¿Qué sucede durante un "ataque de inundación SYN" y cómo afecta a los sistemas afectados?
- 9.4. ¿Qué medidas de seguridad pueden implementar las empresas y los usuarios para protegerse contra los ataques de denegación de servicio?

10. Filtración de datos

- 10.1. ¿Qué es la filtración de datos y cómo puede ocurrir?
- 10.2. ¿Puedes dar un ejemplo de cómo un hacker podría llevar a cabo una filtración de datos en una empresa?
- 10.3. ¿Cómo puede un empleado contribuir a una filtración de datos sin darse cuenta?
- 10.4. ¿Qué medidas pueden tomar tanto las empresas como los individuos para protegerse contra la filtración de datos?

11. Hijacking

- 11.1. ¿Qué es el hijacking en términos de ciberseguridad?
- 11.2. ¿Puedes explicar cómo funciona el "secuestro de sesión" como un ejemplo de hijacking?
- 11.3. ¿Qué es el "secuestro de dominio" y cómo puede afectar a un sitio web?
- 11.4. ¿Qué medidas pueden tomar los usuarios para protegerse contra el hijacking de sus cuentas en línea?

12. Malvertising

- 12.1. ¿Qué es el malvertising y cómo funciona como forma de ciberataque?
- 12.2. ¿Puedes explicar cómo un anuncio malicioso puede infectar un dispositivo sin necesidad de que el usuario haga clic en él?

- 12.3. ¿Cuál es un ejemplo de un engaño común utilizado en el malvertising para atraer a los usuarios a hacer clic en un anuncio?
- 12.4. ¿Qué medidas pueden tomar los usuarios para protegerse contra el malvertising al navegar por Internet?

13. Password spraying

- 13.1. ¿Qué es el password spraying y cómo difiere de otros métodos de ataque de contraseñas?
- 13.2. ¿Cuál es el propósito del password spraying para los ciberdelincuentes?
- 13.3. ¿Puedes dar un ejemplo de cómo un atacante podría llevar a cabo un password spraying en cuentas de correo electrónico?
- 13.4. ¿Qué medidas pueden tomar tanto los usuarios como las organizaciones para protegerse contra el password spraying?

14. Pharming

- 14.1. ¿Qué es el pharming y cómo difiere del phishing en términos de cómo los usuarios son redirigidos a sitios web falsos?
- 14.2. ¿Cómo puede un atacante llevar a cabo un pharming al manipular la configuración de los servidores DNS?
- 14.3. ¿Qué riesgos plantea el pharming para los usuarios al acceder a sitios web legítimos?
- 14.4. ¿Qué medidas pueden tomar los usuarios para protegerse contra el pharming al navegar por Internet?

15. Vulnerabilidad

- 15.1. ¿Qué es una vulnerabilidad en ciberseguridad y cómo puede ser aprovechada por los ciberdelincuentes?
- 15.2. ¿Cuál es un ejemplo de vulnerabilidad relacionada con la falta de actualización de software?
- 15.3. ¿Cómo puede una contraseña débil representar una vulnerabilidad en la seguridad de una cuenta en línea?
- 15.4. ¿Qué medidas pueden tomar los usuarios y las organizaciones para mitigar los riesgos asociados con las vulnerabilidades en los sistemas informáticos?