# Seguridad en redes y protocolos HTTPS

Nombre: _____

Fecha: _____

Puntaje: _____

---

**1.**

¿Cuál es el propósito principal del protocolo HTTPS?

1. Acelerar la carga de páginas web
2. Cifrar la comunicación entre cliente y servidor
3. Reducir el ancho de banda utilizado
4. Almacenar contraseñas de forma segura

**Respuesta correcta:**
**B.**

Cifrar la comunicación entre cliente y servidor

**2.**

¿Qué componente del ecosistema TLS emite y firma los certificados digitales?

1. El servidor web
2. El navegador del cliente
3. Una Autoridad de Certificación (CA)
4. El registrador de dominios

**Respuesta correcta:**
**C.**

Una Autoridad de Certificación (CA)

**3.**

En el handshake TLS 1.2, ¿qué intercambian cliente y servidor para acordar el cifrado?

1. Las claves privadas
2. Una lista de cifrados (cipher suites) soportados
3. Los certificados raíz de las CA
4. Las contraseñas de usuario

**Respuesta correcta:**
**B.**

Una lista de cifrados (cipher suites) soportados

**4.**

¿Qué tipo de certificado valida solo que el dominio está controlado por quien solicita el certificado, sin verificar la identidad legal?

1. Extended Validation (EV)
2. Organization Validation (OV)
3. Domain Validation (DV)
4. Wildcard

**Respuesta correcta:**
**C.**

Domain Validation (DV)

**5.**

¿Cómo se llama el mecanismo que obliga al navegador a comunicarse solo por HTTPS, evitando conexiones HTTP inseguras? (siglas)

Respuesta: _____

**Respuesta correcta:**

HSTS

**6.**

¿Qué ventaja de seguridad aporta el uso de forward secrecy en TLS?

1. Permite reutilizar la misma clave de sesión en múltiples conexiones
2. Asegura que la clave de sesión no se pueda derivar a partir de la clave privada del servidor
3. Simplifica el proceso de renovación de certificados
4. Evita la necesidad de certificados digitales

**Respuesta correcta:**
**B.**

Asegura que la clave de sesión no se pueda derivar a partir de la clave privada del servidor

**7.**

En un ataque Man-in-the-Middle (MitM) contra HTTPS, ¿qué debe hacer el atacante para que el navegador confíe en la conexión?

1. Modificar los registros DNS sin alterar certificados
2. Insertar un certificado falso firmado por una CA que el navegador no conoce
3. Interceptar el tráfico y presentar un certificado válido para otro dominio
4. Obtener un certificado firmado por una CA de confianza para el dominio legítimo, pero usando una clave privada propia

**Respuesta correcta:**
**D.**

Obtener un certificado firmado por una CA de confianza para el dominio legítimo, pero usando una clave privada propia

**8.**

¿Qué protocolo de verificación permite consultar en tiempo real si un certificado ha sido revocado?

1. CRL (Certificate Revocation List)
2. OCSP (Online Certificate Status Protocol)
3. SSL Pinning
4. Certificate Transparency

**Respuesta correcta:**
**B.**

OCSP (Online Certificate Status Protocol)

**9.**

¿Cuál de las siguientes afirmaciones sobre TLS 1.3 es correcta?

1. Elimina la posibilidad de negociar cifrados inseguros y reduce los viajes de ida y vuelta (round trips) a 1 o 2
2. Requiere obligatoriamente el uso de certificados EV
3. No soporta el intercambio de claves con Diffie-Hellman
4. Solo permite cifrados simétricos, sin autenticación

**Respuesta correcta:**
**A.**

Elimina la posibilidad de negociar cifrados inseguros y reduce los viajes de ida y vuelta (round trips) a 1 o 2

**10.**

El ataque que consiste en interceptar una conexión HTTPS y degradarla a HTTP para leer el tráfico en texto plano se llama _____.

Respuesta: _____

**Respuesta correcta:**

SSL stripping

**11.**

¿Qué campo de un certificado X.509 indica los nombres de dominio para los cuales es válido?

1. Subject
2. Issuer
3. Subject Alternative Name (SAN)
4. Basic Constraints

**Respuesta correcta:**
**C.**

Subject Alternative Name (SAN)

**12.**

Un certificado wildcard (*.ejemplo.com) es válido para:

1. Cualquier subdominio de ejemplo.com, incluyendo subdominios de segundo nivel como a.b.ejemplo.com
2. Solo subdominios directos (un solo nivel), como www.ejemplo.com, pero no a.b.ejemplo.com
3. Cualquier dominio que termine en .com
4. Únicamente el dominio ejemplo.com, sin subdominios

**Respuesta correcta:**
**B.**

Solo subdominios directos (un solo nivel), como www.ejemplo.com, pero no a.b.ejemplo.com

**13.**

¿Qué ventaja tiene el uso de Certificate Transparency (CT)?

1. Elimina la necesidad de CA
2. Permite detectar certificados emitidos de forma fraudulenta al requerir que sean registrados en logs públicos
3. Acelera el handshake TLS en un 50%
4. Reemplaza a OCSP para la revocación

**Respuesta correcta:**
**B.**

Permite detectar certificados emitidos de forma fraudulenta al requerir que sean registrados en logs públicos

**14.**

En la autenticación mutua TLS (mutual TLS), el servidor también verifica la identidad del cliente mediante un certificado. ¿Cómo se denomina este flujo? (siglas)

Respuesta: _____

**Respuesta correcta:**

mTLS

**15.**

¿Cuál de los siguientes ataques aprovecha vulnerabilidades en la implementación de SSL/TLS para descifrar datos cifrados sin conocer la clave?

1. POODLE
2. Slowloris
3. SQL Injection
4. Cross-Site Scripting (XSS)

**Respuesta correcta:**
**A.**

POODLE

**16.**

¿Qué significa que un sitio web utilice 'mixed content' en una página servida por HTTPS?

1. Que incluye recursos (imágenes, scripts) cargados a través de HTTP
2. Que utiliza múltiples certificados SSL diferentes
3. Que combina contenido de texto e imágenes
4. Que ofrece versiones en varios idiomas

**Respuesta correcta:**
**A.**

Que incluye recursos (imágenes, scripts) cargados a través de HTTP

**17.**

¿Cuál es el propósito de la bandera 'Secure' en una cookie HTTP?

1. Indica que la cookie debe ser enviada solo a través de conexiones HTTPS
2. Firma digitalmente la cookie para verificar su integridad
3. Encripta el valor de la cookie en el lado del servidor
4. Impide que scripts del lado del cliente accedan a la cookie

**Respuesta correcta:**
**A.**

Indica que la cookie debe ser enviada solo a través de conexiones HTTPS

**18.**

Nombre del ataque que reutiliza una sesión TLS previamente establecida sin autenticación adecuada para suplantar al cliente: _____.

Respuesta: _____

**Respuesta correcta:**

replay attack

**19.**

¿Qué elemento del certificado X.509 permite vincular la clave pública a la identidad del titular?

1. La huella digital (thumbprint) del certificado
2. La firma digital de la CA emisora
3. El número de serie del certificado
4. La fecha de expiración

**Respuesta correcta:**
**B.**

La firma digital de la CA emisora

**20.**

En el contexto de HTTPS, ¿qué significa que un sitio implemente 'certificate pinning'?

1. El navegador almacena una copia local del certificado para acelerar conexiones futuras
2. El sitio asocia una o varias claves públicas específicas con su nombre de dominio, rechazando otras incluso si están firmadas por CA
3. Se exige que el certificado sea renovado cada 30 días
4. El servidor envía el certificado comprimido para reducir latencia

**Respuesta correcta:**
**B.**

El sitio asocia una o varias claves públicas específicas con su nombre de dominio, rechazando otras incluso si están firmadas por CA

## Respuestas

1. **B.**

   Cifrar la comunicación entre cliente y servidor

2. **C.**

   Una Autoridad de Certificación (CA)

3. **B.**

   Una lista de cifrados (cipher suites) soportados

4. **C.**

   Domain Validation (DV)

5. HSTS

6. **B.**

   Asegura que la clave de sesión no se pueda derivar a partir de la clave privada del servidor

7. **D.**

   Obtener un certificado firmado por una CA de confianza para el dominio legítimo, pero usando una clave privada propia

8. **B.**

   OCSP (Online Certificate Status Protocol)

9. **A.**

   Elimina la posibilidad de negociar cifrados inseguros y reduce los viajes de ida y vuelta (round trips) a 1 o 2

10. SSL stripping

11. **C.**

    Subject Alternative Name (SAN)

12. **B.**

    Solo subdominios directos (un solo nivel), como www.ejemplo.com, pero no a.b.ejemplo.com

13. **B.**

Permite detectar certificados emitidos de forma fraudulenta al requerir que sean registrados en logs públicos

14. mTLS
15. **A.**

    POODLE

16. **A.**

    Que incluye recursos (imágenes, scripts) cargados a través de HTTP

17. **A.**

    Indica que la cookie debe ser enviada solo a través de conexiones HTTPS

18. replay attack
19. **B.**

    La firma digital de la CA emisora

20. **B.**

    El sitio asocia una o varias claves públicas específicas con su nombre de dominio, rechazando otras incluso si están firmadas por CA