

PARCIAL 1Nombre: ALEJANDRO Apellidos: SANTORUM VARELA**Modelo 1**

Las siguientes preguntas solo tienen una respuesta correcta. Cada respuesta correcta suma 1 punto, cada incorrecta resta 1/3 y las no contestadas no puntúan. El test completo evalúa sobre 4 puntos del total del examen.

1. En el API de sockets POSIX ¿la implementación de qué función es susceptible a un ataque de denegación de servicio?
  - A. connect
  - B. bind
  - ☒ C. listen
  - D. socket
2. A través de las cookies, ¿puede saber Google qué artículos he comprado en Amazon?
  - A. Si tienen acuerdos de compartición de bases de datos, sí.
  - B. Si Google puede leer nuestra cookie de Amazon puede obtener toda la información de dicha cookie.
  - ☒ C. Es completamente imposible.
  - ☒ D. En las cookies que almacenamos en nuestro ordenador se encuentra almacenada toda nuestra actividad en internet y por tanto se dispone de toda la información.
3. Si en el protocolo HTTP realizamos ahora mismo una petición y en uno de los campos de cabecera se encuentra: "If-modified-since: Wed, 28 May 2019 18:38:00 GMT.", ¿qué devolverá el servidor?
  - A. 404 Not found
  - ☒ B. 304 Not modified
  - C. Ese campo de cabecera sólo es interpretable por los *proxy* y no por los servidores web.
  - D. 200 OK
4. En el protocolo HTTP, ¿cómo sabe el receptor dónde acaban los campos de la cabecera?
  - A. Porque se encuentra un `< /head >`
  - ☒ B. Porque hay dos `\r\n` consecutivos.
  - C. Porque se encuentra un `< body >`
  - D. Porque se envía en un paquete separado del cuerpo del mensaje.
5. Una conexión HTTP persistente significa que:
  - A. El cliente puede realizar varias peticiones simultáneas por la misma conexión
  - B. Ninguna de las anteriores es cierta
  - C. Un cliente puede conectarse a varios servidores diferentes con la misma conexión
  - ☒ D. El cliente puede realizar varias peticiones sin cerrar la conexión
6. Se dispone de un servidor y un cliente usando UDP como capa de transporte. ¿Cuál de las siguientes operaciones no hace ni el servidor ni el cliente?
  - A. socket
  - ☒ B. listen
  - C. sendto
  - D. bind
7. Si pones en una página WEB la URL "mailto:example@foo.com?subject=micontenido", ¿qué crees que hace?
  - A. Le indicará al usuario que debe mandar un correo a la dirección mostrada
  - ☒ B. Intentará cargar la página 'micontenido' del área del usuario example del servidor foo.com
  - ☒ C. Todas las URLs deben empezar con "http://".
  - ☒ D. Intentará enviar un correo con el asunto 'micontenido' a example@foo.com.



PARCIAL 2Nombre: ALEJANDRO Apellidos: SANTORUM VARELA**Modelo 6**

Las siguientes preguntas solo tienen una respuesta correcta. Cada respuesta correcta suma 1 punto, cada incorrecta resta 1/3 y las no contestadas no puntúan. El test completo evalúa sobre 4 puntos del total del examen.

1. ¿En qué modos de encadenamiento tiene sentido utilizar un *vector de inicialización*?
  - A. Solo en CBC
  - ☒ B. En todos aquellos en los que un bloque dependa de los anteriores
  - C. Solo en ECB
  - D. El IV no necesita ser secreto, solo impredecible
2. Imagina que tu red corporativa está a punto de quedarse sin direcciones IP para asignar a las nuevas máquinas. ¿Qué esquema podría ayudarte?
  - A. NAT
  - B. DHCP
  - C. VPN
  - ☒ D. Todas las anteriores
3. ¿Cual de las siguientes afirmaciones es cierta?
  - ☒ A. La confidencialidad de un mensaje es la propiedad que permite que sólo el destinatario pueda leer el mensaje
  - ✗ B. La confidencialidad es la propiedad que permite que sólo el emisor pueda leer el mensaje
  - ✗ C. La autenticación de un mensaje es la propiedad que permite determinar que el destinatario es el correcto.
  - ✗ D. La autenticación de un mensaje es la propiedad que permite determinar que el mensaje no ha sido modificado.
4. Si Bernardo ( $K_B^+$ ,  $K_B^-$ ) le envía un mensaje a Alicia ( $K_A^+$ ,  $K_A^-$ ) y disponen de una función hash ( $H$ ) común y donde  $\oplus$  significa concatenación, ¿cual de los siguientes esquemas de mensaje carece de sentido?
  - ☒ A.  $K_B^+(m) \oplus K_B^+(H(m)) \oplus K_s(m)$
  - B.  $K_B^+(K_s) \oplus K_s(m \oplus H(m))$
  - ✗ C.  $K_B^+(K_A^-(K_s)) \oplus K_s(m) \oplus H(m)$
  - ✗ D.  $K_B^+(K_A^-(K_s)) \oplus K_s(m \oplus H(m))$
5. Para almacenar contraseñas de forma segura en disco se suele utilizar un valor aleatorio, denominado *salt*. ¿Cuál es su función?
  - A. Hacer la comida más sabrosa.
  - B. Evitar los ataques *offline*.
  - ☒ C. Evitar ambos tipos de ataques, *offline* y *online*.
  - D. Evitar los ataques *online*.
6. ¿Cual de las siguientes afirmaciones es falsa?
  - A. Un certificado puede recibirse directamente de la persona propietaria del certificado.
  - ☒ B. Es necesario tener la clave pública del propietario del certificado.
  - ✓ C. La clave pública de la entidad certificadora siempre está disponible
  - D. Un certificado puede recibirse directamente de la entidad certificadora
7. En una infraestructura de clave pública, PKI, el agente que valida la identidad del usuario se denomina:
  - ☒ A. RA, autoridad de registro
  - B. Ninguna de las anteriores
  - C. CA, autoridad de certificación



VA, autoridad de validación

8. En el handshake de SSL cada parte envía un número aleatorio a la otra. ¿Cuál es su finalidad?

- A. Evitar el ataque de *spoofing*
- B. Evitar el ataque de denegación de servicio
- ☒ C. Evitar el ataque de replicación
- D. Evitar el ataque de *man-in-the-middle*.

PARCIAL 3

Nombre: ALEJANDRO Apellidos: SANTORUM VAZELA

## Modelo 7

Las siguientes preguntas solo tienen una respuesta correcta. Cada respuesta correcta suma 1 punto, cada incorrecta resta 1/3 y las no contestadas no puntúan. El test completo evalúa sobre 4 puntos del total del examen.

- El OID de un objeto SNMP permite ...
  - ... definir los elementos básicos del protocolo SNMP con el que se va a operar.
  - ... describir las características del objeto SMI en el árbol MIB
  - ... introducir un objeto de la MIB en la SMI.
  - ☒ ... determinar de forma única el objeto SMI en el árbol MIB
- ¿Cuál de las siguientes características no es propia del protocolo SIP?
  - ☒ A. Provee mapeos de nombres a direcciones IP.
  - ☒ B. Provee mecanismos de establecimiento de llamada.
  - ☐ C. Provee de mecanismos para agregar nuevos medios durante la llamada
  - ☒ D. Provee mecanismos de transporte de contenido.
- ¿Cuál es el objetivo principal de un sistema de reproducción con retraso adaptativo?
  - ☒ A. Mejorar la reproducción multimedia
  - ☒ B. Adaptarse a la calidad del vídeo o del audio para enviarlos con la compresión adecuada.
  - ☒ C. Adaptarse a los gustos del usuario.
  - ☒ D. Notificar al gestor multimedia de adaptaciones necesarias a la red.
- ¿Cuál de las siguientes características no es propia de RTP?
  - A. Provee un número de identificación de paquete.
  - B. Provee de marcas de tiempo
  - C. Determina el tipo de carga.
  - ☒ D. Provee sincronización de flujos.
- ¿Qué mecanismo de recuperación de errores se comportará mejor ante una pérdida muy alta de los paquetes emitidos (igual o superior al 50%)?
  - ☒ A. Flujo embebido
  - B. Se comportan igual
  - C. FEC simple
  - D. Depende del patrón en el que se pierdan los paquetes
- Imagina una sesión RTP, en la que se está enviando video a 8 receptores a una tasa de 1 Mbps. ¿Cuál será la tasa a la que cada receptor puede devolver tráfico RTCP?
  - A. Aproximadamente 7,5 Kbps
  - B. Aproximadamente 5 Kbps
  - ☒ C. Aproximadamente 10 Kbps
  - D. Aproximadamente 12,5 Kbps
- ¿Cuál de los siguientes campos no es un campo de un objeto SMI?
  - A. Description
  - ☒ B. Object descriptor
  - ☒ C. Version
  - ☒ D. Syntax
- Se diseña un esquema de flujo embebido de tal forma que cada paquete con contenido multimedia incluye el propio paquete  $n$ , el paquete  $n-1$  en baja calidad y el paquete  $n-2$  en muy baja calidad. Si en determinado momento se pierden los paquetes  $m$ ,  $m+1$ ,  $m+2$  y  $m+3$ , pero se recibe el  $m+4$ . ¿En qué condiciones se reproduce el contenido multimedia?

no se repr.  
m y m+1

- A. El paquete  $m$  se reproduce en baja calidad; el  $m + 1$  en muy baja calidad y los otros dos no pueden reproducirse.
- B. Se pueden reproducir todos los paquetes, pero el paquete  $m$  en muy baja calidad y el  $m + 1$  en baja calidad.
- C. Se han perdido cuatro paquetes y es imposible recuperar su contenido de ninguna forma.
- ☒ D. El paquete  $m + 3$  se reproduce en baja calidad, el  $m + 2$  en muy baja calidad y los otros dos no pueden reproducirse.