Bloque I

1. Justifica por qué son falsas las siguientes afirmaciones: [1 punto]

a) Un cifrado que pretenda simular One Time Pad usando una clave aleatoria de un sólo uso de tamaño fijo, repetida hasta "cubrir" la totalidad del mensaje a cifrar, es suficiente para asegurar la propiedad de ser indondicionalmente seguro.

No es verdadera, para ser incondicionalmente seguro debería usar una clave binaria aleatoria, de un sólo uso, tan grande como el texto en claro. Sin embargo el enunciado presenta una de tamaño fijo que se repite hasta llegar al tamaño del texto en claro.
Incondicionalmente seguro: propiedad de los criptosistemas que garantizan que en el texto cifrado no existe información suficiente para determinar el texto en claro original. Son inmunes a análisis estadísticos (no hay relación estadística entre el texto en claro y el cifrado).

b) Para considerar que la vinculación entre un "usuario" y su clave pública presente en un certificado digital confiable basta con que se verifique que (1) el certificado esté emitido por una autoridad certificadora reconocida y (2) que no esté caducado en la fecha actual.

No es verdadera porque (1) además de ser emitido tuvo que ser creado y firmado por una CA reconocida por ambos y (2) si el participante que recibió el certificado digital puede recuperar la clave pública del otro participante y verificar su validez/autenticidad, usando para ello la clave pública de la CA para comprobar la firma digital.

c) En las firmas digitales basadas en algoritmos asimétricos se suelen emplear cifradores simétricos (por ejemplo DES o APS) como primer paso, para evitar tener que procesar la totalidad de los datos a firmar con cifradores asimétricos más costosos.

Es falsa, lo que se usa son funciones hash (por ejemplo MD5, SHA-256…). Son unos algoritmos unidireccionales que toman una cantidad arbitraria de datos y generan un valor de tamaño fijo (el resumen) específico para dichos datos.

d) Una de las formas de evitar las vulnerabilidades XSS en aplicaciones web es mediante el empleo de procedimientos almacenados, siempre y cuando éstos no utilicen directamente los parámetros introducidos por el usuario.

Eso es un método de evitar la vulnerabilidad SQL injection. Para XSS existen otras, tales como: (1) escapar caracteres problemáticos (<, >, `, ", &); (2) descartar cadenas con etiquetas peligrosas; (3) especial atención en zonas peligrosas, en etiquetas susceptibles de desencadenar ejecución de código JavaScript; (4) usar algún framework web que incluya soporte para evitar XSS, que proporcionen mecanismos para emitir código HTML sanitizado a partir de datos de la aplicación.

e) En el modo túnel de IPSec, utilzado por el protocolo AH (Authentication Header) se garantiza la confidencialidad de la carga útil como de las cabeceras de cada paquete.

Es falso ya que AH define una cabecera adicional donde se contiene información para autenticar del origen y asegurar integridad, en ningún momento menciona que garantiza la confidencialidad.
<u>Protocolo AH:</u> ofrece autenticación del origen de los paquetes IP (cabecera + datos). Soporta integridad + autentificación añadiendo al paquete IP un código MAC (Message Authenticaion Code) basado en funciones hash y claves secretas de autenticación.

2. Describe brevemente los siguientes conceptos: [0,6 puntos]

   a) Red Feistel.

   Es un esquema de cifrado por bloques basado en un cifrado producto que combina operaciones de confusión y difusión. Simula un cifrado de sustitución complejo mediante 2 o más operaciones de cifrado sencillas. Cada etapa de cifrado elemental combina sustituciones y permutaciones. El resultado final es criptográficamente más fuerte que cifrados elementales aislados.
   <u>Cifrador de bloque:</u> realiza las transformaciones de cifrado/descifrado sobre un bloque de elementos de tamaño fijo cada vez.
   <u>Cifrado producto:</u> combinar varias etapas de operaciones de sustitución y transposición/permutación aplicadas de forma secuencial.
   <u>Confusión:</u> pretender hacer que la relación entre la clave y el texto cifrado resulte lo más compleja posible.
   <u>Difusión:</u> pretender disipar la estructura estadística del texto en claro en el texto cifrado resultante.

   b) Random canary.

   Son unos valores aleatorios que el compilador coloca en las stack frames como separadores entre variables locales y datos de control. Se usan como contramedida en tiempo de compilación para prevenir el desbordamiento de buffer en pila. Ya que la secuencia de retorno generada por el compilador comprueba si al retornar de una llamada a función, estos random canaries fueron sobreescritos por un desbordamiento, abortando el programa.

   c) NIDS basado en firmas.

   Un NIDS (Network Intrusion Detection System), como su propio nombre indica, es un detector de intrusiones red. Capturan el tráfico de la red y lo evalúan para determinar si corresponde con una intrusión. Uno basado en firmas cuenta con una BD con firmas de ataques conocidos. (Una firma es un patrón que se corresponde con una amenaza/ataque/vulnerabilidad conocida) Sus ventajas son: (1) simple y eficiente; (2) efectivo detectando amenazas conocidas; (3) menos falsos positivos. Sus desventajas son: (1) baja utilidad ante amenazas nunca vistas; (2) vulnerable a técnicas de evasión; (3) en NIDS no pueden analizar tráfico de protocolos cifrados.

3. Describe en que consiste la inyección SQL en aplicaciones Web y señala qué posibles contramedidas existen para evitarla. [0,6 puntos]

   La inyección SQL consiste en insertar sentencias y/o comandos SQL en datos de entrada de usuario. Permite la generación dinámica de sentencias SQL usando parámetros que proporciona el usuario, pudiendo así cambiar la naturaleza de la petición que se va a ejecutar en el servidor de BD, pudiendo obtener un acceso no autorizado o no restringido a la BD. Este ataque es posible cuando hay entradas de usuario que se envían directamente desde la aplicación Web a la BD.
   Las contramedidas que existen son:
   (1) usar consultas parametrizadas, ya que separan la compilación de la consulta de su ejecución con los parámetros indicados.
   (2) usar procedimientos almacenados, de esta forma el código de acceso a la BD reside en el propio gestor en forma de procedimientos ya compilados.
   (3) uso de frameworks ORM (Object Relational Mapping) ya que por defecto suelen hacer uso de consultas parametrizadas.
   (4) escapado de caracteres problemáticos en SQL, esos caracteres seran interpretados como cadena.
   (5) filtrado de cadenas peligrosas, si se encuentra una de esas cadenas la descarta.

4. Enumera los servicios de seguridad ofrecidos por el protocolo SSL (Secure Socket Layer) / TLS (Transport Layer Security), detallando las estrategias que se siguen para implementarlos.

   Uno de los servicios es la <u>confidencialidad</u> y para ello se intercambian mensajes cifrados con claves simétricas. Al inicio de la sesión cliente y servidor acuerdan las claves que usarán.
   Otro de los servicios es la <u>autenticación de entidades</u>, en el que el cliente puede verificar la entidad del servidor mediante un mecanismo basado en firmas digitales + certificados digitales.
   El último servicio que ofrece es la <u>autenticación de mensajes</u>. Los paquetes SSL, además de ir cifrados, incluyen códigos HMAC para garantizar su integridad y autenticidad.

Bloque II

1. Describe las alternativas que existen en cuanto al funcionamiento interno de detectores de intrusiones (IDS/IPS). [0,4 puntos]

   Una de las alternativas es detectar intrusiones <u>en red</u>. Esto se hace capturando el tráfico de la red y evaluándolo para determinar si se corresponde con una intrusión. El análisis es a nivel de paquetes de red. Monitoriza el tráfico de una porción de la red. Suelen centrarse en ataques DoS, escaneo de puertos, explotación de vulnerabilidades…
   Otra alternativa es detectar intrusiones <u>en host</u>. Esto se hace analizando los eventos que se producen en un equipo determinado para saber si está sufriendo un ataque. Uno sensores (agentes) monitorizan un equipo en concreto. Tienen en cuenta logs del sistema y de aplicaciones, llamadas al sistema, modificaciones sobre el sistema de ficheros… Suelen centrarse en el abuso de privilegios.

2. ¿Qué es un certificado digital? ¿Para qué sirve? ¿Qué información contiene usualmente? Enumera qué otros elementos típicos conforman una infraestructura de clave pública (PKI), además de la propia autoridad de certificación. [0,4 puntos]

   Un certificado digital es un fichero generado por una autoridad certificadora (CA) que permite garantizar que una clave pública pertenece al usuario identificado en el certificado. La información que suele contener es: indentificación del propietario, clave pública del propietario, información adicional (validez, uso previsto…) y firma de la CA.
   Otros elementos, además de CA, que componen el PKI son: RA (autoridad de registro), repositorios (repositorio de certificados + CRL), VA (autoridad de validación), TSA (autoridad de sellado de tiempo) y entidades finales solicitantes del certificado (servidores, personas, software...)

3. Enumera y describe las características teóricas que deben de cumplir los algoritmos de hash criptográficos. Indica al menos dos ejemplos del uso práctico de los hash criptográficos. [0,4 puntos]
   (1) produce una salida de tamaño fijo
   (2) computacionalmente fácil de calcular
   (3) unidireccionalidad: para un valor hash(x) dado, es computacionalmente impracticable encontrar/construir el bloque x que lo origina.
   (4) resistencia débil a colisiones: para un bloque X es computacionalmente impracticable construir otro bloque Y != X con hash(Y) = hash(X)
   (5) resistencia fuerte a colisiones: computacionalmente impracticable encontrar/construir un par (X, Y) tal que hash(X) = hash(Y).
   Un ejemplo de uso sería el de disminuir el coste computacional a la hora de cifrar/descifrar con un alogritmo asimétrico información de gran tamaño, ya que habiendo pasado primero los datos por una función hash sólo debemos cifrar su resumen.
   Otro uso sería el de comprobar que un elemento en origen es el mismo que en destino. Si el creador original nos muestra cual es el resumen del fichero a descargar, una vez descargado en nuestro ordenador podemos comprobar que ese resumen sea igual, si no lo es, podemos decir que fue alterado y que por lo tanto no tenemos una copia del original.

4. Describe en qué consisten las vulnerabilidades de desbordamineto de buffer en pila (stack buffer overflow) y enumera las posibles contramedidas de emplear en tiempo de ejecución. [0,4 puntos]

   Las vulnerabilidades de stack buffer overflow consisten en ejecutar código arbitrario aportado por un atacante, normalmente shellcode que le proporcione un intérprete de comandos. Para ello el atacante desborda variables locales situadas debajo de la dirección de retorno de la función, estos datos que sobran sobreescriben dicha dirección de retorno, esta será sustituída por una nueva dirección que contenga el código malicioso.
   Las contramedidas que se pueden emplear en tiempo de ejecución son: usar CPUs y SOs con soporte de non executable address space, aleatorizar las posiciones relativas al stack, heap y código al cargar un ejecutable en memoria, usar IDS, seguimiento de alertas de vulnerabilidades e instalación de parches (actualizaciones, correcciones…) del software instalado y también consultar las bases de datos de vulnerabilidades.

5. Diferencias entre modo túnel y modo transporte en IPSec. [0,4 puntos]
   Modo túnel: (1) protege el paquete IP original al completo. (2) Se encapsual por completo en un nuevo paquete IPSec con su propia cabecera IP. (3) Se usa entre dos pasarelas IPSec creando una ruta segura entre ellas, un túnels seguro dentro del cuál viajan los paquetes IP originales. (4) Permite interconectar de forma segura equipos no-IPSec mediante el establecimiento de pasarelas IPSec, estructura típica en VPNs.
   Modo transporte: (1) protege sólo los datos del protocolo de nivel superior. (2) Las cabeceras AH ó ESP van a continuación de la cabecera IP original, forman parte de la carga útil del paquete IP y se mantiene la cabecera IP original. (3) Es de uso típico en SA extremo-extremo. (4) Los cálculos criptográficos se realizan sólo en los extremos de la comunicación.