Test Tema 126 #1

Actualizado el 13/04/2025

1. ¿Qué propiedades ofrecen las conexiones VPN que usan protocolos como PPTP, L2TP/IPsec y SSTP?

a) Encapsulación y autenticación.

b) Encapsulación y cifrado de datos.

c) Autenticación y cifrado de datos.

d) Encapsulación, autenticación y cifrado de datos.

2. Un detector de intrusiones actúa a:

a) nivel físico

b) nivel de enlace

c) nivel de red

d) nivel de aplicación

3. Según OWASP TOP TEN 2021, ¿cuál es el riesgo que ocupa la primera posición?:

a) Inyección

b) Falsificación de solicitudes del lado del servidor

c) Pérdida de control de acceso

d) Fallos en el cifrado

4. ¿Cuál de las siguientes respuestas NO es una estrategia para gestionar los riesgos?

a) Evitar el riesgo

b) Mitigar el riesgo

c) Transferir el riesgo

d) Subestimar el riesgo

5. ¿Qué se entiende por Smishing?

a) Utilización de técnicas de phishing pero para servicios asociados con voz sobre IP (VoIP).

b) Utilización de técnicas de phishing en los mensajes de texto de teléfonos móviles.

c) Es un mensaje de correo electrónico con contenido falso o engañoso y normalmente distribuído en cadena.

d) Es la capacidad de duplicar una página web para hacer creer al visitante que se encuentra en la página original en lugar de en la copiada.

6. La última revisión del Top Ten de OWASP data del año:

a) 2002

b) 2012

c) 2017

d) 2021

7. Proof Key for Code Exchange, PKCE, (RFC 7636) es una extensión del flujo de código autorización de OAuth 2.0 con el objetivo de:

a) Mejorar el rendimiento en el proceso de autorización.

b) Limitar ataques CSRF y de inyección de código de autorización.

c) Compatibilizar el flujo de autorización con sistemas legacy basados en WSS.

d) Permitir la concesión implícita, un flujo simplificado en el que el token de acceso se devuelve directamente al cliente.

8. Señale qué número de puerto debería usarse si se quiere configurar un servicio para la autenticación de redes Kerberos:

a) 88

b) 42

c) 74

d) 105

9. La intrusión de un virus informático del tipo gusano (worm) en un ordenador puede afectar, en primer lugar, por ocupación de todo el espacio disponible en disco:

a) La dimensión de confidencialidad de la información almacenada

b) La dimensión de disponibilidad de la información almacenada

c) La dimensión de integridad de la información almacenada

d) Las respuestas ‘a’ y ‘c’ son correctas

10. Un buen libro de claves podría ser:

a) Los números primos de 128 cifras

b) La guía de Paginas Blancas de Madrid 2005

c) El CD "Hung up" de Madonna

d) todas las anteriores

11. En el ámbito de la ciberseguridad, OWASP es:

a) El Proyecto Abierto de Seguridad en Acceso WIFI, que publica el documento "OWASP TOP-10" con los diez riesgos más críticos en el acceso a través de red inalámbrica.

b) El Protocolo Abierto de Seguridad en Aplicaciones Web. Una especificación abierta que permite que las organizaciones desarrollen sus aplicaciones de forma interoperable y confiable con otras organizaciones.

c) El Proyecto Online de Seguridad en Aplicaciones Web. Una plataforma que permite concienciar a las organizaciones sobre los riesgos de desarrollar, adquirir y mantener aplicaciones que estén en Internet.

d) El Proyecto Abierto de Seguridad en Aplicaciones Web. Una comunidad abierta dedicada a permitir que las organizaciones desarrollen, adquieran y mantengan aplicaciones y APIs en las que se pueda confiar.

12. ¿Qué se suele encontrar en una DMZ?

a) un proxy de correo

b) un cache web

c) un server web

d) todas las anteriores

13. En el establecimiento de una comunicación mediante SSL (Secure Sockets Layer), ¿cuál es el protocolo que especifica la forma de encapsular los datos que se van a intercambiar?

a) SSL Handshake.

b) SSL Record.

c) Cipher Secure Layer.

d) Secure Stocker Layer.

14. El sistema de gestión de la seguridad que autoriza el acceso de usuarios a recursos en entorno z/OS se llama:

a) ACF2

b) RACF

c) RADIUS

d) CICS

15. Señale la respuesta correcta. En una comunicación HTTPS, ¿qué tipo de cifrado se utiliza?

a) Simétrico exclusivamente.

b) Asimétrico exclusivamente.

c) No se utiliza ningún cifrado.

d) Tanto el simétrico como el asimétrico.

16. ¿Cómo podemos evitar el problema de la inyección de SQL a nivel de JDBC?:

a) Deben filtrarse previamente los ataques CSRF y XSS.

b) Debe evitarse el uso de procedimientos almacenados en la base de datos.

c) Debe utilizarse instrucciones SQL parametrizadas.

d) Si la consulta se realiza con Javascript, el filtrado debe realizarse en la parte del cliente mientras que si se realiza con PHP, el filtrado lo hará el servidor web.

17. Señale la respuesta FALSA:

a) HTTPS es la versión segura del protocolo HTTP.

b) Utiliza cifrado basado en SSL.

c) El puerto estándar es el 443.

d) Basta con que la dirección web empiece por https para que sea una página segura.

18. Un test de penetración proporciona todo lo siguiente salvo:

a) identificación de fallos de seguridad

b) demostración de los efectos de los fallos de seguridad

c) un método de corrección de los fallos

d) verificación de los niveles actuales de resistencia a la infiltración

19. ¿A qué nivel de la capa OSI actúan los WAFs?:

a) Nivel de la capa 4 - Transporte.

b) Nivel de la capa 5 - Sesión.

c) Nivel de la capa 6 - Presentación.

d) Nivel de la capa 7 - Aplicación.

20. El Centro Criptológico Nacional (CCN) es el organismo responsable de velar por la seguridad de las TIC en las administraciones públicas, y de formar en este campo a sus profesionales. El CCN depende de:

a) El Consejo Superior para la Administración Electrónica (Ministerio de la Presidencia)

b) La Fábrica Nacional de Moneda y Timbre (Ministerio de Economía y Hacienda)

c) La Dirección General de la Policía y la Guardia Civil (Ministerio del Interior)

d) El Centro Nacional de Inteligencia (Ministerio de Defensa)

21. Señale cuál de las siguientes es una variante de phishing, que en lugar del correo electrónico, se realiza a través de llamadas telefónicas a las víctimas:

a) Spear phishing

b) Smishing

c) Whaling

d) Vishing

22. ¿Cuál de los siguientes no es un requisito indispensable para una comunicación segura?

a) Auditoría

b) Confidencialidad

c) Integridad

d) Disponibilidad

23. Cuando las tareas de operación y programación no están segregadas, el responsable de seguridad debe de proveer controles:

a) compensatorios
b) administrativos
c) correctivos
d) de acceso

24. La inundación de un buzón de correo electrónico con un gran número de mensajes (e-mail spamming) afecta a:

a) La dimensión de confidencialidad de la información
b) La dimensión de disponibilidad de la información
c) La dimensión de integridad de la información
d) Las respuestas 'c' y 'a' son correctas

25. La intrusión basada en la habilidad del intruso en engañar a la gente para que rompa los procedimientos normales de seguridad se llama:

a) surfeo sobre los hombros (shoulder surfing)
b) huellas del cerebro (brain fingerprinting)
c) ingeniería social
d) subterfugio

26. Para detectar vulnerabilidades en el código fuente de una aplicación, ¿qué tipos de herramientas sirven de apoyo?:

a) SAST
b) DAST
c) WAF
d) WebGoat

27. La técnica maliciosa ClickJacking consiste en:

a) Introducir una capa de interfaz de usuario que simula la original con el fin de capturar datos comprometidos o privados

b) Introducir código SQL a través de un aplicación para conseguir ejecución de comandos de base de datos en el servidor

c) Programación masiva de clics (peticiones al servidor) con el fin dejar fuera de uso a un servidor de aplicaciones

d) Cifrado de documentos que se produce al seleccionar archivos a través de clics con el fin de obtener un rescate

28. ¿Cuál de las siguientes opciones se considera una metodología aplicada a estrategias de Seguridad del Software?

a) OWASP XP
b) OWASP SCRUM
c) OWASP RUP
d) OWASP SAMM

29. Al conjunto de tecnologías, normas y casos de uso que sirve para intercambiar información sobre identidad de usuarios en diferentes dominios de seguridad, y que permite que los usuarios de un dominio puedan acceder de forma segura a los datos o sistemas de otro dominio, sin la necesidad de que la administración de usuarios sea completamente redundante, se denomina:

a) Círculo de confianza.
b) Federación de identidades.
c) Bosque de Identidades.
d) Single Sign-On.

30. ¿Cuál de los siguientes no es un tipo de ataque?

a) Ataque por entropía

b) Ataque por fuerza bruta

c) Ataque con Tablas Arcoiris

d) Todos son tipos de ataques

31. ¿Cuál de los siguientes NO es un token de seguridad definido en las especificaciones Web Services Security (WS-Security)?

a) Username Token.

b) Binary Security Token.

c) Certificate Token.

d) SAML Token.

32. Cada uno de los equipos comprometidos y utilizados para lanzar un ataque de denegación de servicio distribuido contra un objetivo concreto se llama:

a) dongle

b) token

c) repetidor

d) zombie

33. Protocolo cliente/servidor que permite la autenticación y control de acceso de usuarios PPP:

a) ACF2

b) RACF

c) RADIUS

d) Kerberos

34. ¿Cómo se podrían mitigar los ataques XSS (Cross-Site Scripting) a una aplicación web?

a) Mediante el uso de certificados electrónicos.

b) Mediante el filtrado de datos maliciosos en la entrada de la aplicación, en la salida o en ambas.

c) Mediante la creación de reglas que permite un cortafuegos tradicional.

d) Mediante la configuración de listas de control de accesos (ACL).

35. Siguiendo el estándar OWASP de verificación de la Seguridad en Aplicaciones, cuál de estos factores de Protección General de Datos sólo es obligatorio en el nivel 3:

a) Verificar que la aplicación evita que los datos sensibles se almacenen en balanceadores de carga y caché de aplicaciones.

b) Verificar que la aplicación minimiza el número de parámetros en una petición, como parámetros ocultos, cookies y valores de encabezados.

c) Verificar que los backups se almacenan de forma segura, que impidan el robo o la corrupción de datos.

d) Verificar que la aplicación pueda detectar un número de peticiones anormalmente altos: por ejemplo, de IP's, de usuarios: totales por hora o por día.

36. En seguridad, que elemento no forma parte de los servicios de AAA:

a) Registro (accounting)

b) Autorización

c) Adaptación

d) Autenticación

37. ¿Qué tipos de token están establecidos en OAuth 2.0 (RFC 6749)?:

a) Token de acceso y token de actualización.

b) Token de acceso, ID token y JWT autofirmados.

c) Token Kerberos, token SAML y JSON Web Token (JWT).

d) Token federado y token de portador.

38. La política de mínimo privilegio trata de forzar los derechos de usuario más restrictivos:

a) Para ejecutar procesos de sistema

b) En su descripción de puesto de trabajo

c) Para realizar tareas autorizadas

d) En el acceso a servicios de red

39. El protocolo SSL (Secure Sockets Layer):

a) Es una capa de seguridad que opera siempre sobre el protocolo UDP.

b) No garantiza la integridad de la información intercambiada entre el cliente y el servidor.

c) Proporciona conexiones seguras solo en redes privadas y siempre que el cliente y el servidor pertenezcan a la misma subred IP.

d) Proporciona conexiones seguras sobre una red insegura garantizando, entre otros aspectos, integridad de datos transmitidos, privacidad de la conexión y autentificación del cliente y del servidor.

40. Señale cuál de entre los protocolos que componen SSL reside al nivel más bajo y proporciona el encapsulado a los protocolos del nivel superior:

a) Record.

b) Handshake.

c) Alert.

d) Change Cipher Spec.

41. Respecto a las normas técnicas elaboradas por la Internet Engineering Task Force (IETF) para mejorar la seguridad en Internet:

a) Kerberos proporciona la seguridad extremo a extremo en la capa IP.

b) Kerberos proporciona un medio de verificar la identidad de las entidades en una red abierta (sin protección).

c) Kerberos garantiza la integridad y autenticidad de las respuestas DNS.

d) Kerberos complementa DNSSEC para permitir a los administradores de dominio especificar las claves utilizadas para establecer una conexión criptográficamente segura a un servidor con ese nombre de dominio.

42. La vulnerabilidad de seguridad que ocurre cuando una aplicación web incluye contenido no fiable (por ejemplo, contenido suministrado por el usuario) en sus páginas por no haberlo validado o eliminado su contenido activo ('escapado') previamente de forma correcta, recibe el nombre de:

a) Defacing

b) Cross-Site Scripting (XSS)

c) Deserialization

d) Hijacking

43. ¿Cuál de estos protocolos criptográficos es el más seguro?:

a) SSL 3.0

b) TLS 1.1

c) TLS 1.2

d) TLS 1.3

44. El protocolo SSL (Secure Sockets Layer):

a) Proporciona conexiones seguras sólo en redes privadas y siempre que el cliente y el servidor pertenezcan a la misma subred IP.

b) No garantiza la integridad de la información intercambiada entre el cliente y el servidor.

c) Es una capa de seguridad que opera siempre sobre protocolo UDP.

d) Proporciona conexiones seguras sobre una red insegura garantizando la integridad de los datos transmitidos, privacidad de la conexión y autentificación del cliente y servidor.

45. ¿Cuál es el objetivo principal perseguido por un keylogger?

a) "Intercepción" y captura de datos.

b) Suplantación de identidad.

c) Denegación de servicio.

d) Manipulación de un recurso.

46. Indique cuál de estos productos no forman parte de los que proporcionan seguridad en el correo electrónico:

a) PGP

b) PEM

c) MOSS

d) Single MIME

47. Si quiero autenticar a un usuario:

a) Le pido su nombre

b) Le pido su DNI

c) Le pido su nombre y lo compruebo en una lista

d) todas las anteriores

48. En el contexto de la seguridad, el shoulder surfing consiste en:

a) Espiar a los usuarios modificando los navegadores web para obtener sus claves de acceso

b) Uso de aplicaciones intermedias llamadas shoulders para la obtención de los datos de navegación

c) Espiar físicamente a los usuarios, para obtener generalmente claves de acceso al sistema

d) Es un sinónimo del ataque man in the middle

49. En el ámbito de SIEM (Security Information and Event Management) es FALSO:

a) La tecnología SIEM nace de la combinación de las funciones de dos categorías de productos: SEM (gestión de eventos de seguridad) y SIM (gestión de información de seguridad).

b) La mayoría de los sistemas SIEM funcionan desplegando múltiples agentes de recopilación de forma jerárquica para recopilar eventos relacionados con la seguridad de dispositivos.

c) Son soluciones orientadas a mitigar ataques DDOS.

d) Las soluciones SIEM pueden ayudar al cumplimiento normativo, como por ejemplo, LOPD.

50. En un entorno de control de acceso a red basado en 802.1x, ¿qué protocolo de autenticación extendida utilizado para pasar la información de autenticación entre un suplicante y el servidor proporciona autenticación mutua mediante certificados digitales tanto en el cliente como en el servidor?

a) 802.1x PEAP

b) 802.1x EAP-TTLS

c) 802.1x EAP-TLS

d) 802.1x EAP-FAST

51. Un programa aparentemente inócuo y útil que al instalarlo el usuario, es utilizado por un tercero para realizar acciones no autorizadas sobre el sistema se llama:

a) honeypot
b) bomba lógica
c) virus
d) troyano

52. Sobre los ataques de fijación de sesión, ¿Cuál de las siguientes afirmaciones NO es aplicable?

a) Se trata de un ataque que se puede realizar mediante XSS (Cross-Site Scripting).
b) En este tipo de ataques se establece el valor de la cookie o el identificador de la sesión
c) Para que sea efectivo, la víctima no debe tener una sesión abierta
d) Este tipo de ataque sólo es efectivo en HTTP (nunca en HTTPS)

53. Una variante del phishing cuyo ataque se dirige hacia los objetivos de alta importancia dentro de una organización (altos directivos, políticos, etc.) o simplemente de gran transcendencia social (cantantes, artistas, famosos, etc.) se denomina:

a) Phreaking
b) Whaling
c) Phishing CEO
d) Cracker

54. Cada uno de los equipos que, dentro de un servicio distribuido de detección de intrusión, se instalan en los diferentes segmentos de red se llama:

a) cortafuegos
b) sonda
c) honeypot
d) bastión

55. Sobre los ataques CSRF (Cross-Site Request Forgery), ¿cuál de las siguientes afirmaciones NO es cierta?

a) Este ataque se puede realizar mediante XSS (Cross-Site Scripting) usando un objeto Image.

b) Permite al atacante generar peticiones a sitios web de terceros empleando los datos de autenticación del usuario víctima

c) Este ataque se puede realizar mediante XSS (Cross-Site Scripting) usando un objeto XMLHttpRequest

d) Este tipo de ataque es fácilmente identificable por el usuario y el navegador, existiendo mecanismos para mitigarlo

56. Un programa aparentemente inócuo y útil que al instalarlo el usuario comienza a realizar acciones destructivas sobre el sistema en un momento determinado de tiempo o a raíz de una acción concreta se llama:

a) sniffer
b) bomba lógica
c) troyano
d) gusano

57. Indicar cuál de las siguientes ventajas corresponde al uso de una pasarela de aplicación como cortafuegos:

a) Simplicidad
b) Facilidad de control
c) Rapidez
d) Transparencia

58. El término SQLInjection describe

a) Una posible forma de ataque sobre sentencias SQL

b) Una forma de introducir sentencias SQL dentro del código de un programa

c) Una técnica para dar valor a parámetros de entrada o de salida en una sentencia SQL

d) Un parámetro de optimización de sentencias SQL en Oracle

59. WTLS:

a) está basado en el protocolo TLS, pero optimizado para dispositivos móviles

b) proporciona mayor seguridad que TLS

c) es independiente de TLS, un protocolo diseñado específicamente para redes inalámbricas

d) ningunas de las anteriores

60. S/MIME utiliza los siguientes algoritmos de firma:

a) RC2

b) MD5

c) RSA

d) todos los anteriores

61. ¿Es posible que en una misma sesión/aplicación sobre Internet se utilicen simultáneamente los protocolos de seguridad IPSec y SSL?

a) No, se debe elegir en la implementación de la aplicación una de las dos, pues trabajan en el mismo nivel.

b) No, se debe elegir en la implementación de la aplicación una de las dos, pues son incompatibles a nivel de socket.

c) Sí, no debe presentar especiales problemas.

d) Sí, pero necesita una adaptación especial para que no se produzca una transposición de claves.

62. ¿Cuál de estas afirmaciones respecto a un WAF (Web Application Firewall) es correcta?:

a) Es un dispositivo que trabaja en la capa de red, nivel 2 OSI y que protege de diversos ataques tales como SQL Injection, Cross Site Scripting, etc

b) Un ejemplo de dispositivo WAF hardware es el mod_security desarrollado por la compañía Breach Security

c) Los dispositivos WAF permiten enrutar tráfico y/o traducir direcciones IPs mediante el uso de NAT, para la detección y protección de posibles ataques

d) Uno de los principales objetivos del proyecto WAFEC (Wireless Application Firewall Evaluation Criteria), es difundir la bondades de implantación de dispositivos WAF

63. En el ámbito de la ciberseguridad, respecto de las APT (Advanced Persistent Threats), señale la respuesta correcta:

a) Una APT comprende distintas fases entre las que se encuentra la extracción de datos.

b) Una APT no utiliza técnicas de ingeniería social para lograr el acceso al sistema objetivo.

c) Una APT es un conjunto de software malicioso con poca repercusión en el sistema objetivo y de fácil detección por las herramientas antivirus.

d) Una APT consiste en ataques avanzados próximos en el tiempo hacia objetivos generales e impersonales.

64. Un usuario de Kerberos:

a) Recibe un ticket para garantizar el acceso TGT

b) El ticket permite al usuario pedir acceso a los distintos recursos

c) El servicio de generación de tickets TGS genera los tickets con las claves de sesión

d) Todas las respuestas anteriores son correctas

65. Señale cuál de estas entidades no pertenece a una arquitectura SAML:

a) SP (Service Provider)

b) AP (Authentication Provider)

c) IdP (Identity Provider)

d) -

66. ¿Qué no se suele permitir en una DMZ?

a) Conexiones de ordenadores en la red externa a ordenadores en la red interna

b) Conexiones de ordenadores en la red interna a ordenadores en la dmz

c) Conexiones de ordenadores en la dmz a ordenadores en la red externa

d) Se permiten todas las anteriores

67. ¿Cómo evita SSL un ataque de "hombre en el medio"?

a) Usa certificados para autenticar la clave pública del servidor

b) Usa un valor aleatorio único por conexión en el protocolo de intercambio de credenciales

c) Usa claves de 128 bits

d) Cada mensaje enviado incluye un número de secuencia

68. En la arquitectura SSL/TLS, ¿cuál es su capa inferior situada sobre la capa de transporte de la pila TCP/IP?

a) Handshake Protocol

b) Record Protocol

c) SSL Asert Protocol

d) Change Cipher Spec

69. De las vulnerabilidades del software respecto a la seguridad informática es falso que:

a) el ataque de buffer overflow se basa en desbordar un buffer de memoria a la pila del sistema y forzar un retorno de una función al sitio deseado

b) el ataque más famoso en internet (gusano de internet) se basaba en fallo del software de los servidores HTTP en la entrega de páginas

c) el ataque de IP spoofing consiste en falsificar la dirección IP para suplantar la identidad

d) DDOS es un método de ataque de denegación del servicio de forma distribuida

70. Señale de entre los siguientes, cuál no es un ataque en una red:

a) Ping de la muerte

b) ARP poisoning

c) Smurf

d) Snicker

71. La actividad conocida como spamming es:

a) uso de una dirección IP falsa para suplantar identidades en Internet

b) uso de mecanismos de proxy para ocultar identidades y direcciones en Internet

c) uso del correo electrónico para enviar publicidad no solicitada

d) uso de algoritmos de rastreo en Internet para localizar bases de datos y servidores

72. Señale la afirmación es correcta respecto a firmar digitalmente mediante XML Signature al usar WS-Security:

a) WS-Security no contempla el uso de XML Signature por no adaptarse bien al modelo petición respuesta de Web Services.

b) WS-Security contemplaba el uso de XML Signature en la versión 1.0 pero se abandonó en favor de XML DynaSign.

c) WS-Security contempla el uso de XML Signature con algunas limitaciones, como recomendar el no usar Enveloped Signature Transform.

d) WS-Security contempla el uso de XML Signature, sin establecer limitaciones ni extensiones especiales.

73. Cuál de los siguientes tipos de virus sería más complicado o imposible de analizar por un sistema de antivirus perimetral (antivirus en servidores de correo con sandboxing, antivirus en proxys de navegación con sandboxing):

a) Virus de macro en un documento de Word con contraseña de apertura del documento.

b) Virus de archivo conocido en un documento exe.

c) Virus de archivo conocido en un documento zip sin contraseña.

d) Virus de archivo desconocido o de día O pero con un comportamiento sospechoso en ejecución.

74. XACML es:

a) Un estándar de firma de documentos.

b) Un estándar que define un esquema XML para el intercambio de autorización y autenticación.

c) Un estándar basado en la especificación XML para definir políticas de control de acceso.

d) Especifica un proceso para cifrar datos y representar esa información cifrada en XML.

75. La transmisión de datos a través de la red pública de forma que los nodos de enrutado no sean conscientes de que la transmisión es parte de una red privada se llama:

a) Tunel

b) Red Privada Virtual (VPN)

c) IPSec

d) SSL

76. WS-Security contiene especificaciones sobre:

a) La publicación, localización y enlazado de los Servicios Web.

b) La forma de conseguir integridad y seguridad en los mensajes SOAP.

c) Las políticas en materia de seguridad aplicables a un sistema de información.

d) El envío de datagramas sin establecimiento previo de una conexión.

77. En el contexto de un WAF (Web Application Firewall), es CIERTO:

a) Las soluciones WAF nunca realizan inspección de tráfico HTTP.

b) Existen soluciones WAF basadas en la nube.

c) Un WAF siempre se instala en la intranet, detrás de las aplicaciones web.

d) El objetivo de un WAF es proteger el tráfico entre servidores.

78. De los siguientes ataques, cuál se corresponde con la obtención de información de una red sin modificar la información:

a) Explot

b) Snooping

c) Wardriving

d) Teardrop

79. Si accedemos a un sitio https y recibimos un aviso de que la autoridad de certificación que ha emitido el certificado de servidor no es reconocida por nosotros, y aun así aceptamos establecer comunicación con ese servidor, ¿la comunicación entre cliente y servidor será cifrada?

a) No, puesto que el certificado no es válido.

b) Sí, puesto que el certificado permite cifrar esa comunicación, aunque haya sido emitido por una autoridad en la que no confiamos.

c) No, puesto que aunque hayamos aceptado ese certificado no podemos utilizarlo para hacer el cifrado de información.

d) Sí, porque al aceptar el cifrado se va a realizar con un certificado de cliente.

80. El método de infiltración que se vale de una vulnerabilidad informática a la hora de validar las entradas del usuario para realizar operaciones sobre una base de datos, se denomina:

a) Inyección de código SQL.

b) Troyano.

c) Vising.

d) Ataque man in the middle.

81. Un mensaje se puede cifrar:

a) Mediante mecanismos de cifrado simétrico y asimétrico

b) Sólo mediante mecanismos de cifrado simétrico como DES

c) Sólo mediante mecanismos de cifrado asimétrico como RSA

d) Se puede cifrar con mecanismos de cifrado simétrico, aunque por velocidad es preferible cifrar con criptografía de clave asimétrica

82. La Herramienta de detección desarrollada para el análisis estático de código dañino y antimalware para plataformas Windows y Linux, desarrollada por el CCN-CERT, se conoce con el nombre de:

a) Reyes.

b) Rocío.

c) Marta.

d) ADA

83. Señale la falsa:

a) XML Encryption es un lenguaje cuya función principal es asegurar la confidencialidad de partes de documentos XML a través de la encriptación parcial del documento transportado

b) XML Encryption se puede aplicar a cualquier recurso Web, incluyendo contenido que no es XML

c) XML Encryption establece que es posible cifrar datos a distintos niveles de granularidad, desde elementos simples hasta documentos enteros

d) Ninguna de las anteriores es falsa

84. Si hablamos de seguridad en el desarrollo de software, seleccione la opción correcta, de entre las siguientes, que indique un aspecto en el que coinciden "OWASP" (Open Web Application Security Project) y el Esquema Nacional de Seguridad:

a) Ambos establecen la necesidad de la "Seguridad desde el Diseño".

b) Ambos definen la necesidad de usar AES como método de cifrado de las bases de datos.

c) Ambos se han desarrollado por el Centro Criptológico Nacional.

d) No hay ninguna coincidencia entre ambos.

85. En el año 2017 apareció un incidente de seguridad denominado WannaCry que aprovechando equipos Windows 7 no parcheados se expandió muy rápidamente por todo el mundo afectando a importantes infraestructuras como de telecomunicaciones o de energía. De qué tipo de programa maligno estaremos hablando:

a) Adaware.

b) Ransomware.

c) Keylogger.

d) Flooder.

86. De IPSec, una de las siguientes afirmaciones no es cierta. Indicar cuál:

a) Para transmitir IPSec, tanto en modo transporte como en modo túnel se ha de incluir una cabecera justo delante de la cabecera IP original y una cola detrás de los datos

b) En modo transporte, IPSec se tiene entre los sistemas finales, mientras en modo túnel se tiene IPSec entre routers pero IP en los tramos routers-sistemas finales

c) El protocolo por defecto para la gestión de claves en IPSec se denomina IKE (Internet Key Exchange)

d) Entre otros, IPSec proporciona mecanismos anti-replay, autenticación, control de acceso y confidencialidad de datos

87. En el ámbito de la seguridad, ¿qué es FALSO si hablamos de SET?

a) Es una aplicación distribuida que en particular usa canales virtuales seguros y sirve para pagos con tarjetas de crédito.

b) Es un estándar privado propuesto por Visa-Microsoft, Mastercard-Netscape.

c) Es más sencillo de implementar que SSL, lo que contribuye a su rápida y progresiva implantación en el mercado.

d) Es el acrónimo de Secure Electronic Transactions, Transacciones Electrónicas Seguras.

88. Según la terminología usual, la intrusión de un cracker en un servidor web, en el peor de los casos, puede afectar a:

a) La dimensión de confidencialidad de la información

b) La dimensión de disponibilidad de la información

c) La dimensión de integridad de la información

d) Todas las anteriores

89. Un sistema, si se desea que controle los intentos de violación debe incorporar:

a) Análisis y validación de la llamada

b) Registro de la historia y fecha de la contraseña

c) Forzar a que los usuarios cambien la contraseña

d) Todas las respuestas anteriores son ciertas

90. Si pido a alguien su nombre le estoy pidiendo:

a) Identificación

b) Autorización

c) Autenticación

d) Ninguna de las anteriores

91. En el ámbito de Internet, cuando hablamos de PHISHING nos estamos refiriendo a:

a) Un determinado virus informático

b) Difusión masiva de noticias falsas

c) Suplantación fraudulenta que intentan conseguir información valiosa

d) Reenvío de mensajes a mucha gente

92. Al ataque criptográfico consistente en el barrido del espacio de claves se le denomina:

a) Criptoanálisis lineal.

b) Criptoanálisis continuo.

c) Sweep-attack.

d) Fuerza bruta.

93. Un buen sistema de gestión de contraseñas se caracteriza por:

a) El sistema, si procede, permitirá a los usuarios que seleccionen sus contraseñas

b) Las contraseñas de los usuarios con más privilegios se cambiarán con mayor frecuencia

c) El sistema no mantendrá un registro de las últimas contraseñas usadas, manteniendo sólo la actual

d) A y B son correctas

94. Las siglas SSL y TLS se refieren a:

a) Diferentes estados lógicos del microprocesador

b) Protocolos criptográficos para establecer conexiones seguras a través de una red

c) Sistemas de localización geodésica para GPS

d) Diferentes tipos de memoria física

95. ¿Cuál de los siguientes sistemas proporciona la funcionalidad de Single Sign-On basada en tickets?

a) KERBEROS.

b) STORK.

c) SAML.

d) OPENID.

96. Según OWASP TOP TEN 2021, ¿cuál es un nuevo riesgo?:

a) Inyección

b) Exposición de datos sensibles

c) XXE

d) Diseño inseguro

97. Método seguro de autorización de acceso a un servicio en una red desarrollado en el proyecto Athena del MIT:

a) Carnivore

b) Internet Key Exchange (IKE)

c) Kerberos

d) SSL

98. ¿Qué es Loapi?

a) Es un malware móvil para iOS que implementa una compleja arquitectura modular para llevar a cabo diferentes actividades ilícitas.

b) Es un malware móvil para Android que implementa una compleja arquitectura modular para llevar a cabo diferentes actividades ilícitas.

c) Es un malware móvil para Android iOS que implementa una compleja arquitectura modular para llevar a cabo diferentes actividades ilícitas.

d) Es un malware móvil para Android diseñado para lanzar exclusivamente ataques de denegación de servicio (DDoS).

99. Para establecer una comunicación segura, el protocolo SSL usa:

a) Una clave de sesión y un vector inicial

b) Una clave de sesión

c) Una clave pública y una privada

d) Una clave simétrica tipo Diffie-Hellman

100. ¿Qué es OWASP?

a) Una herramienta de gestión de proyectos que se utiliza para gestión de dependencias y como herramienta de compilación y documentación.

b) Un proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro.

c) Un framework que da soporte para aplicar la metodología de desarrollo BDD (Behavior Driven Development).

d) Un servicio web que permite acceder a la cuenta de correo electrónico de Exchange on line.

101. ¿Cuál de los siguientes ataques afecta a la disponibilidad de la información?

a) e-mail Spamming

b) DoS (Denial of Service)

c) DDoS (Distributed Denial of Service)

d) Todos los anteriores

102. ¿Qué sucede si se pierde el primer paquete de una transferencia TFTP?

a) La aplicación TFTP volverá a intentar la solicitud si no se recibe una respuesta.

b) El router del siguiente salto o la puerta de enlace predeterminada proporcionarán una respuesta con un código de error.

c) El cliente esperará indefinidamente la respuesta.

d) La capa de transporte volverá a intentar la consulta si no se recibe una respuesta.

103. En cuanto a las medidas de prevención contra un incidente de ransomware, cual será de las siguientes la medida más adecuada a tomar y que nos evitará, en caso de que el ransomware haya actuado, perder todos los datos o tener que pagar el rescate por recuperar la información:

a) Disponer de un buen sistema antispam ya que la mayoría de los ransomware entran por correo electrónico.

b) Disponer de un buen antivirus, pues el proteger los pcs es fundamental.

c) Disponer de copias de seguridad fuera de línea.

d) Disponer de shadow-copies activadas en los volúmenes de disco.

104. Señale la falsa:

a) XML Signature asegura la integridad de partes de documentos XML transportados

b) XML Signature puede aplicarse a cualquier contenido digital (objeto de datos), incluyendo XML

c) XML Key Management es un protocolo para distribuir y registrar claves públicas. Lo que hace es ocultar la parte compleja que surge con PKI. Está compuesto de: el registro de la clave pública (X-KRSS) y la información de clave pública (X-KISS)

d) Todas las anteriores son ciertas

105. El sistema más económico y sencillo para proporcionar autenticación y autorización es:

a) Utilización de passwords (palabras de paso).

b) Utilización de certificados digitales.

c) Utilización de mecanismos biométricos.

d) Utilización de un cortafuego (firewall).

106. En el contexto de la seguridad en el desarrollo de software, OWASP 4.0 (Open Web Application Security Project) define un marco de pruebas que se divide en:...

a) Tres fases.

b) Cinco fases.

c) Siete fases.

d) Cuatro procesos.

107. Para la comunicación web segura, la norma de seguridad independiente del protocolo de aplicación y, por tanto, válida para http, ftp, telnet… es la siguiente:

a) DNS
b) SSL
c) XAdES-A
d) WML

108. Indique cuál de los siguientes no es un ataque en seguridad informática:

a) Pharming
b) Phishing
c) Gloofing
d) Spoofing

109. En seguridad informática, cuál de los siguientes procesos, puede considerarse un método de hardening de un sistema:

a) La reducción de software innecesario en el sistema.
b) La instalación de software para comprobar el estado de la red.
c) La conexión a sistemas de almacenamiento (SAN o NAS).
d) La aplicación de bonding (agrupación o trunking) en las interfaces de red.

110. ¿Qué es un sistema de detección de intrusos (IDS)?

a) Un software que protege contra virus y malware.
b) Un sistema que protege contra ataques de phishing.
c) Una webcam con detección de movimiento.
d) Un sistema que monitorea y controla el tráfico de red.

111. Una aplicación que se localiza en un servidor con el fin de ofrecer seguridad a la red interna, por lo que ha sido especialmente configurado para la recepción de ataques es un...

a) cortafuegos
b) sonda
c) honeypot
d) bastión

112. Un ataque del tipo denegación de servicio (DoS = Denial of Service) a un servidor Web afecta a:

a) Las respuestas 'c' y 'd' son correctas
b) La dimensión de autenticación de los usuarios
c) La dimensión de integridad de la información
d) La dimensión de disponibilidad de la información

113. Es necesario publicar información de una organización en un portal Web en Internet. Indique cuál es la opción más segura ante intrusiones:

a) Instalar un servidor web en una DMZ actuando como "reverse-proxy" hacia el servidor Web interno de la organización.

b) Instalar una granja de servidores Web en una DMZ de modo que, si uno resulta comprometido, el resto siga funcionando.

c) Instalar un servidor Web entre la DMZ y el resto de Internet, para mayor seguridad.

d) Bastionar el servidor Web interno de la organización y abrir su puerto 80 a Internet de modo que los accesos queden securizados.

114. Para acceder a un recurso protegido con JWT (Json Web Token) es necesario incluir el valor del token en la cabecera HTTP usando:

a) Authorization: Bearer [token]

b) Authorization: Mutual [token]

c) Authorization: Json [token]

d) Authorization: Accept [token]

115. ¿Qué amenaza de seguridad se trata de SW que se adhiere a otro SW para ejecutar funciones no deseadas?

a) Virus

b) Gusano

c) Caballo de Troya Proxy

d) Caballo de Troya de denegación de servicio

116. ¿A qué corresponde el concepto Cross-Site Scripting (XSS)?

a) Una aplicación web que se visualiza y funciona correctamente en todos los navegadores.

b) Una norma para garantizar que un lenguaje de script funcione en distintos navegadores.

c) Técnica de programación por la que una aplicación web reutiliza el mismo script en múltiples páginas.

d) Un agujero de seguridad típico de aplicaciones web.

117. El estandar de seguridad ubicado en la capa de procesamiento de paquetes en lugar de en la capa de aplicación se llama:

a) SSL

b) HTTPS

c) FTP pasivo

d) IPSec

118. ¿Cuál de las siguientes empresas no está entre las que desarrollaron originalmente el protocolo WS-Security?

a) IBM

b) Microsoft

c) VeriSign

d) SUN

119. SSL son las iniciales de Secure Socket Layer, S-HTTP son las siglas de Secure HyperText Transfer Protocol, protocolos para la comunicación segura entre dos ordenadores, normalmente entre un cliente y un servidor y su objetivo es similar, pero:

a) SSL es más amplio que S-HTTP ya que puede ser utilizado como un intermediario entre el TCP/ IP y cualquier otro protocolo (por ejemplo, el HTTP) para añadir seguridad a cualquier tipo de comunicación entre un cliente y un servidor.

b) SSL es menos amplio que S-HTTP ya que es una parte de este que puede ser utilizada para añadir seguridad a cualquier tipo de comunicación http entre un cliente y un servidor.

c) S-HTTP sustituye al protocolo HTTP, aunque el cliente no esté preparado para utilizar ese nivel de seguridad, lo que no se puede conseguir con SSL, que necesita cliente y servidor preparados para utilizar ese nivel de seguridad.

d) SSL sustituye al protocolo HTTP, aunque el cliente no esté preparado para utilizar ese nivel de seguridad, lo que no se puede conseguir con S-HTTP, que necesita cliente y servidor preparados para utilizar ese nivel de seguridad.

120. Si tenemos un web server en la DMZ ¿Qué puerto típicamente debemos abrir en el firewall?

a) El primer puerto libre del firewall

b) El puerto 80

c) El primer puerto libre desde el 80

d) No es necesario abrir puerto alguno

121. ¿Qué es un honeypot?

a) Un sistema especialmente preparado para ser o parecer vulnerable.
b) Un sistema que contiene información importante y programas valiosos.
c) Un sistema capaz de detectar cambios realizados sobre archivos alojados en un servidor.
d) Un sistema que busca en el tráfico de la red firmas o patrones relacionados con virus.

122. El protocolo que contiene las especificaciones para garantizar la integridad y seguridad en mensajería de Servicios Web es:

a) RSA
b) WS-Security (WSS)
c) X.509
d) Kerberos

123. Señale cómo se denomina el protocolo sucesor de SSL (Secure Sockets Layer), estandarizado por el IETF:

a) TSL
b) TLS
c) IPSEC
d) SECIP

124. Sobre los algoritmos Hash o función resumen:

a) Todos tienen una clave de longitud de 160 bits
b) La longitud de la clave dependerá del algoritmo utilizado
c) Es imposible que la longitud de la clave sea menos de 160
d) Da igual la longitud de clave

125. Para prevenir un ataque de SQL Injection:

a) Debe detenerse la base de datos para evitar su infección por el código malicioso.
b) Debe evitarse el uso de procedimientos almacenados en la base de datos.
c) Debe eliminarse del equipo del usuario el código SQL descargado, para evitar su propagación.
d) Debe utilizarse instrucciones SQL parametrizadas.

126. En referencia a las amenazas que afectan a la seguridad en las redes de comunicaciones, señale la respuesta incorrecta:

a) La interrupción puede ser tanto física como lógica
b) El llamado sniffing es un tipo de intercepción
c) Los ataques de tipo pasivo son fáciles de detectar
d) Los ataques pueden ser activos y pasivos

127. ¿Cuál de los siguientes NO es un protocolo perteneciente a IPSec?

a) IKE (Internet Key Exchange)
b) HMAC (Keyed-Hashing for Message Authentication)
c) AH (Authentication Header)
d) ESP (Encapsulating Security Payload)

128. S-HTTP:

a) es lo mismo que HTTPS (HTTP + SSL)
b) responde por Secure-HTTP, y está escasamente implantado
c) Está diseñado por los creadores del protocolo HTTP
d) Es un protocolo del nivel de transporte

129. Entre los ataques de seguridad que se producen a través de redes como internet, aparece el concepto de Phishing. ¿Cuál de las siguientes definiciones se ajustan a este concepto?

a) Suplantación de la dirección IP

b) Suplantación de identidades de organizaciones para conseguir información confidencial (contraseñas o palabras de acceso)

c) Escuchas en red con el fin de conseguir información confidencial (contraseñas o palabras de acceso)

d) Ninguna de las anteriores

130. Deficiencias dentro del sistema Kerberos:

a) El centro de distribución de claves es un único punto de fallo

b) Privacidad

c) Integridad

d) Todas las respuestas anteriores son incorrectos