Ordinaria-parte1-sol.pdf

osnofla

Ciberseguridad

4º Grado en Ingeniería Informática

Escuela Politécnica Superior
Universidad Autónoma de Madrid

Ciberseguridad

Convocatoria Ordinaria - 24/04/2023

Parte 1 – Modelo 1

Las preguntas sólo tienen una respuesta correcta. Cada respuesta correcta suma 0.4 puntos y cada incorrecta resta 0.2. Las respuestas en blanco no suman ni restan puntos.

1. ¿Cómo se calcula el riesgo de un activo o proceso?
   - **a. Riesgo = Impacto * Probabilidad**
   - b. Riesgo = Amenaza * Probabilidad
   - c. Riesgo = Impacto * Amenaza
   - d. Riesgo = Impacto * Pérdidas

2. ¿Cuáles son las opciones típicas en el tratamiento de riesgos?
   - a. Sustitución, mitigación y transferencia a terceros.
   - **b. Evitación, mitigación, transferencia a terceros y aceptación.**
   - c. Sustitución, mitigación, transferencia a terceros y aceptación.
   - d. Evitación, reducción de impacto, transferencia a terceros y aceptación.

3. ¿Cuál es el papel de un analista de riesgos en un proceso de gestión de riesgos?
   - a. Evalúa el riesgo en términos de negocio.
   - **b. Selecciona y evalúa salvaguardas.**
   - c. Establece sus propios requisitos de seguridad.
   - d. Toma decisiones sobre el tratamiento del riesgo.

4. ¿Cuál de los siguientes hashes corresponde a la salida de un SHA1?
   - **a. 0x791b59714594e3f2089b3092e5abec2019d7531b**
   - b. 0xb1220c74cf6a71d7fd0241811a7645f6
   - c. 0x18080aac2402ef34176f500052de6cb28f2c8b58c48036db7f05499cf4f2c0b6
   - d. 0x6264338f40f6e8df9569ae89ef3994962c31f8

5. En una PKI, ¿qué entidad se encarga de comprobar la validez de un certificado ya expedido?
   - a. Las listas CRL
   - b. La CA
   - c. La RA
   - **d. La VA**

6. ¿Qué es un PCKS12?
   - a. Un algoritmo de protección de claves hardware.
   - b. Un algoritmo de cifrado.
   - **c. Un contenedor de claves criptográficas.**
   - d. Un sistema de ficheros cifrado.

7. ¿Cuál es el orden adecuado a la hora de cifrar y firmar datos?
   - a. Primero cifrar y, luego, firmar el resultado.
   - **b. Primero firmar y, luego, cifrar el resultado.**
   - c. No hay un orden mejor que otro.
   - d. Primero firmar y, luego, cifrar los datos.

8. Imagina un banco que autentica a sus clientes a través de un token recibido en su teléfono móvil. ¿De qué tipo de mecanismo de autenticación se trata?
   - **a. Autenticación 1F.**
   - b. Autenticación 2F.
   - c. Autenticación 3F.
   - d. Autenticación fuerte.

9. Imagina que deseas utilizar un sistema de autenticación para una aplicación Web basado en JSON Web Tokens. ¿Dónde incluirías los roles de los usuarios?
    a. En la cabecera.
    b. En el payload.
    c. En la firma.
    d. En cualquiera de los anteriores.

10. ¿Cuál de los siguientes ataques se lleva a cabo fuera de banda?
    a. Ataques MITB.
    b. Ataques SMS.
    c. Ataques SQL injection.
    d. Ataques CORS.

11. ¿Cuál de las siguientes afirmaciones es cierta?
    a. El principal objetivo de un test de penetración es encontrar todos los errores de una aplicación
    b. Una auditoría de caja blanca NO tiene acceso al código y documentación interna de una aplicación
    c. Las auditorías suelen utilizar una metodología sistemática, para encontrar todos los problemas de una aplicación
    d. Las auditorías suelen trabajar en "línea recta", para encontrar un problema tan rápido como sea posible.

12. Los ataques MITB (Man-in-the-browser) son especialmente peligrosos. ¿Cuáles son las razones?
    a. Pueden modificar los datos que se visualizan en el navegador antes y después de ser enviados o recibidos.
    b. No funcionan cuando se utilizan conexiones seguras SSL o TLS
    c. Son un tipo de ataque de ingeniería social, por lo que es fácil que engañen a la mayoría de usuarios
    d. Pueden infectar otros usuarios en la misma red local y propagarse rápidamente.

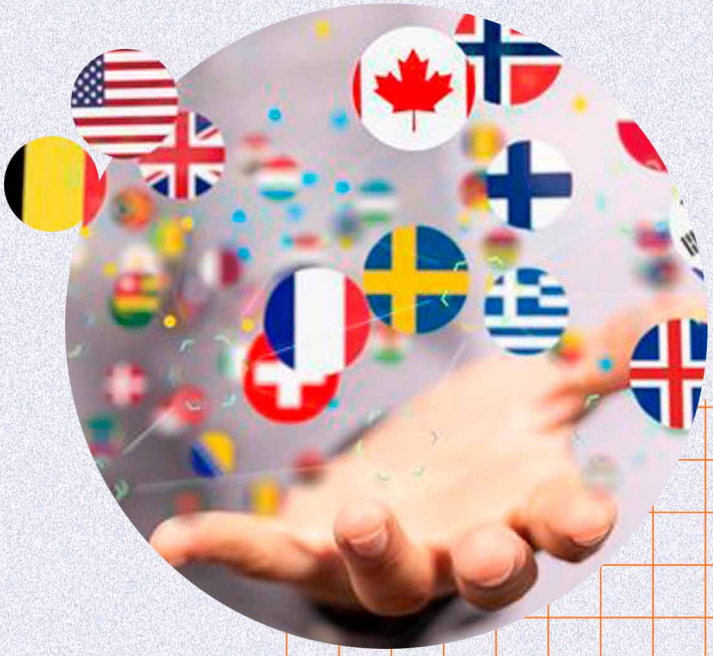
13. El principal objetivo de las cookies es:
    a. Impedir los ataques por inyección SQL
    b. Eludir el robo de credenciales mediante XSS
    c. Subsanar la falta de control de estado por parte del protocolo HTTP
    d. Evitar ataques Path traversal.

14. ¿Cuál de las siguientes afirmaciones es cierta?
    a. Un certificado digital es, esencialmente, una vinculación entre una identidad y una clave pública
    b. Un certificado digital es, esencialmente, una vinculación entre una identidad y una clave privada
    c. Un certificado digital es firmado con la clave pública de la CA correspondiente
    d. Un certificado digital es firmado con la clave privada del usuario correspondiente

15. El objetivo principal de la Respuesta a Incidentes es:
    a. Poner fin inmediatamente al ataque, para minimizar el impacto (económico o de cualquier tipo).
    b. Encontrar, obtener y procesar de manera forense las pruebas con las que poder procesar judicialmente al atacante.
    c. En general, explicar el estado actual de un artefacto digital.
    d. Descubrir la vulnerabilidad del sistema que ha permitido el ataque, para así evitar futuros ataques.

Plazo de matriculación abierto - ¡PLAZAS LIMITADAS!

¡NO PIERDAS LA OPORTUNIDAD, APÚNTATE AHORA!



Grupos reducidos máx 8 personas

10% dto para miembros de la misma familia

INGLÉS, ALEMÁN, FRANCÉS, ITALIANO, PORTUGUÉS, CHINO, ÁRABE, JAPONÉS, ESPAÑOL PARA EXTRANJEROS...

De todos los niveles (A1-C2), en grupo o one-to-one, presencial u online.

Profesores nativos y calificados.

¡Prepárate para tu examen oficial y consigue tu certificado internacional (PET, FCE, CAE, CPE, TOEIC, TOEFL, APTIS, IELTS, DELF, etc.) mejorando con nosotros!

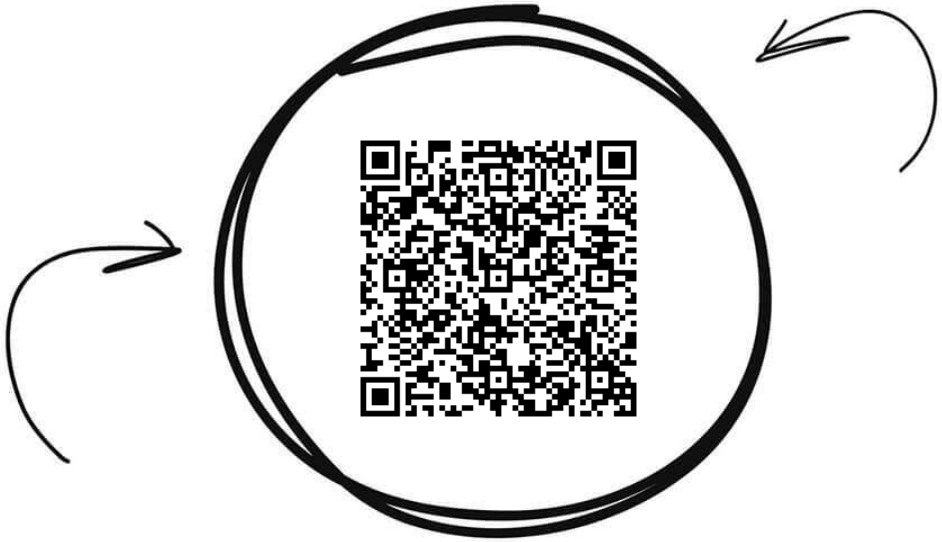
Contáctanos

www.bostonhouse.es

91 011 11 52 - bostonhouse@bostonhouse.es

BOSTON HOUSE SCHOOL OF ENGLISH

Ciberseguridad



Banco de apuntes de la

WUOLAH

Comparte estos flyers en tu clase y consigue más dinero y recompensas

1. Imprime esta hoja
2. Recorta por la mitad
3. Coloca en un lugar visible para que tus compis puedan escanar y acceder a apuntes
4. Llévate dinero por cada descarga de los documentos descargados a través de tu QR

16. ¿Cuál de estas afirmaciones sobre el análisis forense digital es **falsa** ?
    a. El principal inconveniente del ingeniero forense es la fragilidad del insumo con el cual trabaja.
    b. El objetivo fundamental es evitar comprometer el proceso, sea legal u organizacional.
    c. Las acciones tomadas no deben cambiar por ningún motivo la evidencia digital. En ningún caso este principio puede ser omitido o siquiera flexibilizado.
    d. En muchas situaciones es imposible no alterar los datos extraídos.

17. ¿Cuál de las siguientes **no** es un método usado para la ocultación de virus?
    a. Virus cifrado
    b. Virus isomórfico
    c. Virus polimórfico
    d. Virus **metamórfico**

18. ¿Cuál de las siguientes afirmaciones sobre el Análisis y Gestión de Riesgos es **falsa**?
    a. Tradicionalmente las metodologías de análisis de riesgo proponen que se realice un inventario de activos, se determinen las amenazas, las probabilidades de que ocurran y los posibles impactos.
    b. Para aquellos riesgos cuyo nivel está por encima del umbral deseado la empresa debe decidir cuál es el mejor tratamiento que permita reducirlos.
    c. Para estimar la frecuencia podemos basarnos en datos empíricos (datos objetivos) del histórico de la empresa, o en opiniones de expertos o del empresario (datos subjetivos).
    d. El coste del tratamiento o protección sólo puede superar el coste de riesgo disminuido cuando la probabilidad o el impacto sean muy altos.

19. ¿Cuál de las siguientes afirmaciones sobre la gestión de riesgos es verdadera?
    a. Aquellos riesgos con alto impacto y baja probabilidad se deben transferir.
    b. Aquellos riesgos con baja probabilidad y bajo impacto es mejor evitar.
    c. Aquellos riesgos con bajo impacto y alta probabilidad se deben aceptar.
    d. Aquellos riesgos con alta probabilidad y alto impacto se deben mitigar.

20. ¿Cuál de esas afirmaciones sobre los virus ejecutables versus los scripts es verdadera?
    a. Los scripts son más peligrosos porque son específicos de una plataforma y se diseñan para aprovechar alguna vulnerabilidad de la misma.
    b. Los scripts son más peligrosos porque es más frecuente "meter" documentos que programas nuevos en un sistema.
    c. Los ejecutables son más peligrosos porque los controles sobre estos son menores que sobre los ficheros de datos.
    d. Los ejecutables son más peligrosos porque las macros son más difíciles de crear y modificar.

21. ¿Cuál de las siguientes **no** es parte de un virus?
    a. **Vulnerabilidad**.
    b. Vector de infección.
    c. Activador (trigger).
    d. Carga útil (payload).

22. ¿Cuál de las siguientes afirmaciones sobre el análisis de malware es **verdadera**?
    a. El análisis dinámico de malware permite analizar fragmentos que normalmente no se ejecutan.
    b. El análisis post-mortem suele ser el único posible tras un incidente de seguridad.
    c. El análisis estático de malware permite análisis completos, incluyendo conexiones al exterior.
    d. El análisis post-mortem suele ser del que más información se obtiene, porque el malware ya se ha ejecutado en su totalidad.

23. ¿Cuál de las siguientes afirmaciones sobre Stuxnet es **falsa**?
    a. Como en todos los casos de ataques avanzados, es extremadamente difícil saber quién es el responsable del mismo.
    b. Es un malware desarrollado principalmente para exhibir las capacidades ofensivas de Estados Unidos e Israel.
    c. Es la primera vez que se identificó un malware que utilizaba hasta 4 vulnerabilidades de día cero.
    d. Era extremadamente difícil de detectar, y es posible que sólo se haya conocido por error.

24. ¿Cuál de los siguientes **no** es un motivo para realizar análisis de Malware?
    a. Detectar y responder ante intrusiones.
    b. Prevenir futuras amenazas.
    c. Eliminar infecciones.
    d. Realizar una valoración económica de las pérdidas ocasionadas.

25. ¿Cuál de estas afirmaciones es **falsa**?
    a. El *Deadbox forensics* permite acceder a casi toda la información del dispositivo objetivo, menos a la del sistema operativo ya que se utiliza un sistema operativo distinto.
    b. El *Deadbox forensics* permite acceder al almacenamiento permanente pero no a información volátil (RAM, conexiones de red, etc.).
    c. En el *Livebox forensics* para recoger los datos se utilizan los recursos del propio dispositivo (memoria, conexiones de red, etc.).
    d. El *Livebox forensics* es la forma más completa para acceder a la memoria RAM, aunque también se podría hacer analizando ficheros para hibernación del sistema o del gestor de memoria virtual, entre otros.