Ordinaria-parte2-sol.pdf

osnofla

Ciberseguridad

4º Grado en Ingeniería Informática

Escuela Politécnica Superior
Universidad Autónoma de Madrid

Ciberseguridad

Convocatoria Ordinaria - 24/04/2023

Parte 2 – Modelo 1

Las preguntas sólo tienen una respuesta correcta. Cada respuesta correcta suma 0.5 puntos y cada incorrecta resta 0.2. Las respuestas en blanco no suman ni restan puntos.

1. ¿Cómo gestionaría un HIDS y un antivirus el ataque de un ransomware a un equipo que llega a éste por correo electrónico?
   a. **Tanto el HIDS como el antivirus podrían detectar y evitar el ataque.**
   b. Solo el antivirus podría parar el ataque, no el HIDS.
   c. Solo el HIDS podría parar el ataque, no el antivirus.
   d. Ninguna de las dos herramientas podría detectar un ataque de este tipo.

2. Imagina que necesitas configurar un NIDS que puede procesar hasta un 1 Gbps de tráfico conectado, a través de un switch de 1 Gbps, a una red compuesta de 4 subredes que generan hasta 0,25 Gbps cada una. ¿Qué mecanismo podrías utilizar para agregar el tráfico de las mismas?
   a. Configurando un *spanning port* en el switch, y conectado un TAP a dicho puerto.
   b. Configurando un TAP en el switch.
   c. **Agregando el tráfico en un TAP, y conectando éste a un puerto del switch. Luego, conectando el NIDS a dicho puerto**.
   d. Agregando el tráfico en el NIDS, y conectando éste a un puerto del switch. Luego, conectando el TAP a dicho puerto.

3. ¿Qué sistema utilizarías para generar un red que imite a la de tu institución con el fin de estudiar y redirigir a unos posibles atacantes?
   a. Un IDS.
   b. Un IPS.
   c. Un honeypot.
   d. Ninguna de las otras respuestas.

4. ¿Qué es OWASP?
   a. Una guía de desarrollo de aplicaciones seguras.
   b. Un proyecto, que incluye documentación y software, para el desarrollo de aplicaciones seguras.
   c. Una lista de las vulnerabilidades más comunes y graves.
   d. Un estándar sobre los requisitos y controles de seguridad más comunes.

5. Considera la siguiente porción de código. ¿Qué tipo de vulnerabilidad contiene?
   a. Consumo excesivo de memoria, al no comprobar los valores de *m* y *n*.
   b. Buffer overflow.
   c. Inyección de código SQL.
   d. Posibilidad de división por cero

```
#define MAX_DIM 100
#include <stdio.h>
#include <stdlib.h>

struct board_square_t {
   int height;
   int width;
};


int main(){
    /* board dimensions.*/
    int m,n, error;
```

```
    struct board_square_t *board;
    printf("Please specify the board height: \n");
    error = scanf("%d", &m);
    if ( EOF == error ){
        printf("No integer passed: Die evil hacker!\n");
    }
    printf("Please specify the board width: \n");
    error = scanf("%d", &n);
    if ( EOF == error ){
         printf("No integer passed: Die evil hacker!\n");
    }
    if ( m > MAX_DIM || n > MAX_DIM ) {
        printf("Value too large: Die evil hacker!\n");
    }
    board = (struct board_square_t*) malloc( m * n * sizeof(struct
board_square_t));
    return 0;
}
```

6. ¿En qué consiste el ataque por deserialización en Python?
    a. La inclusión de código arbitrario en un objeto deserializado, que es ejecutado durante la serialización del mismo.
    b. La inclusión de código arbitrario en un objeto JSON, que es ejecutado al ser parseado.
    c. La inclusión de código arbitrario en un objeto JSON, que es ejecutado durante la deserialización del mismo.
    d. La inclusión de código arbitrario en un objeto serializado, que es ejecutado durante la deserialización del mismo.

7. En Python, ¿cómo podrías evitar que un archivo JSON incluyera tipos de datos no permitidos, como una cadena en una variable dedicada a almacenar la edad de un individuo?
    a. Utilizando una librería como Bandit.
    b. Utilizando una librería como Schema.
    c. Comprobando manualmente el tipo del dato durante su parseo.
    d. Incluyendo filtros específicos al proceso de deserialización.

8. ¿Qué comando utilizarías para obtener los paquetes Python y sus versiones instaladas, de cara a generar un futuro entorno virtual de ejecución?
    a. pip list
    b. pip env
    c. pip freeze
    d. pip env/activate

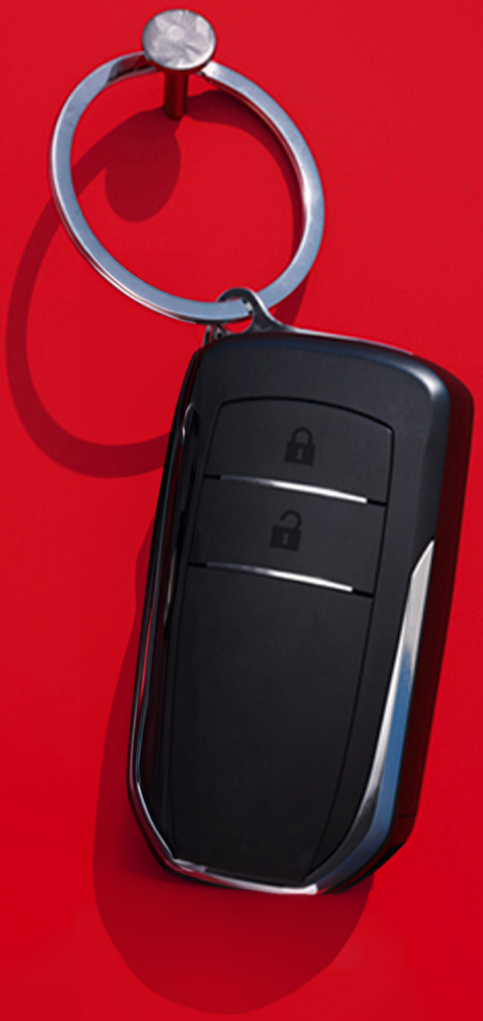
9. ¿A qué hace referencia el concepto de *compliance* en lo referente a la seguridad en entornos *cloud*?
    a. Entender las leyes y reglamentos que imponen obligaciones de seguridad y privacidad en las organizaciones.
    b. Extender las prácticas de la organización respecto de las políticas, procedimientos y estándares para el desarrollo de aplicaciones y suministro de servicios en la nube.
    c. Asegurar la visibilidad de los controles y procesos de seguridad y privacidad del proveedor cloud, y su desempeño en el tiempo.
    d. Establecer claramente los derechos de propiedad sobre los datos.

10. ¿En qué consiste la primitiva criptográfica *proof-of-work* utilizada en muchas cadenas de bloques?
    a. Ninguna de las otras respuestas es válida.
    b. Es un registro distribuido e inmutable de datos.
    c. Es el algoritmo de almacenamiento utilizado por la cadena de bloques.
    d. En una prueba matemática de que hemos dedicado una cantidad de trabajo computacional a resolver una tarea.

coches.net

En este momento hay alguien teniendo relaciones sexuales dentro de un coche.

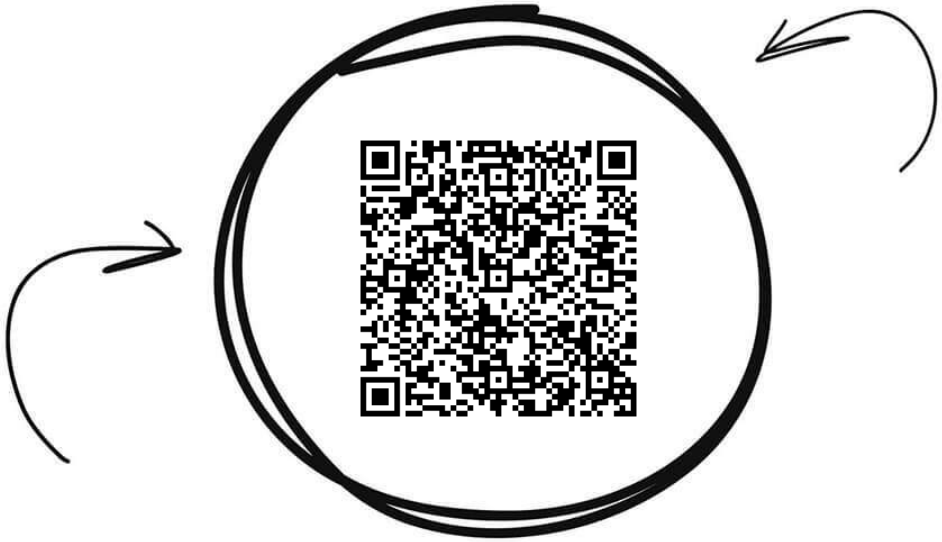
Y no eres tú.
Pero podrías serlo.



coches.net

No pierdas ni un minuto

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

11. ¿Cómo se ajusta la dificultad de la prueba de trabajo en cadenas de bloques basadas en este algoritmo?
    a. **Ajustando el número de ceros delanteros en la función de inversión parcial de hash.**
    b. Ajustando el número de bloques a minar para que, en término medio, se tarden 10 minutos en encontrar una solución válida.
    c. Ajustando el *nonce* que se entrega a los mineros en la función de inversión parcial de hash.
    d. Ajustando el número total de cálculos por segundo realizados para que, en término medio, se tarden 10 minutos en encontrar una solución válida.

~~12. ¿Cuál de los siguientes algoritmos de consenso en cadenas de bloques consume menos recursos energéticos?~~
    ~~a. Ajustando el número de ceros delanteros en la función de inversión parcial de hash.~~
    ~~b. Ajustando el número de bloques a minar para que, en término medio, se tarden 10 minutos en encontrar una solución válida.~~
    ~~c. Ajustando el *nonce* que se entrega a los mineros en la función de inversión parcial de hash.~~
    ~~d. Ajustando el número total de cálculos por segundo realizados para que, en término medio, se tarden 10 minutos en encontrar una solución válida.~~

13. Imagina un algoritmo para una cadena de bloques que deseara mantener altos, simultáneamente, sus niveles de seguridad y descentralización. ¿Qué ocurriría con su escalabilidad?
    a. **Se vería afectada negativamente.**
    b. Se incrementaría.
    c. No se vería afectada.
    d. El resultado depende de factores no considerados en la pregunta.

14. Según el framework de pruebas OWASP, ¿cuál de las siguientes **no** es una consideración de la Fase 1?
    a. Incluir específicamente la seguridad en nuestra metodología de desarrollo
    b. Comprobar que existen políticas y estándares de seguridad conocidos por el equipo de desarrollo.
    c. **Revisar la arquitectura desde el punto de vista de la seguridad.**
    d. Designar una persona como responsable de la seguridad en el código

15. ¿Cuál de las siguientes **no** es una recomendación del framework OWASP?
    a. Antes del paso a producción, un test de penetración por un equipo especializado.
    b. **El equipo de desarrollo y el de seguridad deben ser el mismo.**
    c. Atención específica a la gestión de la configuración.
    d. Se debe crear un modelo de amenaza (escenarios realistas de ataques y atacantes).

16. ¿Cuál de los siguientes sería un requisito correcto?
    a. **El usuario se autenticará con credenciales usuario/contraseña.**
    b. El sistema será lo más seguro posible.
    c. El sistema proporcionará una respuesta rápida.
    d. El sistema se recuperará automáticamente tras producirse un fallo.

17. ¿Cuál de las siguientes **no** es una recomendación de seguridad para la programación Python?
    a. **Usar preferentemente la versión preinstalada del intérprete.**
    b. Utilizar entornos virtuales.
    c. Configurar DEBUG=False en producción.
    d. Utilizar las anotaciones de tipos.

18. ¿Cuál de las siguientes **no** es una recomendación de seguridad para la programación Java?
    a. Evita la serialización.
    b. No utilizar funciones o atributos públicos.
    c. Utilizar bibliotecas probadas.
    d. **Utilizar atributos estáticos.**

19. ¿Cuál de los siguientes **no** es un servicio ofrecido típicamente como parte de un servicio SecaaS?
    a. Gestión de identidades y acceso
    b. Prevención de pérdidas de datos
    c. Análisis de la arquitectura del sistema.
    d. Evaluaciones de seguridad
20. Al analizar la necesaria protección de datos en un entorno Cloud, ¿cuál de los siguientes **no** es un factor a evaluar?
    a. La adecuación de las soluciones de gestión de datos del proveedor a los datos de la organización.
    b. Capacidad de controlar accesos a los datos.
    c. Capacidad de asegurar los datos en uso, en tránsito y "at rest".
    d. Capacidad de recuperar los datos en caso de desastre.