Nombre Completo: **LU:**
Parcial – Seguridad de la Información – DC - 10/6/2024

Elija la opción correcta (2 ptos):

1. Qué forma de control de acceso está relacionada con la siguiente pregunta: ¿Es la persona que está procurando entrar realmente quién dice ser?
a) Autorización
b) Autenticación.
c) Auditoría
d) Control de acceso mandatario.

2. ¿Cuál de las siguientes definiciones describe mejor el “spoofing”?
a) El proceso de enviar información desde múltiples equipos con la intención de sobrecargar a la víctima.
b) El proceso de capturar datos, cambiar el contenido, y reenviarlos.
c) El proceso de insertar código extra que puede ser utilizado luego para ganar acceso al sistema.
d) El proceso de reemplazar la dirección de origen de un paquete para hacerse pasar por otro equipo.

3. La utilización de política targeted en SElinux garantiza:
a) que toda aplicación del sistema está segurizada por SELinux.
b) que la política se verifica (loguea) pero no se fuerza.
c) que un conjunto de servicios del sistema se encuentran segurizados por SELinux.
d) que no se pueden instalar aplicaciones adicionales al sistema.

4. Los principios de kerckhoffs tratan sobre:
a) Criptografía
b) Diseño seguro
c) Desarrollo Seguro
d) Control de acceso mandatorio

5. ¿Por qué 3DES es una mejora sobre el DES standard?
a) Utiliza claves públicas y privadas.
b) Genera un hash del texto claro antes de cifrar.
c) Utiliza 3 claves y varias pasadas de cifrado y/o descifrado.
d) 3DES es más rápido que DES.

6. ¿Cuál de las siguientes afirmaciones describe mejor el concepto de "TOPT"? a) Es una técnica de cifrado de datos utilizada para proteger la integridad de la información. b) Se refiere a una lista de las principales amenazas de seguridad informática que enfrentan las organizaciones.
c) Es un método para autenticar a los usuarios utilizando un código único generado en tiempo real.
d) Se utiliza para prevenir ataques de denegación de servicio (DDoS) mediante la limitación de la tasa de solicitudes.

Desarrolle (identifique todo lo que asume):

1. Se desea implementar una variante del mecanismo de Challenge-Response durante la etapa de autenticación entre un cliente y un servidor, utilizando criptografía asimétrica. El servidor tiene almacenada la clave pública del cliente. Describa dicha implementación. ¿Qué ventaja provee? (1 pto)

2. Describa brevemente SHA1 indicando qué es y para qué se utiliza. ¿Por qué no se recomienda utilizarlo en nuevas aplicaciones? (1pto)

3. ¿Cómo se puede determinar de manera remota el sistema operativo de un equipo (sin tener credenciales en el mismo)?

4. Describa las vulnerabilidades de inyección en aplicaciones web, indicando por lo menos dos tipos distintos, y dos mecanismos de prevención.

5. Defina y compare los conceptos de honeypot y honeytoken. (1 pto)

6. La empresa joyanuncataxi.com provee un servicio web para publicar, en forma gratuita, anuncios clasificados de productos de segunda mano. Al realizar el alta de los mismos, además de la descripción del producto o servicio, se piden datos del anunciante, como email o teléfono celular. La empresa recibió reportes de varias personas que recibieron llamados a sus teléfonos celulares, en cualquier horario, relacionados con anuncios del sitio, pero que ellos no habían publicado. Proponga un mecanismo para minimizar la posibilidad de ocurrencia de estos incidentes. (1 pto)

7. Estás liderando el equipo de desarrollo de una nueva aplicación de citas en línea “DCinder” que se centra en garantizar el anonimato de los usuarios. Se te pide que diseñes e implementes una funcionalidad que proteja la privacidad de los usuarios mientras aún les permite interactuar de manera significativa. Describe cómo planificarías e implementarías esta funcionalidad. Incluye consideraciones sobre la recopilación y el almacenamiento de datos personales, la forma en que los usuarios interactúan entre sí y cómo se podría garantizar el anonimato sin comprometer la seguridad de la plataforma ni de los usuarios. Proporciona ejemplos concretos de cómo se podría llevar a cabo esta implementación, desde la arquitectura de la aplicación hasta la experiencia del usuario. (2 ptos)