Nombre Completo: **LU:**

Parcial – Seguridad de la Información – 6/6/2018

Elija la opción correcta (2 ptos):

1. Juan, el administrador de red, está conectando un web server de acceso público en un área aislada de las redes de la empresa por motivos de seguridad. ¿Qué concepto está implementando?
A. Honeynet
B. DMZ
C. Proxy
D. Intranet

2. ¿Cuál de las siguientes no es una propiedad característica de una función criptográfica de hash?
A. Convierte un mensaje de longitud arbitraria en un valor de longitud fija.
B. Dado el hash resultante, es computacionalmente imposible encontrar el mensaje original correspondiente.
C. Es imposible obtener el mismo hash a partir de dos mensajes diferentes.
D. Convierte un mensaje de longitud fija en un valor de longitud arbitraria.

3. Indique la opción falsa. Un ataque de reset de conexiones TCP
A. Requiere conocer direcciones ip y puertos de origen y destino.
B. Requiere conocer los nros. de secuencia
C. Requiere que la conexión no esté cifrada.
D. Es unilateral.

4. ¿Cuál de los siguientes no es un objetivo de los sistemas criptográficos?
A. No repudio
B. Confidencialidad
C. Integridad
D. Disponibilidad

5. Marina es responsable de monitorear el IDS de la empresa. Ayer hubo actividad reportada por el IDS que luego de ser investigada se concluyó que era tráfico legítimo. ¿Que concepto describe esto?
A. Falso negativo
B. Pasivo
C. Activo
D. Falso positivo

6. ¿Qué tipo de ataque puede utilizarse para aprovechar la relación de confianza que existe entre dos sistemas?
A. Spoofing
B. Cracking de contraseñas
C. Brute Force
D. SQL Injection

Desarrolle (identifique todo lo que asume):

1. Describa qué son y para qué sirven los hmacs. (1 pto)

2. Usando dibujos y unas pocas palabras, ilustre como un atacante puede sniffear tráfico en una red switcheada. No escriba oraciones ni párrafos.(1pto)

3. Describa la diferencia entre vulnerabilidad y amenaza. (1pto)

4. ¿Cuales son las limitaciones de los permisos básicos de acceso a archivos (lectura, escritura, ejecución) en los sistemas linux? ¿Como se pueden resolver?(1pto)

5. Una aplicación web utiliza datos no confiables en la construcción del código HTML sin validarlos o codificarlos. ¿Con qué nombre se conoce a esta vulnerabilidad? (1pto)

6. Le piden diseñar e implementar una aplicación web para el Instituto Nacional Central Único Coordinador de Ablación e Implante (Incucai), organismo que impulsa, normatiza, coordina y fiscaliza las actividades de donación y trasplante de órganos en nuestro país. Actúa en las provincias argentinas junto a 24 organismos jurisdiccionales de ablación e implante con el fin de brindar a la población un acceso trasparente y equitativo al trasplante. El sistema debe permitir la administración, gestión, fiscalización y consulta de la actividad de procuración y trasplante de órganos en el ámbito nacional. Debe proveer un mecanismo de acceso con escalones jurisdiccionales, regionales e integrado nacionalmente, que permita el registro en tiempo real de la actividad, listas de espera y asignación de órganos con fines de implante en nuestro país. Debe permitir el monitoreo y evaluación permanente, así como ofrecer a la sociedad la garantía de transparencia de la actividad. Indique detalladamente como protegería cada componente de la solución, teniendo en cuenta los principios de arquitectura y diseño seguro, los distintos actores involucrados, el uso de criptografía, los mecanismos de autenticación y control de acceso, y los problemas de seguridad más comunes en aplicaciones web, haciendo especial hincapié en la confidencialidad y la integridad de la lista de espera de potenciales receptores de órganos. Tenga en cuenta los aspectos relacionados con la instalación y operación del mismo. (1,5 ptos)

7. Mediante el decreto 892/2017, el Poder Ejecutivo oficializó la creación de la Plataforma de Firma Digital Remota. Con esta plataforma todos los ciudadanos van a poder tener una firma digital en la nube, para firmar no solamente en sus relaciones con el Estado sino también entre ciudadanos. Indique las consideraciones de seguridad a tener en cuenta para implementar esta plataforma, teniendo especialmente en cuenta el proceso de emisión de certificado, la protección de la clave privada del ciudadano, y la disponibilidad del servicio. (1,5 ptos)