Nombre Completo: **LU:**

Parcial – Seguridad de la Información – 1/11/2017

Elija la opción correcta (2 ptos):

1. ¿Qué política de control de acceso está relacionada principalmente con la función que cumple un individuo en la organización?
A. MAC
B. DAC
C. RBAC
D. PAC

2. Toma tiempo distribuir completamente la CRL. ¿Qué protocolo nos permite verificar en forma inmediata el estado de un certificado X509?
A. CA
B. CP
C. TLS
D. OCSP

3. ¿Qué tipo de ataque está diseñado para sobrecargar un protocolo o servicio en particular?
A. Spoofing
B. MiTM
C. Backdoor
D. Flood

4. En criptografía, ¿con que está relacionada la sigla MAC?
A. Media Access Control
B. Message authentication code
C. Multiple advisory committees
D. Mandatory Access Control.

5. ¿Qué algoritmo de clave simétrica usa cifrado por flujos para cifrar la información?
A. RC4
B. Blowfish
C. Rijndael
D. DSA

6. ¿Cuál de las siguientes medidas no agrega seguridad contra los ataques de sql injection en aplicaciones web?
A. Validación de parámetros de entrada que recibe la aplicación.
B. Uso de Firewall Stateful Inspection.
C. Uso de Web Application Firewall
D. Asignación de mínimos privilegios a los usuarios de bases de datos utilizados por la aplicación web.

Desarrolle (identifique todo lo que asume):

1. ¿Para qué sirven y cuándo se utilizan los mecanismos de challenge-response? (1 pto)

2. Describa en qué consiste el arp spoofing. ¿Cómo se puede detectar? (1pto)

3. Tiene que diseñar e implementar una aplicación web para acceso por parte de sus clientes a información confidencial a través de Internet. Proponga un algoritmo seguro de almacenamiento de claves. Adicionalmente, proponga un mecanismo de autenticación más robusto, que no utilice usuario/clave. (1pto)

4. ¿Para qué mecanismo de cifrado se utiliza el ataque de Kasiski? ¿Cuál es la idea del mismo? (1pto)

5. Indique qué es un IDS, para que sirve y para que no. Clasifique según el tipo. (1pto)

6. Juan y Marina quieren jugar al “piedra, papel o tijera”, pero lo quieren hacer a través de Internet, sin ningún tipo de intermediarios ni terceras partes. Proponga un protocolo criptográfico que no permita a ninguno de los dos hacer trampa. No se preocupe demasiado por los protocolos de red. (1,5 ptos)

7. El ministerio de Modernización, a través de la Resolución 204-E/2017, dispuso la obligatoriedad de uso de un mecanismo de control de acceso biométrico para administrar el control de asistencia y presentismo del personal de la administración pública nacional. Describa como implementaría la solución, teniendo en cuenta la seguridad de los lectores de huella digital, la conectividad, la protección de los registros de acceso, y la seguridad de una aplicación web que le permite a cada empleado ver su historial de ingresos/egresos y presentar justificaciones, por ejemplo, por enfermedad. (1,5 ptos)