BLOQUE 1

1. Justifica por qué son falsas las siguientes afirmaciones: [1 punto]

a) Un cifrado que pretenda simular One Time Pad usando una clave aleatoria de un sólo uso de tamaño fijo, repetida hasta “cubrir” la totalidad del mensaje a cifrar, es suficiente para asegura la propiedad de ser incondicionalmente seguro.

Ventajas(Tema2:Criptografía clásica (III))  
Es incondicionalmente seguro si se verificada que la clave es:

1.- totalmente aleatoria

2.-tan larga como el mensaje  
 3.-de un sólo uso (una clave distinta para cada mensaje)  
No habrá traza estadística del texto en claro en el texto cifrado (Esto es el significado de incondicionalmente segura).

No se cumple la segunda condición.

b) Para considerar que la vinculación entre un "usuario" y su clave pública presente en un certificado digital confiable basta con que se verifique que (1) el certificado este emitido por una autoridad certificadora reconocida (2) que no esté caducado en la fecha actual.

(Tema2:Certificados)

El participante que lo reciba puede verificar que el certificado es auténtico:

1.- Fué creado y firmado por la CA correspondiente (reconocida por ambos)

2.-Puede recuperar la clave pública del otro participante y verificar su validez/autenticidad (comprobando la firma digital con la clave pública de la CA)

c) En las firmas digitales basadas en algoritmos asimétricos se suelen emplear cifradores simétricos (por ejemplo DES o APS) como primer paso, para evitar tener que procesar la totalidad de los datos a firmar con cifradores asimétricos más costosos.

d) Una de las formas de evitar las vulnerabilidades XSS (Cross Site Seripting) en aplicaciones web es mediante el empleo de procedimientos almacenados, siempre y cuando éstos no utilicen directamente los parámetros introducidos por el usuario.

( TEMA3: Úlima diapositiva)

Protecciones: filtrar los datos que el usuario introduce y (especialmente) los que el servidor sirve:

1.-”Escapar” caracteres problemáticos (<, >, ’, ", &) conviertiéndolos en entidades HTML.

2.-Descartar cadenas con etiquetas sospechosas (lista negra)

3.-Especial atención en ”zonas peligrosas” (etiquetas susceptibles de desencadenar ejecución código Javascript)

4.-Algunos frameworks Web (p.e. JSF Java Server Faces) incluyen soporte para evitar XSS proporcionando mecanismos para ”emitir” código HTML sanitizado a partir de datos de la aplicación.

Esa razón no es una de las formas de protección para XSS

e) En el modo túnel de IPsec, utilizando el protocolo AH (authenticating header) se garantiza la confidencialidad tanto de la carga útil como de las cabeceras de cada paquete.

(Tema5:IPec)

AH define una cabecera adicional donde se contiene

información para:

1.- autenticar del origen

2.- asegurar integridad

Es falsa dado que solo sirve para autentificar el origen y asegurar la integridad. No nombra para nada la confidencialidad.

2. Describe brevemente los siguientes conceptos [0,6 puntos]

a) Red Feis (Tema2:Feistel)

b) Random Canary (canario aleatorio)(Tema3:Contramedidas)

c) NIDS basado en firmas(Tema6:Funcionamiento) NDIS: detectores de intrusiones en red. Y con respecto a basado en firmas cuenta con una BD con firmas de ataques conocidos(aproximación similar a los antivirus).

Ej:Paquete cuya carga útil incluya fragmentos de shellcode concocido.

3. Describe en qué consiste la inyeción SQL en aplicaciones web y señala qué posibles contramedidas existen para evitarla. [0.6 puntos]

(Tema3:Iny.SQL y dentro de este prevención)

4. Enumera los servicios de seguridad ofrecidos por el protocolo SSL(Secure Sockets Layer)/TLS(Transport Layer Security), detallando las estrategias que se siguen para implementarlos[0,6 puntos]

(Tema5:SSL/TLS)

1.-Confidencialidad

2.-Autentificación de entidades

3.-Consideraciones adicionales

BLOQUE 2

1. Describe las alternativas que existen en cuanto al funcionamiento interno de detectores de intrusiones (IDS/IPS). [0,4 puntos]

2. Qué es un certificado digital, para qué sirve y qué información contiene usualmente?. Enumera qué otros elementos típicos conforman una infraestructura de clave publica (PKI), además de la propia autoridad de certificación. [0,4 puntos]

3. Enumera y describe las características teóricas que deben de cumplir los algoritmos de HASH criptográficos. Indica al menos dos ejemplos del uso práctico de los HASH criptográficos. [0,4 puntos]

4. Describe en qué consisten las vulnerabilidades de desbordamiento de buffer en pila (stack buffer overflow) y enumera las posibles contramedidas a emplear en tiempo de ejecución. [0,4 puntos]

5. Diferencias entre modo túnel y modo transporte en IPSec. [0,4 puntos]