Curso: IFCT0109 Seguridad informática
Expte.: 29/2020/LJ/0019
Evaluación:
Acción y grupo:
Módulo: MF0489_3 Diseñar e implementar sistemas seguros de acceso y transmisión de datos

Fecha examen:	10/03/2023
Nombre y apellidos:	
NIF:	
Docente:	Juan Antonio Ferrández Rodríguez

Tipo de Evaluación (Señale con una X la que corresponda)			
Evaluación 1	X	Recuperación I	

1) ¿Cuál es la diferencia entre los algoritmos de cifrado simétrico y asimétrico?

a) Los algoritmos de cifrado simétrico utilizan claves precompartidas. En los algoritmos de cifrado asimétrico se utilizan claves diferentes para cifrar y descifrar datos. ←
b) Los algoritmos de cifrado simétrico se utilizan para cifrar los datos. Los algoritmos de cifrado asimétrico se utilizan para descifrar los datos.
c) Los algoritmos de cifrado simétricos se utilizan para autenticar las comunicaciones seguras. Los algoritmos de cifrado asimétrico se utilizan para negar mensajes.
d) Por lo general, los algoritmos simétricos son cientos o miles de veces más lentos que los algoritmos asimétricos.

2) Una compañía implementa una política de seguridad que garantiza que un archivo enviado desde la oficina de la sede central y dirigido a la oficina de la sucursal pueda abrirse solo con un código predeterminado. Este código se cambia todos los días. Indiquen dos algoritmos que se pueden utilizar para realizar esta tarea. (Elija dos opciones).

a) MD5
b) SHA-1
c) HMAC
d) AES ←
e) 3DES ←

3) Un cliente compra un artículo en un sitio de comercio electrónico. El sitio de comercio electrónico debe tener un comprobante de que el intercambio de datos sucedió entre el sitio y el cliente. ¿Qué característica de las firmas digitales es necesaria?

a) Imposibilidad de negación de la transacción ←
b) Confidencialidad de la clave pública

c) Integridad de los datos con firma digital
d) Autenticidad de los datos con firma digital

4) ¿Cuál es el propósito del uso de firmas digitales para la firma de código?

a) Establecer una conexión encriptada para intercambiar datos confidenciales con un sitio web del proveedor
b) Autenticar la identidad del sistema con un sitio web del proveedor
c) Verificar la integridad de los archivos ejecutables descargados del sitio web del proveedor ←
d) Generar un ID virtual

5) ¿Qué tecnología tiene una función que implica el uso de protocolos de terceros de confianza para emitir credenciales que son aceptadas como una identidad autorizada?

a) Firmas digitales
b) Algoritmos de hash
c) Claves simétricas
d) Certificados de PKI ←

6) ¿Cuál es el propósito de un certificado digital?

a) Ofrece prueba de que los datos tienen una firma tradicional adjunta.
b) Garantiza que la persona que obtiene acceso a un dispositivo de red está autorizada.
c) Garantiza que un sitio web no haya sido hackeado.
d) Autentica un sitio web y establece una conexión segura para el intercambio de datos confidenciales. ←

7) En una topología jerárquica de CA, ¿dónde puede una CA subordinada obtener un certificado para sí misma?

a) De la CA raíz o a partir de la autogeneración
b) Solo de la CA raíz
c) De la CA raíz o de otra CA subordinada en un nivel superior ←
d) De la CA raíz o de otra CA subordinada en cualquier parte del árbol
e) De la CA raíz o de otra CA subordinada en el mismo nivel

8) ¿Qué dos afirmaciones describen correctamente las clases de certificado utilizadas en la PKI? (Elija dos opciones).

a) Un certificado de clase 5 es para los usuarios que se centran en la verificación de correo electrónico.
b) Un certificado de clase 0 es para fines de pruebas. ←
c) Un certificado de clase 4 es para transacciones comerciales en línea entre empresas. ←
d) Cuanto menor sea el número de clase, más confiable será el certificado.
e) Un certificado de clase 0 es más confiable que un certificado de clase 1.

9) Una compañía está desarrollando una política de seguridad para tener comunicaciones seguras. En el intercambio de mensajes críticos entre una oficina de la sede central y una oficina de sucursal, un valor de hash debe recalcularse solo con un código predeterminado, para así garantizar la validez de la fuente de datos. ¿Qué aspecto de las comunicaciones seguras se aborda?

a) Autenticación de origen. ←
b) Imposibilidad de negación
c) Confidencialidad de los datos
d) Integridad de los datos

10) ¿Qué dos afirmaciones describen las características de los algoritmos simétricos? (Elija dos.)

a) Se denominan clave precompartida o clave secreta. ←
b) Utilizan un par de clave pública y clave privada.
c) Se utilizan comúnmente con tráfico VPN. ←
d) Proporcionan confidencialidad, integridad y disponibilidad.

11) ¿Qué tres servicios de seguridad proporcionan las firmas digitales? (Elija tres.)

a) Proporciona no repudio mediante funciones HMAC ←
b) Garantiza que los datos no han cambiado en tránsito ←
c) Proporciona cifrado de datos
d) Autentica la fuente ←
e) Proporciona confidencialidad de los datos firmados digitalmente
f) Autentica el destino

12) ¿Qué describe mejor la amenaza de seguridad de la suplantación de identidad?

a) Enviar correo electrónico masivo a individuos, listas o dominios con la intención de evitar que los usuarios accedan al correo electrónico
b) Enviar cantidades anormalmente grandes de datos a un servidor remoto para evitar que los usuarios accedan a los servicios del servidor
c) Interceptar el tráfico entre dos hosts o insertar información falsa en el tráfico entre dos hosts
d) Hacer que los datos parezcan provenir de una fuente que no es la fuente real ←

13) ¿Qué dos tipos de tráfico de red ilegible podrían eliminarse de los datos recopilados por los analistas de seguridad? (Elija dos.)

a) Tráfico STP
b) Tráfico Ipsec ←
c) Tráfico de actualizaciones de enrutamiento
d) Tráfico SSL ←
e) Tráfico de solicitud de IP

14) Una empresa de TI recomienda el uso de aplicaciones PKI para intercambiar información de forma segura entre los empleados. ¿En qué dos casos podría una organización utilizar aplicaciones PKI para intercambiar información de forma segura entre usuarios? (Elija dos opciones).

a) Transferencias FTP
b) Servidor DNS local
c) Servicio web HTTPS ←
d) Permiso de acceso a archivos y directorios
e) Autenticación 802.1x ←

15) ¿Qué método se puede usar para fortalecer un dispositivo?

a) Mantener el uso de las mismas contraseñas
b) Permitir que los servicios predeterminados permanezcan habilitados
c) Permitir la detección automática de USB
d) Usa SSH y deshabilita el acceso a la cuenta raíz a través de SSH ←

Firma: