1. **Una vez instalado un IPS ya no hace falta instalar un antivirus.**
    a. Verdadero
    b. Falso
2. **El principio de defensa en profundidad, coloca la información**
    a. En compartimientos separados
    b. En un centro de cómputo
    c. Dentro del perímetro más profundo
    d. En la nube
    e. En el perímetro más superficial
3. **El entorno de internet es un medio hostil en el que las aplicaciones deben ser seguras y resilientes, robustas y capaces de soportar ataques**
    a. Verdadero
    b. Falso
4. **El software en internet suele funcionar a través de la Web, consiste en aplicaciones del lado del cliente y aplicaciones del lado del servidor. ¿Usted diría que una aplicación es confiable en ambos lados de la comunicación?**
    a. Verdadero
    b. Falso
5. **Los IDS suelen tener mecanismos tales como Honeypots y se complementa con IPS.**
    a. Verdadero
    b. Falso
6. **Cuando se detecta un incidente de seguridad se debe:**
    a. Ejecutar el plan de recuperación de desastres
    b. Ejecutar el plan de respuesta ante incidentes
    c. Ejecutar el programa de protección contra intrusiones
    d. Ejecutar el plan de emergencia
    e. Ejecutar el plan de contingencias
7. **Existen cortafuegos de Hardware, Software e Incrustados en el sistema operativo, uno especial es el WAF**
    a. Verdadero
    b. Falso
8. **¿La seguridad multinivel implica el uso de esquemas tales como Bell La Padula?**
    a. Verdadero
    b. Falso
9. **Para proteger el perímetro y segmentar la red se deben usar: (emparejar)**
    a. Honeypot: Actúa como un señuelo para detectar intrusos
    b. IDS: es un sistema que sirve para detectar intrusiones
    c. AAA: Permite autorizar, autentificar y auditar la actividad
    d. Firewall: Provee seguridad perimetral
    e. VPN: Permite crear redes privadas sobre Internet
    f. VLAN: Provee separación de segmentos de la red.
10. **Ransomware es un tipo de ataque que ocurre con más frecuencia en plataformas de PC.**
    a. Verdadero
    b. Falso

11. **No es posible ofrecer una seguridad al 100% sino solo una seguridad lo suficientemente buena**
    a. Verdadero
    b. Falso
12. **El principio de seguridad de control de acceso cerrado por default significa:**
    a. Todo está cerrado de modo que el usuario requiere autorización del administrador
    b. Todo está abierto y disponible para el usuario
    c. Se utilizan las configuraciones por default de los sistemas operativos.
    d. Todo acceso está cerrado, excepto el que está expresamente definido para cada usuario
    e. Algunas cosas están abiertas y accesibles y otras no a criterio del administrador
13. **El principio de mínimos privilegios implica que:**
    a. Cada día el oficial de seguridad debe revisar como mínimo lo que hacen los usuarios cuando están conectados
    b. Cada administrador define los privilegios de grupo y coloca a los usuario en uno más grupos.
    c. Cada usuario tiene su identidad de usuario y de grupo.
    d. Cada usuario debe tener los privilegios indispensables necesarios para realizar su labor
    e. Cada usuario tiene privilegios acorde a su cargo en la empresa
14. **Empareje lo que corresponda**
    a. Autenticidad: Ser capaz de comprobar que la parte interviniente no ha sido suplantada
    b. Integridad: Ser capaz de comprobar que un mensaje llega a destino inalterado
    c. Confidencialidad: Mantener los datos privados y accesibles sólo a las partes interesadas
    d. Verificabilidad: Registrar una transacción de modo que se pueda demostrar los detalles de cómo se realizó
    e. Disponibilidad: Mantener los servicios operativos con normalidad, sin degradación ni bloqueos
15. **Un ataque zero day, corresponde a un ataque cuya propagación por la red hace inefectivos los mecanismos tales como antivirus, antispyware y similares**
    a. Verdadero
    b. Falso
16. **Los privilegios del usuario controlan lo que el usuario puede hacer cuando está conectado en la red, se utilizan los mínimos privilegios posibles para realizar su trabajo y el usuario está siendo monitoreado y se registra lo que hace cuando está conectado en la red. Creo que esto habla de AAA**
    a. Verdadero
    b. Falso
17. **El control de acceso a los recursos de la red está plasmado en los permisos de acceso de lectura, escritura, ejecución y también la posibilidad de añadir y eliminar contenidos. ¿El control de acceso involucra además la configuración del S.O., servicios, puertos y protocolos que se habilitan o no?**
    a. Verdadero

b. Falso

18. **Un mecanismo AAA, realiza funciones relacionadas con las actividades de usuarios internos y externos de la red.**
    a. Verdadero
    b. Falso
19. **La seguridad se gestiona utilizando una matriz de riesgo, los riesgos conllevan el grado de severidad, impacto causado y probabilidad de ocurrencia de un evento**
    a. Verdadero
    b. Falso
20. **Un Firewall, denominado también cortafuegos, es un dispositivo que permite separar una parte de la red del resto, provee seguridad de perímetro y protege la zona desmilitarizada DMZ y también puede separar segmentos de la red del resto de la red.**
    a. Verdadero
    b. Falso

Prueba 2

1. **Existen protocolos de seguridad que contienen varios subprotocolos tales como TLS o IPSec.**
    a. Verdadero
    b. Falso
2. **Kerberos es un protocolo que combina autentificación de los usuarios con tickets de acceso a cada servicio**
    a. Verdadero
    b. Falso
3. **IPSec es nativo en IP versión 6, pero opcional en IP versión 4.**
    a. Verdadero
    b. Falso
4. **Los protocolos Kerberos, SSH, PGP s/MINE, SFTP, se encuentran en la capa:**
    a. Capa de Red IP
    b. Capa de Aplicación
    c. Física y de enlace de datos
    d. Capa de sesión
    e. Capa de transporte
5. **IPSec Funciona en la capa de red en TCP/IP, par el intercambio de claves de sesión utiliza el protocolo:**
    a. ESP
    b. Diffie Hellman
    c. IKE
    d. Oakley
    e. Authentication Header
6. **Señale los protocolos que utilizan sobre digital (*digital signature*/firma digital)**
    a. S/MIME
    b. Secure Shell
    c. Kerbero
    d. ISAKMP
    e. sFTP
7. **Authentication Header y Encapsulating security Payload son modalidades del protocolo:**
    a. TLS
    b. SSL
    c. Kerberos
    d. PGP
    e. IPSec
8. **El protocolo transport security versión 1.2 tiene varios sub protocolos, el protocolo que se encarga de determinar las clase y algoritmos que se usarán durante la transmisión segura se llama:**
    a. Handshake Protocol
    b. Record protocol
    c. Change Cipher Protocol
    d. Alert Protocol
    e. Confirmation protocol

9. **El juego de protocolos de TCP/IP tiene varios protocolos de seguridad en sus diferentes capas**
    a. Verdadero
    b. Falso
10. **Los protocolos de seguridad de la capa de aplicación de TCP/IP son específicos de cada protocolo de aplicación, esto implica que ambos extremos de la comunicación deban usar la misma versión del protocolo**
    a. Verdadero
    b. Falso

Capítulo 1 - Descripción general de los sistemas informáticos
PREGUNTAS VERDADERAS / FALSAS:

V F 1. Las amenazas son ataques llevados a cabo.

V F 2. La seguridad informática es la protección de la integridad, disponibilidad y confidencialidad de los recursos del sistema de información.

V F 3. La integridad de los datos asegura que la información y los programas se cambien solo de una manera especificada y autorizada.

V F 4. La disponibilidad asegura que los sistemas funcionen rápidamente y que no se niegue el servicio a los usuarios autorizados.

V F 5. La "A" en la tríada de la CIA significa "autenticidad".

V F 6. Cuanto más crítico sea un componente o servicio, mayor será el nivel de disponibilidad requerido.

V F 7. La seguridad informática es esencialmente una batalla de ingenio entre un perpetrador que trata de encontrar huecos y el administrador que intenta cerrarlos.

V F 8. Los mecanismos de seguridad normalmente no involucran más de un algoritmo o protocolo en particular.

V F 9. Muchos administradores de seguridad ven la seguridad sólida como un impedimento para el funcionamiento eficiente y fácil de usar de un sistema de información.

V F 10. En el contexto de la seguridad, nuestra preocupación son las vulnerabilidades de los recursos del sistema.

V F 11. El hardware es el más vulnerable a los ataques y el menos susceptible a los controles automatizados.

V F 12. La planificación de contingencias es un área funcional que requiere principalmente medidas técnicas de seguridad informática.

V F 13. La arquitectura X.800 se desarrolló como un estándar internacional y se centra en la seguridad en el contexto de las redes y las comunicaciones.

V F 14. El primer paso para diseñar servicios y mecanismos de seguridad es desarrollar una política de seguridad.

V F 15. La garantía es el proceso de examinar un producto o sistema informático con respecto a ciertos criterios.

PREGUNTAS DE RESPUESTAS MÚLTIPLES:

1. _____ asegura que las personas controlan o influyen en la información relacionada con ellos que se puede recopilar y almacenar y por quién y a quién se puede divulgar esa información.
A. Disponibilidad C. Integridad del sistema
B. Privacidad D. Integridad de los datos

2. _____ asegura que un sistema realiza su función prevista de manera intacta, libre de manipulación no autorizada deliberada o inadvertida del sistema.
A. Integridad del sistema C. Integridad de los datos
B. Disponibilidad D. Confidencialidad

3. Una pérdida de _____ es la divulgación no autorizada de información.
A. confidencialidad C. integridad
B. autenticidad D. disponibilidad

4. Se puede esperar que una violación de seguridad de nivel _____ tenga un efecto adverso grave o catastrófico en las operaciones de la organización, los activos de la organización o las personas.
A. bajo C. normal
B. moderado D. alto

5. Una falla o debilidad en el diseño, implementación u operación y administración de un sistema que podría explotarse para violar la política de seguridad del sistema es una (a) _____.
A. contramedida C. vulnerabilidad
B. adversario D. riesgo

6. Un asalto a la seguridad del sistema que se deriva de un acto inteligente que es un intento deliberado de evadir los servicios de seguridad y violar la política de seguridad de un sistema es un (a) _____.
A. riesgo C. activo
B. ataque D. vulnerabilidad

7. Un (a) _____ es una acción, dispositivo, procedimiento o técnica que reduce una amenaza, una vulnerabilidad o un ataque eliminándolo o previniéndolo, minimizando el daño que puede causar, o descubriéndolo y reportándolo para que se puede tomar la acción correcta.
A. ataque C. contramedida
B. adversario D. protocolo

8. Un (a) _____ es un intento de aprender o hacer uso de información del sistema que no afecta los recursos del sistema.
A. ataque pasivo C. ataque interior
B. ataque exterior D. ataque activo

9. La mascarada, la falsificación y el repudio son acciones de amenaza que causan consecuencias de amenaza _____.
A. divulgación no autorizada C. engaño
B. disrupción D. usurpación

10. Una acción de amenaza en la que los datos confidenciales se entregan directamente a una entidad no autorizada es _____.
A. corrupción C. disrupción
B. intrusión D. exposición

11. Un ejemplo de _____ es un intento de un usuario no autorizado de obtener acceso a un sistema haciéndose pasar por un usuario autorizado.
A. mascarada C. intercepción
B. repudio D. inferencia

12. El _____ impide o inhibe el uso o manejo normal de las instalaciones de comunicaciones.
A. ataque pasivo C. cifrado de tráfico
B. denegación de servicio D. mascarada

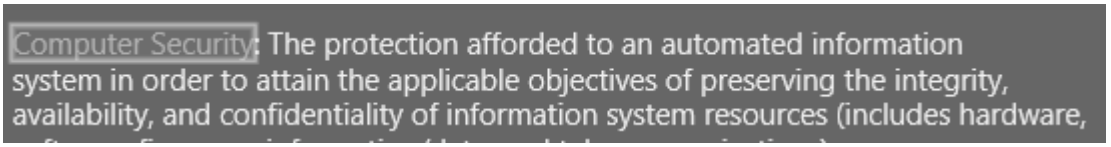
13. Un _____ es cualquier acción que compromete la seguridad de la información propiedad de una organización.
A. mecanismo de seguridad C. ataque de seguridad
B. política de seguridad D. servicio de seguridad

14. La garantía de que los datos recibidos son exactamente como los envió una entidad autorizada es _____.
A. autenticación C. confidencialidad de los datos
B. control de acceso D. integridad de los datos

15. _____ es la inserción de bits en espacios en un flujo de datos para frustrar los intentos de análisis de tráfico.
A. Relleno de tráfico C. Enrutamiento de tráfico
B. Control de tráfico D. Integridad del tráfico

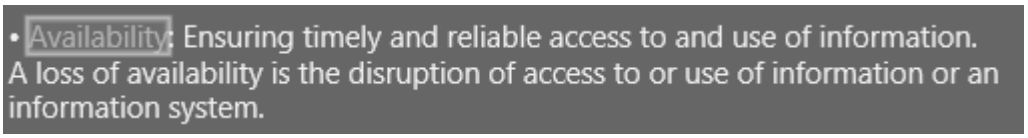
PREGUNTAS DE RESPUESTA BREVE:

1.**Computer security** es la protección otorgada a un sistema de información automatizado para lograr los objetivos aplicables de preservar la integridad, disponibilidad y confidencialidad de los recursos del sistema de información.

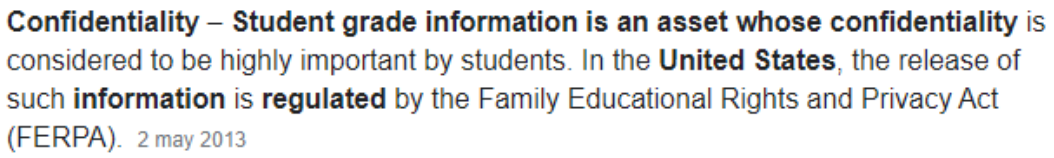


2. Confidencialidad, integridad y disponibilidad forman lo que a menudo se denomina **La triada de la CIA**

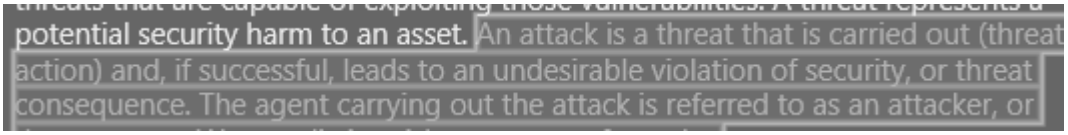
3. Una pérdida de **disponibilidad** es la interrupción del acceso o uso de información o un sistema de información.



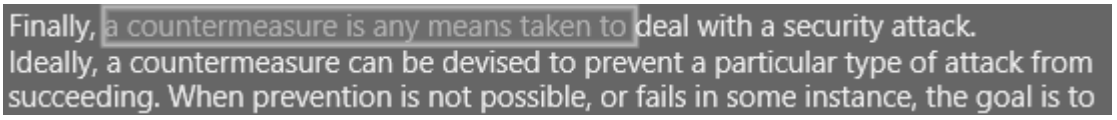
4. En los Estados Unidos, la información sobre las calificaciones de los estudiantes es un activo cuya confidencialidad está regulada por **Family Educational Rights and Privacy Act (FERPA**)



5. Un (a) **ataque** es una amenaza que se lleva a cabo y, si tiene éxito, conduce a una violación indeseable de la seguridad o una consecuencia de la amenaza.



6. Un (a) **contramedida** es cualquier medio utilizado para hacer frente a un ataque a la seguridad.



7. La apropiación indebida y el uso indebido son ataques que tienen como resultado consecuencias de amenaza de **usurpación/robo**.

8. Los activos de un sistema informático se pueden clasificar como hardware, software, líneas y redes de comunicación y **datos**.

9. La liberación del contenido del mensaje y el análisis del tráfico son dos tipos de ataques **pasivos**.

10. La reproducción, el enmascaramiento, la modificación de mensajes y la denegación de servicio son ejemplos de ataques **activos.**

11. Establecer, mantener e implementar planes para respuesta a emergencias, operaciones de respaldo y recuperación post desastre para sistemas de información organizacional para asegurar la disponibilidad de recursos de información crítica y la continuidad de operaciones en situaciones de emergencia es un plan **contingencia**.

12. Una (a) evaluación de **riesgo** es evaluar periódicamente el riesgo para las operaciones de la organización, los activos de la organización y las personas, resultante de la operación de los sistemas de información de la organización y el procesamiento, almacenamiento o transmisión o información de la organización asociados.

13. La arquitectura de seguridad OSI se centra en los ataques de seguridad, **mecanismo** y servicios.

14. Una **seguridad digital** son datos adjuntos a, o una transformación criptográfica de una unidad de datos que permite al destinatario de la unidad de datos probar el origen y la integridad de la unidad de datos y protegerse contra la falsificación.

15. La implementación de la seguridad involucra cuatro cursos de acción complementarios: prevención, detección, respuesta y **Recuperación**.

Capítulo 2 - Herramientas criptográficas
PREGUNTAS VERDADERAS / FALSAS:

V F 1. El cifrado simétrico se utiliza principalmente para brindar confidencialidad.

V F 2. Dos de las aplicaciones más importantes del cifrado de clave pública son firmas digitales y gestión de claves.

V F 3. Los ataques criptoanalíticos prueban todas las claves posibles en un fragmento de texto cifrado hasta que se obtenga una traducción inteligible en texto plano.

V F 4. La clave secreta se ingresa al algoritmo de cifrado.

V F 5. Triple DES toma un bloque de texto plano de 64 bits y una clave de 56 bits para producir un bloque de texto cifrado de 64 bits.

V F 6. Los modos de operación son las técnicas alternativas que se han desarrollado para aumentar la seguridad del cifrado de bloques simétricos para grandes secuencias de datos.

V F 7. La ventaja de un cifrado de flujo es que puede reutilizar claves.

V F 8. Un código de autenticación de mensaje es un pequeño bloque de datos generado por una clave secreta y adjunta a un mensaje.

V F 9. Como el MAC, una función hash también toma una clave secreta como entrada.

V F 10. La fuerza de una función hash contra ataques de fuerza bruta depende únicamente en la longitud del código hash producido por el algoritmo.

V F 11. La criptografía de clave pública es asimétrica.

V F 12. Los algoritmos de clave pública se basan en operaciones simples en patrones de bits.

V F 13. El propósito del algoritmo DSS es permitir que dos usuarios puedan llegar a un acuerdo sobre un secreto compartido que se puede utilizar como clave secreta para el posterior cifrado simétrico de mensajes.

V F 14. Un elemento importante en muchos servicios de seguridad informática y aplicaciones es el uso de algoritmos criptográficos.

V F 15. Se necesita alguna forma de protocolo para la distribución de claves públicas.

PREGUNTAS DE RESPUESTAS MÚLTIPLES:

1. El mensaje o los datos originales que se introducen en el algoritmo es _____.
   A. algoritmo de cifrado B. clave secreta
   C. algoritmo de descifrado D. texto plano

2. El _____ es el algoritmo de cifrado que se ejecuta a la inversa.
   A. Algoritmo de descifrado B. texto sin formato
   C. texto cifrado D. algoritmo de cifrado

3. _____ es el mensaje codificado producido como salida.
   A. Texto sin formato B. Texto cifrado
   C. Clave secreta D. Criptoanálisis

4. En promedio, se deben probar _____ de todas las claves posibles para lograr el éxito con un ataque de fuerza bruta.
   A. un cuarto B. la mitad
   C. dos tercios D. tres cuartos

5. Los algoritmos simétricos más importantes, todos los cuales son cifrados en bloque, son DES, DES triple y _____.
   A.SHA B. RSA
   C. AES D. DSS

6. Si la única forma de ataque que se podría realizar en un algoritmo de cifrado es la fuerza bruta, entonces la forma de contrarrestar esos ataques sería _____.
   A. usar teclas más largas B. usar teclas más cortas
   C. usar más teclas D. usar menos teclas

7. _____ es un procedimiento que permite a las partes que se comunican verificar que los mensajes recibidos o almacenados sean auténticos.
    a. Criptoanálisis B. Descifrado
    b. C. Autenticación de mensajes D. Resistencia a colisiones
8. El propósito de un _____ es producir una "huella digital" de un archivo,
    a. mensaje u otro bloque de datos.
        i. clave secreta B. firma digital
    b. C. keystream D.función hash

    _____ es un cifrado de bloque en el que el texto plano y el texto cifrado son
    c. números enteros entre 0 y n-1 para algunos n.
    d. A. DSS B. RSA
    e. C. SHA D. AES
9.
    a. 10. Un _____ se crea utilizando una función hash segura para generar un valor
    b. hash para un mensaje y luego encriptar el código hash con una clave privada.
    c. A. firma digital B. keystream
    d. C. función hash unidireccional D. clave secreta
10.
    a. 11. Los datos transmitidos almacenados localmente se denominan _____.
    b. A. texto cifrado B. DES
    c. C. datos en reposo D. ECC

11. Las firmas digitales y la gestión de claves son las dos aplicaciones más importantes del cifrado _____.
    A. clave privada B. clave pública
    C. resistente a preimagen D. avanzado

12. Un _____ es probar todas las claves posibles en un fragmento de texto cifrado hasta que se obtenga una traducción inteligible a texto plano.
    A. modo de operación B. función hash
    C. criptoanálisis D. ataque de fuerza bruta

13. Combinado un byte a la vez con el plaintext stream usando la operación XOR, un _____ es la salida del generador de bits pseudoaleatorio.
    A. keystream B. firma digital
    C. hash seguro D. código de autenticación de mensaje
14. Un _____ protege contra un ataque en el que una parte genera un mensaje para que otra parte lo firme.
    A. autenticador de datos B. función hash fuerte
    C. función hash débil D. firma digital

PREGUNTAS DE RESPUESTA BREVE:

1. También conocido como cifrado de clave única, la técnica universal para brindar confidencialidad a los datos transmitidos o almacenados es **cifrado simétrico / symmetric encryption**.
2. Hay dos enfoques generales para atacar un esquema de cifrado simétrico: ataques criptoanalíticos y ataques **fuerza bruta / brute-force**.
3. El algoritmo **descifrado / decryption** toma el texto cifrado y la clave secreta y produce el texto plano original.
4. Un ataque **criptoanalítico/cryptanalytic** explota las características del algoritmo para intentar deducir un texto sin formato específico o deducir la clave que se está utilizando.
5. Un **cifrado de bloque / block cipher** procesa la entrada de texto sin formato en bloques de tamaño fijo y produce un bloque de texto cifrado de igual tamaño para cada bloque de texto sin formato.
6. Un **cifrado de flujo / stream cipher** procesa los elementos de entrada de forma continua, produciendo una salida de uno en uno.
7. El cifrado de clave pública fue propuesto públicamente por primera vez por **Diffie y Hellman** en 1976.
8. Los dos criterios que se utilizan para validar que una secuencia de números es aleatoria son la independencia y **distribución uniforme / uniform distribution**.
9. Un **dispositivo de back-end / back-end appliance** es un dispositivo de hardware que se encuentra entre los servidores y los sistemas de almacenamiento y cifra todos los datos que van desde el servidor al sistema de almacenamiento y descifra los datos que van en la dirección opuesta.
10. En julio de 1998, **Fundación Frontera Electrónica (EFF) / Electronic Frontier Foundation (EFF)** anunció que había roto un cifrado DES utilizando una máquina "cracker DES" de propósito especial.
11. El enfoque más simple para el cifrado de múltiples bloques se conoce como modo **libro de códigos electrónico (ECB) / electronic codebook (ECB)** , en el que el texto sin formato se maneja en b bits a la vez y cada bloque de texto sin formato se cifra con la misma clave.
12. Una secuencia **pseudoaleatorio / pseudorandom** es aquella que es impredecible sin el conocimiento de la clave de entrada y que tiene un carácter aparentemente aleatorio.
13. La **clave pública y privada / public and private key** es un par de claves que se han seleccionado de modo que si una se usa para encriptar, la otra se usa para desencriptar.
14. **Cifrado de cinta basado en biblioteca / library-based tape encryption** se proporciona mediante una placa de coprocesador incrustada en la unidad de cinta y el hardware de la biblioteca de cintas.
15. El propósito del algoritmo **Acuerdo clave Diffie-Hellman / Diffie-Hellman Key Agreement** es permitir que dos usuarios lleguen a un acuerdo de forma segura sobre un secreto compartido que se puede utilizar como clave secreta para el cifrado simétrico posterior de mensajes.

Capítulo 3 - Autenticación de usuarios
PREGUNTAS VERDADERAS / FALSAS:

V F 1. La autenticación de usuario es el bloque de construcción fundamental y la principal línea de defensa.
V F 2. La identificación es el medio de establecer la validez de una identidad reclamada proporcionada por un usuario.
V F 3. Un token es el mejor medio de autenticación porque un adversario no puede falsificarlo ni robarlo.
V F 4. Muchos usuarios eligen una contraseña que es demasiado corta o demasiado fácil de adivinar.
V F 5. La autenticación de usuario es un procedimiento que permite a las partes comunicantes verificar que el contenido de un mensaje recibido no ha sido alterado y que la fuente es auténtica.
V F 6. Una buena técnica para elegir una contraseña es usar la primera letra de cada palabra de una frase.
V F 7. La autenticación del usuario es la base para la mayoría de los tipos de control de acceso y para la responsabilidad del usuario.
V F 8. Las tarjetas de memoria almacenan y procesan datos.
V F 9. Dependiendo de la aplicación, la autenticación de usuario en un sistema biométrico implica verificación o identificación.
V F 10. La inscripción crea una asociación entre un usuario y las características biométricas del usuario.
V F 11. La firma de un individuo no es lo suficientemente única como para usarla en aplicaciones biométricas.
V F 12. Los identificadores deben asignarse con cuidado porque las identidades autenticadas son la base de otros servicios de seguridad.
V F 13. Una tarjeta inteligente contiene un microprocesador completo.
V F 14. El keylogging es una forma de ataque al host.
V F 15. En un esquema biométrico, algunas características físicas del individuo se mapean en una representación digital.

PREGUNTAS DE RESPUESTAS MÚLTIPLES:

1. _____ define la autenticación de usuario como "el proceso de verificar una identidad reclamada por o para una entidad del sistema".
   A.RFC 2828 C. RFC 2298
   B.RFC 2493 D. RFC 2328
2. Presentar o generar información de autenticación que corrobora la vinculación entre la entidad y el identificador es el _____.
   A.paso de identificación C. paso de verificación
   B.paso de autenticación D. paso de corroboración
3. El reconocimiento por huella dactilar, retina y rostro son ejemplos de _____.
   A.reconocimiento facial C. biometría dinámica
   B.biometría estática D. autenticación de token
4. Un _____ es un programa de adivinación de contraseñas.
   A.contraseña hash C. password cracker
   B.contraseña biométrica D. contraseña salt

5. La estrategia _____ es cuando a los usuarios se les dice la importancia de usar contraseñas difíciles de adivinar y se les proporcionan pautas para seleccionar contraseñas seguras.
   A.Verificación reactiva de contraseñas
   B. contraseñas generadas por computadora
   C. Verificación proactiva de contraseñas
   D. Educación del usuario

6. Una estrategia _____ es aquella en la que el sistema ejecuta periódicamente su propio descifrador de contraseñas para encontrar contraseñas adivinables.
   A.educación del usuario
   B.verificación reactiva de contraseñas
   C. verificación proactiva de contraseñas
   D. contraseña generada por computadora

7. Los medios más comunes de identificación de persona a persona son _____.
   A.características faciales
   B.patrones retinianos
   C. firmas
   D. huellas dactilares

8. _____ sistemas identifican las características de la mano, incluida la forma y el largo y ancho de los dedos.
   A.Firma
   B.Huella digital
   C. Geometría de la mano
   D. Impresión de palma

9. Cada individuo que se incluirá en la base de datos de usuarios autorizados primero debe estar _____ en el sistema.
   A.verificado
   B.identificado
   C. autenticado
   D. inscrito

10. Para contrarrestar las amenazas a la autenticación de usuarios remotos, los sistemas generalmente se basan en alguna forma de protocolo _____.
    A.escuchando a escondidas
    B.desafío-respuesta
    C. caballo de Troya
    .D. denegación de servicio

11. Un _____ es cuando un adversario intenta lograr la autenticación del usuario sin acceso al host remoto o al camino de comunicaciones intermedio.
    A. ataque de cliente
    B. ataque de host
    C. ataque de espionaje
    D. ataque de caballo de Troya

12. Un _____ se dirige al archivo de usuario en el host donde se almacenan las contraseñas, los códigos de acceso del token o las plantillas biométricas.
    A. ataque furtivo
    B. ataque de cliente
    C. ataque de denegación de servicio
    D. ataque de host

13. Un ataque _____ implica que un adversario repita una respuesta de usuario capturada previamente.
    A.cliente
    B. Caballo de Troya
    C. repetición
    D. Espionaje

14. Una institución que emite tarjetas de débito a los titulares de tarjetas y es responsable de la cuenta del titular de la tarjeta y autoriza las transacciones es _____.
    A. tarjetahabiente C. auditor
    B. emisor D. procesador

15. _____ permite que un emisor acceda a redes regionales y nacionales que conectan dispositivos de punto de venta y cajeros automáticos en todo el mundo.
    A.EFT C. POS
    B.ATM D. ALF

PREGUNTAS DE RESPUESTA BREVE:

1. Un proceso de autenticación consta del paso **identificación** y el paso de verificación.
2. El patrón de voz, las características de la escritura a mano y el ritmo de escritura son ejemplos de biometría **dinámica**.
3. Un **archivo de contraseña oculta** es un archivo separado de las ID de usuario donde se guardan las contraseñas con hash.
4. Con la política **comprobación proactiva de contraseñas(PPC)**, un usuario puede seleccionar su propia contraseña, pero el sistema comprueba si la contraseña está permitida.
5. La técnica para desarrollar un verificador de contraseñas proactivo eficaz y eficiente basado en rechazar palabras en una lista se basa en el uso de un filtro **bloom**.
6. Los objetos que posee un usuario con el propósito de la autenticación del usuario se denominan **tokens**
7. Los protocolos de autenticación utilizados con tokens inteligentes se pueden clasificar en tres categorías: generador de contraseñas estáticas, dinámicas y **desafío - respuesta**.
8. Un sistema de autenticación **biométrico** intenta autenticar a una persona basándose en sus características físicas únicas.
9. El **patrón retiniano** es el patrón formado por las venas debajo de la superficie de la retina.
10. Un número aleatorio generado por el anfitrión a menudo se llama **mientras tanto/ nonce**.
11. **Escuchando a escondidas / Eavesdropping**, en el contexto de las contraseñas, se refiere al intento de un adversario de aprender la contraseña observando al usuario, encontrando una copia escrita de la contraseña, o alguna ataque similar que involucra la proximidad física del usuario y el adversario.
12. En un ataque de **caballo de Troya**, una aplicación o dispositivo físico se disfraza de aplicación o dispositivo auténtico con el fin de capturar una contraseña de usuario, código de acceso o biométrico.
13. Un ataque **denegación de servicio** intenta deshabilitar un servicio de autenticación de usuarios inundando el servicio con numerosos intentos de autenticación.
14. Un **titular de la tarjeta / cardholder** es un individuo a quien se le emite una tarjeta de débito.
15. El paso **verificación** es presentar o generar información de autenticación que corrobora el vínculo entre la entidad y el identificador.

Link:
https://www.staequiz.com/product/computer-security-principles-and-practice-4th-edition-by-william-stallings-test-bank/

Capítulo 4 - Access Control
PREGUNTAS VERDADERAS / FALSAS:

V F 1. El control de acceso es el elemento central de la seguridad informática.

V F 2. La función de autenticación determina en quién se confía para un propósito determinado.

V F 3. Una función de auditoría monitorea y mantiene un registro de los accesos de los usuarios a los recursos del sistema.

V F 4. Los dispositivos externos, como los cortafuegos, no pueden proporcionar servicios de control de acceso.

V F 5. Los principales objetivos de la seguridad informática son evitar que los usuarios no autorizados obtengan acceso a los recursos, evitar que los usuarios legítimos accedan a los recursos de manera no autorizada y permitir que los usuarios legítimos accedan a los recursos de manera autorizada.

V F 6. Las etiquetas de seguridad indican qué entidades del sistema son elegibles para acceder a ciertos recursos.

V F 7. La entrada confiable es un requisito de control de acceso.

V F 8. Un usuario puede pertenecer a varios grupos.

V F 9. Un derecho de acceso describe la forma en que un sujeto puede acceder a un objeto.

V F 10. El conjunto de derechos predeterminado siempre debe seguir la regla de privilegio mínimo o acceso de solo lectura

V F 11. Un programa de usuario se ejecuta en modo kernel en el que ciertas áreas de la memoria están protegidas del uso del usuario y es posible que no se ejecuten ciertas instrucciones.

V F 12. Cualquier programa que sea propiedad de, y SetUID para, el “superusuario” potencialmente otorga acceso sin restricciones al sistema a cualquier usuario que ejecute ese programa.

V F 13. Los sistemas RBAC tradicionales definen los derechos de acceso de usuarios individuales y grupos de usuarios.

V F 14. Una restricción es una relación definida entre roles o una condición relacionada con roles.

V F 15. Un modelo ABAC puede definir autorizaciones que expresan condiciones sobre las propiedades tanto del recurso como del sujeto.

Other Questions

Control de acceso discrecional / DAC(Discretionary Access Control) controla el acceso basándose en la identidad del solicitante y en las reglas de acceso que indican qué pueden hacer los solicitantes.

MAC / Control de acceso obligatorio(Mandatory Access Control) controla el acceso basándose en la comparación de etiquetas de seguridad con autorizaciones de seguridad.

RBAC / Control de acceso basado en roles(Role Based Access Control) controla el acceso según los roles que tienen los usuarios dentro del sistema y las reglas que establecen qué accesos están permitidos a los usuarios en roles determinados.

ABAC / Control de acceso basado en atributos(Attribute Based Access Control) controla el acceso en función de los atributos del usuario, el recurso al que se accede y las condiciones ambientales actuales.

PREGUNTAS DE RESPUESTAS MÚLTIPLES:

_____ implementa una política de seguridad que especifica quién o qué puede tener acceso a cada recurso específico del sistema y el tipo de acceso que se permite en cada instancia.
Control de auditoría B. Control de recursos
Control del sistema D. Control de acceso

_____ es la verificación de que las credenciales de un usuario u otra entidad del sistema son válidas.
Adecuación B. Autenticación
Autorización D. Auditoría

_____ es la concesión de un derecho o permiso a una entidad del sistema para acceder a un recurso del sistema.
Autorización B. Autenticación
Control D. Seguimiento

_____ es el método tradicional de implementar el control de acceso.
MAC B. RBAC
DAC D. MBAC

_____ controla el acceso basándose en la comparación de etiquetas de seguridad con autorizaciones de seguridad.
MAC B. DAC
RBAC D. MBAC

Un concepto que evolucionó a partir de los requisitos para la seguridad de la información militar es _____.
entrada confiable B. control de acceso obligatorio
políticas abiertas y cerradas D. entrada discrecional

Un _____ es una entidad capaz de acceder a objetos.
grupo B. objeto
sujeto D. propietario

Un (a) _____ es un recurso al que se controla el acceso.
objeto B. propietario
mundo D. sujeto

El bit de permiso final es el bit _____.
superusuario B. kernel
establecer usuario D. pegajoso(sticky)

_____ se basa en los roles que asumen los usuarios en un sistema en lugar de en la identidad del usuario.
DAC B. RBAC
MAC D. URAC

Un _____ es una función de trabajo con nombre dentro de la organización que controla este sistema informático.
usuario B. rol
permiso D. sesión

_____ proporciona un medio para adaptar RBAC a los aspectos específicos de las políticas administrativas y de seguridad en una organización.
Restricciones B. Roles mutuamente excluyentes
Cardinalidad D. Requisitos previos

_____ se refiere a establecer un número máximo de roles.
Cardinalidad B. Requisito previo
Exclusiva D. Jerarquía

Los atributos del sujeto, los atributos del objeto y los atributos del entorno son los tres tipos de atributos en el modelo _____.
DSD B. RBAC
ABAC D. SSD

El componente _____ se ocupa de la gestión y el control de las formas en que las entidades tienen acceso a los recursos.

A. gestión de recursos B. gestión de acceso
C.gestión de privilegios D. gestión de políticas

PREGUNTAS DE RESPUESTA BREVE:

X.800 define **el control de acceso** como la prevención del uso no autorizado de un recurso, incluida la prevención del uso de un recurso de una manera no autorizada.

Se realiza una revisión y examen independientes de los registros y actividades de los sistemas con el fin de probar la idoneidad de los controles del sistema, garantizar el cumplimiento de la política y los procedimientos operativos establecidos, detectar brechas en la seguridad y recomendar cualquier cambio indicado en el control, la política y los procedimientos. una **auditoría**

El control de acceso **basado en roles** controla el acceso según los roles que los usuarios tienen dentro del sistema y las reglas que establecen qué accesos se les permite a los usuarios en roles dados.

El Control de acceso **discrecional** controla el acceso basado en la identidad del solicitante y en las reglas de acceso que establecen lo que los solicitantes pueden o no pueden hacer.

Los elementos básicos del control de acceso son: sujeto, **objeto** y derecho de acceso.

Los sistemas básicos de control de acceso suelen definir tres clases de materias: propietario, **grupo** y mundo.

Un esquema de control de acceso **discrecional** es aquel en el que a una entidad se le pueden otorgar derechos de acceso que permiten a la entidad, por su propia voluntad, permitir que otra entidad acceda a algún recurso.

El ID de usuario **superusuario** está exento de las restricciones habituales de control de acceso a archivos y tiene acceso a todo el sistema.

Una **sesión** es un mapeo entre un usuario y un subconjunto activado del conjunto de roles al que está asignado el usuario.

Las jerarquías de roles hacen uso del concepto de **herencia** para permitir que un rol incluya implícitamente derechos de acceso asociados con un rol subordinado.

Un **prerrequisito** dicta que a un usuario solo se le puede asignar un rol en particular si ya está asignado a algún otro rol especificado y puede usarse para estructurar la implementación del concepto de privilegio mínimo.

Hay tres elementos clave para un modelo ABAC: atributos que se definen para entidades en una configuración; un modelo de política, que define las políticas de ABAC; y el modelo **arquitectura**, que se aplica a las políticas que hacen cumplir el control de acceso.

Los tres tipos de atributos en el modelo ABAC son atributos de sujeto, atributos de objeto y atributos de **entorno**.

Una **credencial** es un objeto o estructura de datos que vincula de manera autoritaria una identidad a un token que posee y controla un suscriptor.

En los sistemas de identidad digital, un **marco de confianza** funciona como un programa de certificación.

Capítulo 5 - Seguridad de la base de datos y la nube

PREGUNTAS VERDADERAS / FALSAS:

V F 1. Un lenguaje de consulta proporciona una interfaz uniforme para la base de datos.

V F 2. Una sola contramedida es suficiente para los ataques SQLi.

V F 3. Para crear una relación entre dos tablas, los atributos que definen la clave principal en una tabla debe aparecer como atributos en otra tabla, donde se denominan clave foránea.

V F 4. El valor de una clave primaria debe ser único para cada tupla de su tabla.

V F 5. Un valor de clave externa puede aparecer varias veces en una tabla.

V F 6. Una vista no puede proporcionar acceso restringido a una base de datos relacional, por lo que no puede utilizarse con fines de seguridad.

V F 7. El sistema de gestión de la base de datos utiliza la descripción de la base de datos. tablas para administrar la base de datos física.

V F 8. Dos desventajas del cifrado de bases de datos son la administración de claves y inflexibilidad.

V F 9. Los roles de servidor fijos operan a nivel de una base de datos individual.

V F 10. SQL Server permite a los usuarios crear roles a los que luego se les puede asignar acceso derechos a partes de la base de datos.

V F 11. Un centro de datos generalmente incluye fuentes de alimentación de respaldo.

V F 12. La seguridad del sitio del centro de datos en sí incluye barreras de entrada, junto con técnicas de autenticación para obtener acceso físico.

V F 13. La seguridad de la red es extremadamente importante en una instalación en la que la colección de activos se concentra en un solo lugar y es accesible mediante conexiones de red externas.

V F 14. La seguridad adaptada específicamente a las bases de datos es un factor cada vez más importante componente de una estrategia de seguridad organizacional general.

V F 15. El cifrado se convierte en la última línea de defensa en la seguridad de las bases de datos.

PREGUNTAS DE RESPUESTAS MÚLTIPLES:

1. Un (a) _____ es una colección estructurada de datos almacenados para su uso por una o más aplicaciones.

A.atributo B. base de datos
C.tupla D. inferencia

2. El bloque de construcción básico de un _____ es una tabla de datos, que consta de filas y columnas, similar to una hoja de cálculo.

A. base de datos relacional B. conjunto de consultas
C. DBMS D. perturbación

3. En el lenguaje de las bases de datos relacionales, el bloque de construcción básico es un _____, que es una tabla plana.

A. atributo B. tupla
C. clave primaria D. relación

4. En una base de datos relacional, las filas se denominan _____.

relaciones B. atributos
vistas D. tuplas

5. Un _____ se define como una parte de una fila que se utiliza para identificar de forma única una fila en una tabla.

A. clave externa B. consulta
C. clave primaria D. perturbación de datos

6. Un _____ es una tabla virtual.

A.tupla B. consulta
C.ver (vista) D. DBMS

7. Un (a) _____ es un usuario que tiene la responsabilidad administrativa de una parte o la totalidad de la base de datos.

A. administrador B. gerente de relaciones con la base de datos
C. propietario de la aplicación D. usuario final que no sea el propietario de la aplicación.

8. Un usuario final que opera en los objetos de la base de datos a través de una aplicación en particular, pero que no posee ninguno de los objetos de la base de datos, es _____.

A. propietario de la aplicación B. usuario final que no sea el propietario de la aplicación
C. administrador de clave externa D.

9. _____ es el proceso de realizar consultas autorizadas y deducir información no autorizada de las respuestas legítimas recibidas.

Perturbación B. Inferencia
Compromiso D. Particionamiento

10. Un _____ es la parte del centro de datos que alberga el equipo de procesamiento de datos.

A.sala de computadoras B. área de distribución principal
C.sala de entrada D. área de distribución horizontal

11. _____ alberga conexiones cruzadas y equipos activos para la distribución de cables al área de distribución de equipos.

A.Área de distribución principal B. Área de distribución de equipos
C.Área de distribución horizontal D. Área de distribución de zona

12. _____ abarca la detección, prevención y respuesta de intrusiones.

A.Gestión de intrusiones B. Evaluaciones de seguridad
C.Control de acceso a la base de datos D. Prevención de pérdida de datos

13. _____ es una organización que produce datos para que estén disponibles para su publicación controlada, ya sea dentro de la organización o para usuarios externos.

Cliente B. Titular de los datos
Usuario D. Servidor

14. _____ es una organización que recibe los datos encriptados de un propietario de datos y los pone a disposición para su distribución a los clientes.

A.Usuario B. Cliente
C.Propietario de los datos D. Servidor

15. _____ especifica los requisitos mínimos para la infraestructura de telecomunicaciones de los centros de datos.

TIA-942 B. RFC-4949
NIST-7883 D. RSA-298

PREGUNTAS DE RESPUESTA BREVE:

1. Un **sistema de gestión de bases de datos (DBMS)** es un conjunto de programas para construir y mantener la base de datos y para ofrecer servicios de consulta ad hoc a múltiples usuarios y aplicaciones.
2. En una base de datos relacional, las columnas se denominan **atributos**.
3. Un **vista / view** es el resultado de una consulta que devuelve filas y columnas seleccionadas de una o más tablas.
4. **Lenguaje de consulta estructurado (SQL)** es un lenguaje estandarizado que se puede utilizar para definir esquemas, manipular y consultar datos en una base de datos relacional.
5. Con la administración **basada en la propiedad**, el propietario (creador) de una mesa puede otorgar y revocar derechos de acceso a la mesa.

6. En una administración **centralizada**, un pequeño número de usuarios privilegiados puede otorgar y revocar derechos de acceso.
7. Además de otorgar y revocar derechos de acceso a una tabla, en una administración **descentralizada** el propietario de la tabla puede otorgar y revocar derechos de autorización a otros usuarios, permitiéndoles otorgar y revocar derechos de acceso a la tabla.
8. En un entorno de control de acceso discrecional, los usuarios de la base de datos se clasifican en tres categorías generales: administrador, usuario final que no sea el propietario de la aplicación y **Dueño de la aplicación**.
9. La ruta de transferencia de información mediante la cual se obtienen datos no autorizados se denomina canal **de inferencia**.
10. El ataque **inyeccion SQL (SQLi)** normalmente funciona terminando prematuramente una cadena de texto y agregando un nuevo comando.
11. La forma **Tautología** de ataque inyecta código en una o más declaraciones condicionales para que siempre se evalúen como verdaderas.
12. Un lenguaje **de consulta** proporciona una interfaz uniforme a la base de datos para usuarios y aplicaciones.
13. **En banda**, fuera de banda e inferencial son las tres categorías principales Riesgos de tipos de ataques SQLi.
14. Un **centro de datos** es una instalación empresarial que alberga una gran cantidad de servidores, dispositivos de almacenamiento, conmutadores y equipos de red.

15. El estándar de la Asociación de la Industria de las Telecomunicaciones **TIA-492** especifica los requisitos mínimos para la infraestructura de telecomunicaciones de los centros de datos.

Capítulo 6 Software malicioso
Mejores fichas para la unidad Chapter 6 | Quizlet
PREGUNTAS VERDADERAS / FALSAS:
Computer Security Principles And Practice 3rd Edition by Stalling – Test Bank.docx - StuDocu

V F 1. El software malicioso tiene como objetivo engañar a los usuarios para que revelen datos personales sensibles

V F 2. El software de claves captura las pulsaciones de teclas en un sistema comprometido

V F 3.El código metamórfico es un software que puede ser enviado sin cambios a una colección heterogénea de plataformas y ejecutarse con semántica idéntica.

V F 4.Un virus que se adhiere a un programa ejecutable puede hacer cualquier cosa que el programa está permitido hacer

V F 5.No es posible propagar un virus a través de una memoria USB

V F 6. Una bomba lógica es el evento o condición que determina cuando la carga útil es activada o entregada

V F 7.Muchas formas de infección pueden bloquearse negando a los usuarios normales el derecho de modificar programas del sistema.

V F 8.Un macro virus infecta porciones ejecutables de código

V F 9.El correo electrónico es un método común para propagar macrovirus.

V F 10. Además de propagarse, un gusano suele llevar algún tipo de carga útil.

V F 11.Un caballo de Troya es un programa aparentemente útil que contiene código oculto que, cuando se invoca, realiza alguna función perjudicial

V F 12.Los rastreadores de paquetes se utilizan principalmente para recuperar información confidencial como nombres de usuario y contraseñas.

V F 13. Un robot se propaga y se activa a sí mismo, mientras que un gusano se controla inicialmente desde alguna instalación central.

V F 14. Cada bot tiene una dirección IP distinta

V F 15. Los programadores utilizan puertas traseras para depurar y probar programas.
PREGUNTAS DE RESPUESTAS MÚLTIPLES:

Un programa que se inserta secretamente en un sistema con la intención de comprometer la integridad o confidencialidad de los datos de la víctima es _____.
A. Adobe
B. Animoto
C. malware
D. Prezi

_____ se utilizan para enviar grandes volúmenes de correo electrónico no deseado.
A. Rootkits
B. Programas de spammer
C. Descargadores de datos
D. Auto-rooter

A _____ es el código insertado en el malware que se encuentra inactivo hasta que se cumple una condición predefinida, que desencadena un acto no autorizado.
A. bomba lógica
B. trampilla
C. gusano
D. Caballo de Troya

El término "virus informático" se atribuye a _____.
A. Herman Hollerith
B. Fred Cohen
C. Charles Babbage
D. Albert Einstein

Los virus informáticos aparecieron por primera vez a principios de _____.
A. 1960
B. El decenio de 1970
C. 1980
D. Decenio de 1990

El _____ es lo que el virus "hace".
A. mecanismo de infección
B. gatillo
C. Bomba lógica
D. Carga útil

El _____ es cuando se realiza la función del virus.
A. fase latente
B. Fase de propagación
C. Fase de activación
D. Fase de ejecución

Durante el _____ el virus está inactivo.
A. fase latente
B. Fase de propagación
C. Fase de activación
D. Fase de ejecución
Un _____ usa código macro o scripting, normalmente incrustado en un documento y activado cuando el documento se ve o se edita, para ejecutarse y replicarse en otros documentos.
A. infector del sector del arranque
B. infector del archivo
C. macro virus
D. virus multipartito

_____ es la primera función en la fase de propagación de un gusano de red.
A. La propagación
B. Toma de huellas dactilares
B. Registro de teclas
D. Phishing con lanzas

El correo electrónico masivo no solicitado se conoce como _____.
A. spam
B. propagación
C. phishing
D. Artículos de cerámica

_____ es un malware que encripta los datos del usuario y exige el pago para acceder a la clave
necesario para recuperar la información.
A. Caballo de Troya

B. Ransomware
C. Crimeware
D. Polimórfico

Un ataque _____ es un ataque de bot en un sistema informático o red que causa una pérdida de servicio a los usuarios.
A. spam
B. phishing
C. DDoS
D. olfatear

La solución ideal a la amenaza de malware es _____.
A. identificación
B. remoción
C. detección
D. prevención

_____ se integrará con el sistema operativo de un ordenador host y supervisará el comportamiento del programa en tiempo real para acciones maliciosas.
A. Escáneres basados en huellas dactilares
B. Software de bloqueo de comportamiento
C. Tecnología genérica de descifrado
D. Escáneres heurísticos

PREGUNTAS DE RESPUESTA BREVE:

1. A **Rootkit** es un conjunto de programas instalados en un sistema para mantener un acceso encubierto a ese sistema con privilegios de administrador (root) mientras oculta evidencia de su presencia.
2. **Ataque combinado** utiliza múltiples métodos de infección o propagación para maximizar la velocidad de contagio y la gravedad del ataque.
3. Un ordenador **virus** es un software que puede "infectar" otros programas o cualquier tipo de contenido ejecutable e intenta replicarse.
4. A veces conocido como el "vector de infección", el **mecanismo de infección** es el medio por el cual un virus se propaga o se propaga.
5. A veces conocida como una "bomba lógica", la **trigger** es el evento o condición que determina cuando la carga útil se activa o se entrega.
6. Las cuatro fases de un virus típico son: fase latente, fase desencadenante, fase de ejecución y fase **propagación**
7. Durante la fase **triggering** el virus se activa para realizar la función para la que estaba destinado.
8. Un virus **sigiloso** está explícitamente diseñado para ocultarse de la detección por software antivirus.
9. **Movil** código se refiere a programas que pueden ser enviados sin cambios a una colección heterogénea de plataformas y ejecutarse con semántica idéntica.

10. **Conducir por descarga** es cuando un usuario ve una página Web controlada por el atacante que contiene un código que explota el error del navegador y descarga e instala malware en el sistema sin el conocimiento o consentimiento del usuario.
11. Un **botnet** es una colección de robots capaces de actuar de manera coordinada.
12. Un bot puede usar un **keylogger** para capturar pulsaciones de teclado en la máquina infectada para recuperar información sensible.
13. Las contramedidas para el malware se conocen generalmente como mecanismos **antivirus** porque se desarrollaron primero para atacar específicamente infecciones de virus.
14. Desarrollado por IBM y refinado por Symantec, el **Sistema inmunológico digital (DIS)** proporciona un sistema de detección de malware que automáticamente capturar, analizar, añadir detección y blindaje, o eliminar nuevo malware y pasar información sobre él a los sistemas clientes para que el malware se puede detectar antes de que se le permite ejecutar en otro lugar.
15. La tecnología de **Descifrado genérico DG** es un enfoque antivirus que permite al programa antivirus detectar fácilmente incluso los virus polimórficos más complejos y otros programas maliciosos, manteniendo al mismo tiempo rápidas velocidades de escaneo.

Capítulo 7 - Ataques de denegación de servicio
PREGUNTAS VERDADERAS / FALSAS:

V F 1. Un ataque de denegación de servicio(DoS) es un intento de comprometer la disponibilidad al obstaculizar o bloquear por completo la prestación de algún servicio.

V F 2. Los ataques DoS causan daños o destrucción de las infraestructuras de TI.

V F 3. Un ataque DoS dirigido a los recursos de la aplicación generalmente apunta a sobrecargar o bloquear su software de manejo de red.

V F 4. El ataque de suplantación de identidad SYN se dirige a la tabla de conexiones TCP en el servidor.

V F 5.Un cyberslam es un ataque a una aplicación que consume importantes recursos, lo que limita la capacidad del servidor para responder a solicitudes válidas de otros usuarios.

V F 6. La fuente del ataque se identifica explícitamente en el clásico ataque de inundación de ping.(ping flood attack)

V F 7. Dado un acceso suficientemente privilegiado al código de manejo de la red en un sistema informático, es difícil crear paquetes con una dirección de origen falsificada.

V F 8. Los paquetes SYN-ACK y ACK se transportan mediante IP, que es un protocolo de red poco fiable.

V F 9. El atacante necesita acceso a una conexión de red de alto volumen para un ataque de suplantación de SYN.

V F 10. Los ataques de inundación adoptan una variedad de formas según el protocolo de red que se esté utilizando para implementar el ataque.

V F 11. La mejor defensa contra ser un participante involuntario en un ataque DDoS es evitar que sus sistemas se vean comprometidos

V F 12. Un ataque de inundación SIP aprovecha el hecho de que una sola solicitud INVITE desencadena un consumo considerable de recursos.
.

V F 13. Slowloris es una forma de inundación ICMP.

V F 14. Los ataques de reflector y amplificador utilizan sistemas comprometidos que ejecutan los programas del atacante.

V F 15. Es muy poco lo que se puede hacer para evitar una multitud repentina.

PREGUNTAS DE RESPUESTAS MÚLTIPLES:

1. _____ se relaciona con la capacidad de los enlaces de red que conectan un servidor a Internet en general.
   A. Recurso de la aplicación B. Ancho de banda de la red
   C. Carga útil del sistema D. Difusión dirigida

2. Un _____ desencadena un error en el software de manejo de la red del sistema, lo que hace que se bloquee y el sistema ya no pueda comunicarse a través de la red hasta que se vuelva a cargar este software.
   A. Eco B. reflexión
   C. paquete de veneno D. inundación repentina

3. El uso de direcciones de origen falsificadas se conoce como _____.
   A. suplantación de la dirección de origen B. una dirección de tres vías
   C. caída aleatoria D. transmisión dirigida

4. El _____ ataca la capacidad de un servidor de red para responder a las solicitudes de conexión TCP desbordando las tablas utilizadas para administrar tales conexiones.
   A. Ataque de amplificación de DNS B. Ataque de suplantación de identidad SYN
   C. ataque de inundación básico D. ataque de paquetes de veneno

5. TCP usa _____ para establecer una conexión.
   A. zombie B. cookie SYN
   C. transmisión dirigida D. apretón de manos de tres vías

6. Los ataques de ancho de banda de _____ intentan aprovechar el consumo de recursos desproporcionadamente grande en un servidor.

A. Basado en aplicaciones B. Basado en sistema
C. Aleatoria D. Amplification

7. _____ es un protocolo basado en texto con una sintaxis similar a la de HTTP.
A. RIP B. DIP
C. SIP D. HIP

8. Los bots que comienzan desde un enlace HTTP dado y luego siguen todos los enlaces en el sitio web proporcionado de forma recursiva se denominan _____.
A. arrastrando B. arañas(spidering)
C. spoofing D. hacinamiento

9. _____ intenta monopolizar todos los subprocesos de manejo de solicitudes disponibles en el servidor web mediante el envío de solicitudes HTTP que nunca se completan.
A. HTTP B. Ataques de reflexión
C. SYN inundaciones D. Slowloris

10. Una característica de los ataques de reflexión es la falta de tráfico _____.
A. retrodispersión B. red
C. botnet D. de tres vías

11. Tanto en los ataques de inundación directos como en _____, el uso de direcciones fuente falsificadas da como resultado que los paquetes de respuesta se dispersen por Internet y, por lo tanto, sean detectables.
A. Ataques de suplantación de SYN B. ataques de inundación indirecta
C. Ataques ICMP D. suplantación de direcciones del sistema

12. En un ataque _____, el atacante crea una serie de solicitudes de DNS que contienen la dirección de origen falsificada para el sistema de destino.
A. SYN flood B. Amplificación de DNS
C. paquete de veneno D. Inundación UDP

13. Es posible defenderse específicamente contra el _____ usando un modversión modificada del código de manejo de la conexión TCP.
A. Apretón de manos de tres vías B. Inundación UDP
C. Ataque de suplantación de SYN D. multitud flash

14. Modificar el código de red TCP / IP del sistema para eliminar selectivamente una entrada para una conexión incompleta de la tabla de conexiones TCP cuando se desborda, lo que permite que continúe un nuevo intento de conexión es _____.
A. paquete de veneno B. slashdot
C. tráfico de retrodispersión D. caída aleatoria

15. Cuando se detecta un ataque DoS, el primer paso es _____.
A. identificar el ataque B. analizar la respuesta
C. diseñar filtros de bloqueo D. apagar la red

PREGUNTAS DE RESPUESTA BREVE:

1. Los paquetes de respuesta de eco ICMP generados en respuesta a una inundación de ping utilizando direcciones de origen falsificadas aleatoriamente se conocen como tráfico **backscatter/retrodispersión**.

2. Los ataques **flooding/inundación** inundan el enlace de red al servidor con un torrente de paquetes maliciosos que compiten con el tráfico válido que fluye hacia el servidor.

3. El protocolo estándar utilizado para la configuración de llamadas en VoIP es el Protocolo de **session initiation/inicio de sesión**.

4. Las solicitudes y **responses/respuestas** son los dos tipos diferentes de mensajes SIP.
5. Una inundación **HTTP** se refiere a un ataque que bombardea los servidores web con solicitudes HTTP.

6. Durante un ataque **reflection/reflección**, el atacante envía paquetes a un servicio conocido en el intermediario con una dirección de origen falsificada del sistema objetivo real y cuando el intermediario responde, la respuesta se envía al objetivo.

7. En los ataques de reflexión, la dirección **spoofed source/fuente falsificada** dirige todos los paquetes al objetivo deseado y cualquier respuesta al intermediario.

8. Los ataques de **amplification/amplificación** son una variante de los ataques de reflector y también implican el envío de un paquete con una dirección de origen falsificada para el sistema de destino a los intermediarios.

9. La mejor defensa contra los ataques de amplificación de transmisión es bloquear el uso de transmisiones **IP-directed/Dirigido por IP**.

10. Las cuatro líneas de defensa contra los ataques DDoS son: prevención y prevención de ataques, detección y filtrado de ataques, rastreo e identificación de la fuente del ataque y **attack reaction/reacción de ataque**.

11. Dado que el filtrado debe realizarse lo más cerca posible de la fuente mediante enrutadores o puertas de enlace que conozcan los rangos de direcciones válidos de los paquetes entrantes, un **ISP** está en la mejor posición para garantizar que se utilicen direcciones de origen válidas en todos los paquetes de sus clientes.

12. Un **capcha** es un acertijo gráfico que se utiliza para intentar identificar interacciones legítimas iniciadas por humanos.

13. Para responder con éxito a un ataque DoS, se necesita un buen plan de i**ncident response/respuesta al incidente** que incluya detalles de cómo contactar al personal técnico de su (s) ISP (s).

14. Si una organización depende de los servicios de red, debería considerar la posibilidad de duplicar y **replicating/replicar** estos servidores en varios sitios con varias conexiones de red.

15. Un **denial service/servicio de negación** es una acción que evita o perjudica el uso autorizado de redes, sistemas o aplicaciones al agotar recursos como unidades centrales de procesamiento, memoria, ancho de banda y espacio en disco.

Capítulo 8 Intrusión - Detección

PREGUNTAS DE VERDADERO / FALSO:

V F 1. Un intruso también puede ser llamado hacker o cracker.

V F 2. Los activistas son individuos o miembros de un grupo delictivo organizado con el objetivo de obtener una recompensa económica.

V F 3. Ejecutar un rastreador de paquetes en una estación de trabajo para capturar nombres de usuario y contraseñas es un ejemplo de intrusión.

V F 4. Aquellos que piratean computadoras lo hacen por la emoción de hacerlo o por su estatus.

V F 5. Los intrusos suelen utilizar pasos de una metodología de ataque común.

V F 6. El componente de IDS responsable de recopilar datos es la interfaz de usuario.

V F 7. La detección de intrusiones se basa en la suposición de que el comportamiento del intruso difiere del de un usuario legítimo en formas que pueden cuantificarse.

V F 8. El propósito principal de un IDS es detectar intrusiones, registrar eventos sospechosos y enviar alertas.

V F 9. Los enfoques basados en firmas intentan definir el comportamiento normal o esperado, mientras que los enfoques de anomalías intentan definir el comportamiento adecuado.

V F 10. La detección de anomalías es eficaz contra los infractores.

V F 11. Para ser de uso práctico, un IDS debe detectar un porcentaje sustancial de intrusiones mientras mantiene la tasa de falsas alarmas en un nivel aceptable.

V F 12. Un sensor en línea monitorea una copia del tráfico de la red; el tráfico real no pasa por el dispositivo.

V F 13. Una ubicación común para un sensor NIDS es justo dentro del firewall externo.

V F 14. La detección de intrusiones basada en la red utiliza la detección de firmas y la detección de anomalías.

V F 15. Snort puede realizar la prevención de intrusiones pero no la detección de intrusiones.

PREGUNTAS DE ELECCIÓN MÚLTIPLE:

1. _____ son individuos o miembros de un grupo más grande de atacantes externos que están motivados por causas sociales o políticas.
   A.Organizaciones patrocinadas por el estado B. Activistas
   C.Ciberdelincuentes D. Otros
2. Un _____ es un evento de seguridad que constituye un incidente de seguridad en el que un intruso obtiene acceso a un sistema sin tener autorización para hacerlo.
   A.detección de intrusiones B. empresa criminal
   C.IDS D. intrusión de seguridad
3. A _____ monitorea las características de un solo host y los eventos que ocurren dentro de ese host para detectar actividad sospechosa.
   A.IDS basado en host B. intrusión de seguridad
   C.IDS basado en red D. detección de intrusión
4. A _____ monitorea el tráfico de red para segmentos o dispositivos de red particulares y analiza la red, el transporte y los protocolos de aplicación para identificar actividad sospechosa.
   A.IDS basado en host B. intrusión de seguridad
   C.IDS basado en red D. detección de intrusión
5. El _____ es responsable de determinar si se ha producido una intrusión.
   A.analizador B. interfaz de usuario
   C.host D. sensor
6. _____ implica un intento de definir un conjunto de reglas o patrones de ataque que se pueden usar para decidir si un comportamiento dado es el de un intruso.
   A.Detección basada en perfiles B. Detección de firmas
   C.Detección de umbral D. Detección de anomalías
7. _____ implica la recopilación de datos relacionados con el comportamiento de usuarios legítimos durante un período de tiempo.
   A.Detección basada en perfiles B. Detección de firmas
   C.Detección de umbral D. Detección de anomalías
8. Un (a) _____ es un pirata informático con una habilidad técnica mínima que utiliza principalmente conjuntos de herramientas de ataque existentes.
   A.Maestro B. Aprendiz
   C.Oficial D. Activista
9. El módulo _____ analiza el tráfico de la LAN e informa los resultados al gerente central.
   A. Agente de monitor de LAN B. agente de host
   C. agente de administrador central D. agente de arquitectura

10. El propósito del módulo _____ es recopilar datos sobre eventos relacionados con la seguridad en el host y transmitirlos al administrador central.
    A. Agente de administrador central B. Agente de monitor de LAN
    C. Agente de host D. Agente de arquitectura
11. Un (a) _____ se inserta en un segmento de red para que el tráfico que está monitoreando debe pasar a través del sensor.
    A.sensor pasivo B. sensor de análisis
    C.sensor LAN D. sensor en línea
12. Un evento _____ es una alerta que se genera cuando el tráfico de chismes permite que una plataforma concluya que se está produciendo un ataque.
    A.PEP B. DDI
    C.IDEP D. IDME
13. _____ es un documento que describe el protocolo de nivel de aplicación para el intercambio de datos entre entidades de detección de intrusos.
    A.RFC 4767 B. RFC 4766
    C.RFC 4765 D. RFC 4764
14. La regla _____ le dice a Snort qué hacer cuando encuentra un paquete que coincide con los criterios de la regla.
    A.protocolo B. acción
    C.dirección D. puerto de destino
15. El _____ es el componente de identificación que analiza los datos recopilados por el sensor en busca de señales de actividad no autorizada o no deseada o de eventos que puedan ser de interés para el administrador de seguridad.
    A.fuente de datos B. operador
    C.sensor D. analizador

PREGUNTAS DE RESPUESTA BREVE:

1. Las amplias clases de intrusos son: ciberdelincuentes, organizaciones patrocinadas por el estado, **activistas** y otros.

2. Un **journeyman/oficial** es un pirata informático con suficientes habilidades técnicas para modificar y ampliar los conjuntos de herramientas de ataque para utilizar vulnerabilidades recién descubiertas.

3. la **interfaz de usuario** de un IDS permite al usuario ver la salida del sistema o controlar el comportamiento del sistema.

4. **Detección de intrusión** es un servicio de seguridad que monitorea y analiza los eventos del sistema con el propósito de encontrar y proporcionar advertencias en tiempo real de los intentos de acceder a los recursos del sistema de manera no autorizada.

5. Un IDS consta de tres componentes lógicos: analizadores, interfaz de usuario y **sensores**.

6. Copiar una base de datos que contiene números de tarjetas de crédito, ver datos confidenciales sin autorización y adivinar y descifrar contraseñas son ejemplos de **intrusión**.

7. La detección de anomalías **Basado en perfil** se centra en caracterizar el comportamiento pasado de usuarios individuales o grupos relacionados de usuarios y luego detectar desviaciones significativas.

8. Las técnicas de detección de **firma** detectan la intrusión al observar eventos en el sistema y aplicar un conjunto de reglas que conducen a una decisión sobre si un patrón de actividad determinado es o no sospechoso.

9. Una **Red neuronal** simula el funcionamiento del cerebro humano con neuronas y hace sinapsis entre ellas que clasifican los datos observados.

10. Un IDS **basado en la red (NIDS)** supervisa el tráfico en puntos seleccionados de una red o conjunto de redes interconectadas.

11. El documento **Requisitos de intercambio de mensajes de detección de intrusiones** (RFC 4766) define los requisitos para el formato de intercambio de mensajes de detección de intrusiones (IDMEF).

12. Los componentes funcionales de un **IDS** son: fuente de datos, sensor, analizador, administración, gerente y operador.

13. La **politica de seguridad** es la declaración predefinida formalmente documentada que define qué actividades pueden tener lugar en la red de una organización o en hosts particulares para respaldar los requisitos de la organización.

14. **Honeypots** son sistemas de señuelo diseñados para alejar a un atacante potencial de los sistemas críticos.

15. El **administrador** es el ser humano con la responsabilidad general de establecer la política de seguridad de la organización y, por lo tanto, de las decisiones sobre la implementación y configuración del IDS.

Capítulo 9 - Cortafuegos y sistemas de prevención de intrusiones

PREGUNTA VERDADERAS / FALSAS:

V F 1. El cortafuegos puede ser un solo sistema informático o un conjunto de dos o más sistemas que cooperan para realizar la función de cortafuegos.

V F 2. Un firewall puede servir como plataforma para IPSec.

V F 3. El firewall puede proteger contra ataques que eluden el firewall.

V F 4. Un firewall de filtrado de paquetes generalmente se configura para filtrar los paquetes que se envían en ambas direcciones.

V F 5. Una desventaja de un firewall de filtrado de paquetes es su simplicidad.

V F 6. La contramedida a los ataques de fragmentos diminutos es descartar los paquetes con una dirección de origen interna si el paquete llega a una interfaz externa.

V F 7. Un filtro de paquetes tradicional toma decisiones de filtrado en un individuo en base a paquetes y no toma en consideración ningún contexto de capa superior.

V F 8. Una de las principales desventajas de una puerta de enlace de nivel de aplicación es la procesamiento de gastos generales en cada conexión.

V F 9. La función principal del cortafuegos personal es negar el acceso no autorizado acceso remoto a la computadora.

V F 10. Una DMZ es uno de los cortafuegos internos que protege la mayor parte del red empresarial.

V F 11. Un medio lógico de implementar un IPSec es un firewall.

V F 12. Los firewalls distribuidos protegen contra ataques internos y brindan protección adaptada a máquinas y aplicaciones específicas.

V F 13. Un aspecto importante de la configuración de un firewall distribuido es la seguridad supervisión.

V F 14. A diferencia de un firewall, un IPS no bloquea el tráfico.

V F 15. Snort Inline permite que Snort funcione como una prevención de intrusiones capacidad.

PREGUNTAS DE RESPUESTAS MÚLTIPLES:

1. **Servicio** el control determina los tipos de servicios de Internet a los que se puede acceder, entrantes o salientes.
   A. Comportamiento B. Dirección
   C. Servicio D. Usuario
2. **Comportamiento** control controla cómo se utilizan servicios particulares.
   A. Servicio B. Comportamiento
   C. Usuario D. Dirección

3. El control **Direction** determina la dirección en la que se pueden iniciar solicitudes de servicio particulares y permitir que fluyan a través del firewall.
   A. Comportamiento B. Usuario
   C. Dirección D. Servicio

4. El control de **Usuario** controla el acceso a un servicio según el usuario que intenta acceder a él.
   A. Usuario B. Dirección
   C.Servicio D. Comportamiento
5. El **campo de protocolo IP** define el protocolo de transporte.
   a. A. dirección IP de destino B. dirección IP de origen
   b. C.interfaz D. campo de protocolo IP

6. Una puerta de enlace **a nivel de circuito** establece dos conexiones TCP, una entre ella y un usuario de TCP en un host interno y otra entre ella y un usuario de TCP en un host externo.
   A. filtrado de paquetes B. inspección de estado
   C. nivel de aplicación D. nivel de circuito

7. Un ejemplo de implementación de una puerta de enlace a nivel de circuito es el paquete **SOCKS** .
   A. nivel de aplicación B. SOCKS
   C. SMTP D. inspección de estado

8. Normalmente, los sistemas de _____ requieren o fomentan la conectividad externa, como un sitio web corporativo, un servidor de correo electrónico o un servidor DNS.
   A. DMZ B. Campo de protocolo IP
   C. cortafuegos límite D. VPN

9. Un _____ consiste en un conjunto de computadoras que se interconectan por medio de una red relativamente insegura y hace uso de encriptación y protocolos especiales para brindar seguridad.
   A. proxy B. UTM
   C. VPN D. firewall de inspección de estado

10. Una configuración _____ implica dispositivos de firewall independientes más firewalls basados en host que trabajan juntos bajo un control administrativo central.
   A. firewall de filtrado de paquetes B. firewall distribuido
   C. cortafuegos personal D. cortafuegos de inspección de estado

11. Típico de las aplicaciones SOHO, un **enrutador de detección** es un enrutador único entre redes internas y externas con filtrado de paquetes completo o sin estado.
   A. bastión único T B. bastión doble en línea
   C. enrutador de detección D. cortafuegos residente en el host

12. _____ son ataques que intentan dar acceso root a los usuarios normales.
   A. Explotaciones de escalamiento de privilegios
   B. Transversales de directorio
   C. Acceso al sistema de archivos
   D. Modificación de los recursos del sistema

13. _____ busca firmas de ataques en el contexto de un flujo de tráfico en lugar de paquetes individuales.
    A. Coincidencia de patrones B. Anomalía del protocolo
    C. Anomalía de tráfico D. Coincidencia con estado

14. _____ busca desviaciones de los estándares establecidos en las RFC.
    A. Anomalía estadística B. Anomalía del protocolo
    C. Coincidencia de patrones D. Anomalía de tráfico

15. El ataque _____ está diseñado para eludir las reglas de filtrado que dependen de la información del encabezado TCP.
    A. pequeño fragmento B. suplantación de direcciones
    C. enrutamiento de origen D. host bastión

PREGUNTAS DE RESPUESTA BREVE:

1. El **firewall** se inserta entre la red de las instalaciones e Internet para establecer un enlace controlado y para erigir un muro o perímetro de seguridad exterior para proteger la red de las instalaciones de los ataques basados en Internet.

2. Un **packet filtering/filtrado de paquetes** de firewall aplica un conjunto de reglas a cada paquete IP entrante y saliente y luego reenvía o descarta el paquete.

3. La dirección IP **source/fuente** es la dirección IP del sistema que originó el paquete IP.

4. Un intruso que transmite paquetes desde el exterior con un campo de dirección IP de origen que contiene una dirección de un host interno se conoce como dirección IP **spoofing**.

5. El protocolo **SOCKS** es un ejemplo de implementación de una puerta de enlace a nivel de circuito que es conceptualmente una "capa de compensación" entre la capa de aplicación y la capa de transporte y no proporciona servicios de puerta de enlace de la capa de red.

6. Identificado como un punto fuerte crítico en la seguridad de la red, el **bastion host/anfitrión bastión** sirve como plataforma para una puerta de enlace a nivel de aplicación o de circuito.

7. Un firewall **personal** controla el tráfico entre una computadora personal o estación de trabajo en un lado e Internet o la red empresarial en el otro lado.

8. Un **VPN** utiliza cifrado y autenticación en las capas de protocolo inferiores para proporcionar una conexión segura a través de una red que de otro modo sería insegura, normalmente Internet.

9. Los protocolos **IPSec** operan en dispositivos de red, como un enrutador o firewall, y cifrarán y comprimirán todo el tráfico que ingresa a la WAN y descifrarán y descomprimirán el tráfico proveniente de la WAN.

10. Un **host-based IPS (HIPS)/IPS basado en host** hace uso de técnicas de detección de firmas y anomalías para identificar ataques.

11. **Pattern/Patron** matching analiza los paquetes entrantes en busca de secuencias de bytes específicas (la firma) almacenadas en una base de datos de ataques conocidos.

12. Observaciones de anomalías de **Traffic/Tráfico** para detectar actividades de tráfico inusuales, como una avalancha de paquetes UDP o la aparición de un nuevo servicio en la red.

13. Snort Inline agrega tres nuevos tipos de reglas: descartar, rechazar y **Sdrop**.

14. Un único dispositivo que integra una variedad de enfoques para hacer frente a los ataques basados en la red se denomina sistema **UTM (unified threat management)/gestión unificada de amenazas**.

15. El cortafuegos sigue la doctrina militar clásica de **defensa en profundidad/ defense in depth** porque proporciona una capa adicional de defensa.

Capítulo 10 -

Capítulo 11 - Seguridad del software

PREGUNTAS VERDADERAS / FALSAS:

1. V F 1. Muchas vulnerabilidades de seguridad informática son el resultado de prácticas de programación deficientes.

2. V F 2. Las fallas de seguridad ocurren como consecuencia de una verificación y validación suficientes de los datos y códigos de error en los programas.

3. V F 3. La seguridad del software está estrechamente relacionada con la calidad y confiabilidad del software.

4. V F 4. Una diferencia entre la programación defensiva y las prácticas normales es que todo está asumido.

5. V F 5. Los programadores suelen hacer suposiciones sobre el tipo de entradas que el programa recibirá.

6. V F 6. La programación defensiva requiere un cambio de mentalidad a la tradicional prácticas de programación.

7. V F 7. Para contrarrestar los ataques XSS, un programador defensivo necesita explícitamente identificar cualquier supuesto en cuanto a la forma de entrada y verificar que cualquier datos de entrada se ajustan a esas suposiciones antes de cualquier uso de los datos.

8. V F 8. Las variantes de ataques de inyección pueden ocurrir siempre que un programa invoca el servicios de otro programa, servicio o función y los pasa información de origen externo y potencialmente no confiable sin suficiente inspección y validación del mismo.

9. V F 9. Los ataques de secuencias de comandos entre sitios intentan eludir la seguridad del navegador verificaciones para obtener privilegios de acceso elevados a datos confidenciales que pertenecen a Otro sitio.

10. V F 10. Para evitar ataques XSS, se debe examinar cualquier entrada proporcionada por el usuario y cualquier código peligroso eliminado o escapado para bloquear su ejecución.

11. V F 11. Un carácter ASCII se puede codificar como una secuencia de 1 a 4 bytes usando la codificación UTF-8.

12. V F 12. Existe un problema al anticipar y probar todos los tipos potenciales de Entradas no estándar que un atacante podría aprovechar para subvertir un programa.

13. V F 13. Las cuestiones clave desde la perspectiva de la seguridad del software son si el algoritmo implementado resuelve correctamente el problema especificado, si las instrucciones de la máquina ejecutadas correctamente representan la especificación del algoritmo de alto nivel y si la manipulación de los valores de los datos en las variables es válida y significativa.

14. V F 14. Sin una sincronización adecuada de los accesos es posible que los valores pueden estar dañados o perderse cambios debido a la superposición de acceso, uso y reemplazo de valores compartidos.

15. V F 15. La implementación correcta en el caso de una operación atómica es pruebe por separado la presencia del archivo de bloqueo y no siempre intente crearlo.

PREGUNTAS DE RESPUESTAS MÚLTIPLES:

- El “cálculo incorrecto del tamaño del búfer” se encuentra en la categoría de error de software _____.
    A. Defensas porosas
    B. Asignación de recursos
    C. Gestión de recursos riesgosos

D. Interacción insegura entre componentes

- "Control de acceso inadecuado (autorización)" está en el _____ error de software categoría.
  A. Defensas porosas
  B. Asignación de recursos
  C. Gestión de recursos riesgosos
  D. Interacción insegura entre componente

- La programación defensiva a veces se denomina _____.
  A. programación variable
  B. programación segura
  C. programación interpretativa
  D. programación chroot

- El manejo incorrecto del programa _____ es una de las fallas más comunes en seguridad del software.
  A. líneas
  B. entrada
  C. salida
  D. disciplinas

- _____ es una falla del programa qué ocurre cuando los datos de entrada del programa pueden influir accidental o deliberadamente en el flujo de ejecución del programa.
  A. Ataque PHP
  B. Ataque de inyección de formato de cadena
  C. Ataque XSS
  D. Ataque por inyección

- Un ataque _____ ocurre cuando la entrada se usa en la construcción de un comando que posteriormente es ejecutado por el sistema con los privilegios del servidor web.
  A. inyección de comando
  B. Inyección SQL
  C. inyección de código
  D. inyección de código remoto PHP

- Un ataque _____ es donde la entrada incluye código que luego es ejecutado por el sistema atacado.
  A. Inyección de SQL
  B. secuencias de comandos entre sitios
  C. inyección de código
  D. inyección de intérprete

- Bloqueo de asignaciones de valores de campo de formulario a variables globales es una de las defensas disponibles para prevenir un ataque _____.
  A. Inyección remota de código PHP

B. inyección de correo
C. comando inyección
D. inyección SQL

- Los ataques _____ son vulnerabilidades que involucran la inclusión de código de secuencia de comandos en el contenido HTML de una página web mostrada por el navegador de un usuario.
  A. Inclusión de archivos PHP
  B. Inyección de correo
  C. Inyección de código
  D. Secuencias de comandos entre sitios

- Un _____ es un patrón compuesto por una secuencia de caracteres que describen variantes de entrada permitidas.
  A. canonicalización
  B. condición de carrera
  C. expresión regular
  D. script de shell

- La intención de _____ es determinar si el programa o la función maneja correctamente todas las entradas anormales o si falla o no responde adecuadamente.
  A.secuencias de comandos de shell
  B. fuzzing
  C. canonicalización
  D. interbloqueo

- Una reducción constante en la memoria disponible en el montón hasta el punto en que se agota por completo se conoce como _____.
  A.fuzzing
  B. punto muerto
  C.inyección de memoria
  D. fuga de memoria

- La técnica más común para utilizar un mecanismo de sincronización apropiado para serializar los accesos para evitar errores es adquirir un _____ en el archivo compartido, asegurando que cada proceso tenga el acceso apropiado a su vez.
  A.bloqueo B. inyección de código
  C. chroot jail D. escalada de privilegios

- _____ son una colección de valores de cadena heredados por cada proceso de su padre que pueden afectar la forma en que se comporta un proceso en ejecución.
  A.Interbloqueos B. Privilegios
  C. Variables ambientales D. Condiciones de carrera

- La variante más común de inyectar contenido de script malicioso en páginas devueltas a los usuarios por los sitios de destino es la vulnerabilidad _____.

A.Reflexión XSS B. cárcel de chroot
C.bomba atómica D. inclusión de archivos PHP

PREGUNTAS DE RESPUESTA BREVE:

1. "No conservar la estructura de consulta SQL" se encuentra en la categoría de errores de software de **interacción insegura entre componentes** CWE / SANS.

2. La programación **defensive/defensiva** es una forma de diseño destinada a garantizar la función continua de una pieza de software a pesar del uso imprevisible del software.

3. La **entrada** del programa se refiere a cualquier fuente de datos que se origina fuera del programa y cuyo valor no es conocido explícitamente por el programador cuando se escribió el código.

4. Dos áreas clave de preocupación para cualquier entrada son el **tamaño** de la entrada y el significado e interpretación de la entrada.

5. Varias **rutinas de la biblioteca** estándar ampliamente utilizadas agravan el problema del desbordamiento del búfer al no proporcionar ningún medio de limitar la cantidad de datos transferidos al espacio disponible en el búfer.

6. Los datos de entrada del programa pueden clasificarse en términos generales como textuales o **binarios**.

7. En el ataque **Inyección SQL**, la entrada proporcionada por el usuario se usa para construir una solicitud SQL para recuperar información de una base de datos.

8. Los ataques **XSS** se observan con mayor frecuencia en aplicaciones web con secuencias de comandos.

9. Una variante en la que el atacante incluye contenido de script malicioso en los datos proporcionados a un sitio es la vulnerabilidad **XSS reflection/Reflexión XSS**.

10. El proceso de transformación de datos de entrada que implica reemplazar codificaciones alternativas equivalentes por un valor común se llama **canonicalization/canonicalización**.

11. La principal ventaja de **fuzzing** es su simplicidad y su ausencia de suposiciones sobre la entrada esperada a cualquier programa, servicio o función.

12. Un **condición de carrera / race condition** ocurre cuando varios procesos y subprocesos compiten para obtener acceso incontrolado a algún recurso.

13. Los sistemas relacionados con UNIX proporcionan la función del sistema chroot para limitar la vista de un programa del sistema de archivos a solo una sección cuidadosamente configurada que se conoce como **cárcel de chroot /chroot jail**.

14. Si los privilegios son mayores que los que ya están disponibles para el atacante, el resultado es una **escalada de privilegios / privilege escalation**.

15. El principio de **mínimo privilegio / least privilege** sugiere fuertemente que los programas deben ejecutarse con la menor cantidad de privilegios necesarios para completar su función.

Capítulo 12 - Seguridad del sistema operativo

PREGUNTAS VERDADERAS / FALSAS:

V F 1. La mayoría de los sistemas de software grandes no tienen debilidades de seguridad.

V F 2. Cada capa de código necesita medidas de endurecimiento adecuadas para proporcionar los servicios de seguridad adecuados.

V F 3. La seguridad de la capa inferior no afecta a las capas superiores.

V F 4. Es posible que un sistema se vea comprometido durante la instalación proceso.

V F 5. Un plan debe identificar al personal adecuado para instalar y administrar el sistema, teniendo en cuenta la formación necesaria.

V F 6. No es necesario tener en cuenta el propósito del sistema durante el proceso de planificación de la seguridad del sistema.

V F 7. La configuración predeterminada para muchos sistemas operativos generalmente maximiza la seguridad.

V F 8. Idealmente, los nuevos sistemas deberían construirse en una red desprotegida. para evitar restricciones de instalación.

V F 9. Un controlador malintencionado puede eludir muchos controles de seguridad para instalar malware.

V F 10. Debe ejecutar actualizaciones automáticas en sistemas controlados por cambios.

V F 11. Las contraseñas instaladas de forma predeterminada son seguras y no es necesario cambiarlas.

V F 12. Un error de configuración muy común que se observa con la transferencia de archivos y la Web servidores es para que todos los archivos suministrados por el servicio sean propiedad de la misma cuenta de "usuario" con la que se ejecuta el servidor.

V F 13. El análisis manual de registros es un medio confiable de detectar eventos.

V F 14. Realizar copias de seguridad periódicas de los datos en un sistema es un control crítico que ayuda a mantener la integridad del sistema y los datos del usuario.

V F 15. Los procesos de copia de seguridad y archivo suelen estar vinculados y gestionados juntos.

PREGUNTAS DE RESPUESTAS MÚLTIPLES:

1. El primer paso para implementar nuevos sistemas es _____.
   A. pruebas de seguridad B. instalación de parches
   C. planificación D. contenido crítico seguro
2. ¿Cuál de los siguientes debe tenerse en cuenta durante el sistema proceso de planificación de la seguridad?
   a. cómo se autentican los usuarios
   b. las categorías de usuarios del sistema
   c. qué acceso tiene el sistema a la información almacenada en otros hosts
   d. Todas las anteriores
3. El primer paso crítico para asegurar un sistema es asegurar el _____.
   a. sistema operativo base
   b. administrador de sistema
   c. mecanismos de protección contra malware
   d. privilegios de acceso remoto
4. Deben seguirse los siguientes pasos para proteger un sistema operativo:
   a. probar la seguridad del sistema operativo básico
   b. eliminar servicios innecesarios
   c. instalar y parchear el sistema operativo
   d. Todas las anteriores
5. _____ applications es un control que limita los programas que se pueden ejecutar en el sistema a solo aquellos en una lista explícita.
   A. Virtualización B. Lista blanca
   C. Registro D. Aplicación de parches
6. Los sistemas de archivos criptográficos son otro uso de _____.
   A. encriptación B. prueba
   C. virtualizar D. aceleración
7. Una vez que el sistema está construido, asegurado e implementado adecuadamente, el proceso de mantener la seguridad es _____.
   A. completar B. ya no es una preocupación
   C. continuo D. esporádico
8. El rango de datos de registro adquiridos debe determinarse _____.
   a. durante las pruebas de seguridad
   b. como paso final
   c. después de monitorear el volumen de flujo de datos promedio
   d. durante la etapa de planificación del sistema
9. El proceso _____ hace copias de datos a intervalos regulares para recuperar datos perdidos o dañados en períodos cortos de tiempo.

A. registro B. copia de seguridad
C.endurecimiento D. archivo

10. El proceso _____ retiene copias de los datos durante períodos de tiempo prolongados para cumplir con los requisitos legales y operativos.
    a. A. archivo B. virtualización
    b. C. parcheando D. copia de seguridad
11. Se deben determinar las necesidades y la política relacionadas con la copia de seguridad y el archivo _____.
    a. como paso final
    b. durante la etapa de planificación del sistema
    c. durante las pruebas de seguridad
    d. después de registrar el volumen de flujo de datos promedio
12. _____ son recursos que deben usarse como parte del proceso de planificación de la seguridad del sistema.
    a. Textos
    b. Recursos en línea
    c. Guías de endurecimiento del sistema específico
    d. Todas las anteriores
13. Los sistemas _____ no deben ejecutar actualizaciones automáticas porque posiblemente pueden introducir inestabilidad.
    a. A. Configuración controlada B. Política controlada
    b. C. Cambio controlado D. Proceso controlado
14. Los cambios más importantes necesarios para mejorar la seguridad del sistema son _____.
    a. deshabilitar los servicios de acceso remoto que no son necesarios
    b. Asegurarse de que las aplicaciones y los servicios necesarios estén configurados correctamente.
    c. deshabilitar servicios y aplicaciones que no son necesarios
    d. Todas las anteriores
15. Las preocupaciones de seguridad que resultan del uso de sistemas virtualizados incluyen _____.
    a. aislamiento del sistema operativo invitado
    b. supervisión del sistema operativo invitado por el hipervisor
    c. seguridad del entorno virtualizado
    d. Todas las anteriores

PREGUNTAS DE RESPUESTA BREVE:

1. Las tres capas de seguridad del sistema operativo son: física hardware, kernel del sistema operativo y **Aplicaciones y utilidades de usuario**.

2. El objetivo del proceso de planificación de la instalación del sistema específico es maximizar **la seguridad** y minimizar los costos.
3.

4. La seguridad del sistema comienza con la instalación del **sistema operativo**.

5. El paso final en el proceso de asegurar inicialmente el sistema operativo base es **pruebas de seguridad / security testing**.

6. **Inicio sesión / Logging** es un control reactivo que solo puede informarle sobre cosas malas que ya han sucedido.

7. **Backup** es el proceso de realizar copias de datos a intervalos regulares que permite la recuperación de datos perdidos o dañados durante períodos de tiempo relativamente cortos de unas pocas horas a algunas semanas.

8. **Archivar / Archive** es el proceso de retener copias de datos durante períodos prolongados de tiempo, ya sean meses o años, con el fin de cumplir con los requisitos legales y operativos para acceder a datos pasados.

9. Los sistemas **controlados** deben validar todos los parches en los sistemas de prueba antes de implementarlos en los sistemas de producción.

10. Los sistemas Unix y Linux otorgan permisos de acceso para cada recurso mediante el comando **chmod**.

11. Los sistemas Unix y Linux usan una **cárcel de chroot** / **chroot jail** que restringe la vista del servidor del sistema de archivos a solo una parte específica.

12. La información de configuración en los sistemas Windows está centralizada en **Registro / Registry**, que forma una base de datos de claves y valores.

13. **Virtualización** se refiere a una tecnología que proporciona una abstracción de los recursos informáticos que se ejecutan en un entorno simulado.

14. Los SO invitados son administrados por un **hypervisor**, o VMM, que coordina el acceso entre cada uno de los invitados y los recursos físicos de hardware reales.

15. Los sistemas de virtualización **alojada / Hosted** son más comunes en los clientes, donde se ejecutan junto con otras aplicaciones en el sistema operativo host y se utilizan para admitir aplicaciones para versiones o tipos de sistemas operativos alternativos.

16. Los sistemas de virtualización **nativa** generalmente se ven en servidores, con el objetivo de mejorar la eficiencia de ejecución del hardware.

LINKs:
https://solutionsmanualtb.blogspot.com/2014/09/computer-security-principles-and.html

CUARTO LINK:
https://www.quizsol.com/shop/test-bank-for-computer-security-principles-and-practice-4th-edition-by-william-stallings/

SEGUNDO LINK:
https://www.homeworkmerit.com/test-bank-for-computer-security-principles-and-practice-2nd-edition-william-stallings-test-bank/

algunas respuestas:
https://www.coursehero.com/file/38271922/Chapter-3-Test-CS2pdf/
https://quizlet.com/270086585/chapter-3-user-authentication-flash-cards/

Otro link:
https://www.homeworkmerit.com/test-bank-for-computer-security-principles-and-practice-2nd-edition-william-stallings/

Enumere los tipos de protecciones de datos

- Confiabilidad
- Disponibilidad
- Integridad

Enumere los tipos de protecciones de transacciones de datos

- Verificabilidad
- No Repudio

Enumere los planos de actuación de la seguridad informática

- Humano
- Organizacional
- Legal
- Crítico

Enumere los principios de seguridad informática

- Principio de Defensa en Profundidad
- P. de mínimos privilegios
- P. seguro por omisión
- P. Compartimentalización
- P. de Transparencia

¿Sobre qué se aplica el control de acceso?

- Carpetas, archivos, base de datos, impresoras o sea sobre Hardware y Software

¿Cómo se maneja la seguridad de los usuarios?

Los usuarios tienen restricciones de seguridad basados en los principios de mínimos privilegios y de acuerdo al rol en el que están, entonces nosotros damos los permisos mínimos necesarios para que puedan operar sin ningún problema.

¿Cómo se elabora una matriz de riesgo?

La matriz de riesgo tiene dos: la probabilidad de que un riesgo ocurra y otra el grado de severidad o daño. Los riesgos peores son los que tiene mayor probabilidad que ocurra y un grado de severidad alto.

¿En qué consiste la clave pública?

La clave pública es un esquema en el cual cada participante tiene dos claves, una pública y otra privada o secreta que es con la que descifra los mensajes que llegan o también se puede usar para tener autenticación.

¿Qué es una marca de tiempo timestamp?

Marca de tiempo es un número pseudoaleatorio que se suele utilizar con una clave para restringir el tiempo de validación de la clave.

¿Por qué son importantes las políticas de seguridad?

Las políticas de seguridad son los lineamientos generales o de base, son las primeras premisas sobre las que se construye el aparataje de seguridad y este incluye el diseño de la red, desarrollo seguras, restricciones, como se va a compartimentalizar.

Preguntas Interciclo

Una vez instalado un IPS ya no hace falta instalar un antivirus
Falso

El principio de defensa en profundidad, coloca a la información
Dentro del perímetro más profundo

El entorno de internet es un medio hostil en el que las aplicaciones deben ser seguras y resilientes, robustas y capaces de soportar ataques
Verdadero

El software en internet suele funcionar a través de la web, consiste en aplicaciones del lado del cliente y aplicaciones del lado del servidor. Usted diría que una aplicación es confiable en ambos lados de la comunicación?
Falso

Un IDS suele tener mecanismos tales como Honeypots y se complementa con IPS
Verdadero

Cuando se detecta un incidente de seguridad se debe
Ejecutar el plan de respuesta ante incidentes

Existe cortafuegos de hardware, software e incrustados en el sistema operativo, uno especial es el WAF
Verdadero

La seguridad multinivel implica el uso de esquemas tales como Bell La Padula?
Verdadero

Para proteger el perímetro y segmentar la red se deben usar:
Honeypot : Actúa como un señuelo para detectar intrusos
IDS: Es un sistema que sirve para detectar intrusiones
AAA: Permite autorizar, autentificar y auditar la actividad
Firewall: Provee seguridad perimetral
VPN: Permite crear redes privadas sobre internet
VLAN: Provee separación de segmentos de la red.

Ransomware es un tipo de ataque que ocurre con más frecuencia en plataformas de PC.
Verdadero

No es posible ofrecer una seguridad al 100% sino solo una seguridad lo suficientemente buena
Verdadero

El principio de seguridad de control de acceso cerrado por default significa:
Todo acceso está cerrado, excepto el que está expresamente definido para cada usuario.

El principio de mínimo privilegios implica que:
Cada usuario debe tener los privilegios indispensables necesarios para realizar su labor.

Empareje lo que corresponda
Autenticidad: Ser capaz de comprobar que la parte interviniente no ha sido suplantada
Integridad: Ser capaz de comprobar que un mensaje llega a destino inalterado
Confidencialidad: Mantener los datos privados y accesibles sólo a las partes interesadas.
Verificabilidad: Registrar una transacción de modo que se pueda demostrar los detalles de cómo se realizó.
Disponibilidad: Mantener los servicios operativos con normalidad, sin degradación ni bloqueos.

Un ataque zero day, corresponde a un ataque cuya propagación por la red hace inefectivos los mecanismos tales como antivirus, antispyware y similares.
Verdadero

Los privilegios del usuario controlan lo que el usuario puede hacer cuando está conectado en la red, se utilizan los mínimos privilegios posibles para realizar su trabajo y el usuario está siendo monitoreado y se registra lo que hace cuando está conectado en la red.
Verdadero

El control de acceso a los recursos de la red está plasmado en los permisos de acceso de lectura, escritura, ejecución y también la posibilidad de añadir y eliminar contenidos. El control de acceso involucra además la configuración del S.O., servicios, puertos y protocolos que se habilitan o no?
Verdadero

Cuando se detecta un incidente de seguridad se debe:
Ejecutar el plan de respuesta ante incidentes

Un mecanismo AAA, realiza funciones relacionadas con las actividades de usuarios internos y externos de la red.
Verdadero

La seguridad se gestiona utilizando una matriz de riesgos, los riesgos conllevan el grado de severidad, impacto causado y probabilidad de ocurrencia de un evento.
Verdadero

Un firewall denominado también cortafuegos es un dispositivo que permite separar una parte de la red del resto, provee seguridad de perímetro y protege la zona desmilitarizada DMZ y también puede separar segmentos de la red del resto de la red.
Verdadero

La seguridad se gestiona utilizando una matriz de riesgo, los riesgos conllevan el grado de severidad impacto causado y probabilidad de ocurrencia de un evento
Verdadero

Preguntas del examen final de hace un año

1. **La gestión de la seguridad es un proceso continuo dentro de la empresa, un plan de contingencias refiere a tener previamente establecido como actuar en caso de un incidente de seguridad y quienes intervienen y cómo se compartan en cada caso.**
   Es necesario monitorear y preservar los logs de auditoría en forma continua solo cuando se ha presentado un incidente.
   - solo cuando se presenta un incidente
   - en forma continua
2. **En el plano humano la ingeniería social es una amenaza**
   - verdadero
   - falso
3. **La seguridad informática tiene varios planos y son:**
   - privacidad, autenticidad e integridad
   - humano, legal, organizacional y técnico
   - directivo, auditoría, usuarios, personal de seguridad
4. **El principio de defensa en profundidad establece que los usuarios han de gozar de los mínimos privilegios necesarios para realizar su labor**
   - Verdadero
   - Falso
5. **Los entornos informáticos y la información que albergan requiere de diferentes tipos de protección, estas pueden ser:**
   - Para proteger la transmisión y el almacenamiento de datos hablamos de → **Confidencialidad**
   - Para identificar a los participantes → **Autenticidad**
   - Para garantizar que un mensaje en destino no ha sido alterado → **Integridad**
   - Para esclarecer cualquier reclamo o disputa → **Verificabilidad**
   - Para garantizar que los servicios funciones y estén disponibles → **Disponibilidad**
6. **El Hacking ético permite que un empresario contrate los servicios profesionales para realizar un análisis de vulnerabilidades sobre un sistema informático, una de las pruebas requiere un test de penetración, entre las herramientas comúnmente se encuentra Kali Linux, existen otras más.**
   ¿Puede un hacker ético realizar el examen de porciones del sistema informático que no se ha solicitado por el interesado?
   - Verdadero
   - Falso
7. **Empareje lo que corresponde:**
   La seguridad perimetral depende principalmente → **cortafuegos**
   Un mecanismo de detección de intrusos se denomina con las siglas → **IDS**
   Un IDS funciona usualmente en conjunto con → **IPS**
   La autenticidad utiliza mecanismos tales como → **Radius o Tacacs**
   Un sistema de antivirus utiliza la importa (signature) y patrones de comportamiento estadístico de tráfico así como → **Inteligencia Artificial**
   AAA significa → **Autorización, Autenticación y Auditoría.**

8. **Todo sistema informático y telemático es complejo y tiene vulnerabilidades, en un entorno informático siempre riesgos, en el internet así como en el entorno empresarial están presentes amenazas al normal funcionamiento de los sistemas y aplicaciones, cuando una amenaza se concreta se produce un ataque**
    - Verdadero
    - Falso
9. **La protección de los datos requiere de mecanismos basados en algoritmos criptográficos, así hay distintos tipos de algoritmos destinados a ofrecer diferentes tipos de protección, emparejar lo que corresponda:**
   Para garantizar la integridad de los datos → **funciones de hash**
   Existen algoritmos que pueden funcionar para proveer confidencialidad y autenticidad, uno de ellos es muy conocido es → **RSA**
   Para proveer confidencialidad → **Algoritmos de cifrado**
   Para garantizar la autenticidad → **Firma electrónica**
   Para probar la autenticidad de las partes utilizamos clave simétrica o clave pública → **clave pública**
10. **OWASP es un foro dedicado al desarrollo seguro de software que funcionará en entornos Web.**
    - Verdadero
    - Falso
11. **La seguridad informática es un proceso que requiere de la gestión continua, esta gestión involucra a personal de auditoría informática, la que dependiendo del tamaño de la empresa puede ser interna y externa.**
    En el caso de empresas pequeñas es común tener un departamento de auditoría interna?
    - Verdadero
    - Falso
12. **El Ransoming es un tipo de ataque en que se cifran los datos contenidos principalmente en un teléfono celular inteligente y el secuestro de los datos conlleva extorsión para poder recuperarlos, muchas veces el atacante solicita dinero, el que una vez entregado no garantiza el desbloqueo de los datos.**
    - Verdadero
    - Falso
13. **La mejor manera de combatir el cibercrimen es la prevención. Se concibe así el criterio de seguridad suficientemente buena, a aquel diseño de seguridad que cubre los potenciales riesgos reales sobre una instalación informática, sus usuarios y la información.**
    - Verdadero
    - Falso
14. **Un ataque zero day tiene una propagación tan rápida que deja inútiles mecanismos tales como antivirus, es necesario incorporar a los mecanismos sistemas expertos y sistemas basados en inteligencia artificial?**
    - Verdadero
    - Falso

15. **La teoría de números posibilita la construcción de algoritmos criptográficos, los algoritmos criptográficos forman parte de los protocolos de seguridad, los protocolos de seguridad forman parte de los mecanismos de seguridad y estos del sistema integral de seguridad.**
    - Verdadero
    - Falso