Curso: Seguridad informática
Expte.: 29/2020/LJ/0019
Evaluación:
Acción y grupo:
Módulo: MF0486_3

Fecha examen:	19/12/2022
Nombre y apellidos:	
NIF:	
Docente:	Juan Antonio Ferrández Rodríguez

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

1) ¿Cuál es un motivo por el que las amenazas de seguridad internas pueden provocar mayores daños en una organización que las amenazas de seguridad externas?

a) Los usuarios internos tienen acceso directo a los dispositivos de infraestructura. *
b) Los usuarios internos pueden acceder a los datos corporativos sin autenticación.
c) Los usuarios internos tienen mejores habilidades de hackeo.
d) Los usuarios internos pueden acceder a los dispositivos de infraestructura a través de Internet.

2) ¿Cuál es otro nombre para la confidencialidad de la información?

a) Credibilidad
b) Privacidad *
c) Precisión
d) Coherencia

3) ¿Cuáles de los siguientes elementos son tres componentes de la tríada CIA? (Elija tres opciones).

a) Confidencialidad *
b) Disponibilidad *
c) Acceso
d) Escalabilidad
e) Integridad *
f) Intervención

4) ¿Cuál es un ejemplo de «hacktivismo»?

a) Los delincuentes usan Internet para intentar robar dinero de una empresa bancaria.
b) Un adolescente ingresa en el servidor web de un periódico local y publica una imagen de su personaje de dibujos animados preferido.
c) Un país intenta robar secretos de defensa de otro país infiltrando las redes gubernamentales.
d) Un grupo de ecologistas inicia un ataque de denegación de servicio contra una empresa petrolera responsable de un gran derrame de petróleo. *

Curso: Seguridad informática
Expte.: 29/2020/LJ/0019
Evaluación:
Acción y grupo:
Módulo: MF0486_3

5) ¿Cuál es la motivación de un atacante de sombrero blanco?

a) Ajustar los dispositivos de red para mejorar su rendimiento y eficiencia.
b) Aprovechar cualquier vulnerabilidad para beneficio personal ilegal.
c) Detectar debilidades en la red y los sistemas para mejorar su nivel de seguridad. *
d) Estudiar los sistemas operativos de diversas plataformas para desarrollar un nuevo sistema.

6) ¿Cuáles son los tres métodos que se pueden utilizar para proteger la confidencialidad de la información? (Elija tres opciones).

a) Control de versiones
b) Cifrado de datos *
c) Configuración en los permisos de los archivos
d) ID de nombre de usuario y contraseña *
e) Autenticación de dos pasos *
f) Copia de seguridad

7) ¿Cuáles son las dos características que describen un gusano? (Elija dos opciones).

a) Infecta las PC al unirse a los códigos de software.
b) Se oculta en estado latente hasta que un atacante lo requiere.
c) Se desplaza a nuevas PC sin la intervención o el conocimiento del usuario. *
d) Se ejecuta cuando se ejecuta un software en una PC.
e) Se autoduplica. *

8) ¿Qué ejemplo muestra cómo es que el malware puede estar oculto?

a) Se inicia un ataque contra el sitio web público de un minorista en línea con el objetivo de bloquear su respuesta a los visitantes.
b) Un botnet de zombies transporta información personal al hacker.
c) Un hacker utiliza técnicas para mejorar la clasificación de un sitio web a fin de redirigir a los usuarios a un sitio malicioso.
d) Se envía un correo electrónico a los empleados de una organización con un archivo adjunto que asemeja una actualización de antivirus, pero el archivo adjunto en realidad consta de un spyware. *

9) ¿Qué tipo de ataque permite que un atacante utilice el método de fuerza bruta?

a) Denegación de servicio
b) Programas detectores de paquetes
c) Ingeniería social
d) Decodificación de contraseñas *

10) ¿Cuál es el objetivo principal de un ataque DoS?

a) Facilitar el acceso a redes externas.
b) Examinar los datos en el servidor de destino.
c) Obtener todas las direcciones de la libreta de direcciones dentro del servidor.
d) Evitar que el servidor de destino pueda controlar solicitudes adicionales. *

11) ¿Qué herramienta se usa para brindar una lista de puertos abiertos en los dispositivos de red?

a) Ping
b) Tracert
c) Whois
d) Nmap *

Curso: Seguridad informática
Expte.: 29/2020/LJ/0019
Evaluación:
Acción y grupo:
Módulo: MF0486_3

12) Un usuario tiene dificultad para recordar las contraseñas de múltiples cuentas en línea. ¿Cuál es la mejor solución que puede intentar el usuario?

a) Compartir las contraseñas con el técnico de la computadora o el administrador de la red.
b) Anotar las contraseñas y ocultarlas de la vista.
c) Crear una sola contraseña segura que se utilizará en todas las cuentas en línea.
d) Guardar las contraseñas en un programa de administración de contraseñas centralizado. *

13) ¿Qué configuración en un router inalámbrico no se considera adecuadamente segura para una red inalámbrica?

a) Habilitar la seguridad inalámbrica.
b) Modificar una contraseña y un SSID predeterminados en un router inalámbrico.
c) Impedir la transmisión de un SSID. *
d) Implementar el cifrado WPA2.

14) Un administrador de red lleva a cabo una sesión de capacitación para el personal de la oficina sobre cómo crear una contraseña segura y eficaz. ¿Qué contraseña le tomará más tiempo a un usuario malintencionado adivinar o «romper»?

a) 10characters
b) super3secret2
c) drninjaphd
d) mk$$cittykat104# *

15) Mientras los datos se almacenan en un disco duro local, ¿qué método protege los datos del acceso no autorizado?

a) Una copia duplicada del disco duro.
b) Autenticación de dos pasos
c) Cifrado de datos *
d) La eliminación de archivos confidenciales.

16) ¿Qué tipo de tecnología puede evitar que el software malicioso monitoree las actividades del usuario, recopile información personal y genere anuncios móviles no deseados en el ordenador de un usuario?

a) Firewall
b) Autenticación de dos pasos
c) Administrador de contraseñas
d) Antispyware *

17) ¿Por qué los dispositivos de IoC representan un riesgo mayor que otros dispositivos informáticos en una red?

a) Los dispositivos de IdC no pueden funcionar en una red aislada con una sola conexión a Internet.
b) La mayoría de los dispositivos de IdC no reciben actualizaciones de firmware frecuentes. *
c) Los dispositivos de IoC requieren conexiones inalámbricas sin encriptar.
d) La mayoría de los dispositivos de IoC no requieren una conexión a Internet y, por tanto, no pueden recibir actualizaciones nuevas.

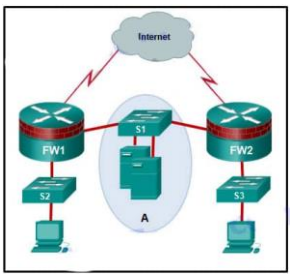
18) ¿Qué herramienta puede identificar el tráfico malicioso comparando el contenido del paquete con las firmas de ataque conocidas?

a) NetFlow
b) IDS *
c) Nmap
d) Zenmap

19) ¿Qué enunciado describe una política de seguridad típica para una configuración de firewall DMZ?

a) El tráfico que se origina en la red interna generalmente se bloquea por completo o se permite de manera muy selectiva a la red externa.
b) El tráfico que se origina en la red DMZ se permite de forma selectiva a la red exterior. *
c) El tráfico que se origina en la red exterior puede atravesar el cortafuegos hasta la red interna con pocas o ninguna restricción.
d) El tráfico de retorno desde la red interna que está asociado con el tráfico que se origina desde la red externa puede atravesar desde la red interna a la red externa.
e) El tráfico de retorno desde la red externa que está asociado con el tráfico que se origina desde la red interna puede atravesar desde la red externa hasta la interfaz DMZ.

20) Consulte la imagen:



La red «A» contiene varios servidores corporativos a los que los hosts acceden desde Internet para obtener información sobre la corporación. ¿Qué término se utiliza para describir la red marcada como «A»?

a) Red interna
b) Red no confiable
c) Límite de seguridad del perímetro
d) DMZ *

21) ¿Cuál es la desventaja de un mecanismo de detección basado en patrones?

a) Primero se debe perfilar el patrón de tráfico de red normal.
b) No puede detectar ataques desconocidos. *
c) Es difícil de implementar en una red grande.
d) Su configuración es compleja.

22) ¿Cuáles son dos desventajas de usar un IDS? (Escoge dos)

a) El IDS analiza los paquetes reenviados reales.
b) El IDS no detiene el tráfico malicioso. *
c) El IDS no tiene ningún impacto en el tráfico.
d) El IDS funciona sin conexión utilizando copias del tráfico de la red.
e) El IDS requiere otros dispositivos para responder a los ataques. *

23) ¿Cuáles son las dos características compartidas del IDS y el IPS? (Escoge dos)

a) Ambos usan firmas para detectar tráfico malicioso. *
b) Ambos analizan copias del tráfico de la red.
c) Ambos tienen un impacto mínimo en el rendimiento de la red.
d) Ambos dependen de un dispositivo de red adicional para responder al tráfico malicioso.
e) Ambos se implementan como sensores. *

24) ¿Cuáles son las tres mejores prácticas que pueden ayudar a defenderse de los ataques de ingeniería social? (Elija tres opciones).

a) Implementar dispositivos de firewall bien diseñados.
b) Habilitar una política que establezca que el departamento de TI deba proporcionar información telefónica solo a los gerentes.
c) Capacitar a los empleados sobre las políticas. *
d) Agregar más protecciones de seguridad.
e) Resista el impulso de hacer clic en enlaces de sitio web atractivos. *
f) No ofrecer restablecimientos de contraseña en una ventana de chat. *

25) ¿Mantener las copias de respaldo de datos externos es un ejemplo de qué tipo de control de recuperación tras un desastre?

a) Control organizativo
b) Control preventivo *
c) Control de detección
d) Control correctivo

26) ¿Qué tipo de redes presentan desafíos cada vez mayores para los especialistas en ciberseguridad debido al crecimiento de BYOD en el campus?

a) Red de transferencia
b) Redes cableadas
c) Redes inalámbricas *
d) Redes virtuales

27) ¿Qué utilidad de Windows debe utilizarse para configurar las reglas de contraseña y las políticas de bloqueo de cuenta en un sistema que es parte de un dominio?

a) Administración de equipos
b) Herramienta de seguridad de Active Directory *
c) Registro de seguridad del visor de eventos
d) Herramienta de política de seguridad local

28) ¿Qué amenaza se mitiga mediante la capacitación de conocimiento del usuario y la vinculación del conocimiento de seguridad con las revisiones de rendimiento?

a) Amenazas relacionadas con el usuario *
b) Amenazas físicas
c) Amenazas relacionadas con el dispositivo
d) Amenazas relacionadas la nube

29) ¿Qué enfoque en la disponibilidad proporciona la protección más integral porque las múltiples defensas se coordinan para prevenir ataques?

a) Limitación
b) Diversidad
c) Organización en capas *
d) Oscuridad

30) Una organización permite que los empleados trabajen desde su hogar dos días a la semana. ¿Qué tecnología debería implementarse para garantizar la confidencialidad de los datos mientras estos se transmiten?

a) SHS
b) VLANS
c) RAID
d) VPN *

31) ¿Qué protocolos presentan amenazas al switch? (Elija dos opciones).

a) IP
b) WPA2
c) STP *
d) RIP
e) ICMP
f) ARP *

32) ¿Qué métodos se pueden utilizar para implementar la autenticación de varios factores?

a) IDS e IPS
b) Token y hashes
c) Contraseñas y huellas digitales *
d) VPN y VLAN

33) ¿Cómo se denomina cuando una organización instala solamente las aplicaciones que cumplen con las pautas y los administradores aumentan la seguridad al eliminar las demás aplicaciones?

a) Estandarización de activos *
b) Disponibilidad de activos
c) Identificación de activos
d) Clasificación de activos

34) ¿Qué tecnología se puede utilizar para garantizar la confidencialidad de los datos?

a) Encriptación *
b) Raid
c) Administración de identidades
d) Hash

35) ¿Qué marco de trabajo se debe recomendar para establecer un sistema completo de administración de seguridad informática en una organización?

a) ISO/IEC 27000 *
b) Modelo de OSI ISO
c) Marco de trabajo de NIST/NICE
d) Tríada de CIA

36) ¿En qué dominios de ciberseguridad se incluyen los sistemas de agua y de incendio?

a) Red
b) Instalaciones físicas *
c) Dispositivo
d) Usuario

37) ¿Qué utilidad utiliza el Protocolo de mensajería de control de Internet?

a) DNS
b) NTP
c) Ping *
d) RIP

Curso: Seguridad informática
Expte.: 29/2020/LJ/0019
Evaluación:
Acción y grupo:
Módulo: MF0486_3

38) Los empleados de una empresa reciben un correo electrónico que indica que la contraseña de la cuenta caducará inmediatamente y requiere el restablecimiento de la contraseña en 5 minutos. ¿Qué declaración clasificaría este correo electrónico?

a) Es un ataque de suplantación de identidad.
b) Es un ataque de DDoS.
c) Es un ataque combinado.
d) Es un correo electrónico engañoso. *

39) Se le solicita asesoramiento a un especialista en seguridad sobre una medida de seguridad para evitar que hosts no autorizados accedan a la red doméstica de los empleados. ¿Qué medida sería la más eficaz?

a) Implementar una RAID.
b) Implementar un VLAN.
c) Implementar sistemas de detección de intrusiones.
d) Implementar un firewall. *

40) ¿Cuáles son los dos métodos más eficaces para defenderse del malware? (Elija dos opciones).

a) Implementar firewalls de red.
b) Actualizar el sistema operativo y otro software de la aplicación. *
c) Implementar una RAID.
d) Implementar una VPN.
e) Implementar contraseñas seguras.
f) Instalar y actualizar el software antivirus. *

Firma del alumno:
(obligatorio)