
Solucionario de

ejercicios de autoevaluación

Ejercicios de autoevaluación

Unidad de Aprendizaje 1

1. ¿Dónde se encuentran las principales debilidades en un sistema informático?

- a. *Hardware* y *software*.
- b. *Hardware*, *software* y datos.
- c. *Hardware*, *software*, datos, memoria y usuarios.**
- d. *Hardware*, *software*, datos, memoria y red.

2. ¿Qué grupo es el más peligroso cuando hablamos de ataques informáticos en la red?

- a. *Hackers*
- b. *Lamers*
- c. *Newbie*
- d. Creadores de virus**

3. ¿Qué sector registra el mayor número de ataques globales?

- a. Industria militar
- b. Vendedores de *hardware*
- c. Educación**
- d. Consultores

4. Señala las opciones correctas.

- a. *Scanning* se trata de obtener información en la primera fase del ataque.
- b. Una forma de hacer *phishing* puede ser enviar correos electrónicos a la víctima para persuadirla de alguna forma.**
- c. El *phishing* es una técnica de ingeniería social.
- d. El *sniffing* es lo mismo que *phishing*, pero utilizando la interacción directa con la víctima.

5. Un *rootkit* es...

- a. ... un dispositivo electrónico.
- b. ... un *exploit*.
- c. ... un programa informático que busca obtener privilegios de *root* en el sistema donde se ejecuta.**
- d. ... un programa informático que busca bloquear el acceso *root* a todo el que intenta acceder de forma externa.

6. ¿Cuáles son las categorías de *exploit*?

- a. *Exploits* sobre internet y sobre LAN.
- b. *Exploits* conocidos y no conocidos.
- c. *Exploits* activos y pasivos.
- d. *Exploits* sobre internet, sobre LAN, locales y fuera de línea.**

7. La fase de explotación de vulnerabilidades en un ataque informático consiste en...

- a. ... buscar vulnerabilidades en el sistema.
- b. ... la búsqueda de información de la víctima.
- c. ... realizar el ataque, utilizando la vulnerabilidad escogida.**
- d. ... eliminar el rastro del ataque.

8. ¿Cuál de las siguientes causas pueden originar una vulnerabilidad en un sistema?

- a. Errores de programación.**
- b. Instalación de un troyano.**
- c. Conectar un disco duro nuevo en el sistema sin apagarlo.
- d. La desconexión del sistema de la red.

9. ¿Para qué sirve la herramienta *nmap*?

- a. Se suele utilizar para control remoto de un sistema.
- b. Se suele utilizar para configurar la red de un sistema.
- c. Se suele utilizar para ganar el acceso de un sistema.
- d. Se suele utilizar para obtener las máquinas que componen una red.**

10. La seguridad informática se preocupa de...

- a. ... proteger la red.
- b. ... proteger la información de los sistemas.
- c. ... proteger los documentos impresos de la entidad.
- d. Las opciones a y b son correctas.**

Ejercicios de autoevaluación

Unidad de Aprendizaje 2

1. ¿Cuáles son los principios que rigen la seguridad de la información?

- a. Disponibilidad, integridad, confidenciabilidad, autentico y repudio.
- b. Disponibilidad, confidenciabilidad, autentico y repudio.
- c. Disponibilidad, integridad, confidenciabilidad, autenticación y no repudio.**
- d. Integridad, confidenciabilidad, autenticación y no repudio.

2. ¿Cuánto creció la inversión en ciberseguridad en 2023?

- a. Menos del 10 %
- b. Un 20 %
- c. Más del 50 %
- d. Entre el 10 y el 15 %**

3. ¿En qué etapas se divide el análisis y clasificación de la información?

- a. Identificar el flujo de la información y analizar sus transformaciones.
- b. Identificar y clasificar el tipo de dato, y analizar el flujo que sigue.**
- c. Clasificar el riesgo y analizar el flujo que sigue.
- d. Clasificar los permisos de la información.

4. Determina si la siguiente oración es verdadera o falsa: "El riesgo no se define en función de la magnitud del daño de una amenaza".

- Verdadero
- **Falso**

5. La política de seguridad es...

- a. ... incompatible con algunos modelos de negocio.
- b. ... un conjunto de instrucciones que son elaboradas con el fin de actuar sobre un aspecto particular para minimizar el riesgo de amenaza.**
- c. ... un conjunto de planes.
- d. ... un conjunto de mecanismos para optimizar el modelo de negocio.

6. La política de seguridad se compone de:

- a. Planes, procedimientos, tareas, registros.**
- b. Planes y procesos.
- c. Procesos y registros.
- d. Planes, procedimientos, tareas, registros, acciones.

7. Una política define _____ y un procedimiento define _____ .

- a. el qué/el cómo**
- b. el qué/el cuándo
- c. algo/nada
- d. acciones/procesos

8. Determina si la siguiente oración es verdadera o falsa: "Una política de seguridad correcta debe estar adaptada solo a la organización".

- Verdadero
- Falso

9. ¿Para qué sirve un plan de contingencia?

- a. Sirve para conocer mejor los tipos de amenazas a los que nos enfrentamos.
- b. Sirve para clasificar la información.
- c. Sirve para prevenir amenazas a los sistemas de información.
- d. Sirve para concretar la secuencia de acciones que hay que llevar a cabo si se produce un ataque informático.**

10. Determina si la siguiente oración es verdadera o falsa: "Cuando se define una política de seguridad, el alcance especifica todos los recursos, instalaciones y procesos sobre los que se aplica dicha política de seguridad".

- Verdadero
- Falso

Ejercicios de autoevaluación

Unidad de Aprendizaje 3

1. ¿Qué es la criptografía?

- a. Es un conjunto de técnicas para clasificar la información.
- b. Es un conjunto de técnicas que se utilizan para el cifrado o codificado de la información.**
- c. Es sinónimo de encriptación.
- d. Es un conjunto de técnicas para ocultar cierta información.

2. En un algoritmo simétrico...

- a. ... existe una sola clave con la que se cifra y descifra la información.**
- b. ... existen dos claves, una para cifrar y otra para descifrar la información.
- c. ... no existen claves, solo se utiliza un algoritmo para cifrar.
- d. Todas las opciones son incorrectas.

3. Determina si la siguiente oración es verdadera o falsa: "La encriptación asimétrica puede ser rota fácilmente mediante ataque por fuerza bruta".

- Verdadero
- Falso**

4. Determina si la siguiente oración es verdadera o falsa: "La encriptación asimétrica se basa en seleccionar dos números primos y factorización".

- Verdadero**
- Falso

5. El principal inconveniente de la encriptación asimétrica es...

- a. ... la lentitud.**
- b. ... la rapidez.

- c. ... el peso del algoritmo.
- d. ... que hay muchas formas de evitarla.

6. Determina si la siguiente oración es verdadera o falsa: “En la actualidad se suele mezclar las dos técnicas de encriptación: simétrica y asimétrica conjuntamente”.

- Verdadero
- Falso

7. ¿Qué es el *hash*?

- a. **Es un algoritmo matemático para transformar y resumir información.**
- b. Es un algoritmo matemático para crear información.
- c. Es una técnica de cifrado.
- d. Es una técnica de descifrado.

8. Determina si la siguiente oración es verdadera o falsa: “La firma digital no es un mecanismo que proporcione autenticación”.

- Falso
- Verdadero

9. El certificado digital es un mecanismo por el cual...

- a. ... la firma digital queda obsoleta.
- b. ... podemos transformar la información para transmitirla más eficientemente.
- c. ... podemos solicitar nuestros datos a las empresas públicas.
- d. **... podemos realizar transacciones administrativas de forma rápida y sin esfuerzo.**

10. Determina si la siguiente oración es verdadera o falsa: “SSL/TLS es un protocolo de transporte cuyo objetivo es proveer al informático de herramientas para programar protocolos con seguridad”.

- Verdadero
- Falso

Ejercicios de autoevaluación

Unidad de Aprendizaje 4

1. ¿Cuáles son los tres elementos presentes siempre en un proceso de autenticación?

- a. Elementos primarios, secundarios y terciarios.
- b. Elementos activos, pasivos y retroactivos.
- c. Elementos activos, pasivos y procesos.**
- d. Cliente, servidor y clave.

2. ¿Cuál de estas definiciones corresponde al concepto de autenticación?

- a. Acción para certificar que el usuario es quien dice ser.**
- b. Acción por la cual el usuario o entidad se da a conocer en el sistema.
- c. Acción que consiste en dar acceso a una serie de recursos a un usuario o sistema (para ello, el usuario o el sistema previamente tendrán que haberse autenticado).
- d. Acción por la cual el usuario o entidad no se da a conocer en el sistema.

3. ¿A qué sistemas de identificación corresponde el uso de tarjeta inteligente y código PIN?

- a. A los sistemas de autenticación de 1 factor.
- b. A los sistemas de autenticación de 2 factores.**
- c. A los sistemas de autenticación de 3 factores.
- d. A ninguno de los anteriores.

4. Determina si la siguiente oración es verdadera o falsa: "Los protocolos PAP y CHAP permiten la autenticación entre sistemas".

- Verdadero
- Falso

5. RADIUS es un protocolo que permite realizar las siguientes acciones:

- a. Autenticación, autorización y contabilización.
- b. Autenticación y autorización.
- c. Autenticación.
- d. Autenticación e identificación.

6. Determina si la siguiente oración es verdadera o falsa: "El proceso de contabilización en RADIUS comienza antes del proceso de autenticación".

- Verdadero
- Falso

7. En el protocolo 802.1x, el autenticador...

- a. ... envía un paquete "de solicitud/identidad EAP (Request/Identity)" para el suplicante tan pronto como detecta que el enlace está activo (por ejemplo, el sistema solicitante se ha asociado con el punto de acceso).
- b. ... envía un desafío al autenticador.
- c. ... proporciona identidad propia, el servidor de autenticación responde con un mensaje de éxito.
- d. ... envía un desafío al servidor.

8. Determina si la siguiente oración es verdadera o falsa: "En la familia de protocolos EAP, el cliente se identifica mediante un paquete de tipo *identify-response*".

- Verdadero
- Falso

9. ¿Cuáles de estos grupos son protocolos de la familia EAP?

- a. EAP-MD6, LEAP, EAP.
- b. EAP-MD5, LEAP, EAP-TLS, EAP-TTLS, EAP-PEAP.
- c. EAP-MD5, LEAP, CHAP, PAP.
- d. RADIUS, LEAP, CHAP.

10. Determina si la siguiente oración es verdadera o falsa: “Los sistemas biométricos están basados en identificar al usuario mediante una clave o palabra de paso”.

- Verdadero
- Falso

Ejercicios de autoevaluación

Unidad de Aprendizaje 5

1. En una VPN, la red privada se define sobre...

- a. ... una red compartida y pública.
- b. ... una red compartida.**
- c. ... una red compartida y privada.
- d. ... una red no compartida.

2. ¿A qué tipo de red es equivalente una VPN desde el punto de vista lógico?

- a. A una red LAN.**
- b. A una red WAN.
- c. A una red MAN.
- d. No tiene equivalencia.

3. ¿Qué protocolo VPN ha sido utilizado desde su origen?

- a. SMTP
- b. PPTP**
- c. OpenVPN
- d. L2TP

4. Determina si la siguiente oración es verdadera o falsa: "En OpenVPN no se puede utilizar autenticación por certificados".

- Verdadero
- Falso**

5. ¿Cuál es una ventaja del uso del protocolo SSTP?

- a. Puede convertir la conexión en una conexión anónima.**
- b. La VPN se reciente cuando la distancia es elevada.
- c. Las conexiones anónimas no se pueden conseguir.
- d. Permite que el ISP pueda filtrar nuestro tráfico.

6. Determina si la siguiente oración es verdadera o falsa: "IPSEC proporciona seguridad a la capa 2 (IP) y 3 (TCP) del modelo de comunicaciones TCP/IP".

- Verdadero
- Falso

7. IPSec está formado por tres protocolos fundamentales:

- a. AH, ESP e IKE.
- b. AH, ESP y KEI.
- c. AH, OpenVPN y ESP.
- d. GRE, ESP y KEI.

8. Determina si la siguiente oración es verdadera o falsa: "Las VPN con SSL/TLS realizan las conexiones en la capa de aplicación".

- Verdadero
- Falso

9. En una conexión VPN con SSL/TLS, ¿cuál es el orden de las acciones que ocurren?

- a. Comunicar credenciales, establecer el túnel y actualizar VPN.
- b. Establecer el túnel, comunicar credenciales y actualizar VPN.
- c. Actualizar VPN, establecer el túnel y comunicar credenciales.
- d. Establecer el túnel, actualizar VPN y comunicar credenciales.

10. Determina si la siguiente oración es verdadera o falsa: "Cuando instalamos OpenVPN necesitamos generar credenciales para cada usuario que vaya a utilizar la VPN".

- Verdadero
- Falso

Ejercicios de autoevaluación

Unidad de Aprendizaje 6

1. ¿Qué es un *firewall*?

- a. Una puerta de acceso a la red.
- b. Dispositivo *software* o *hardware* que se sitúa entre dos puntos de red para controlar y filtrar el tráfico.**
- c. Un dispositivo que revisa el tráfico de red y lo marca de alguna manera.
- d. Un elemento que no otorga ningún valor añadido a la red.

2. ¿Cuáles de estos dos conceptos son arquitecturas de *firewall*?

- a. *Single Homed Bastion/Dual Homed Bastion***
- b. *Single Bastion/Dual Homed*
- c. *Router/Router*
- d. *Router/Dual Homed*

3. ¿Cuáles son los dos tipos de filtrado que puede implementar un *firewall*?

- a. Filtrado estático/dinámico.
- b. Filtrado de paquetes sin estado/filtrado de paquetes con estado.**
- c. Filtrado proxy/Filtrado por servicio.
- d. Todas las opciones son incorrectas.

4. Determina si la siguiente oración es verdadera o falsa: "En un *firewall* con filtrado dinámico sin estado, el paquete atraviesa el *firewall* sin tener en cuenta el momento de la conexión ni el estado de dicha conexión".

- Verdadero
- Falso

5. ¿Qué función adicional implementa un servidor *proxy*?

- a. Una función de caché que le permite mejorar la velocidad de acceso a las páginas web ya descargadas.
- b. Una función de filtrado de paquetes que le permite mejorar la seguridad de la red.
- c. Una función de análisis de todo el tráfico de la red.
- d. Una función de alerta para la detección de intrusos en la red.

6. Determina si la siguiente oración es verdadera o falsa: “El tipo de *proxy* que realiza peticiones a servicios de internet solicitados por otros equipos o dispositivos es el *proxy* abierto”.

- Verdadero
- Falso

7. Una ventaja y un inconveniente del uso de *proxy* es:

- a. Ahorro del trabajo/incoherencia por culpa del sistema de caché.
- b. Ahorro del trabajo/el *proxy* resuelve las peticiones.
- c. Velocidad de respuesta/baja carga si se conectan muchos equipos.
- d. Incoherencia por culpa del sistema de caché/sistemas no preparados para representar a más de un usuario.

8. Determina si la siguiente oración es verdadera o falsa: “El filtrado dinámico en un *firewall* se implementa en las capas inferiores del modelo OSI de comunicaciones”.

- Verdadero
- Falso

9. Indica cuál de estos servicios no es un servicio implementado en un *firewall* de nueva generación:

- a. Comunicar credenciales, establecer el túnel, actualizar VPN.
- b. Gestión del tráfico desconocido.

- c. Identificación y control de la evasión de seguridad.
- d. Detección de intrusiones.

10. Determina si la siguiente oración es verdadera o falsa: "El funcionamiento de un *firewall* con estado se basa en los estados por los que pasa una conexión TCP en la comunicación".

- Verdadero
- Falso

Ejercicios de autoevaluación

Unidad de Aprendizaje 7

1. ¿Qué significan las siglas IDS e IPS?

- a. *Internet Digital Software* y *Internet Prevent Software*.
- b. Sistema de detección de intrusos y sistema de prevención de intrusiones.**
- c. Sistema de control de intrusos y sistema de anulación de intrusiones.
- d. Todas las opciones son incorrectas.

2. ¿Cuáles son las principales funciones de un IDS?

- a. Monitorizar/Detectar/Alertar/Analizar.**
- b. Monitorizar/Detectar.
- c. Alertar/Analizar.
- d. Filtrar/Detectar/Alertar.

3. ¿A qué clasificación corresponde el tipo de IDS basado en NIDS?

- a. Clasificación por tipo de análisis.
- b. Clasificación por fuente de información.**
- c. Clasificación por estructura.
- d. Clasificación por comportamiento.

4. Determina si la siguiente oración es verdadera o falsa: "Las arquitecturas IDS basadas en HIDS examinan las acciones de cada *host* en el que residen".

- Verdadero
- Falso

5. ¿Cuál es la diferencia más importante entre un IDS y un IPS?

- a. Un IPS es capaz de bloquear paquetes del atacante modificando su contenido, un IDS no.**
- b. Un IPS no es capaz de bloquear paquetes, un IDS sí.

- c. El IDS detecta y el IPS solo previene.
- d. Un IDS puede convertirse en un IPS si se configura en modo más activo.

6. Determina si la siguiente oración es verdadera o falsa: “Snort es una herramienta IDS muy utilizada para arquitecturas NIDS”.

- Verdadero
- Falso

7. Una ventaja que posee *suricata* respecto a *snort* es que...

- a. ... *suricata* posee soporte multihilo.
- b. ... *suricata* no posee aceleración por *hardware*.
- c. ... no posee tantos paquetes.
- d. ... no extrae ficheros.

8. Determina si la siguiente oración es verdadera o falsa: “OSSEC utiliza el modelo cliente-servidor para gestionar la información que es necesario sincronizar entre los *hosts* y el servidor IDS”.

- Verdadero
- Falso

9. Si tuvieras que elegir una palabra para describir un *honeypot*, ¿cuál de estas usarías?

- a. Tarro de miel
- b. Filtro
- c. **Señuelo**
- d. *Software*

10. Los tipos de *honeypots* que se basan en el despliegue son:

- a. **Físicos/virtuales**
- b. Baja/media/alta interacción
- c. Lógicos/físicos
- d. Lógicos/virtuales