Solucionario de

ejercicios de autoevaluación

Ejercicios de autoevaluación
Unidad de Aprendizaje 1

1. Indica si las siguientes afirmaciones son verdaderas o falsas.

a. Las actividades que están orientadas a comprometer la seguridad informática, la seguridad de las redes y la de los dispositivos inteligentes se denominan *hackeos*.

- **Verdadero**
- Falso

b. Un *hacker* es siempre un delincuente cibernético.

- Verdadero
- **Falso**

c. Un *cracker* es un *hacker* ético.

- Verdadero
- **Falso**

2. ¿Qué significado tiene el lexema *hack-*?

a. Dañar.
b. Dar un hachazo.
c. Romper.
d. Todas las opciones son correctas.

3. El concepto *hacker* nació de la mano de un grupo de programadores del Instituto Tecnológico de Massachusetts (MIT). ¿En qué década comenzaron a emplear este término?

a. Años setenta.
b. Años sesenta.
c. Años cincuenta.
d. Años cuarenta.

4. ¿Con qué nombre se reconoce el lado oscuro de internet?

a. *Dark red.*
b. *Dark hack.*
c. *Dark Internet.*
d. *Dark web.*

5. ¿Qué tipo de *hacker* es el que lleva a cabo tareas sin infringir la ley?

a. *Black Hat.*
b. *Grey Hat.*
c. *White Hat.*
d. *Green Hat.*

6. ¿Qué tipo de *hacker* son los *crackers?*

a. *Hackers* de sombrero blanco.
b. *Hackers* de sombrero gris.
c. *Hackers* de sombrero negro.
d. *Hackers* de sombrero verde.

7. ¿Qué nombre recibe el colectivo de *hackers* cuyas acciones están motivadas por la reivindicación social o política?

a. *Lamers*
b. *Newbies*
c. Hacktivistas
d. *Phereakers*

8. ¿Qué nombre recibió el evento tecnológico que impulsó el acceso libre a la información base de la ética *hacker?*

a. Proyecto MIT.
b. Proyecto GNU.
c. Proyecto Linux.
d. Proyecto Apple.

9. ¿Qué sistema operativo es considerado como el sistema operativo de los *hackers*?

a. *macOS*
b. *Windows*
c. *Linux*
d. *Android*

10. ¿Con qué apodo se conoce al mítico *hacker* Kevin Mitnick?

a. Águila
b. Buitre
c. Cóndor
d. Avestruz

Ejercicios de autoevaluación Unidad de Aprendizaje 2

1. Indica si las siguientes afirmaciones son verdaderas o falsas.

a. De la imperiosa necesidad por localizar y prevenir fallos de seguridad en los entornos o sistemas de información de las organizaciones nacen las técnicas de *hacking* ético o *Pentesting.*

- **Verdadero**
- Falso

b. Un *Pentester* es un delincuente cibernético.

- Verdadero
- **Falso**

c. *Pentesting* significa test de penetración.

- **Verdadero**
- Falso

2. ¿Cuántos tipos de *Pentesting* existen?

a. Cinco
b. Cuatro
c. Tres
d. Dos

3. ¿Qué nombre recibe el tipo de *Pentesting* que desconoce cualquier información sobre el sistema de información que va a poner a prueba?

a. *Grey Box.*
b. *White Box.*
c. *Black Box.*
d. *Green Box.*

4. ¿Cuál de los tipos de test de penetración se acerca más a la manera de actuar de un delincuente cibernético?

a. *Green Box.*
b. *Grey Box.*
c. *White Box.*
d. *Black Box.*

5. ¿En qué fase del *Pentesting* se implementan medidas correctivas con idea de solucionar fallos de seguridad en los sistemas de información?

a. En las primeras fases donde se comienza a valorar el sistema.
b. En fases intermedias donde se han detectado ya algunas vulnerabilidades.
c. En la fase final tras elaborar el informe de la auditoría de ciberseguridad.
d. Nunca. Entre las funciones del *Pentester* no está la de implementar medidas correctivas.

6. ¿Qué nombre recibe el principio de protección de la seguridad de la información que persigue proteger la información tal como fue generada para evitar que sea modificada, alterada o manipulada por sujetos no autorizados?

a. Disponibilidad
b. Integridad
c. Confidencialidad
d. Exclusividad

7. ¿Qué nombre recibe la debilidad de un sistema de información de una organización y que lo hace susceptible de ataques?

a. Impacto
b. Riesgo
c. Amenaza
d. Vulnerabilidad

8. ¿Cómo se define la probabilidad de que se presente una incidencia de seguridad que termine con la confirmación de una amenaza y, por consiguiente, en pérdidas en la organización fruto de daños al sistema de información?

a. Nivel de riesgo.
b. Riesgo.
c. Impacto.
d. Coste de protección.

9. ¿Qué es el coste de protección?

a. El umbral de protección que tiene asumido la empresa.
b. El mantenimiento del riesgo por debajo del umbral elegido como riesgo asumible por la empresa.
c. El esfuerzo económico que supone el empleo de recursos y de la dedicación en tiempo, que implica mantener un nivel de riesgo adecuado.
d. Todas las opciones son incorrectas.

10. ¿Cuál es el objetivo principal de la gestión de riesgos?

a. La protección de la actividad logística de la empresa.
b. La protección de los sistemas informáticos de la empresa.
c. La protección de los activos de la información de la empresa.
d. La protección de los activos materiales de la empresa.

Ejercicios de autoevaluación Unidad de Aprendizaje 3

1. Indica si las siguientes afirmaciones son verdaderas o falsas.

a. El interesante mundo de la seguridad cibernética gira en torno al estudio y gestión de vulnerabilidades para su control.

- **Verdadero**
- Falso

b. MITRE, al igual que otras organizaciones, está enfocada en investigar los problemas de seguridad informática.

- **Verdadero**
- Falso

c. En *Common Vulnerabilities and Exposures,* solo se registran vulnerabilidades informadas por organizaciones americanas.

- Verdadero
- **Falso**

2. Las informaciones de las vulnerabilidades recogidas en la lista CVE son:

a. Privadas.
b. De acceso restringido.
c. Públicas.
d. Públicas mediante registro.

3. ¿Cuál de las siguientes nomenclaturas de códigos representaría un código de reserva CVE?

a. *CRV-YYYY-NNNN.*
b. *CAN-YYYY-NNNN.*
c. *CVE-YYYY-NNNN.*
d. *CNA-YYYY-NNNN.*

4. ¿Qué nombre recibe el sistema que permite valorar de forma objetiva las vulnerabilidades detectadas en un sistema de información, utilizando una metodología de estandarización?

a. *Common Vulnerability Standard System.*
b. *Common Vulnerability Level System.*
c. *Common Vulnerability Puntuation System.*
d. *Common Vulnerability Scoring System.*

5. ¿Con qué idea nace CVSS?

a. Evitar los problemas de interpretación que implica la gravedad de una vulnerabilidad.
b. Valorar de forma objetiva las vulnerabilidades detectadas en un sistema de información.
c. Calificar las vulnerabilidades y determinar el nivel de peligrosidad mediante una puntuación.
d. Todas las opciones son correctas.

6. ¿Qué nombre recibe el foro de equipos de seguridad y respuesta a emergencias de internet, con reconocimiento internacional, que da respuestas eficaces tanto a incidencias de seguridad ya acontecidas como a otras de carácter preventivo?

a. FESR
b. FIRST
c. FREIR
d. FERTS

7. ¿Cuál de los siguientes grupos de métricas CVSS proporciona la puntuación básica que representa la gravedad de la vulnerabilidad?

a. *Environmental Metric Group.*
b. *Temporal Metric Group.*
c. *Base Metric Group.*
d. *Confidencial Metric Group.*

8. ¿Qué factor se tiene en cuenta para definir las métricas base?

a. El impacto.
b. La explotabilidad.

c. El impacto y la explotabilidad.
d. Todas las opciones son incorrectas.

9. ¿Qué concepto expresa el nivel de complejidad que requiere el proceso de autenticación para llevar a cabo una intrusión o ataque valiéndose de la vulnerabilidad?

a. El impacto.
b. La explotabilidad.
c. La confidencialidad.
d. El intrusismo.

10. ¿A qué grupo de métricas pertenece la métrica *Integrity Impact*?

a. Al grupo de métricas base.
b. Al grupo de métricas temporales.
c. Al grupo de métricas ambientales
d. Al grupo de métricas de entorno.

Ejercicios de autoevaluación Unidad de Aprendizaje 4

1. Indica si las siguientes afirmaciones son verdaderas o falsas.

a. La maniobra planificada e intencionada para causar daño a un sistema de información aprovechando alguna vulnerabilidad del sistema para derivar en alguna consecuencia y obtener algún tipo de beneficio por ello recibe el nombre de ataque cibernético.

- **Verdadero**
- Falso

b. Los ataques cibernéticos pueden dirigirse remotamente y tienen una misión que cumplir, pero para llevarlos a cabo no es necesario utilizar ningún método de ataque.

- Verdadero
- **Falso**

c. Las técnicas específicas de ataques cibernéticos forman parte de un método delictivo planificado.

- **Verdadero**
- Falso

2. ¿Qué nombre recibe el robo de información confidencial de alto valor en los mercados mediante ataques cibernéticos?

a. *Hacktivismo.*
b. Ciberespionaje político.
c. Ciberespionaje industrial.
d. Ciberespionaje militar.

3. ¿Qué clasificación de ataque cibernético implica intrusiones que tienen por objetivo atacar al eslabón más débil?

a. Ciberataques a redes.
b. Ciberataques a entornos móviles.
c. Ciberataques de ingeniería social.
d. Ciberataques a webs.

4. ¿Qué nombre recibe la fase del ciclo de vida de un ataque en la que, tras recopilar datos, el ciberatacante examina toda la información con idea de localizar algún agujero de seguridad?

a. Mantenimiento de acceso.
b. Reconocimiento.
c. Acceso.
d. Escaneo.

5. En el ámbito de la ciberseguridad, ¿con qué nombre se reconoce a la acción delictiva "secuestros de sesión"?

a. Ataques DDos.
b. *Hijacking.*
c. Ataques de fuerza bruta.
d. Ingeniería social.

6. ¿Con qué nombre se conocen las técnicas de *hacking* que se utilizan para llevar a cabo engaños a usuarios con idea de poder infectar sus sistemas de información por medio de archivos maliciosos?

a. *Sniffing.*
b. Ingeniería social.
c. Ataques DDos.
d. Todas las opciones son incorrectas.

7. ¿A qué se llama *rootkits*?

a. A técnicas de ocultamiento.
b. A la denegación de servicio.
c. A un tipo de ataque de fuerza bruta.
d. A la técnica *hacking* para capturar información que viaja por la red.

8. A tenor del modelo de análisis de intrusión *Cyber Kill Chain,* ¿de cuántas fases se compone este método?

a. Cinco
b. Seis
c. Siete
d. Ocho

9. ¿Qué es un *Endpoint?*

a. Estrategia de defensa.
b. Punto de ataque final.
c. Ataque avanzado.
d. Estrategia de ataque.

10. Desde el campo de la ciberseguridad, ¿para qué sirven las pruebas forenses?

a. Para detectar ciberataques en fases tempranas.
b. Para analizar y determinar las causas que originaron el ciberataque.
c. Para determinar el proceso por el que avanzó un ciberataque por todas las fases.
d. Todas las opciones son incorrectas.

Ejercicios de autoevaluación Unidad de Aprendizaje 5

1. Indica si las siguientes afirmaciones son verdaderas o falsas.

a. El concepto *malware* viene a definir lo que vulgarmente se conoce como *software* malicioso.

- **Verdadero**
- Falso

b. Podemos afirmar que un *malware* es el instrumento principal que utilizan los *crackers* para perpetrar su misión delictiva.

- **Verdadero**
- Falso

c. Un *malware* es un subtipo de virus informático.

- Verdadero
- **Falso**

2. ¿Qué es un troyano?

a. Un tipo de virus informático.
b. Un programa malicioso.
c. Un *malware.*
d. Todas las opciones son correctas.

3. ¿Qué tipo de *malware* es capaz de realizar copias de sí mismo?

a. Troyano.
b. Gusano.
c. *Spyware.*
d. *Ransomwared.*

4. ¿Qué nombre recibe el mecanismo incluido dentro de un *software* malicioso que es capaz de detectar, registrar e informar a cibercriminales de las pulsaciones que realiza un usuario en el teclado de su equipo informático?

a. *Botnet.*
b. *Adware.*
c. *Phising.*
d. *Keylogger.*

5. ¿Qué característica define a un *malware* tipo *spyware*?

a. Tiene la capacidad de pasar totalmente inadvertido por la víctima mientras se apodera de datos relevantes para informar a su ejecutor.
b. Tiene la capacidad de contagiar a todos los equipos conectados a la misma red de internet.
c. Tiene la capacidad de convertir toda la infraestructura informática en una red de equipos zombis.
d. Todas las opciones son incorrectas.

6. ¿Cuál de los siguientes conceptos define la actividad *hackeniana* que se apodera de información a modo de *malware* para ejecutar un ataque?

a. RAT.
b. *Exploits.*
c. Apps maliciosas.
d. *Conan mobile.*

7. *Trojan-clicker* es un tipo de...

a. *... spyware.*
b. *... adware.*
c. *... ransomware.*
d. ... troyano.

8. Según la organización SOPHOS, en el año 2020 el 53 % de las empresas sufrieron un ataque de...

a. ... un troyano.
b. ... un gusano.
c. ... un *ransomware.*
d. ... un *cryptojacking*.

9. ¿Qué tipo de problema resuelve el *malware* llamado *cryptojacking*?

a. Bloqueos antivirus.
b. De encriptación.
c. De ataques remotos.
d. Todas las opciones son incorrectas.

10. ¿Con qué nombre se identifica la capacidad de ocultación de un *malware* con idea de evitar que sea descubierto el código malicioso bajo un programa aparentemente inocuo?

a. Perdurabilidad
b. Ofuscación
c. Transparencia
d. *Backdoord*

Ejercicios de autoevaluación Unidad de Aprendizaje 6

1. Indica si las siguientes afirmaciones son verdaderas o falsas.

a. La transformación digital de los negocios está requiriendo de mecanismos ágiles para desarrollar todos y cada uno de los procesos productivos con resolución y apremio.

- **Verdadero**
- Falso

b. La ciberseguridad juega un papel clave dentro de las infraestructuras de las tecnologías de la información.

- **Verdadero**
- Falso

c. La red LAN ofrece disponibilidad de comunicaciones desde cualquier lugar fuera del espacio físico de la empresa con una red territorial amplia.

- Verdadero
- **Falso**

2. ¿Qué nombre recibe el conjunto de equipos informáticos conectados entre sí que pueden comunicarse utilizando distintas mecánicas de conexión (cables, señales, ondas, etc.) para compartir servicios, recursos e información?

a. *Cowork*
b. *Coworking*
c. *Networking*
d. *Network*

3. Para ayudar a definir una nueva estructura de red de comunicaciones entre ordenadores de red o estructura de redes como sistema computacional con funcionalidades diversas, ¿qué lenguaje universal de comunicación se utiliza?

a. Modelo ISO.
b. Modelo OSI.

c. Modelo IAF.
d. Modelo AIF.

4. ¿Qué mecanismo de seguridad red no es muy utilizado hoy en día por ser fácilmente vulnerable?

a. WPA2.
b. WPA.
c. WEP.
d. WEP2.

5. ¿Qué funcionalidad tiene la interfaz de capa?

a. La interfaz de capa agrupa las reglas de intercomunicación entre niveles o capas.
b. La interfaz de capa agrupa las reglas de intercomunicación entre componentes de una misma capa.
c. La interfaz de capa agrupa las reglas de intercomunicación de todos los niveles o capas.
d. Todas las opciones son incorrectas.

6. ¿Con qué concepto se reconoce la manera de definir cómo queda organizado el cableado que representa la interconexión entre las distintas estaciones y el trayecto de transferencia de datos en el canal de comunicación?

a. Método de acceso a la red.
b. Topología.
c. Protocolo de comunicación.
d. Protocolo de transporte.

7. ¿Con qué nombre se reconoce cada máquina conectada a la red SNA?

a. *Hosts.*
b. Procesadores frontales.
c. Terminales.
d. Nodo.

8. ¿Con qué iniciales se reconoce el protocolo de internet?

a. IP
b. IPX
c. TCP
d. TCPX

9. ¿Cuál de los siguientes protocolos se encuentra en la capa de interfaz de red en el modelo TCP/IP?

a. FTP
b. SMTP
c. IP
d. Ethernet

10. ¿Cómo se llaman las redes que tienen como objetivo proporcionar un servicio integrado en el que convergen redes de datos, de voz y vídeo, utilizando un tipo de tecnología basada en paquetes para todo tipo de información?

a. *Network.*
b. *Next Generation Networking.*
c. *Network Applications.*
d. Todas las opciones son incorrectas.

Ejercicios de autoevaluación Unidad de Aprendizaje 7

1. Indica si las siguientes afirmaciones son verdaderas o falsas.

a. La tecnología inalámbrica está basada en la conexión a internet sin necesidad de la utilización de cableado.

- **Verdadero**
- Falso

b. Hace más de dos décadas que se consolidaron las redes wifi.

- **Verdadero**
- Falso

c. El *router* es el equipo de red que asigna la dirección IP a cada dispositivo conectado a la red.

- **Verdadero**
- Falso

2. ¿De cuántos puertos dispone un módem?

a. Uno
b. Dos
c. Tres
d. Cuatro

3. ¿Qué son los puertos del *router*?

a. Son protocolos de seguridad que cifran los mensajes transmitidos y recibidos en redes inalámbricas.
b. Son paquetes de información que viaja de un lado a otro de las redes wifi.
c. Son compuertas que se abren y cierran para dejar pasar información de una red a otra.
d. Todas las opciones son incorrectas.

4. ¿De qué se vale el *router* para enviar los datos a los servidores de las páginas web a las que se quiere acceder?

a. De los canales.
b. De las puertas.
c. De los puertos.
d. Los términos canal, puerta y puerto hacen referencia al mismo concepto.

5. Los puertos del *router* son un área vulnerable objeto de ataque. ¿Cuántos puertos posee un *router*?

a. 65.536
b. 6.553
c. 655
d. 65

6. ¿Para qué quedan reservados los primeros 1.023 puertos de un *router?*

a. Para el sistema operativo del equipo informático y para los juegos y aplicaciones que se instalan en los equipos.
b. Para el sistema operativo del equipo informático y para los protocolos encargados de que todo funcione correctamente.
c. Para aquellas aplicaciones que requieren conexión a un servidor para descarga de programas como, por ejemplo, programas como *eMule, P2P o Torrent.*
d. Un *router* no dispone de 1.023 puertos.

7. ¿Qué necesidad cubrieron los protocolos de comunicación WEP, WPA, WPA2 y WPS?

a. Proveer de tecnología innovadora a las comunicaciones *Wireless.*
b. Proveer de un lenguaje estandarizado que permitiera a las máquinas entenderse.
c. Proveer de seguridad a los usuarios que se conectan a las redes.
d. La naturaleza de los protocolos WEP, WPA, WPA2 y WPS es puramente técnica.

8. ¿Cuál de las siguientes herramientas no es un *software* orientado a realizar auditorías wifi?

a. *Netstumbler.*
b. SSID.
c. *WiFi Collector.*
d. *Aircrack-ng*.

9. ¿Qué mecanismo de seguridad aporta el protocolo WPA?

a. Se alarga la longitud del VI (vector de inicialización).
b. Se incorporan medidas para proteger las temidas inyecciones de tráfico en la red inalámbrica.
c. Se adopta un nuevo protocolo denominado TKIP.
d. Todas las opciones son correctas.

10. ¿Qué nuevo protocolo de seguridad se desarrolló por la *Wi-Fi Alliance* en el año 2007?

a. *WiFi Protected Setup.*
b. *Near Field Communication.*
c. WPA3.
d. WPA6.

Ejercicios de autoevaluación Unidad de Aprendizaje 8

1. Indica si las siguientes afirmaciones son verdaderas o falsas.

a. El *hacking* ético es una disciplina que evalúa la seguridad de los sistemas de información de las organizaciones.

- **Verdadero**
- Falso

b. Un *hacker* ético utiliza una plataforma de entrenamiento virtual para monitorizar los ciberataques en tiempo real.

- Verdadero
- **Falso**

c. Una plataforma de entrenamiento virtual es una máquina virtual.

- Verdadero
- **Falso**

2. ¿Qué nombre recibe la herramienta que se vale de un *software* que tiene la capacidad de emular un sistema operativo insertado dentro de otro pero emancipado de él?

a. *VirtualBox*.
b. Máquina virtual.
c. Laboratorio de entrenamiento.
d. Plataforma de entrenamiento.

3. ¿De qué se nutre la máquina virtual para funcionar?

a. De un *software*.
b. De un *hardware* anfitrión.
c. De un *software* y un *hardware* anfitrión.
d. Todas las opciones son incorrectas.

4. ¿A qué se llama equipo anfitrión?

a. A la primera máquina virtual creada en la plataforma.
b. Al ordenador que suministra los recursos físicos a la máquina virtual invitada.
c. A todas las máquinas virtuales creadas en la plataforma.
d. A la máquina virtual creada con el sistema operativo que más memoria RAM requiere.

5. ¿Qué nombre recibe la máquina que se considera una aplicación capaz de generar un entorno de ejecución de un proceso determinado?

a. Máquina de sistemas.
b. Máquina de programa.
c. Máquina de aplicación.
d. Máquina de procesos.

6. ¿Para qué sirven las máquinas virtuales?

a. Para experimentar con distintos sistemas operativos en un mismo equipo.
b. Para experimentar con diferentes configuraciones de sistema.
c. Para ejecutar algún viejo *software* incompatible con el S. O. actual.
d. Todas las opciones son correctas.

7. ¿Qué nombre recibe el más conocido *software* de creación y gestión de máquinas virtuales desarrollado por Oracle?

a. *Xen*
b. *VMWare*
c. *VirtualBox*
d. *Hyper-V*

8. ¿Cuántas máquinas virtuales se pueden crear dentro de una plataforma de entrenamiento?

a. Una
b. Dos

c. Tres
d. Tantas como quieras.

9. ¿Es posible arrancar todas las máquinas virtuales creadas dentro de una misma plataforma de entrenamiento?

a. Solo es posible iniciar dos máquinas a la misma vez.
b. Se pueden arrancar todas las máquinas a la vez.
c. Solo es posible arrancar tres máquinas a la vez.
d. Es posible arrancar tantas máquinas como admitan los recursos proporcionados por el equipo anfitrión.

10. Una vez creada la máquina virtual, ¿qué se necesita para instalar el sistema operativo *Kali Linux?*

a. *VirtualBox.*
b. *Imagen ISO de Kali Linux.*
c. El sistema operativo del equipo anfitrión.
d. Todas las opciones son incorrectas.

Ejercicios de autoevaluación Unidad de Aprendizaje 9

1. Indica si las siguientes afirmaciones son verdaderas o falsas.

a. Gracias a los distintos protocolos de seguridad y las medidas básicas de protección, las redes inalámbricas pueden ser 100 % seguras.

- Verdadero
- **Falso**

b. La existencia de una vulnerabilidad en un protocolo de seguridad red significa que dicha vulnerabilidad es explotable.

- **Verdadero**
- Falso

c. Para realizar auditorías wifi es necesario disponer de una tarjeta extensora de red.

- **Verdadero**
- Falso

2. ¿Qué elemento permite saber que existen redes inalámbricas ocultas?

a. La presencia de *Beacom Frames.*
b. El filtrado de direcciones MAC.
c. El filtrado de direcciones IP.
d. No es posible saber si existen o no redes inalámbricas ocultas.

3. ¿Cuál de las siguientes opciones es una herramienta que sirve para escanear redes y capturar vectores de inicio?

a. *airmon-ng*
b. *aircrack-ng*
c. *airodump-ng*
d. *aireplay-ng*

4. ¿Qué nombre recibe la herramienta *suite* incorporada en las distribuciones de *Kali Linux* más utilizada en auditorías inalámbricas, que sirve para descifrar la clave de los vectores de inicio?

a. *aireplay-ng*
b. *aircrack-ng*
c. *airmon-ng*
d. Todas las opciones son incorrectas.

5. ¿Qué se pretende con la ejecución del código ifconfig en el sistema de comando?

a. Conocer el modelo del adaptador red para comprobar si acepta el modo monitoreo.
b. Conocer el modelo del adaptador red para comprobar si acepta el modo inyección de paquetes.
c. Conocer si el adaptador wifi está en modo monitoreo.
d. Conocer en qué modo está el adaptador de red.

6. ¿Qué nombre recibe el tipo de ataque que consigue desconectar todos los dispositivos clientes que están conectados a una red inalámbrica?

a. Ataque de fuerza bruta.
b. Ataque *DeAuth.*
c. Ataque *PixieDust.*
d. Todas las opciones son incorrectas.

7. ¿Qué nombre recibe el ataque orientado a capturar el intercambio de paquetes entre el punto de acceso de la víctima objeto del ataque y el punto de acceso del atacante?

a. Ataque de fuerza bruta.
b. Ataque *Reaver.*
c. Ataque *PixieDust.*
d. No existe ese tipo de ataques a redes.

8. ¿Qué nombre recibe el protocolo encargado de autenticar a los usuarios para que estos puedan acceder a recursos compartidos por la empresa?

a. RADEX
b. RADEUS
c. RADIUS
d. RADER

9. ¿Cuál de las siguientes opciones no es una medida básica de protección de redes inalámbricas?

a. Aumentar la potencia de emisión de las antenas.
b. Vigilar la configuración básica de la seguridad de las redes inalámbricas.
c. Implementar servidores de identificación.
d. Incorporar elementos de alerta de intrusos en la infraestructura de red.

10. ¿Cuál de las siguientes opciones sirve como recurso para alertar de intrusos en la infraestructura de red de una organización?

a. *Firmware*
b. *Firewall*
c. RADIUS
d. Antivirus

Ejercicios de autoevaluación Unidad de Aprendizaje 10

1. Indica si las siguientes afirmaciones son verdaderas o falsas.

a. Tanto los ataques activos como los ataques pasivos se caracterizan por técnicas específicas que representan cada una de ellas verdaderos retos únicos para los expertos en ciberseguridad.

- **Verdadero**
- Falso

b. Tener conocimientos sobre las diferencias entre los ataques activos y los pasivos permite a los profesionales encargados de proteger los activos de información del negocio identificar en qué momentos se produce un ciberataque con idea de adoptar la medida de protección que sea más efectiva.

- **Verdadero**
- Falso

c. Existe una sola técnica de ataque empleada por los *crackers* para acceder de forma no autorizada a los sistemas de información de una organización.

- Verdadero
- **Falso**

2. ¿A qué tipo de ataque hace referencia esta afirmación? "Al no tener la víctima ningún tipo de pista sobre el ataque que está sufriendo, la detección es realmente dificultosa, centrándose la protección de los sistemas de información en la prevención".

a. Ataque pasivo.
b. Ataque activo.
c. Ataque híbrido.
d. Ataque pasivo y ataque activo.

3. ¿Qué nombre recibe cualquier tipo de herramienta que sirva para capturar tráfico pasivo?

a. *Sniffer*
b. *Hooping*
c. *Wireshark*
d. *Spoofing*

4. ¿Para qué sistema operativo es válida la herramienta *Wireshark*?

a. *Windows*
b. *Linux*
c. *Mac OS*
d. Se trata de una herramienta multiplataforma.

5. ¿Cuál de los siguientes recursos se emplea para abordar la tarea de detectar y expulsar de la red a un *sniffer*?

a. *Promqry*
b. *Promovae*
c. *Scanpromi*
d. *Scanpromovae*

6. ¿Qué término describe mejor las técnicas de *spoofing*?

a. Intrusión
b. Suplantación
c. *Hacking*
d. *Sniffer*

7. ¿Qué nombre recibe el *Spoofing* que engaña al receptor de señal de un satélite?

a. SAT Spoofing.
b. NAT Spoofing.
c. *GPS Spoofing.*
d. Todas las opciones son incorrectas.

8. ¿Qué nombre recibe el *Spoofing* que tratará de desviar el tráfico de la red directamente al dispositivo del *cracker,* permitiendo al atacante definir como puerta de entrada a la red o *proxy* su propia dirección, de manera que podrá modificar los valores de los protocolos DNS?

a. DHCP *Spoofing.*
b. ARP *Spoofing.*
c. MitM *Spoofing.*
d. MAC *Flooding.*

9. ¿Qué técnica utiliza un *cracker* para generar tráfico malicioso con idea de que alcance otra red y configure su propio *host* para que este asuma las funciones de un *switch* y así conseguir beneficiarse de las labores que realiza un *autotrunk?*

a. *Vlan Hooping.*
b. MAC *Flooding.*
c. *Root Bridge.*
d. BDPU.

10. Según el método propuesto por *Sqrrl Securite Analytics Company,* para identificar intrusiones y amenazas y mantener la red en una correcta posición de seguridad, crear una hipótesis significa...

a. ... llevar a cabo un análisis de árbol de ataque.
b. ... evaluar amenazas y vulnerabilidades y realizar un análisis de registro.
c. ... desarrollar técnicas automatizadas de búsqueda.
d. ... generar una inteligencia de amenaza.

Ejercicios de autoevaluación Unidad de Aprendizaje 11

1. Indica si las siguientes afirmaciones son verdaderas o falsas.

a. Cada ciberataque tiene sus propias características, que se rigen principalmente por el objetivo que persigue el atacante, los medios que utiliza para ejecutarlos y finalmente la infraestructura tanto física como de red que posea la víctima.

- **Verdadero**
- Falso

b. La infraestructura de la tecnología (TI) abarca todos aquellos recursos necesarios para que un *hacker* ético pueda maniobrar y gestionar correctamente con seguridad los entornos organizacionales.

- Verdadero
- **Falso**

c. La infraestructura de la tecnología de la información es un compendio de elementos tecnológicos que tiene por objetivo proporcionar diversidad de servicios y todo tipo de soluciones empresariales.

- **Verdadero**
- Falso

2. ¿Qué parte de la infraestructura de la tecnología englobaría la conexión a internet, el *router,* los cables y los conmutadores?

a. *Hardware.*
b. *Software.*
c. Sistema de red.
d. Todo ello no forma parte de la TI.

3. ¿Cuál de las siguientes opciones no entra dentro de la gestión de la TI?

a. Gestión de las API.
b. Gestión de los riesgos.

c. Gestión de la nube.
d. Gestión de estrategias de ventas.

4. ¿Qué nombre recibe la gestión del *hardware* mediante una máquina virtual?

a. Gestión de la virtualización de *hardware.*
b. Gestión de la virtualización de *software.*
c. Automatización de la infraestructura de la tecnología de la información.
d. Gestión de la configuración de los sistemas informáticos.

5. ¿Qué nombre recibe la optimización de la infraestructura tecnológica de una organización que permite que todo se realice desde una interfaz única?

a. Infraestructura convencional.
b. Infraestructura tradicional.
c. Infraestructura hiperconvergente.
d. Infraestructura convergente.

6. Una credencial es...

a. ... un usuario y una contraseña.
b. ... una credencial biométrica.
c. ... un patrón de desbloqueo.
d. Todas las opciones son correctas.

7. ¿Qué tipo de ataque sobre credenciales permite descifrar el mensaje original protegido mediante la función *hash?*

a. *Hashing.*
b. *Hasheo* de contraseñas.
c. *Hash* inverso.
d. Todas las opciones son incorrectas.

8. ¿Qué nombre recibe el tipo de ataque que conjuga la fuerza bruta y el uso de diccionarios?

a. Combinado
b. Mixto
c. Cruzado
d. Híbrido

9. La herramienta de *crackeo* de contraseñas *John the Ripper* admite cuatro fórmulas de ataque. ¿Cuál de ellas consiste en la definición de nuevas reglas para crear nuevas contraseñas que se han de ir probando?

a. *Single crack*
b. *Wordlist*
c. *Incremental*
d. *External*

10. ¿Cuál de las siguientes herramientas es realmente valorada por los *hackers* para crear y explotar vulnerabilidades en sus auditorías de seguridad?

a. *Hydra*
b. *Metasploit*
c. *Hascat*
d. *L0phtCrack*

Ejercicios de autoevaluación Unidad de Aprendizaje 12

1. Indica si las siguientes afirmaciones son verdaderas o falsas.

a. El *hacking* ético se considera una disciplina profesional dentro del ámbito de la seguridad informática que pretende reforzar los mecanismos de protección de las entidades, evaluando los niveles de vulnerabilidad y los riesgos a los que se someten los sistemas de información en las organizaciones.

- **Verdadero**
- Falso

b. La criptografía moderna da sentido a la ciberseguridad como disciplina orientada a estudiar la seguridad informática y de la información.

- **Verdadero**
- Falso

c. El criptoanálisis es una técnica de *hacking* ético.

- Verdadero
- **Falso**

2. ¿Qué nombre recibe la disciplina encargada de todas las metodologías y las técnicas empleadas para hacer inteligible la información para aquellas personas no autorizadas?

a. Criptología
b. Criptografía
c. Criptoanálisis
d. Criptociberseguridad

3. ¿Qué nombre recibe la ciencia encargada del estudio de la comunicación secreta?

a. Esteganografías
b. Estegoanálisis
c. Criptoanálisis
d. Criptología

4. ¿Qué es la esteganografía?

a. La ciencia encargada de hacer inteligibles mensajes ocultados en imágenes, sonidos, vídeos, etc.
b. La ciencia encargada de ocultar mensajes dentro de imágenes, sonidos, vídeos, etc., para que no puedan ser descubiertos por usuarios no autorizados.
c. La ciencia encargada tanto de ocultar los mensajes dentro de imágenes, sonidos, vídeos, etc., como de hacer inteligibles mensajes ocultados.
d. Todas las opciones son incorrectas.

5. ¿Qué nombre recibe la disciplina encargada de identificar los mensajes ocultados por los portadores de los mismos?

a. Esteganografía
b. Esteganocriptografía
c. Estegocriptoanálisis
d. Estegoanálisis

6. ¿Cuál de los siguientes tipos de algoritmos de cifrados genera una clave más robusta?

a. Algoritmos criptográficos de clave secreta o simétrica.
b. Algoritmos criptográficos de clave pública o simétrica.
c. Algoritmos criptográficos de clave pública o asimétrica.
d. Algoritmos criptográficos de clave privada o asimétrica.

7. ¿Con qué otro nombre se reconoce el algoritmo criptográfico *Hash*?

a. Algoritmo criptográfico asimétrico.
b. Algoritmo criptográfico simétrico.
c. Algoritmo de resumen de mensaje.
d. Todas las opciones son incorrectas.

8. El método de cifrado polialfabético es un método...

a. ... de transposición simple.
b. ... de transposición doble.
c. ... de transposición.
d. ... de sustitución.

9. ¿Qué nombre reciben las conocidas competiciones de ciberseguridad en las que los participantes son retados a superar desafíos de seguridad informática?

a. CFD.
b. CDF.
c. CTF.
d. CFT.

10. Los CTF sirven...

a. ... para aprender y desarrollar habilidades y destrezas asociadas a los *hackers,* descubriendo *flags* (banderas).
b. ... como plataformas de aprendizaje para aplicar en un contexto real los conocimientos adquiridos y habilidades desarrolladas de forma virtual.
c. ... para consolidar nuevas líneas de investigación surgidas en el ámbito de la ciberseguridad.
d. Todas las opciones son correctas.

Ejercicios de autoevaluación Unidad de Aprendizaje 13

1. Indica si las siguientes afirmaciones son verdaderas o falsas.

a. El *hacker* ético es un pseudoperfil cibernético no reconocido en el ámbito profesional de la ciberseguridad.

- Verdadero
- **Falso**

b. La relación laboral entre la empresa y el *hacker* ético debe estar sustanciada en un contrato firmado por ambas partes en el que se recojan todos los detalles de la prestación del servicio, los acuerdos de confidencialidad y la duración del mismo.

- **Verdadero**
- Falso

c. Aun siendo el *hacking* ético una práctica totalmente legal y necesaria, existe una línea muy fina entre lo lícito y lo ilícito que nunca hay que sobrepasar.

- **Verdadero**
- Falso

2. ¿Qué normativa está creada específicamente para regular la profesión del *hacker* ético?

a. Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
b. La Circular 3/2017, de 21 de septiembre, sobre la reforma del Código Penal.
c. La Directiva Europea 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información.
d. A día de hoy, no existe una normativa específica que regule la profesión del *hacker* ético.

3. ¿Qué normativa sustituyó la Decisión Marco 2005/222/JAI del Consejo, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información?

a. La Ley Orgánica 1/2015, de 30 de marzo, del Código Penal.
b. La Directiva Europea 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información.
c. Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
d. Ley Orgánica 108/2015, de 15 de abril, relativa a la ciberseguridad informática.

4. Actualmente, ¿qué ordenamiento jurídico es considerado extraoficialmente la ley del *hacking*?

a. Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
b. Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
c. La Directiva Europea 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información.
d. Todas las opciones son incorrectas.

5. ¿Cuál es el propósito de una norma ISO?

a. Dar respuesta a las empresas y organizaciones ante la necesidad de estandarizar fórmulas que describan la mejor manera de realizar algo.
b. Ofrecer protección a los activos de información de una organización.
c. Planear un sistema de gestión de la seguridad de la información para ofrecerla como propuesta a una organización.
d. Ayudar a describir los activos de información de una organización.

6. ¿Qué familia de normas ISO está compuesta por un conjunto de estándares de seguridad de la información que nacen con el objetivo de proporcionar a las organizaciones sellos (certificados de calidad) de seguridad ante los ojos de clientes, usuarios y resto de organizaciones?

a. 27000
b. 27001
c. 27002
d. 27003

7. ¿Cuál es el objetivo principal que persigue el sistema de gestión de la seguridad de la información?

a. Definir los activos de información en la organización.
b. Conocer los activos de información en la organización.
c. Proteger los activos de información en la organización.
d. Analizar los activos de información en la organización.

8. ¿Qué concepto viene a describir un proceso iterativo que, aunque su objetivo fundamental sea el de proteger los activos de información de una organización, busca siempre una mejora continua?

a. SGIS
b. SISG
c. SGSI
d. SSGI

9. Para que una empresa pueda alcanzar una correcta protección de los activos de información, es necesario hacer una adecuada gestión de los riesgos...

a. ... de amenazas físicas.
b. ... de amenazas humanas.
c. ... originados por las tecnologías empleadas.
d. Todas las opciones son correctas.

10. Según el profesor William Edwards, en la puesta en práctica de un SGSI es donde...

a. ... se define un sistema de métricas para medir la eficiencia de los controles.
b. ... se actualizan los planes de seguridad.
c. ... se fija una política de seguridad.
d. ... se comunican las mejoras a todas las partes interesadas con detalles y precisión.