RESPUESTAS HACKING ETICO

1. ¿Cuál es el propósito principal de un ataque de "SQL injection"?

- **A.** Interceptar el tráfico web.
- **B.** Acceder a la red de una organización.
- **C.** Explotar una base de datos manipulando comandos SQL.

Respuesta correcta: C
Explicación: El ataque de inyección SQL (SQLi) permite a un atacante manipular consultas SQL para acceder, modificar o eliminar datos en una base de datos.

---

2. ¿Qué es Nessus?

- **A.** Es una herramienta de escaneo de vulnerabilidades ampliamente utilizada en el ámbito de la ciberseguridad.
- **B.** Es una máquina virtual para vulnerar y practicar hacking.
- **C.** Es una herramienta de escaneo de aplicaciones ampliamente utilizada por cibercriminales.

Respuesta correcta: A
Explicación: Nessus es un escáner de vulnerabilidades de Tenable, usado para detectar fallos de seguridad en redes y sistemas.

---

3. ¿Qué es “root” en Linux?

- **A.** Es el archivo más importante en Linux ya que es la raíz del sistema.
- **B.** Usuario preinstalado en Linux para iniciar sesión.
- **C.** Es el nombre del usuario que tiene el nivel más alto de privilegios dentro del sistema.

Respuesta correcta: C
Explicación: El usuario **root** es el superusuario en Linux con privilegios administrativos totales.

---

4. ¿Qué es Responsabilidad ética en el hacking?

- **A.** Garantizar que el escaneo se realice con permiso y para propósitos legítimos.
- **B.** Garantiza que el escaneo se realice sin permiso y para propósitos legítimos.
- **C.** Es realizar el escaneo con conocimientos.

Respuesta correcta: A
Explicación: La responsabilidad ética consiste en obtener autorización y actuar con fines legítimos al realizar pruebas de seguridad.

---

5. ¿Cuál de los siguientes es un protocolo de seguridad de red diseñado para autenticar y autorizar a usuarios remotos para acceder a recursos de red de forma segura?

- **A.** FTP (File Transfer Protocol).
- **B.** SSH (Secure Shell).
- **C.** SSL (Secure Sockets Layer).

Respuesta correcta: B
Explicación: SSH cifra la conexión y permite la autenticación y el acceso remoto seguro a servidores y dispositivos.

---

6. El grupo WikiLeaks ¿Qué tipo de hackers son?

- **A.** Back Hat.
- **B.** Hackers éticos.
- **C.** Hacktivistas.

Respuesta correcta: C
Explicación: WikiLeaks es considerado un grupo de **hacktivistas**, pues filtra información para promover la transparencia.

---

7. ¿Todas las redes de wifi son seguras?

- **A.** Sí.

- **B.** No.

Respuesta correcta: B
Explicación: Muchas redes WiFi (especialmente públicas o mal configuradas) pueden ser vulnerables a ataques de interceptación o fuerza bruta.

---

8. ¿Qué es un exploit local?

- **A.** Es un tipo de phishing en la red TOR.
- **B.** Es un tipo de ataque informático que se dirige a vulnerabilidades presentes en un sistema operativo, aplicación o software en un entorno local.
- **C.** Es un tipo de ataque informático que se dirige a vulnerabilidades externas.

Respuesta correcta: B
Explicación: Un exploit local se aprovecha de fallos que requieren acceso previo al sistema para escalar privilegios o manipular procesos.

---

9. ¿Qué es un reconocimiento pasivo?

- **A.** Recopilación de información interactuando con el objetivo.
- **B.** Recopilación de información sin interactuar con el objetivo.
- **C.** Reconoce al objetivo, pero no realiza nada.

Respuesta correcta: B
Explicación: El reconocimiento pasivo implica recolectar datos sin generar tráfico directo al objetivo (por ejemplo, búsquedas en Google o redes sociales).

---

10. ¿Se puede realizar phishing de geolocalización?

- **A.** Sí, pero con herramientas de pago.
- **B.** Sí, se puede realizar con Seeker.
- **C.** No, es una técnica muy complicada.

Respuesta correcta: B
Explicación: Seeker es una herramienta que, mediante un enlace malicioso, puede

obtener la geolocalización de la víctima al engañarla para que comparta su ubicación.

---

11. ¿Todos Hackers siempre realizan actividades delictivas?

- **A.** No, los hackers éticos si encuentran una vulnerabilidad la reportan a la empresa o área encargada para la pronta solución.
- **B.** Sí, todos hackean bancos, cuentas de redes sociales.
- **C.** Sí, los hackers venden la información al mejor postor.

Respuesta correcta: A
Explicación: Los **hackers éticos** (white hats) reportan las vulnerabilidades de manera responsable para que sean corregidas.

---

12. ¿Qué comando utilizarías en Nmap para escanear toda la red 192.168.100.1 y visualizar sistema operativo y puertos?

- **A.** nmap -sV -O 192.168.100.1
- **B.** sqlmap -u 192.168.100.1 --dbs
- **C.** nmap -sV -O 192.168.100.1/24

Respuesta correcta: C
Explicación: La notación /24 escanea toda la subred (192.168.100.0–192.168.100.255), con detección de servicios (-sV) y de sistema operativo (-O).

---

13. ¿Es ilegal practicar con máquinas de VulnHub?

- **A.** No, ya que estas máquinas no tienen vulnerabilidades existentes, solo sirve para verlas.
- **B.** Sí, estás practicando hacking en un sistema sin autorización.
- **C.** No, ya que estas máquinas están en un entorno local y no tienen contacto con alguna organización.

Respuesta correcta: C
Explicación: Las máquinas de VulnHub se usan en entornos de laboratorio controlados para fines educativos y no afectan sistemas externos.

---

14. ¿Qué realiza SQLMap?

- **A.** Es una herramienta de código abierto que permite automatizar el proceso de un ataque de inyección de SQL.
- **B.** Es una herramienta de pago para administrar bases de datos SQL.
- **C.** Es la competencia de Google Chrome.

Respuesta correcta: A
Explicación: SQLMap detecta y explota vulnerabilidades de inyección SQL en aplicaciones web.

---

15. ¿Cómo funciona la Ingeniería Social?

- **A.** Pretenden ser personas amables, confiables o autoritarias y engañan a las víctimas para que confíen en ellos. Una vez que la víctima confía en el atacante, puede ser manipulada para revelar información privada.
- **B.** Pretenden ser personas amables, confiables o autoritarias y ayudan a las personas para que confíen en el asesor, pero no es ataque.
- **C.** Pretenden ser personas amables, confiables y proteger a las víctimas para que confíen en ellos.

Respuesta correcta: A
Explicación: La ingeniería social se basa en la manipulación psicológica para obtener información confidencial de la víctima.

---

16. ¿La vulnerabilidad BlueKeep a qué sistema afecta?

- **A.** Windows.
- **B.** Android.
- **C.** Linux.

Respuesta correcta: A
Explicación: BlueKeep (CVE-2019-0708) es una vulnerabilidad en RDP que afecta a versiones antiguas de Windows (Windows 7, XP, Server 2008, etc.).

---

17. ¿Qué es un "sniffer" en términos de seguridad informática?

- **A.** Un tipo de virus que afecta a dispositivos móviles.
- **B.** Un programa para robar contraseñas a través de correos electrónicos.
- **C.** Un software que monitorea y captura datos transmitidos a través de una red.

Respuesta correcta: C
Explicación: Un sniffer captura paquetes de datos para analizar el tráfico de red. Herramientas como Wireshark permiten ver la información que se envía y recibe.

---

18. ¿Las Google dorks muestran equipos hackeados?

- **A.** NO, Google dorks funciona para realizar búsquedas de temas específicos.
- **B.** SÍ, Google dorks hackea las páginas por nosotros.
- **C.** SÍ, Google dorks funciona como una puerta trasera.

Respuesta correcta: A
Explicación: Las Google dorks son búsquedas avanzadas para encontrar información expuesta en internet, pero no hackean ni son una puerta trasera.

---

19. ¿Qué es una brecha de seguridad?

- **A.** Es el hackeo de todo internet.
- **B.** Consiste en un incidente de seguridad cibernética que afecta de diferentes formas a los datos personales o corporativos.
- **C.** Es una ruptura en internet.

Respuesta correcta: B
Explicación: Una brecha de seguridad ocurre cuando datos confidenciales se exponen o acceden sin autorización.

---

20. ¿Los Hackers solo utilizan Linux?

- **A.** Sí, ya que Linux es la única plataforma que funciona correctamente para estas tareas.
- **B.** Solo Linux y Windows.
- **C.** No, los hackers utilizan todos los sistemas operativos.

Respuesta correcta: C
Explicación: Los hackers pueden emplear Linux, Windows, macOS y otros sistemas, según sus objetivos y necesidades.

---

21. ¿Cuál de estos fue un grupo famoso de hacktivismo?

- **A.** Los Hackers.
- **B.** Anonymous.
- **C.** Fan7a5ma.

Respuesta correcta: B
Explicación: Anonymous es un grupo descentralizado de hacktivistas que realiza ataques y filtraciones para protestar contra diversas causas.

---

22. ¿Qué es lo más vulnerable dentro de una organización?

- **A.** Personas.
- **B.** Servidores.
- **C.** Red Wifi.

Respuesta correcta: A
Explicación: El factor humano suele ser el más débil. Mediante ingeniería social (phishing, etc.), los atacantes explotan errores o falta de capacitación.

---

23. ¿Con qué comando actualizas Linux (Kali) desde consola?

- **A.** sudo apt-get update++.

- **B.** sudo apt-get update.
- **C.** sudo update ++ upgrade.

Respuesta correcta: B
Explicación: Para actualizar los repositorios en Kali Linux (basado en Debian) se usa sudo apt-get update, seguido de sudo apt-get upgrade o dist-upgrade.

---

24. ¿Qué es Determinación del riesgo?

- **A.** Es la estimación que deriva de la magnitud estimada de la pérdida y de la frecuencia del evento que provoca la pérdida.
- **B.** Es el proceso para determinar el límite de tareas.
- **C.** Es la estimación de gastos por software.

Respuesta correcta: A
Explicación: La determinación del riesgo analiza la probabilidad de ocurrencia de un incidente y el impacto potencial sobre la organización.

---

25. Además de Kali Linux, ¿qué otro sistema operativo es de uso para hacking?

- **A.** Hannah Montana Linux.
- **B.** Parrot OS.
- **C.** Windows XP.

Respuesta correcta: B
Explicación: Parrot OS es otra distribución basada en Debian, especializada en ciberseguridad, hacking ético y pruebas de penetración.

---

26. ¿Todas las computadoras se pueden vulnerar?

- **A.** Sí, todo equipo de cómputo se puede hackear sin ninguna complicación.
- **B.** Sí, todas son hackeables.
- **C.** No, solo las que no están actualizadas por parches de seguridad tanto sistema operativo como programas y puertos expuestos.

Respuesta correcta: C
Explicación: Aunque teóricamente cualquier sistema puede ser atacado, la falta de actualizaciones, configuraciones inseguras o errores humanos son los factores que lo facilitan.

---

27. ¿Se puede vulnerar un protocolo FTP?

- **A.** NO, es muy seguro.
- **B.** Sí, preguntando al administrador el usuario y la contraseña.
- **C.** Sí, con las técnicas adecuadas.

Respuesta correcta: C
Explicación: FTP por defecto no cifra credenciales, lo que facilita ataques de fuerza bruta, sniffing o explotación de configuraciones débiles.

---

28. ¿Realizar Ping es considerado delito si este se realiza sin autorización?

- **A.** NO, este solo es utilizado para validar si está activo un servicio.
- **B.** SÍ, se está violando la privacidad.
- **C.** NO, el ping no funciona para nada.

Respuesta correcta: A
Explicación: El comando ping simplemente verifica la conectividad. No es ilegal por sí mismo, a menos que forme parte de un escaneo o ataque no autorizado.

---

29. Cuando se detectan vulnerabilidades críticas, ¿qué se debe realizar?

- **A.** Documentar el problema y no hacer nada.
- **B.** Explotarla y sacar la mayor información posible.
- **C.** Informar al área correspondiente para la pronta solución.

Respuesta correcta: C
Explicación: En el hacking ético, se reportan inmediatamente las vulnerabilidades al equipo responsable para que las solucione.

---

30. ¿Qué herramienta utilizarías para realizar fuerza bruta?

- **A.** Hydra.
- **B.** Nmap.
- **C.** Dirb.

Respuesta correcta: A
Explicación: Hydra es una herramienta enfocada en ataques de fuerza bruta contra múltiples protocolos (FTP, SSH, HTTP, etc.).

---

31. ¿Quiénes usan Metasploit?

- **A.** Ingenieros agropecuarios.
- **B.** Ingenieros en alimentos.
- **C.** Expertos en ciberseguridad.

Respuesta correcta: C
Explicación: Metasploit es un framework para desarrollar, probar y ejecutar exploits, usado principalmente por pentesters y profesionales de ciberseguridad.

---

32. De acuerdo con el curso, ¿qué programa utilizamos para hacer OSINT a cuentas de correo?

- **A.** Sherlock.
- **B.** Shodan.
- **C.** Seeker.

Respuesta correcta: A
Explicación: Sherlock busca nombres de usuario en múltiples plataformas, ayudando en la recolección de información (OSINT).

---

33. ¿Qué es Política de Uso Aceptable?

- **A.** Una política de uso aceptable (AUP) es un tipo de política de seguridad dirigida a todos los empleados con acceso a uno o más activos de la organización.

- **B.** Una política de uso NO aceptable (AUP).
- **C.** Son los términos y condiciones en los softwares.

Respuesta correcta: A
Explicación: La AUP define cómo los usuarios deben usar los recursos tecnológicos de la organización de forma segura y ética.

---

34. ¿Qué es el "spoofing" en el contexto de la seguridad informática?

- **A.** Manipulación de archivos de registro.
- **B.** Ataque a través de un correo electrónico malicioso.
- **C.** Suplantación de identidad al falsificar información.

Respuesta correcta: C
Explicación: Spoofing implica falsificar direcciones IP, correos electrónicos u otros datos para engañar a la víctima o evadir controles de seguridad.

---

35. ¿Qué es una bandera dentro de las máquinas que vulneramos?

- **A.** Una bandera común con una calavera pirata en significado de hackers.
- **B.** Una lista de comandos utilizados como guía para hackear la máquina.
- **C.** Un archivo dentro de la máquina con una palabra o letras clave para comprobar que se logró vulnerar.

Respuesta correcta: C
Explicación: En ejercicios de hacking o CTF (Capture The Flag), la “flag” es un archivo con un texto clave que confirma el acceso exitoso.

---

36. ¿Qué es el escalamiento de privilegios?

- **A.** Es el término utilizado cuando solicitas permisos elevados a tu cuenta con el administrador.
- **B.** Es un término utilizado en seguridad informática para describir la situación en la que un usuario o un proceso adquieren permisos o privilegios mayores a los que originalmente tenían.

- **C.** Es el término utilizado por grandes hackers para referirse a la solicitud de nuevos permisos a su cuenta con administradores hackeados.

Respuesta correcta: B
Explicación: El escalamiento de privilegios permite a un atacante (o proceso) aumentar su nivel de permisos, pasando de usuario básico a administrador o root.

---

37. Kali Linux ¿en qué sistema está basado?

- **A.** Debian.
- **B.** Windows.
- **C.** Ubuntu.

Respuesta correcta: A
Explicación: Kali Linux está construido sobre Debian (rama "Testing"), especializado en pruebas de penetración.

---

38. ¿Qué es un firewall?

- **A.** Un software que protege contra virus.
- **B.** Un método para hackear sistemas remotamente.
- **C.** Un dispositivo que controla el tráfico de red y ayuda a prevenir accesos no autorizados.

Respuesta correcta: C
Explicación: Un firewall filtra el tráfico de entrada y salida según reglas definidas, impidiendo accesos no deseados.

---

39. ¿Qué es Metasploit?

- **A.** Es una máquina virtual para practicar hacking.
- **B.** Es un programa de Linux para emular Windows.
- **C.** Es una plataforma de código abierto utilizada para desarrollar, probar y ejecutar exploits, así como realizar pruebas de penetración y seguridad informática.

Respuesta correcta: C
Explicación: Metasploit Framework permite automatizar ataques de prueba, crear y ejecutar exploits, y evaluar la seguridad de sistemas.

---

40. ¿Se puede desencriptar el MD5?

- **A.** Sí, actualmente se puede realizar en páginas web o desde Kali.
- **B.** No, es un protocolo muy seguro.
- **C.** No, es un cifrado muy seguro.

Respuesta correcta: A
Explicación: Aunque MD5 es un **hash**, existen bases de datos en línea y herramientas como hashcat para “romper” o “descifrar” el hash, ya que MD5 se considera inseguro hoy en día.