examundo

# Examen de práctica CEH en español

70 preguntas con respuestas. Las guías y las traducciones las hizo y las revisó un software. Ninguna persona las ha revisado todavía.

Actualizado el 25 de noviembre de 2026 · examundo.tech/es/ceh/

## Hackeo de sistemas y ataques

**1. Un evaluador con credenciales de dominio válidas pero con pocos privilegios solicita tickets de servicio (TGS) de cuentas que tienen Service Principal Names (SPN) registrados. Luego extrae los tickets e intenta crackearlos sin conexión (offline) para obtener la contraseña en texto plano de la cuenta de servicio. ¿Cómo se llama este ataque?**

A tester with valid but low-privileged domain credentials requests service tickets (TGS) for accounts that have registered Service Principal Names, then extracts the tickets and attempts to crack them offline to recover the service account's plaintext password. What is this attack called?

A. AS-REP roasting
B. Ataque Pass-the-ticket
C. Kerberoasting
D. Ataque Golden ticket

**2. Durante la posexplotación en una red Windows, un evaluador extrae un hash NTLM directamente de la memoria de LSASS y lo usa para autenticarse en un segundo servidor por SMB, sin crackearlo nunca para obtener la contraseña en texto plano. ¿Qué técnica de ataque describe esto?**

During post-exploitation on a Windows network, a tester extracts an NTLM hash directly from LSASS memory and uses that hash to authenticate to a second server via SMB, without ever cracking it to recover the plaintext password. Which attack technique does this describe?

A. Ataque Pass-the-hash
B. Envenenamiento LLMNR/NBT-NS
C. Ataque Golden ticket
D. Kerberoasting

**3. Un evaluador sabe que la contraseña de un objetivo sigue este patrón: una mayúscula, cinco minúsculas y dos dígitos (por ejemplo, Summer24). ¿Qué comando de hashcat ataca correctamente este patrón contra un archivo de hashes NTLM?**

A tester knows a target's password follows the pattern of one capital letter, five lowercase letters, and two digits (e.g., Summer24). Which hashcat command correctly targets this pattern against a file of NTLM hashes?

A. hashcat -m 1000 -a 3 hashes.txt ?u?l?l?l?l?l?d?d
B. hashcat -m 1000 -a 0 hashes.txt ?u?l?l?l?l?l?d?d
C. hashcat -m 1000 -a 3 hashes.txt ?l?l?l?l?l?u?d?d
D. hashcat -m 1800 -a 3 hashes.txt ?u?l?l?l?l?l?d?d

**4. Un atacante oculta un ejecutable malicioso en un Alternate Data Stream (ADS) de un archivo de texto legítimo en un volumen NTFS con el comando type malware.exe > notes.txt:hidden.exe. ¿Qué característica de esta técnica la hace eficaz para evitar una detección casual?**

An attacker hides a malicious executable inside an Alternate Data Stream of a legitimate text file on an NTFS volume using the command type malware.exe > notes.txt:hidden.exe. Which characteristic of this technique makes it effective for evading casual detection?

A. La técnica funciona igual en los sistemas de archivos FAT32 y ext4

B. El antivirus no puede analizar los Alternate Data Streams bajo ninguna circunstancia

C. El flujo oculto cifra su contenido automáticamente con EFS

D. El tamaño de notes.txt que muestra el Explorador de Windows no refleja el contenido del flujo oculto

---

**5. Durante una evaluación de posexplotación en un host Linux, un evaluador ejecuta find / -perm -4000 -type f 2>/dev/null y descubre que el propio /usr/bin/find tiene el bit SUID y pertenece a root. ¿Qué acción aprovecha MEJOR esta mala configuración para escalar privilegios?**

During a post-exploitation assessment on a Linux host, a tester runs find / -perm -4000 -type f 2>/dev/null and discovers that /usr/bin/find itself has the SUID bit set and is owned by root. Which action would BEST leverage this misconfiguration to escalate privileges?

A. Reemplazar el binario /usr/bin/find por una carga de reverse shell

B. Ejecutar find con -exec para abrir una shell de root

C. Usar find para buscar hashes de contraseñas en /etc/shadow

D. Modificar /etc/passwd directamente porque find tiene permiso de escritura

---

**6. Un analista forense descubre que los binarios ps, netstat y ls de un servidor Linux comprometido fueron reemplazados por versiones modificadas que ocultan los procesos, las conexiones de red y los archivos del atacante en las consultas normales. ¿Qué TIPO de herramienta maliciosa se describe?**

A forensic analyst discovers that a compromised Linux server's `ps`, `netstat`, and `ls` binaries have been replaced with modified versions that hide the attacker's processes, network connections, and files from standard queries. What TYPE of malicious tool is described?

A. Rootkit de espacio de usuario (userland)

B. Bomba lógica (logic bomb)

C. Caballo de Troya (trojan horse)

D. Rootkit de modo kernel

---

**7. Un atacante usa wevtutil cl Security para borrar el registro de eventos de seguridad de Windows al terminar una operación en una estación de trabajo unida al dominio. ¿Qué artefacto es MÁS probable que revele el borrado, aunque el contenido del registro ya no exista?**

An attacker uses wevtutil cl Security to clear the Windows Security event log after completing an operation on a domain-joined workstation. Which artifact is MOST likely to reveal that log clearing occurred, even though the log's contents are gone?

A. El registro System, que no se puede borrar con wevtutil y siempre queda intacto

B. El archivo Prefetch de wevtutil.exe, que se elimina automáticamente al ejecutar el comando

C. El evento con ID 1102 en el propio registro, que indica "The audit log was cleared"

D. La entrada de $MFT del archivo Security.evtx, que es inmutable y no se puede modificar

---

**8. Un pentester obtiene un archivo de hashes de contraseñas de Windows y quiere recuperar las contraseñas en texto plano comparando los hashes con una gran tabla precalculada que relaciona hashes con texto plano. ¿Qué técnica se está usando?**

A penetration tester obtains a Windows password hash file and wants to recover plaintext passwords by comparing the hashes against a large precomputed table of hash-to-plaintext mappings. Which technique is being used?

A. Ataque con rainbow tables

B. Ataque de fuerza bruta

C. Kerberoasting

D. Ataque de diccionario

---

**9. Un atacante que comprometió el hash NTLM de la cuenta krbtgt falsifica un Ticket Granting Ticket (TGT) que da acceso a cualquier servicio del dominio y sigue siendo válido hasta que la contraseña de krbtgt se restablece dos veces. ¿Qué ataque describe esto?**

An attacker who has compromised the krbtgt account's NTLM hash forges a Ticket Granting Ticket that grants access to any service in the domain and remains valid until the krbtgt password has been reset twice. Which attack does this describe?

A. Ataque Silver ticket
B. Ataque Golden ticket
C. Ataque Pass-the-hash
D. Ataque DCSync

---

**10. Un atacante tiene acceso a nivel SYSTEM en un sistema Windows y quiere lograr persistencia en el registro con una aplicación del subsistema nativo que se inicie durante la inicialización del Session Manager, antes de que cargue el subsistema de Windows. ¿Qué ubicación del registro permite esta fase de ejecución?**

An attacker has SYSTEM-level access to a Windows system and wants to establish registry-based persistence that launches a native-subsystem application during Session Manager initialization, before the Windows subsystem loads. Which registry location supports this execution phase?

A. HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit
B. HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
C. HKLM\System\CurrentControlSet\Control\Session Manager\BootExecute
D. HKLM\Software\Microsoft\Windows\CurrentVersion\Run

---

## Reconocimiento

**11. Un evaluador enumera los registros DNS de target.com y encuentra dos registros MX: mail.target.com con prioridad 10 y backupmx.target.com con prioridad 20. ¿Qué afirmación identifica correctamente el servidor de correo principal?**

A tester enumerates DNS records for target.com and finds two MX records: mail.target.com with priority 10 and backupmx.target.com with priority 20. Which statement correctly identifies the primary mail exchanger?

A. mail.target.com es el principal porque un valor de prioridad más bajo indica mayor preferencia
B. backupmx.target.com es el principal porque un valor de prioridad más alto indica mayor preferencia
C. Los valores de prioridad se ignoran; los registros MX se eligen en orden alfabético
D. Ambos servidores se usan al mismo tiempo con la misma preferencia

---

**12. Un evaluador ejecuta traceroute contra la IP pública de un objetivo para mapear la ruta de red e identificar routers y firewalls intermedios antes de empezar el escaneo. ¿En qué categoría de footprinting entra esta actividad?**

A tester runs traceroute against a target's public IP address to map the network path and identify intermediate routers and firewalls before scanning begins. This activity falls under which footprinting category?

A. Solo footprinting pasivo
B. Footprinting de ingeniería social
C. Footprinting de DNS
D. Footprinting de red

---

**13. Durante el footprinting, un operador de red team consulta los registros DNS de un dominio objetivo para planear una campaña de spear phishing. ¿Qué tipo de registro DNS da la información MÁS directa sobre la infraestructura de correo de la organización?**

During footprinting, a red team operator queries a target domain's DNS records to plan a spear-phishing campaign. Which DNS record type provides the MOST direct information about the organization's email infrastructure?

A. MX
B. NS
C. PTR
D. SOA

---

**14. Un pentester ejecuta `dig axfr @ns1.target.com target.com` para intentar obtener una transferencia de zona DNS completa durante la fase de reconocimiento de una prueba contratada. Desde el punto de vista de la metodología, ¿en qué tipo de reconocimiento se clasifica MEJOR esta acción?**

A penetration tester issues `dig axfr @ns1.target.com target.com` in an attempt to obtain a full DNS zone transfer during the reconnaissance phase of an engagement. From a methodology standpoint, this action is BEST classified as which type of reconnaissance?

A. Reconocimiento activo, porque envía una consulta directa a un sistema que pertenece al objetivo y que este opera
B. Reconocimiento pasivo, porque dig es una utilidad de diagnóstico de solo lectura
C. Reconocimiento pasivo, porque las consultas DNS nunca tocan infraestructura que el objetivo monitoree
D. Reconocimiento activo solo si la transferencia tiene éxito y devuelve registros

---

**15. Un pentester se conecta directamente al puerto 25 de un objetivo con netcat y lee el banner del servidor para determinar el software y la versión del servidor de correo. Esta técnica es un ejemplo de:**

A penetration tester connects directly to a target's port 25 using netcat and reads the returned server banner to determine the mail server software and version. This technique is an example of:

A. Escaneo de vulnerabilidades
B. Enumeración, no footprinting
C. Footprinting activo
D. Footprinting pasivo

---

**16. ¿Qué herramienta de reconocimiento se diseñó específicamente como un framework OSINT modular que automatiza la recolección de datos de fuentes como redes sociales, WHOIS y buscadores, y muestra las relaciones en una visualización de grafo?**

Which reconnaissance tool is purpose-built as a modular OSINT framework that automates data collection from sources such as social media, WHOIS, and search engines, presenting relationships in a graph-based visualization?

A. Maltego
B. Responder
C. Nmap
D. Hydra

---

**17. Un evaluador ejecuta un comando de banner grabbing con telnet contra el servidor de correo de un objetivo y recibe la respuesta "220 mail.targetcorp.com ESMTP Postfix". ¿Qué aprendió el evaluador de forma más directa?**

A tester runs a banner-grabbing command against a target's mail server using telnet and receives the response "220 mail.targetcorp.com ESMTP Postfix". What has the tester most directly learned?

A. Una lista completa de las direcciones de correo de los empleados
B. El registrador del dominio y su contacto administrativo
C. El software del servidor de correo y posiblemente su versión
D. El rango completo de direcciones IP públicas de la organización

---

**18. ¿Qué combinación de operadores de búsqueda de Google localizaría con MÁS eficacia archivos de configuración indexados públicamente que contengan la cadena 'password' en un dominio objetivo específico?**

Which Google search operator combination would MOST effectively locate publicly indexed configuration files containing the string 'password' on a specific target domain?

A. link:target.com password
B. site:target.com inurl:admin password
C. site:target.com filetype:conf intext:password
D. cache:target.com "password"

---

**19. Durante la fase de reconocimiento, un hacker ético consulta una base de datos de registro público para obtener el nombre del titular, la organización registrante y el contacto administrativo del nombre de dominio de un objetivo. ¿Qué actividad se está realizando?**

During the reconnaissance phase, an ethical hacker queries a public registry database to find the registrant name, registering organization, and administrative contact for a target's domain name. Which activity is being performed?

A. Transferencia de zona DNS
B. Escaneo de puertos
C. Consulta WHOIS
D. Banner grabbing

---

**20. ¿Qué filtro de búsqueda de Shodan usaría un analista para encontrar dispositivos conectados a internet ubicados específicamente en un país determinado?**

Which Shodan search filter would an analyst use to find internet-facing devices located specifically within a given country?

A. hostname:
B. country:
C. org:
D. geo:

---

## Redes y perímetro

**21. Al escanear una subred, un evaluador encuentra un host con muchos puertos abiertos, todos con banners de servicio idénticos y muy detallados, sin respuestas que coincidan con los handshakes de protocolos legítimos y con tiempos de respuesta anormalmente rápidos sin importar la consulta. ¿Qué conclusión está MÁS justificada?**

While scanning a subnet, a tester finds a host exposing numerous open ports, all with identical and unusually verbose service banners, no responses matching legitimate protocol handshakes, and abnormally fast response times regardless of the query. Which conclusion is MOST justified?

A. Es probable que el host sea un honeypot de baja interacción
B. El host ejecuta un sistema de prevención de intrusiones (IPS)
C. El host está detrás de un balanceador de carga
D. El host es un servidor de producción reforzado (hardened)

---

**22. Un empleado recibe un correo que parece venir del soporte de TI y le pide restablecer de inmediato su contraseña con un enlace que lleva a una página de inicio de sesión falsa. ¿Qué técnica de ingeniería social representa esto?**

An employee receives an email appearing to be from the IT helpdesk, urging an immediate password reset through an embedded link that leads to a fake login page. Which social engineering technique does this represent?

A. Vishing
B. Phishing
C. Pretexting
D. Tailgating

---

**23. Un atacante inunda la tabla CAM de un switch con miles de asignaciones falsas de dirección MAC a puerto, y el switch pasa a modo abierto (fail-open) y envía las tramas por todos los puertos como un hub. ¿Qué ataque se está realizando?**

An attacker floods a switch's CAM table with thousands of forged MAC address-to-port mappings, causing the switch to fail open and broadcast frames out every port like a hub. Which attack is being performed?

A. VLAN hopping
B. DHCP starvation
C. MAC flooding
D. ARP spoofing

---

**24. Un atacante inunda la tabla CAM de un switch con miles de direcciones MAC de origen falsas. ¿Cuál es el objetivo principal de este ataque?**

An attacker floods a switch's CAM table with thousands of fabricated source MAC addresses. What is the primary goal of this attack?

A. Forzar al switch a modo abierto para que envíe el tráfico a todos los puertos como un hub
B. Hacer fallar el sistema operativo del switch para causar una denegación de servicio
C. Obtener acceso administrativo a la consola del switch
D. Eludir por completo la autenticación 802.1X por puerto

---

**25. Un evaluador envía paquetes de prueba con valores de TTL cada vez mayores hacia un host detrás de un firewall y usa los mensajes ICMP Time Exceeded recibidos para determinar qué puertos específicos permite pasar la ACL del firewall. ¿Qué técnica se está realizando?**

A tester sends probe packets with incrementally increasing TTL values toward a host behind a firewall, using the resulting ICMP Time Exceeded messages to determine which specific ports the ACL permits to pass through the firewall. Which technique is being performed?

A. Mapeo de ruta con traceroute estándar
B. Firewalking
C. Fingerprinting de SO por análisis de TTL
D. Banner grabbing

---

**26. Una técnica de evasión de IDS en la que el atacante reparte deliberadamente la carga del ataque en muchos segmentos TCP pequeños, enviados con retrasos intencionales entre paquetes, de modo que el tiempo de espera de reensamblado del IDS expire antes de poder reconocer la firma completa, se conoce como:**

An IDS evasion technique in which an attacker deliberately spreads an attack payload across many small TCP segments transmitted with intentional inter-packet delay, so that the IDS's reassembly timeout expires before the complete signature can be matched, is known as:

A. Session splicing
B. Codificación polimórfica
C. Firewalking
D. Fragmentation overlap

---

**27. Un evaluador de seguridad física se acerca a una puerta con control de acceso por credencial justo cuando sale un empleado. El empleado ve al evaluador, supone que es un compañero de trabajo y le sostiene la puerta abierta por voluntad propia. Esto es un ejemplo de:**

A physical security assessor approaches a badge-secured door just as an employee is exiting. The employee notices the assessor, assumes they are a coworker, and voluntarily holds the door open for them. This is an example of:

A. Piggybacking, porque el empleado permitió la entrada a sabiendas
B. Tailgating, porque la entrada ocurrió sin ninguna autorización
C. Shoulder surfing
D. Dumpster diving

---

**28. Un pentester prepara datos de carga maliciosa divididos en varios fragmentos IP pequeños y los envía a un objetivo protegido por un sistema de detección de intrusiones (IDS) basado en firmas. ¿Qué técnica de evasión se está empleando?**

A penetration tester crafts malicious payload data split across several small IP fragments before sending it toward a target protected by a signature-based intrusion detection system. Which evasion technique is being employed?

A. Flooding
B. Fragmentación
C. Spoofing
D. Cifrado

---

**29. Durante una evaluación autorizada de ingeniería social, un atacante llama al soporte de TI haciéndose pasar por un ejecutivo de viaje que necesita con urgencia restablecer su contraseña, y da datos inventados de ID de empleado y departamento para ganar credibilidad. ¿Qué técnica de ingeniería social se demuestra?**

During an authorized social engineering assessment, an attacker calls the IT help desk posing as a traveling executive who urgently needs a password reset, offering fabricated employee ID and department details to build credibility. Which social engineering technique is being demonstrated?

A. Pretexting
B. Tailgating
C. Phishing
D. Baiting

---

**30. Después de que un evaluador secuestra una sesión TCP autenticada inyectando segmentos falsificados con un número de secuencia predicho correctamente, el cliente y el servidor legítimos empiezan a intercambiar un flujo continuo de paquetes de acuse de recibo (ACK) no válidos que nunca se resincroniza. ¿Cómo se llama este efecto secundario?**

After a tester hijacks an authenticated TCP session by injecting spoofed segments with a correctly predicted sequence number, the legitimate client and server begin exchanging a continuous stream of invalid acknowledgment packets that never resynchronize. What is this side effect called?

A. SYN flood
B. Amplificación DNS
C. ACK storm
D. Agotamiento de la caché ARP

---

## Hackeo de aplicaciones web

**31. Un servidor web de producción devuelve seguimientos de pila (stack traces) detallados, con números de versión del framework y rutas de archivos, cada vez que ocurre una excepción no controlada. ¿En qué categoría del OWASP Top 10 entra esta debilidad?**

A production web server returns detailed stack traces, including framework version numbers and file paths, whenever an unhandled exception occurs. Which OWASP Top 10 category does this weakness fall under?

A. Inyección (Injection)
B. Configuración de seguridad incorrecta (Security misconfiguration)
C. Fallas criptográficas (Cryptographic failures)
D. Fallas de identificación y autenticación (Identification and authentication failures)

---

**32. Un evaluador envía un punto y coma seguido de un comando de Linux en un campo de un formulario web que hace un ping en el backend, y la respuesta devuelve la salida del comando adicional. ¿Qué clase de vulnerabilidad se explotó?**

A tester submits a semicolon followed by a Linux command into a web form field that performs a network ping lookup on the backend, and the additional command's output is returned in the response. Which vulnerability class was exploited?

A. Inyección de comandos del SO
B. Inyección SQL
C. Deserialización insegura
D. Cross-site scripting

---

**33. Un evaluador envía una búsqueda con una etiqueta script, y la página de error devuelve de inmediato la carga en la respuesta HTML sin codificarla y se ejecuta en el navegador del evaluador. ¿Qué tipo de cross-site scripting es este?**

A tester submits a search query containing a script tag, and the resulting error page immediately echoes the payload back into the HTML response without encoding, executing in the tester's browser. Which type of cross-site scripting is this?

A. XSS reflejado (Reflected XSS)
B. XSS ciego (Blind XSS)
C. XSS almacenado (Stored XSS)
D. XSS basado en DOM (DOM-based XSS)

---

**34. Una aplicación web Java acepta un objeto serializado en el parámetro de una cookie y lo deserializa sin validarlo. Un evaluador crea una carga serializada maliciosa con una cadena de gadgets conocida y logra ejecución remota de código. ¿Qué causa raíz hizo posible el ataque?**

A Java web application accepts a serialized object in a cookie parameter and deserializes it without validation. A tester crafts a malicious serialized payload using a known gadget chain and achieves remote code execution. Which root cause enabled this attack?

A. La aplicación deserializa datos controlados por el atacante sin restringir los tipos ni verificar su integridad
B. La aplicación usa un conjunto de cifrado TLS obsoleto para transportar la cookie
C. La aplicación guarda el estado de la sesión en una cookie del cliente en lugar del servidor
D. La aplicación no activa la bandera HttpOnly en la cookie

---

**35. Una aplicación web permite que los usuarios ingresen una URL que el servidor descarga para generar una vista previa en miniatura. Un evaluador ingresa la dirección interna de metadatos de la nube y la respuesta incluye credenciales de la instancia. ¿Qué vulnerabilidad se explotó?**

A web application lets users enter a URL that the server fetches to generate a thumbnail preview. A tester enters an internal cloud metadata address and the response includes instance credentials. Which vulnerability was exploited?

A. Cross-site scripting
B. Path traversal
C. Referencia directa insegura a objetos (IDOR)
D. Server-side request forgery (SSRF)

---

**36. Una aplicación acepta de una cookie un objeto Java serializado y codificado en base64 y lo reconstruye en el servidor sin validarlo, lo que permite a un atacante lograr ejecución remota de código con un objeto manipulado. ¿Qué vulnerabilidad hizo posible este ataque?**

An application accepts a base64-encoded serialized Java object from a cookie and reconstructs it on the server without validation, allowing an attacker to trigger remote code execution with a crafted object. Which vulnerability enabled this attack?

A. Cross-site request forgery
B. Clickjacking
C. Deserialización insegura
D. Pérdida de control de acceso (Broken access control)

---

**37. Antes de que la víctima inicie sesión, un atacante le envía un enlace con un identificador de sesión ya definido. Después de que la víctima se autentica, la aplicación no regenera el ID de sesión, y el atacante usa el mismo identificador para entrar a la sesión ya autenticada. ¿Qué ataque es este?**

Before a victim logs in, an attacker sends the victim a link containing a pre-set session identifier. After the victim authenticates, the application does not regenerate the session ID, and the attacker uses the same identifier to access the now-authenticated session. Which attack is this?

A. Clickjacking
B. Session fixation
C. Secuestro de sesión por captura de paquetes
D. Cross-Site Request Forgery

---

**38. ¿Qué herramienta usan MÁS comúnmente los pentesters como proxy interceptor para inspeccionar y modificar las solicitudes HTTP entre un navegador y una aplicación web?**

Which tool is MOST commonly used by penetration testers as an intercepting proxy to inspect and modify HTTP requests between a browser and a web application?

A. Burp Suite
B. Hashcat
C. Nmap
D. Wireshark

---

**39. Al probar una aplicación web hecha con Flask, un evaluador envía la entrada '{{7*7}}' en el campo de un formulario de comentarios, y la página que se muestra después presenta '49' en lugar del texto literal. ¿Qué vulnerabilidad confirma este comportamiento?**

During testing of a Flask-based web application, a tester submits the input '{{7*7}}' into a feedback form field, and the rendered page subsequently displays '49' instead of the literal string. Which vulnerability is confirmed by this behavior?

A. Inyección SQL donde 7*7 se evalúa como una expresión aritmética de la base de datos
B. Server-side template injection (SSTI) a través del motor de plantillas Jinja2
C. Cross-site scripting reflejado por salida HTML sin escapar
D. Inyección de plantillas del lado del cliente procesada por el sandbox de expresiones de AngularJS

---

**40. ¿Qué tipo de ataque ocurre cuando una entrada de usuario no confiable se inserta en una consulta a la base de datos sin la sanitización adecuada, y permite al atacante alterar la lógica de la consulta?**

Which type of attack occurs when untrusted user input is inserted into a database query without proper sanitization, allowing an attacker to alter the query's logic?

A. Cross-site request forgery
B. Inyección SQL
C. Server-side request forgery
D. Cross-site scripting

---

## Hackeo de redes inalámbricas

**41. Una organización activa Protected Management Frames (802.11w) en toda su infraestructura inalámbrica. ¿Qué técnica común de ataque inalámbrico mitiga PRINCIPALMENTE este control?**

An organization enables Protected Management Frames (802.11w) across its wireless infrastructure. Which common wireless attack technique does this control PRIMARILY mitigate?

A. Ataques de servidor DHCP no autorizado (rogue DHCP)
B. Ataques de diccionario sin conexión contra handshakes capturados
C. Ataques de fuerza bruta al PIN de WPS
D. Falsificación de tramas de desautenticación y desasociación

---

**42. Un evaluador quiere obtener material de credenciales de una red WPA2-PSK sin esperar a que un cliente legítimo se autentique. ¿Qué técnica logra MEJOR este objetivo?**

A tester wants to obtain credential material from a WPA2-PSK network without waiting for a legitimate client to authenticate. Which technique BEST accomplishes this goal?

A. Ejecutar un ataque de fuerza bruta al PIN de WPS con Reaver

B. Enviar tramas de desautenticación y esperar a capturar el handshake de 4 vías de un cliente

C. Capturar el PMKID de la primera trama EAPOL del AP con hcxdumptool

D. Hacer ARP spoofing contra los clientes ya conectados al AP

---

**43. Un operador de red team monta un punto de acceso falso que transmite el mismo SSID y una potencia de señal parecida a la de una red corporativa para atraer a los empleados, y luego intercepta su tráfico. ¿Qué ataque describe esto y en qué se diferencia de un ataque Karma?**

A red team operator sets up a rogue access point broadcasting the same SSID and comparable signal strength as a corporate network to lure employees into connecting, then intercepts their traffic. This describes which attack, and how does it differ from a Karma attack?

A. Ataque de desautenticación; obliga a los clientes a desconectarse antes de suplantar la red

B. Ataque Evil twin; responde a todos los SSID por los que un cliente haya preguntado alguna vez

C. Ataque Karma; suplanta un solo SSID conocido en lugar de responder a todas las solicitudes de sondeo (probe requests) de un cliente

D. Ataque Evil twin; suplanta un solo SSID conocido en lugar de responder a todas las solicitudes de sondeo (probe requests) de un cliente

---

**44. Un evaluador apunta a un punto de acceso con WPS activado con la esperanza de recuperar la contraseña WPA2. ¿Qué ataque explota la generación débil de números aleatorios en los nonces E-S1/E-S2 del enrollee de ciertos chipsets, y permite calcular el PIN de WPS sin conexión en segundos en lugar de usar fuerza bruta en línea?**

A tester targets an access point with WPS enabled, hoping to recover the WPA2 passphrase. Which attack exploits weak random number generation in certain chipsets' E-S1/E-S2 enrollee nonces, allowing the WPS PIN to be computed offline in seconds rather than brute-forced online?

A. Ataque PMKID contra el RSN IE

B. Fuerza bruta en línea al PIN de WPS con Reaver

C. Ataque KRACK contra el handshake de cuatro vías

D. Ataque Pixie Dust

---

**45. Un pentester tiene autorización para evaluar una red corporativa WPA2-PSK y quiere capturar el handshake de cuatro vías para un ataque de diccionario sin conexión. ¿Qué técnica se usa MÁS comúnmente para forzar a un cliente conectado a reautenticarse y poder capturar el handshake?**

A penetration tester has authorization to assess a corporate WPA2-PSK network and wants to capture the four-way handshake for an offline dictionary attack. Which technique is MOST commonly used to force a connected client to reauthenticate so the handshake can be captured?

A. Enviar tramas de desautenticación con aireplay-ng

B. Degradar la conexión con un proxy de SSL strip

C. Hacer envenenamiento de la caché ARP contra el cliente

D. Enviar respuestas DNS falsificadas al cliente

---

**46. Un pentester monta un punto de acceso falso que transmite el mismo SSID que una red corporativa legítima para atraer a los empleados y poder interceptar sus credenciales. ¿Qué ataque describe esto?**

A penetration tester sets up a rogue access point broadcasting the same SSID as a legitimate corporate network to lure employees into connecting so their credentials can be intercepted. Which attack does this describe?

A. Ataque Evil twin

B. Ataque de ARP spoofing

C. Ataque de Bluejacking

D. Ataque al PIN de WPS

---

**47. Un evaluador crackea en minutos una clave WEP antigua al recopilar un gran volumen de tráfico y analizar los patrones de vectores de inicialización (IV) repetidos que se usan con el cifrado RC4. ¿Qué falla de diseño fundamental de WEP aprovecha esto?**

An assessor cracks a legacy WEP key in minutes by collecting a large volume of traffic and analyzing patterns of repeated initialization vectors used with the RC4 cipher. Which fundamental design flaw in WEP does this exploit?

A. SAE permite a un atacante degradar el intercambio a un conjunto de cifrado más débil

B. La verificación de integridad Michael de TKIP se puede eludir con un ataque chopchop

C. El handshake de cuatro vías omite por completo un código de integridad del mensaje

D. El espacio de IV de 24 bits es tan pequeño que provoca colisiones frecuentes del keystream

---

**48. ¿Qué ataque inalámbrico de ingeniería social hace que un punto de acceso falso responda de forma afirmativa a las solicitudes de sondeo (probe requests) de CUALQUIER SSID de la lista de redes preferidas de un cliente cercano, en lugar de suplantar una sola red conocida?**

Which wireless social-engineering attack causes a rogue access point to respond affirmatively to probe requests for ANY SSID contained in a nearby client's preferred network list, rather than impersonating one specific known network?

A. Ataque Karma

B. Ataque de servidor DHCP no autorizado (rogue DHCP)

C. Ataque Evil twin

D. Ataque de desautenticación

---

**49. Un investigador divulga una vulnerabilidad que permite a un atacante en posición de intermediario (man-in-the-middle) manipular las retransmisiones del handshake y forzar la reinstalación de una clave de cifrado ya usada, lo que permite descifrar el tráfico del cliente sin conocer la contraseña. ¿Cómo se llama este ataque?**

A researcher discloses a vulnerability that allows an attacker positioned as a man-in-the-middle to manipulate handshake retransmissions and force reinstallation of an already-used encryption key, enabling decryption of client traffic without knowing the passphrase. What is this attack called?

A. Ataque Evil twin

B. Ataque de fuerza bruta al PIN de WPS

C. Ataque PMKID

D. Ataque KRACK

---

**50. Una red transmite WPA3-Personal en 'modo de transición' para mantener la compatibilidad con clientes WPA2 antiguos. ¿Qué riesgo introduce esta configuración?**

A network broadcasts WPA3-Personal in 'transition mode' to maintain compatibility with legacy WPA2 clients. Which risk does this configuration introduce?

A. Un atacante puede forzar a un cliente a degradarse al handshake WPA2, más débil, y así hacer un ataque de diccionario sin conexión tradicional

B. El AP transmite la PSK en texto plano para mantener la compatibilidad con versiones anteriores

C. La prueba de conocimiento cero de SAE se desactiva por completo para todos los clientes que se conectan

D. Las Protected Management Frames de 802.11w pasan a ser obligatorias solo para los clientes WPA3, lo que elimina el riesgo de desautenticación para los clientes WPA2

---

## Criptografía

**51. Un pentester descubre que una aplicación web devuelve mensajes de error distintos para relleno (padding) inválido y para MAC inválido cuando se envía una cookie cifrada con CBC modificada. ¿Qué ataque hace posible este comportamiento?**

A penetration tester discovers that a web application returns distinct error messages for invalid padding versus invalid MAC when a modified CBC-encrypted cookie is submitted. Which attack does this behavior enable?

A. Ataque de texto plano elegido (chosen-plaintext)
B. Ataque meet-in-the-middle
C. Ataque de padding oracle
D. Ataque del cumpleaños (birthday attack)

---

**52. Durante una evaluación inalámbrica, un evaluador captura un handshake de 4 vías de WPA2 con airodump-ng después de desautenticar a un cliente con aireplay-ng. ¿Qué herramienta usaría MÁS probablemente a continuación para recuperar la clave precompartida sin conexión?**

During a wireless assessment, a tester captures a WPA2 4-way handshake using airodump-ng after deauthenticating a client with aireplay-ng. Which tool would the tester MOST likely use next to recover the pre-shared key offline?

A. sqlmap
B. Responder
C. hashcat
D. El módulo psexec de Metasploit

---

**53. Un evaluador descubre que un servidor web antiguo todavía acepta conexiones SSLv3, aunque también admite TLS 1.2. ¿Qué ataque es factible contra los clientes a los que se puede forzar a volver a SSLv3?**

A tester discovers that a legacy web server still accepts SSLv3 connections even though it also supports TLS 1.2. Which attack becomes feasible against clients that can be forced to fall back to SSLv3?

A. Heartbleed
B. POODLE
C. BEAST
D. CRIME

---

**54. Un evaluador observa tráfico de red que muestra un intercambio de claves Diffie-Hellman entre un cliente y un servidor. ¿Qué condición haría factible recuperar el secreto compartido con un ataque precalculado tipo Logjam?**

A tester observes network traffic showing a Diffie-Hellman key exchange between a client and server. Which condition would make the shared secret feasibly recoverable via a precomputed, logjam-style attack?

A. El certificado del servidor usa una clave de firma RSA de 2048 bits
B. El servidor negocia un grupo DH de 512 o 1024 bits de uso común y reutilizado
C. El servidor usa ECDHE con la curva P-256
D. El cliente y el servidor negocian el conjunto de cifrado AES-256-GCM

---

**55. ¿Qué tipo de cifrado usa la misma clave para cifrar y para descifrar los datos?**

Which type of encryption uses the same key for both encrypting and decrypting data?

A. Cifrado asimétrico
B. Cifrado simétrico
C. Firma digital
D. Hash (hashing)

---

**56. Un usuario quiere firmar digitalmente un correo para que el destinatario pueda verificar tanto la identidad del remitente como que el mensaje no fue alterado en el camino. ¿Qué proceso describe MEJOR cómo se genera la firma?**

A user wants to digitally sign an email so the recipient can verify both the sender's identity and that the message was not altered in transit. Which process BEST describes how the signature is generated?

A. Cifrar el resumen (digest) del mensaje con una clave simétrica compartida

B. Cifrar todo el mensaje con la clave pública del destinatario

C. Calcular el hash del mensaje y cifrar el hash con la clave privada del remitente

D. Calcular el hash del mensaje y cifrar el hash con la clave pública del destinatario

---

**57. Un auditor inalámbrico captura un solo hash PMKID directamente de la primera trama EAPOL de un punto de acceso, sin observar que un cliente complete el handshake de 4 vías y sin realizar un ataque de desautenticación. ¿Qué técnica de ataque contra WPA2-PSK describe esto?**

A wireless auditor captures a single PMKID hash directly from an access point's first EAPOL frame without observing a client complete the 4-way handshake or performing a deauthentication attack. Which WPA2-PSK attack technique does this describe?

A. Ataque Evil twin

B. Ataque de fuerza bruta al PIN de WPS

C. Ataque de reinstalación de clave KRACK

D. Ataque sin conexión basado en PMKID

---

**58. Durante una evaluación de seguridad de red, un ingeniero observa que dos hosts establecen una clave secreta compartida a través de un canal inseguro sin transmitir nunca la clave en sí. ¿Qué mecanismo criptográfico describe esto?**

During a network security assessment, an engineer observes two hosts establishing a shared secret key over an insecure channel without ever transmitting the key itself. Which cryptographic mechanism does this describe?

A. Firma digital RSA

B. Cifrado AES-256

C. Autenticación HMAC

D. Intercambio de claves Diffie-Hellman

---

**59. Un CISO exige que, si en el futuro se compromete la clave privada RSA de largo plazo del servidor web, no se pueda descifrar el tráfico TLS capturado anteriormente. ¿Qué mecanismo de intercambio de claves cumple este requisito?**

A CISO mandates that a future compromise of the web server's long-term RSA private key must not allow decryption of previously captured TLS traffic. Which key exchange mechanism satisfies this requirement?

A. Intercambio de tickets de Kerberos

B. Intercambio de clave precompartida sin componente efímero

C. Diffie-Hellman efímero (DHE o ECDHE)

D. Intercambio de claves RSA estático

---

**60. Un arquitecto de seguridad necesita un tamaño de clave RSA con una fortaleza criptográfica aproximadamente equivalente a una clave simétrica de 128 bits, según las recomendaciones de NIST SP 800-57. ¿Qué longitud de clave debe elegir?**

A security architect needs an RSA key size that provides cryptographic strength roughly equivalent to a 128-bit symmetric key, per NIST SP 800-57 recommendations. Which key length should be selected?

A. 3072 bits

B. 2048 bits

C. 1024 bits

D. 15360 bits

---

## Fundamentos del hacking ético

**61. Durante una fase previa al ataque, un evaluador ejecuta 'nmap -sV -p 445 10.10.10.5' y confirma un puerto SMB abierto con información de versión. Para extraer nombres de recursos compartidos, listas de cuentas de usuario y detalles de sesiones nulas, ¿qué fase de la metodología debe realizar el evaluador A CONTINUACIÓN?**

During a pre-attack phase, a tester runs 'nmap -sV -p 445 10.10.10.5' and confirms an open SMB port with version information. To extract share names, user account listings, and null session details, the tester should NEXT perform which phase of the methodology?

A. Captura de banners (banner grabbing)
B. Enumeración (enumeration)
C. Reconocimiento activo
D. Escaneo de vulnerabilidades

---

**62. ¿Qué término describe a un profesional de seguridad autorizado por una organización para probar sus sistemas en busca de vulnerabilidades usando las mismas técnicas que los atacantes maliciosos?**

Which term describes a security professional who is authorized by an organization to test its systems for vulnerabilities using the same techniques as malicious attackers?

A. Hacker de sombrero negro (black hat)
B. Hacker de sombrero blanco (white hat)
C. Hacker de sombrero gris (gray hat)
D. Script kiddie

---

**63. Un atacante inunda el servidor web de programación de citas de un hospital con paquetes TCP SYN mal formados e impide durante seis horas que el personal legítimo acceda al sistema. ¿Qué componente de la tríada CIA se ve PRINCIPALMENTE comprometido por este ataque?**

An attacker floods a hospital's patient-scheduling web server with malformed TCP SYN packets, preventing legitimate staff from accessing the system for six hours. Which component of the CIA triad is PRIMARILY compromised by this attack?

A. Integridad
B. Disponibilidad
C. Confidencialidad
D. No repudio

---

**64. Durante una prueba autorizada, un evaluador usa Nmap para identificar puertos abiertos, servicios en ejecución y versiones de sistema operativo en una subred objetivo antes de intentar cualquier explotación. ¿Qué fase de la metodología de hacking representa esta actividad?**

During an authorized engagement, a tester uses Nmap to identify open ports, running services, and operating system versions across a target subnet before attempting any exploitation. Which phase of the hacking methodology does this activity represent?

A. Mantener el acceso
B. Reconocimiento
C. Escaneo y enumeración
D. Obtener acceso

---

**65. Una investigadora de seguridad, actuando por su cuenta y sin ningún contrato, descubre una falla de XSS almacenado en el portal público de inicio de sesión de una empresa con solo navegar por él. No la explota más allá de eso y la informa en privado al equipo de seguridad del proveedor. Esta persona se clasifica MEJOR como:**

A security researcher, acting on her own without any contract, discovers a stored XSS flaw on a company's public login portal simply by browsing it. She does not exploit the flaw further and privately discloses it to the vendor's security team. This individual is BEST classified as a:

A. Hacktivista
B. Hacker de sombrero gris (gray hat)
C. Hacker suicida (suicide hacker)
D. Hacker de sombrero blanco (white hat)

---

**66. Una organización quiere medir qué tan rápido su SOC detecta y responde a una intrusión simulada, sigilosa y de varias etapas, sin avisar antes a los defensores y sin intentar catalogar todas las vulnerabilidades del alcance. Este trabajo se describe MEJOR como:**

An organization wants to measure how quickly its SOC detects and responds to a stealthy, multi-stage simulated intrusion, without alerting defenders beforehand and without attempting to catalog every vulnerability in scope. This engagement is BEST described as a:

A. Programa de recompensas por errores (bug bounty)
B. Prueba de penetración (penetration test)
C. Evaluación de vulnerabilidades (vulnerability assessment)
D. Ejercicio de red team

---

**67. Un documento firmado entre una empresa de pruebas de penetración y su cliente define la metodología exacta de las pruebas, las ventanas de tiempo permitidas, los procedimientos de escalamiento con contactos de emergencia y la exclusión explícita de la pasarela de pagos de producción. Este documento se clasifica MEJOR como:**

A signed document between a pentest firm and its client defines the exact testing methodology, permitted testing windows, emergency contact escalation procedures, and an explicit exclusion of the production payment gateway from testing. This document is BEST classified as the:

A. Acuerdo marco de servicios (Master Service Agreement, MSA)
B. Acuerdo de confidencialidad (Non-Disclosure Agreement, NDA)
C. Reglas de compromiso (Rules of Engagement, ROE)
D. Declaración de trabajo (Statement of Work, SOW)

---

**68. Durante una prueba de penetración externa autorizada, un evaluador encuentra en el servidor web del cliente credenciales que también funcionan en una plataforma SaaS de un tercero que no aparece en el documento de alcance firmado. ¿Cuál es la PRIMERA acción MÁS adecuada del evaluador?**

During an authorized external penetration test, a tester discovers credentials on the client's web server that also successfully authenticate to a third-party SaaS platform not listed anywhere in the signed scope document. What is the tester's MOST appropriate FIRST action?

A. Omitir el hallazgo del informe final, porque el sistema del tercero está fuera del alcance firmado
B. Probar de inmediato las credenciales en la plataforma del tercero para confirmar que el hallazgo es explotable
C. Detenerse, no probar el sistema del tercero e informar el descubrimiento al cliente según el procedimiento de escalamiento de las ROE
D. Explotar la plataforma del tercero solo lo suficiente para demostrar el impacto y luego detenerse

---

**69. Un pentester ejecuta 'nmap -sV -p445 10.0.5.20' y, al encontrar el puerto abierto, usa 'enum4linux' para obtener de ese host los nombres de recursos compartidos y la lista de cuentas de usuario. ¿Qué dos fases de la metodología de hacking ético representa esta secuencia de acciones?**

A penetration tester runs 'nmap -sV -p445 10.0.5.20' and, after finding the port open, uses 'enum4linux' to pull share names and user account listings from the host. Which two phases of the ethical hacking methodology does this sequence of actions represent?

A. Footprinting seguido de borrado de huellas (covering tracks)
B. Enumeración seguida de mantener el acceso
C. Reconocimiento seguido de obtener acceso
D. Escaneo seguido de enumeración

---

**70. Un pentester busca en Shodan.io dispositivos conectados a internet que pertenecen a la organización objetivo, sin enviar ningún paquete directamente a la red del objetivo. Esta actividad es un ejemplo de:**

A penetration tester searches Shodan.io to identify internet-facing devices belonging to the target organization, without sending any packets directly to the target's network. This activity is an example of:

A. Escaneo de vulnerabilidades
B. Reconocimiento activo
C. Reconocimiento pasivo
D. Enumeración

---

## Respuesta correcta

**1. C** Kerberoasting usa credenciales de dominio válidas para pedir tickets de servicio de cuentas con SPN y luego ataca sin conexión la parte cifrada con la clave de la cuenta de servicio. AS-REP roasting apunta a cuentas con la preautenticación de Kerberos desactivada y no necesita credenciales. Golden ticket falsifica un TGT con el hash de krbtgt. Pass-the-ticket reutiliza un ticket robado, no lo crackea.

**2. A** Pass-the-hash abusa de NTLM: envía el hash capturado como prueba de identidad, porque NTLM nunca exige la contraseña en texto plano. Kerberoasting ataca tickets de servicio de Kerberos para crackearlos sin conexión. Golden ticket falsifica TGT con el hash de krbtgt. El envenenamiento LLMNR/NBT-NS captura hashes con una resolución de nombres falsa, pero no es la reutilización del hash.

**3. A** El comando correcto usa el tipo de hash correcto para NTLM (-m 1000), el modo de ataque por máscara (-a 3) y la máscara en el orden correcto: una mayúscula, cinco minúsculas y dos dígitos. La máscara ?l?l?l?l?l?u?d?d pone la mayúscula en la sexta posición. El modo -a 0 es de diccionario y pide una lista de palabras, no una máscara. El modo -m 1800 es sha512crypt, no NTLM.

**4. D** NTFS guarda los datos del flujo oculto aparte del flujo principal. Por eso los listados normales y el tamaño que muestra el Explorador no incluyen la carga oculta. Se descubre con herramientas como dir /r o streams de Sysinternals. ADS no cifra con EFS y existe solo en NTFS, no en FAT32 ni ext4. Los AV/EDR modernos sí analizan ADS, así que la opción del antivirus es falsa.

**5. B** Un binario SUID se ejecuta con el UID efectivo de su dueño. Con find SUID de root se puede ejecutar find . -exec /bin/sh -p \; -quit y obtener de inmediato una shell de root. Modificar /etc/passwd supone un permiso de escritura que find no da por sí solo. Reemplazar el binario exige permisos que un usuario sin privilegios casi nunca tiene. Buscar en /etc/shadow no revela su contenido ni da una shell.

**6. A** Reemplazar binarios del sistema como ps, ls y netstat por versiones troyanizadas para ocultar rastros es el comportamiento clásico de un rootkit de espacio de usuario (userland). Un rootkit de modo kernel oculta cosas parecidas, pero interceptando llamadas al sistema o modificando estructuras del kernel. Un troyano se disfraza de software legítimo. Una bomba lógica se activa con una condición y no oculta nada por sí misma.

**7. C** Borrar el registro Security con wevtutil genera el evento ID 1102, "The audit log was cleared", que queda como una de las pocas entradas del registro recién vaciado. Así un analista del SOC o una regla del SIEM detecta la manipulación. El archivo Prefetch no se borra solo; de hecho queda como otro rastro. El registro System también se puede borrar con wevtutil cl System. Las entradas de $MFT no son inmutables.

**8. A** Un ataque con rainbow tables usa cadenas de hashes precalculadas ligadas a posibles contraseñas. Permite buscar la contraseña de un hash sin recalcular nada, a cambio de más almacenamiento. Un ataque de diccionario calcula en el momento el hash de una lista de palabras. La fuerza bruta prueba todas las combinaciones y es lenta. Kerberoasting obtiene hashes de tickets de servicio, pero no describe este método de búsqueda. La defensa es la sal (salting).

**9. B** Un golden ticket falsifica un TGT de todo el dominio con el hash de krbtgt, y da acceso persistente casi ilimitado hasta que se cambian dos veces las credenciales de krbtgt. Un silver ticket falsifica un TGS de un solo servicio con el hash de esa cuenta, así que su alcance es menor. DCSync abusa de los derechos de replicación del dominio para obtener hashes. Pass-the-hash reutiliza un hash NTLM y no falsifica tickets de Kerberos.

**10. C** HKLM\System\CurrentControlSet\Control\Session Manager\BootExecute ejecuta aplicaciones nativas antes de que cargue el subsistema de Windows, durante la inicialización del Session Manager (SMSS.exe). Son ejecutables PE hechos para el subsistema nativo. Su valor por defecto es 'autocheck autochk *'. Run se ejecuta al iniciar sesión, Userinit controla el inicio de sesión y User Shell Folders define carpetas del usuario. Ninguna sirve para este arranque temprano.

**11. A** Según la RFC 5321, los servidores de correo eligen primero el registro MX con el valor de prioridad más bajo y pasan a los más altos solo si el preferido no responde. Por eso 10 se prefiere sobre 20. La opción que invierte la regla es una trampa clásica de examen. La prioridad es un orden estricto, no un reparto de carga, salvo que dos registros tengan el mismo valor. DNS no usa el orden alfabético.

**12. D** Traceroute mapea el camino salto por salto que siguen los paquetes hasta el objetivo y muestra routers, ISP y posibles límites de firewall o balanceadores de carga. Eso es footprinting de red. No es pasivo, porque envía paquetes con TTL creciente hacia la IP del objetivo y observa las respuestas. No es de ingeniería social, que obtiene información de personas. Tampoco es de DNS, que se enfoca en registros de resolución de nombres.

**13. A** Los registros MX (Mail Exchange) listan los nombres de host y la prioridad de los servidores que reciben el correo del dominio. Muestran justo la infraestructura de correo que un operador de phishing necesita suplantar o atacar. Los NS solo identifican los servidores de nombres autoritativos de la zona. Los SOA tienen datos administrativos, como el número de serie y los intervalos de actualización. Los PTR hacen búsquedas inversas de IP a nombre.

**14. A** La solicitud de transferencia de zona va directo al servidor de nombres autoritativo del objetivo, que puede registrarla, limitarla o generar una alerta. Por eso es reconocimiento activo, aunque la herramienta sea de solo lectura. El reconocimiento pasivo usa fuentes de terceros (WHOIS, cachés de buscadores, registros de Certificate Transparency) sin tocar sistemas del objetivo. Lo que cuenta es la interacción, no el resultado, así que un AXFR fallido sigue siendo activo.

**15. C** El banner grabbing exige abrir una conexión TCP directa con el servicio del objetivo y leer su respuesta. Es una interacción directa con la infraestructura del objetivo, por lo que es footprinting activo. No es pasivo, porque el sistema del objetivo recibe la conexión y responde. No es escaneo de vulnerabilidades, que busca debilidades conocidas y no solo identifica software y versión. Sigue siendo footprinting, de la fase de recopilación previa a la enumeración.

**16. A** Maltego une entidades como personas, dominios, correos y organizaciones que se descubren con muchas transformaciones (transforms) OSINT, y muestra las relaciones en un grafo interactivo. Es la opción habitual para el análisis visual de vínculos durante el reconocimiento. Nmap es un escáner de red y puertos. Hydra ataca credenciales por fuerza bruta. Responder envenena el tráfico LLMNR/NBT-NS en ataques de red. Ninguno ofrece grafos OSINT.

**17. C** El banner grabbing captura la cadena de saludo o respuesta de un servicio abierto. Aquí el banner SMTP revela el agente de transferencia de correo (Postfix) y el nombre del host, pero no el número de versión. Otros banners sí pueden mostrar la versión. No revela el rango de IP, que se obtiene con ASN o WHOIS. El registrador y el contacto salen de WHOIS. Los correos de empleados requieren otra recolección OSINT.

**18. C** La consulta "site:target.com filetype:conf intext:password" limita los resultados al dominio objetivo, a archivos .conf indexados y exige 'password' en su texto. inurl:admin solo busca rutas de URL con 'admin' y no tiene que ver con archivos de configuración. link: es un operador en desuso que buscaba páginas con enlaces a una URL. cache: mostraba la copia guardada por Google, pero Google dejó de ofrecerla.

**19. C** Una consulta WHOIS pregunta a los registros regionales de internet (ARIN, RIPE, etc.) o a los registradores de dominios y devuelve datos del propietario, como el nombre del titular, la organización y los contactos del registro. Una transferencia de zona copia el archivo de zona DNS. El banner grabbing captura la respuesta de un puerto abierto. El escaneo muestra qué puertos están abiertos, cerrados o filtrados. WHOIS es footprinting pasivo, previo al contacto activo.

**20. B** El filtro 'country:' limita los resultados a dispositivos cuya geolocalización de IP coincide con el código de país de dos letras indicado, por ejemplo country:US. El filtro 'geo:' busca por coordenadas de latitud y longitud, no por país. El filtro 'org:' busca por la organización o el ISP asociado a la IP. El filtro 'hostname:' busca un nombre de host y no sirve para filtrar por país.

**21. A** Los honeypots de baja interacción simulan servicios con banners genéricos prefabricados y casi nunca implementan la lógica completa del protocolo. El resultado son respuestas uniformes o incoherentes y tiempos de respuesta demasiado rápidos. Un servidor de producción reforzado respeta el protocolo y suele exponer pocos puertos. Un balanceador de carga reparte tráfico, pero no inventa banners idénticos. Un IPS bloquea o reinicia tráfico malicioso; no genera banners falsos.

**22. B** El phishing usa mensajes de correo engañosos, a menudo haciéndose pasar por una fuente de confianza como el soporte de TI, para que la víctima haga clic en enlaces maliciosos o ingrese sus credenciales en una página falsa. El vishing usa llamadas de voz, no correo. El pretexting usa una identidad o un escenario inventado y también puede darse por correo, pero "phishing" es la respuesta más específica aquí. El tailgating es una intrusión física.

**23. C** MAC flooding satura con entradas falsas la tabla CAM (memoria direccionable por contenido) del switch, que tiene un tamaño limitado. Cuando se llena, muchos switches pasan a modo abierto (fail-open) y envían el tráfico por todos los puertos, lo que permite espiar pasivamente la red conmutada. ARP spoofing manipula las cachés ARP de los hosts, no la tabla CAM. VLAN hopping abusa de errores de configuración de trunks. DHCP starvation agota el rango de direcciones DHCP.

**24. A** El objetivo es llevar al switch a modo abierto (fail-open) para espiar el tráfico, que es el resultado buscado del MAC flooding. El ataque satura la tabla CAM (memoria direccionable por contenido), que es limitada. Las tramas con MAC de destino desconocida pueden enviarse por los demás puertos de la misma VLAN, y así el atacante captura parte del tráfico de otros hosts. El tráfico con destino conocido se sigue conmutando normal. Las otras opciones son técnicas distintas.

**25. B** Firewalking usa el aumento gradual del TTL contra un gateway conocido para saber qué puertos y protocolos permite pasar la ACL, según si llegan mensajes Time Exceeded desde más allá del firewall. El traceroute estándar mapea la ruta hasta el destino, pero no busca las reglas de la ACL. El fingerprinting de SO por TTL deduce el sistema operativo a partir de los TTL iniciales de las respuestas. El banner grabbing captura versiones de servicios.

**26. A** Session splicing aprovecha el tiempo limitado de reensamblado del IDS. Envía la carga en muchos segmentos TCP diminutos con retrasos, y el sensor abandona el reensamblado antes de ver la firma completa. El host de destino, que suele tener un tiempo de espera mayor o ninguno, sí reconstruye la carga. Fragmentation overlap explota el orden ambiguo del reensamblado. Firewalking mapea reglas con TTL. La codificación polimórfica cambia los bytes de la carga.

**27. A** El piggybacking ocurre cuando una persona autorizada deja entrar a sabiendas a otra, aunque se equivoque, como aquí al sostener la puerta creyendo que el evaluador pertenece al lugar. Hay consentimiento, aunque se basa en un engaño. El tailgating describe a alguien no autorizado que cruza una entrada segura detrás de una persona autorizada sin que esta lo sepa. Dumpster diving es buscar material desechado, y shoulder surfing es mirar cómo alguien escribe sus credenciales.

**28. B** La evasión por fragmentación divide la carga del ataque en varios fragmentos IP, de modo que el motor de firmas nunca ve la secuencia maliciosa completa en un solo paquete. Funciona mejor si el IDS reensambla los fragmentos de forma distinta al host de destino. El cifrado oculta el contenido, pero no divide en fragmentos. El flooding sobrecarga recursos. El spoofing falsifica la dirección de origen, no la estructura de la carga.

**29. A** El pretexting consiste en crear un escenario falso o una identidad falsa para ganar confianza y lograr que el objetivo haga algo, como restablecer una contraseña. El phishing usa mensajes electrónicos engañosos (correo o texto) y no una suplantación en vivo. El tailgating es seguir a una persona autorizada por una puerta segura. El baiting atrae a la víctima con un señuelo físico o digital, como una USB infectada, y aquí no hay ninguno.

**30. C** Cuando una sesión se secuestra y se desincroniza, el cliente y el servidor tienen números de secuencia que el otro ya no reconoce como válidos. Cada paquete que uno envía provoca un ACK del otro con el número esperado, que de nuevo se rechaza. Se forma un bucle de ACK que se alimenta solo, llamado ACK storm, hasta que la conexión expira o se reinicia. SYN flood, amplificación DNS y ARP no tienen que ver con la secuencia TCP.

**31. B** La configuración de seguridad incorrecta incluye mensajes de error detallados o información de depuración activa en producción. Eso revela el framework y las versiones, y ayuda a buscar exploits conocidos. La solución es desactivar la depuración y mostrar errores genéricos. No es inyección, porque ninguna entrada altera comandos ni consultas. No es de autenticación, porque no hay login ni sesiones. Tampoco es criptográfica, porque no hay cifrado débil.

**32. A** Agregar un metacarácter de shell como el punto y coma para encadenar un comando del sistema a la llamada de ping prevista es la señal típica de la inyección de comandos del SO (OS command injection). Permite ejecutar comandos con los privilegios del proceso del servidor web. El cross-site scripting ataca el navegador de la víctima, no la shell del servidor. La inyección SQL manipula consultas de base de datos. La deserialización insegura reconstruye objetos serializados de forma insegura.

**33. A** En el XSS reflejado, la entrada se devuelve de inmediato en la respuesta del servidor sin guardarse. La víctima lo activa al seguir un enlace manipulado o enviar un formulario malicioso, por eso no es persistente. El XSS almacenado guarda la carga en el servidor, por ejemplo en una base de datos, y se ejecuta para cada visitante. El XSS basado en DOM ocurre solo en el JavaScript del cliente. El XSS ciego se ejecuta en un contexto que el atacante no ve, como un panel de administración.

**34. A** Las vulnerabilidades de deserialización insegura aparecen cuando la aplicación deserializa datos no confiables sin limitar las clases permitidas ni verificar la integridad. Así el atacante usa una cadena de gadgets: clases legítimas que, encadenadas, ejecutan código. La fuerza de TLS afecta el transporte, no la deserialización. Guardar la sesión en el cliente es otra decisión de diseño. Sin HttpOnly se puede robar la cookie con XSS, pero no causa ejecución remota.

**35. D** En una SSRF se logra que el propio servidor haga una solicitud a un destino elegido por el atacante. Aquí llega a un servicio interno de metadatos al que normalmente no se accede desde internet. El cross-site scripting se ejecuta en el navegador de la víctima, no en el servidor. IDOR es acceso no autorizado a un objeto mediante un identificador manipulable. Path traversal usa secuencias de rutas para salir de un directorio, no solicitudes HTTP remotas.

**36. C** La deserialización insegura ocurre cuando se reconstruyen en objetos datos serializados no confiables sin validar su tipo ni su integridad. Un objeto manipulado puede activar rutas de código no previstas, a menudo con cadenas de gadgets del classpath, y llegar a la ejecución remota de código. Cross-site request forgery falsifica una solicitud autenticada. La pérdida de control de acceso trata de fallas en la autorización. El clickjacking engaña con marcos transparentes en la interfaz.

**37. B** En la session fixation, el atacante impone o entrega un identificador de sesión conocido a la víctima antes de autenticarse. La aplicación no emite un ID nuevo al iniciar sesión, y el atacante reutiliza ese ID para entrar a la sesión autenticada. El secuestro por captura de paquetes intercepta un token existente en tránsito, no lo planta antes. CSRF y clickjacking no asignan un ID de sesión previo. La solución es regenerar el ID al cambiar de privilegio, como al iniciar sesión.

**38. A** El Proxy de Burp Suite se coloca entre el navegador y la aplicación objetivo. Captura las solicitudes y respuestas HTTP y HTTPS en vivo y permite modificarlas de forma manual o automática, algo clave para probar inyecciones, autenticación y fallas de lógica de negocio. Nmap es un escáner de red y puertos, no un proxy HTTP. Hashcat crackea contraseñas a partir de hashes capturados. Wireshark captura y analiza paquetes de forma pasiva, no modifica solicitudes en vivo.

**39. B** Que '{{7*7}}' se muestre como '49' es la prueba clásica de SSTI en Jinja2, el motor de plantillas por defecto de Flask. La entrada se interpreta y evalúa como sintaxis de plantilla en lugar de tratarse como datos. Un XSS reflejado ejecutaría script en el navegador, no una operación en el servidor. La inyección en AngularJS es del lado del cliente. La inyección SQL ocurre en una consulta a la base de datos. Si se escapa del sandbox, una SSTI puede dar ejecución remota de código.

**40. B** La inyección SQL ocurre cuando la entrada del atacante, con metacaracteres SQL como ', -- u OR 1=1, se concatena directo en la consulta y cambia su lógica, para saltarse la autenticación o extraer datos. El cross-site scripting inyecta script en la salida del navegador, no en una consulta. Cross-site request forgery obliga al navegador de un usuario autenticado a enviar una solicitud no deseada. Server-side request forgery hace que el servidor solicite destinos no previstos.

**41. D** 802.11w protege criptográficamente las tramas de administración robustas, incluidas las de desautenticación y desasociación unicast y broadcast. Mitiga así su falsificación contra asociaciones protegidas ya establecidas. No fortalece la PSK frente al cracking sin conexión, porque esa debilidad está en la contraseña, no en las tramas de administración. La fuerza bruta de WPS ataca otro mecanismo de PIN. Los ataques rogue DHCP ocurren por encima de la capa MAC 802.11.

**42. C** El ataque PMKID no necesita clientes: el propio AP entrega el PMKID dentro del elemento de información RSN del mensaje 1 (M1) del handshake de 4 vías. Basta con que el AP sea visible, sin cliente asociado. La captura del handshake por desautenticación exige que haya un cliente que se reautentique. La fuerza bruta de WPS ataca otro mecanismo de PIN, no la PSK. El ARP spoofing es una técnica de intermediario (man-in-the-middle), no de captura de credenciales.

**43. D** Un evil twin imita un solo SSID conocido para que los clientes crean que se conectan a la red corporativa legítima. Un ataque Karma, en cambio, escucha las solicitudes de sondeo (probe requests) y responde con el SSID que cada cliente busca. Así suplanta cualquier red de su lista de redes preferidas, no un nombre fijo. La desautenticación es otra técnica de interrupción, a veces combinada con alguno de los dos ataques, pero no es lo que se describe.

**44. D** Pixie Dust explota implementaciones de WPS cuyos nonces E-S1/E-S2, que prueban el conocimiento del PIN, salen de números aleatorios previsibles. Con un solo intercambio WPS capturado, el atacante obtiene el PIN sin conexión en segundos o minutos, no en horas. La fuerza bruta de Reaver tiene límite de intentos y se detecta o se bloquea. PMKID ataca la PSK de WPA2, no WPS. KRACK reinstala claves en el handshake.

**45. A** Las tramas de desautenticación falsifican la MAC del AP y le dicen al cliente que se desconecte. Cuando se reconecta, el handshake de cuatro vías se repite y se captura con airodump-ng, para crackearlo sin conexión con hashcat o aircrack-ng. Funciona porque en WPA2 las tramas de administración no están autenticadas, algo que 802.11w corrige. El envenenamiento ARP y el DNS falso son ataques de intermediario y no fuerzan la reautenticación. SSL strip ataca sesiones HTTPS.

**46. A** Un evil twin crea un punto de acceso falso que imita el SSID de una red legítima, y a menudo también su BSSID, para que los usuarios se conecten y se capture su tráfico y sus credenciales. Con frecuencia se combina con tramas de desautenticación para sacar a los clientes del AP real. ARP spoofing es una técnica de capa 2 contra hosts que ya están en una red. El ataque al PIN de WPS ataca el WPS del AP legítimo. Bluejacking envía mensajes por Bluetooth.

**47. D** El vector de inicialización de 24 bits de WEP da solo unos 16.7 millones de valores. En una red con mucho tráfico se repiten (colisionan) en cuestión de horas. Con las colisiones capturadas, herramientas como aircrack-ng recuperan estadísticamente la clave RC4 con técnicas como FMS o PTW. TKIP y su verificación Michael son una capa de mitigación de WPA, no de WEP. Los ataques de degradación de SAE son de WPA3. WEP sí incluye integridad (ICV), pero es criptográficamente débil.

**48. A** Un ataque Karma, basado en la herramienta KARMA original, vigila las solicitudes de sondeo dirigidas que los clientes cercanos emiten al buscar SSID guardados en su lista de redes preferidas, y responde a ellas. Así los clientes pueden asociarse solos al AP falso. Un evil twin suplanta una red legítima concreta, que no tiene que estar visible, y no hace falta copiar su BSSID. La desautenticación solo desconecta clientes. El rogue DHCP actúa después de la asociación.

**49. D** El Key Reinstallation Attack (KRACK) explota el handshake de cuatro vías de WPA2 al reenviar el mensaje 3. Así engaña al cliente para que reinicie su nonce y reinstale una clave de sesión ya en uso, lo que reinicia el keystream y permite descifrar o reenviar paquetes. No necesita la contraseña ni la revela, a diferencia de PMKID y los ataques de diccionario. Evil twin es un AP falso de ingeniería social. La fuerza bruta de WPS ataca un PIN de 8 dígitos, que es otra cosa.

**50. A** El modo de transición anuncia WPA2 y WPA3 en el mismo beacon. Los ataques de degradación de tipo Dragonblood mostraron que un AP falso o un atacante en la ruta puede forzar a un cliente compatible con ambos a usar el handshake WPA2. Ese handshake se captura y se ataca con diccionario sin conexión, igual que en WPA2 puro. SAE sigue funcionando con WPA3. La PSK no se transmite en texto plano. PMF suele ser opcional en WPA2, así que el riesgo de desautenticación sigue.

**51. C** Los ataques de padding oracle explotan que la aplicación revela si el relleno descifrado era válido. Así el atacante recupera el texto plano de CBC byte por byte sin la clave (por ejemplo, POODLE). El ataque del cumpleaños busca colisiones de hash. Meet-in-the-middle necesita dos cálculos de texto cifrado para hallar un valor intermedio igual. El texto plano elegido exige controlar el cifrado. Cualquier diferencia observable al descifrar puede ser un canal lateral.

**52. C** hashcat admite el modo 22000 (WPA-PBKDF2-PMKID+EAPOL) para crackear sin conexión, con GPU y una lista de palabras, los handshakes de WPA2 capturados. Es el paso estándar después de la captura. Responder sirve para envenenar LLMNR/NBT-NS en redes cableadas o locales. sqlmap automatiza la explotación de inyección SQL. El módulo psexec de Metasploit ejecuta código remoto con autenticación. Antes de capturar o crackear se necesita autorización para probar la red.

**53. B** POODLE (Padding Oracle On Downgraded Legacy Encryption) explota la validación no determinista del relleno CBC de SSLv3 después de forzar una degradación (downgrade), y permite recuperar el texto plano byte por byte. Heartbleed es una lectura de memoria fuera de límites en OpenSSL. CRIME explota la compresión de TLS y no necesita volver a SSLv3. BEAST ataca una debilidad de encadenamiento CBC en TLS 1.0. La mitigación estándar es desactivar SSLv3.

**54. B** Los ataques tipo Logjam aprovechan que muchos servidores reutilizan unos pocos números primos DH estándar. Actores con recursos de nivel estatal pueden precalcular tablas de logaritmo discreto para esos grupos compartidos de 512 y 1024 bits, y así recuperar la clave casi en tiempo real. ECDHE con P-256 usa matemática de curvas elípticas, sin una ruptura precalculada equivalente a esa fuerza. AES-256-GCM es el cifrado simétrico. El tamaño de la clave RSA afecta la autenticación del certificado.

**55. B** El cifrado simétrico (por ejemplo, AES, DES y 3DES) usa una sola clave secreta compartida para cifrar y descifrar. Es rápido, pero exige distribuir la clave de forma segura. El cifrado asimétrico usa un par de claves, pública y privada, así que cada operación usa una clave distinta. El hash es una función de un solo sentido que produce un resumen de longitud fija y no se puede revertir, por lo que no "descifra". La firma digital usa claves asimétricas para probar autenticidad e integridad.

**56. C** La firma digital se crea calculando el hash del mensaje (un resumen de longitud fija) y cifrándolo con la clave privada del remitente. El destinatario lo descifra con la clave pública del remitente y lo compara con su propio hash. Cifrar el mensaje con la clave pública del destinatario solo da confidencialidad. Cifrar el hash con la clave pública del destinatario impide que otros verifiquen la firma. Una clave simétrica compartida no garantiza el no repudio (non-repudiation).

**57. D** El ataque sin conexión basado en PMKID (PMKID-based offline attack) extrae el identificador PMKID que los puntos de acceso compatibles incluyen en el primer mensaje EAPOL-Key. Se captura con herramientas como hcxdumptool y la PSK se crackea sin conexión con hashcat, sin handshake completo ni desautenticación. KRACK explota la reutilización de nonce para reinstalar una clave. El evil twin suplanta un AP. El ataque al PIN de WPS apunta a otro protocolo. Una PSK fuerte y aleatoria resiste el ataque.

**58. D** Diffie-Hellman permite que dos partes obtengan un secreto compartido usando exponenciación modular con valores públicos y exponentes privados. El secreto nunca viaja por la red, y los valores interceptados no sirven sin los exponentes privados. La firma RSA autentica datos, pero no establece un secreto simétrico compartido. AES-256 es un cifrado simétrico que necesita una clave ya compartida. HMAC da integridad y autenticación, no negociación de claves.

**59. C** Diffie-Hellman efímero genera un par de claves nuevo para cada handshake y descarta el exponente privado después. Por eso, robar la clave de largo plazo no abre sesiones pasadas: es el secreto perfecto hacia adelante (perfect forward secrecy). Con RSA estático, el pre-master secret se cifra con la clave pública del servidor, así que quien robe la clave privada descifra todas las sesiones capturadas. Una PSK sin componente efímero reutiliza el mismo secreto. Kerberos es un protocolo de autenticación.

**60. A** La tabla de fortaleza comparable de NIST SP 800-57 Parte 1 relaciona una clave simétrica de 128 bits con una clave RSA de 3072 bits. RSA de 1024 bits equivale a solo unos 80 bits de seguridad y está obsoleto. RSA de 2048 bits equivale a unos 112 bits, por debajo de lo requerido. RSA de 15360 bits equivale a 256 bits simétricos, mucho más de lo necesario, y añade una carga de rendimiento innecesaria.

**61. B** La enumeración (enumeration) viene después del escaneo. En ella se extraen de forma activa nombres de usuario, recursos compartidos, pertenencia a grupos y datos de sesión nula, normalmente con herramientas como enum4linux o rpcclient. El escaneo de vulnerabilidades busca CVE conocidos y errores de configuración, no usuarios ni recursos. El banner grabbing ya se hizo con -sV. El reconocimiento activo es una etapa anterior al escaneo de puertos.

**62. B** El hacker de sombrero blanco actúa con permiso explícito del dueño del sistema y sigue un alcance firmado, por eso su actividad es legal y ética. El de sombrero negro actúa sin autorización, por beneficio personal o mala intención. El de sombrero gris prueba sistemas sin permiso pero sin mala intención, lo cual sigue siendo ilegal. El script kiddie tiene poca habilidad técnica y usa herramientas ya hechas sin entenderlas. La autorización es lo que define al sombrero blanco.

**63. B** Una inundación SYN es una técnica de denegación de servicio que agota los recursos del servidor para que los usuarios autorizados no puedan acceder. Ataca directamente la disponibilidad (availability): que los datos y servicios estén accesibles cuando se necesitan. La confidencialidad trata de la divulgación no autorizada, y aquí no se expuso nada. La integridad trata de la modificación no autorizada, y no se alteró ningún registro. El no repudio no forma parte de la tríada CIA clásica.

**64. C** El escaneo y la enumeración implican interacción directa y activa con los hosts objetivo: escaneo de puertos, detección de servicios y versiones, y detección del sistema operativo (OS fingerprinting) con herramientas como Nmap. El reconocimiento es la fase anterior de recopilación de información, pasiva o activa, antes de sondear puertos. Obtener acceso es la explotación real, que aún no ocurrió. Mantener el acceso es la persistencia, mucho más adelante.

**65. B** Los hackers de sombrero gris actúan sin autorización formal ni contrato, pero sin mala intención, y suelen informar los hallazgos de forma responsable. Eso coincide con este caso. El sombrero blanco necesita autorización o contrato antes de probar, y aquí no lo hay. El hacker suicida acepta el riesgo legal para exponer un objetivo sin importarle las consecuencias. El hacktivista actúa por causas políticas o sociales. Lo que distingue a cada tipo es la autorización y la intención.

**66. D** El ejercicio de red team se basa en objetivos y evalúa la capacidad de detección y respuesta frente a un adversario realista, no la cobertura total de vulnerabilidades. Normalmente los defensores no lo saben de antemano. Una prueba de penetración tradicional tiene tiempo limitado y busca todas las vulnerabilidades explotables que pueda. La evaluación de vulnerabilidades escanea e informa, sin explotar. El bug bounty es abierto y continuo, sin un escenario coordinado.

**67. C** Las reglas de compromiso (ROE) fijan los detalles operativos de la prueba: metodología, horarios permitidos, contactos de emergencia y exclusiones de alcance, como la pasarela de pagos. La declaración de trabajo (SOW) define entregables, plazos y costo, no los límites operativos. El NDA solo cubre la confidencialidad de la información. El acuerdo marco (MSA) establece los términos legales y comerciales generales, pero no detalla las pruebas ni las exclusiones.

**68. C** Probar o explotar un sistema que no está autorizado de forma explícita en el alcance, aunque sea poco, expone al evaluador a responsabilidad civil y a posibles cargos bajo la ley CFAA, porque el tercero nunca dio su consentimiento. Lo correcto es detenerse en el límite y escalar por el canal definido en las reglas de compromiso (ROE), para que el cliente decida qué hacer. Omitir el hallazgo también incumple el deber de informar, aunque no se deba explotar más.

**69. D** El escaneo de servicios de nmap determina que el puerto 445 (SMB) está abierto. Eso es escaneo (scanning), que mapea hosts activos y servicios. Después enum4linux consulta ese servicio para obtener recursos compartidos, usuarios y grupos, y eso es enumeración (enumeration). Reconocimiento y footprinting pueden ser pasivos o activos. Obtener acceso exige explotar una vulnerabilidad, y aquí no ocurrió. Borrar huellas se hace después de comprometer el sistema.

**70. C** El reconocimiento pasivo (passive reconnaissance) reúne información sin interactuar directamente con los sistemas del objetivo, usando fuentes como Shodan, WHOIS, registros DNS y redes sociales, y no deja rastro en la red objetivo. El reconocimiento activo exige interacción directa, como barridos de ping o escaneos de puertos, que pueden registrarse o detectarse. La enumeración es una fase posterior e invasiva. El escaneo de vulnerabilidades sondea sistemas activos y también es detectable.

## Palabras clave en inglés

| | | |
|---|---|---|
| **reconnaissance** | reconocimiento | Fase de reunir información sobre el objetivo antes de atacar. |
| **footprinting** | recopilación de información del objetivo | Crear un perfil del objetivo: dominios, correos, redes y servidores. |
| **passive reconnaissance** | reconocimiento pasivo | Reunir datos de fuentes públicas sin tocar los sistemas del objetivo. |
| **active reconnaissance** | reconocimiento activo | Reunir datos con contacto directo, que el objetivo puede registrar. |
| **banner grabbing** | captura de banner | Leer el saludo de un servicio para conocer su software. |
| **zone transfer (AXFR)** | transferencia de zona | Solicitud para copiar todos los registros DNS de una zona. |
| **scanning** | escaneo | Buscar equipos activos, puertos abiertos y servicios en una red. |
| **enumeration** | enumeración | Extraer usuarios, grupos y recursos compartidos de un servicio abierto. |
| **vulnerability assessment** | evaluación de vulnerabilidades | Buscar e informar debilidades sin explotarlas. |
| **penetration test** | prueba de penetración | Ataque autorizado y limitado para encontrar fallas que se pueden explotar. |
| **red team engagement** | ejercicio de red team | Ataque simulado que mide la detección y la respuesta de los defensores. |
| **Rules of Engagement (ROE)** | reglas de compromiso | Documento con método, horarios, contactos y exclusiones de la prueba. |
| **scope** | alcance | Lista de sistemas que tienes permiso de probar. |
| **availability** | disponibilidad | Que los datos y servicios estén accesibles cuando se necesitan. |
| **privilege escalation** | escalada de privilegios | Pasar de una cuenta limitada a una con más permisos. |
| **persistence** | persistencia | Técnica para conservar el acceso a un sistema ya comprometido. |
| **pass-the-hash** | ataque pass-the-hash | Autenticarse con un hash NTLM robado, sin recuperar la contraseña. |
| **Kerberoasting** | Kerberoasting | Pedir tickets de servicio y crackear sin conexión la contraseña de la cuenta. |
| **golden ticket** | golden ticket (ticket dorado) | TGT falso creado con el hash de la cuenta krbtgt. |
| **rainbow table** | tabla arcoíris | Tabla precalculada para pasar de un hash a su contraseña. |
| **brute force** | fuerza bruta | Probar todas las combinaciones posibles de una contraseña o PIN. |

| | | |
|---|---|---|
| **rootkit** | rootkit | Software que oculta procesos, archivos o conexiones del atacante. |
| **honeypot** | sistema trampa | Equipo falso que atrae atacantes para observarlos. |
| **spoofing** | suplantación | Falsificar una identidad o dirección, como IP, MAC o ARP. |
| **MAC flooding** | inundación de direcciones MAC | Llenar la tabla CAM de un switch con direcciones falsas. |
| **session hijacking** | secuestro de sesión | Tomar el control de una sesión que otra persona ya inició. |
| **IDS evasion** | evasión de IDS | Evitar que un sistema de detección reconozca el ataque. |
| **social engineering** | ingeniería social | Engañar a personas para obtener acceso o información. |
| **pretexting** | uso de un pretexto | Inventar una historia o identidad para ganar confianza. |
| **tailgating** | entrar detrás de alguien | Pasar por una puerta segura sin que la persona autorizada lo note. |
| **SQL injection** | inyección SQL | Entrada no confiable que cambia la lógica de una consulta. |
| **cross-site scripting (XSS)** | secuencias de comandos entre sitios | Código del atacante que se ejecuta en el navegador de la víctima. |
| **server-side request forgery (SSRF)** | falsificación de solicitudes del servidor | Hacer que el servidor visite una dirección elegida por el atacante. |
| **intercepting proxy** | proxy de interceptación | Herramienta que captura y modifica solicitudes HTTP entre navegador y aplicación. |
| **rogue access point** | punto de acceso no autorizado | Punto Wi-Fi instalado sin permiso, a veces para engañar usuarios. |
| **evil twin** | evil twin (gemelo malvado) | Punto de acceso falso que imita el SSID de una red legítima. |
| **four-way handshake** | handshake de cuatro vías | Intercambio WPA2 que se captura para atacar la contraseña sin conexión. |
| **downgrade attack** | ataque de degradación | Forzar el uso de un protocolo más viejo y débil. |
| **symmetric encryption** | cifrado simétrico | Cifrado que usa la misma clave para cifrar y descifrar. |
| **digital signature** | firma digital | Hash cifrado con clave privada que prueba origen e integridad. |

Examundo es independiente. No está afiliado con los organismos que hacen estos exámenes ni tiene su aprobación. Las preguntas son originales, no son del examen real. examundo.tech/es/ceh/