

Simulacro de Examen - Hacking Ético

**Selecciona la opción correcta para cada una de las siguientes preguntas. Solo hay una respuesta válida por pregunta.**

1. **¿Cuál es el objetivo principal del hacking ético?**

A) Acceder a datos privados sin permiso

B) Eliminar información de un sistema

C) Identificar vulnerabilidades de forma legal

D) Monetizar vulnerabilidades encontradas

1. **¿Qué tipo de hacker es considerado un 'White Hat'?**

A) Aquel que se mueve entre la legalidad y la ilegalidad

B) Aquel que actúa ilegalmente

C) Aquel que roba datos para beneficio propio

D) Aquel que ayuda a proteger sistemas con consentimiento

1. **¿Qué fase del hacking incluye el borrado de huellas?**

A) Fase de mantenimiento

B) Fase de borrado de huellas

C) Fase de explotación

D) Fase de reconocimiento

1. **¿Qué es una auditoría de caja negra?**

A) Prueba sin conocimiento previo del sistema

B) Análisis interno de la infraestructura

C) Evaluación de rendimiento del sistema

D) Prueba de acceso con credenciales

1. **¿Cuáles son los pilares de la seguridad (CID)?**

A) Integridad, Disponibilidad, Acceso

B) Disponibilidad, Confianza, Seguridad

C) Confidencialidad, Inseguridad, Adaptabilidad

D) Confidencialidad, Integridad, Disponibilidad

1. **¿Qué herramienta se utiliza para realizar pruebas de pentesting?**

A) Microsoft Office

B) Kali Linux

C) Adobe Photoshop

D) Google Chrome

1. **¿Qué protocolo de seguridad utiliza cifrado para proteger la información?**

A) FTP

B) IPSec

C) SMTP

D) Telnet

1. **¿Qué función tiene un honeypot en ciberseguridad?**

A) Eliminar virus automáticamente

B) Desfragmentar el disco duro

C) Optimizar el rendimiento del sistema

D) Atraer a atacantes para su análisis

1. **¿Cuál es la diferencia entre ClearNet y DarkNet?**

A) ClearNet es una red privada

B) ClearNet se usa para actividades ilegales

C) La DarkNet es accesible por buscadores comunes

D) La DarkNet requiere herramientas especiales para acceder

1. **¿Qué herramienta permite la navegación anónima en la DarkWeb?**

A) Instagram

B) WhatsApp

C) Facebook

D) TOR

1. **¿Qué protocolo inalámbrico se considera más seguro?**

A) WEP2

B) WEP

C) WPA2

D) WPS

1. **¿Qué es un ataque Man in the Middle (MITM)?**

A) Cifrado de datos sensibles

B) Monitoreo del rendimiento de red

C) Intercepción de la comunicación entre cliente y servidor

D) Optimización del tráfico de internet

1. **¿Qué herramienta se utiliza para analizar tráfico en redes inalámbricas?**

A) Excel

B) Wireshark

C) Notepad

D) Photoshop

1. **¿Qué modo de red permite la conexión directa entre dispositivos sin punto de acceso?**

A) Modo infraestructura

B) Modo monitor

C) Modo ad-hoc

D) Modo pasivo

1. **¿Qué técnica permite descifrar contraseñas mediante intentos repetidos?**

A) DDoS

B) Keylogger

C) Phishing

D) Fuerza bruta

1. **¿Qué es el footprinting en ciberseguridad?**

A) Técnica de escaneo profundo

B) Técnica de monitoreo de tráfico

C) Técnica de reconocimiento previa al ataque

D) Técnica de eliminación de huellas

1. **¿Cuál es la diferencia principal entre footprinting activo y pasivo?**

A) El pasivo requiere ingeniería social

B) El activo implica contacto directo con el objetivo

C) El pasivo usa herramientas automáticas

D) Ambos son iguales

1. **¿Qué herramienta se usa para fingerprinting en redes?**

A) Wireshark

B) Kali Linux

C) Metasploit

D) Photoshop

1. **¿Cuál es un ejemplo de footprinting pasivo?**

A) Envío de correos de phishing

B) Suplantación de identidad

C) Uso de keyloggers

D) Revisión de perfiles públicos en redes sociales

1. **¿Qué se puede obtener mediante fingerprinting?**

A) Solo el nombre del administrador

B) Ubicación física del servidor

C) Información detallada del sistema objetivo

D) Velocidad de la conexión

1. **¿Qué técnica permite la manipulación del tráfico de red?**

A) Phishing

B) Man in the Middle (MITM)

C) Fuerza bruta

D) Keylogger

1. **¿Qué ataque se basa en falsificar direcciones IP para suplantar identidades?**

A) DNS Spoofing

B) IP Spoofing

C) ARP Spoofing

D) SITEL

1. **¿Qué medida ayuda a evitar el phishing?**

A) Verificar el remitente de correos

B) No usar contraseñas complejas

C) Desactivar el antivirus

D) Navegar sin precaución

1. **¿Cuál es una técnica común de ingeniería social?**

A) Escaneo de puertos

B) Phishing

C) Sniffing

D) Pentesting

# Caso Práctico: Acceso remoto sospechoso en una empresa tecnológica

La empresa tecnológica NetSecure ha detectado una actividad inusual en uno de sus servidores. Un empleado reporta que su equipo se comporta de forma extraña: el puntero del ratón se mueve sin intervención y se abren programas automáticamente. El administrador de red sospecha de una conexión remota no autorizada. Para investigar el incidente, se decide realizar una auditoría de accesos, analizar el tráfico de red y buscar puertas traseras posibles. También se revisan posibles escaladas de privilegios realizadas por el atacante para mantener el acceso persistente.

1. **¿Qué tipo de software podría estar controlando remotamente el equipo afectado?**

A) Adware

B) Ransomware

C) Troyano (RAT)

D) Spyware

1. **¿Qué herramienta puede usarse para analizar posibles vulnerabilidades explotadas en este incidente?**

A) Wireshark

B) Photoshop

C) Metasploit

D) Notepad

1. **¿Qué técnica usaría el atacante para mantener el acceso permanente al sistema?**

A) Phishing

B) SQL Injection

C) Pivoting

D) ARP Spoofing

1. **¿Qué medida preventiva habría ayudado a evitar este incidente?**

A) Desactivar antivirus

B) Permitir conexiones remotas sin validación

C) Auditoría de contraseñas y software

D) Compartir credenciales por correo

1. **¿Qué herramienta puede permitir explotación de vulnerabilidades desde el navegador?**

A) AnyDesk

B) BeEF

C) OWASP ZAP

D) Burp Suite

1. **¿Qué protocolo es ideal para comprobar si el host remoto responde?**

A) SMTP

B) HTTP

C) ICMP

D) FTP