CEH – Hacker Ético Certificado

El CEH (Certified Ethical Hacker) es la certificación desarrollada, independientemente de los fabricantes tecnológicos, por el EC-Council (International Council of Electronic Commerce Consultants). Es una de las **más reconocidas internacionalmente** en el campo del Hacking Ético y la Auditoría de Sistemas Informáticos.

1. Introducción al Hacking Ético 2. Introducción a las pruebas de penetración 3. Ingeniería social y seguridad física 4. Reconocimiento 5. Escaneo 6. Enumeración 7. Analizar Vulnerabilidades 8. Piratería del sistema 9. Software Malicioso 10. Sniffers, secuestro de secciones y denegación de servicio 11. IDS, cortafuegos y Honeypots 12. Servidores web, aplicaciones web e inyecciones de SQL 13. Wi-FI, Bluetooth, y dispositivos móviles 14. Computación en la nube e Internet de las cosas 15. Criptografía 16. Exámenes de practica	**1.1 Introducción** 1.1.1 Introducción al Hacking Ético **2.1 Proceso y tipos de pruebas de penetración** 2.1.1 Proceso y tipos de pruebas de penetración – presentación 2.1.2 Proceso de prueba de penetración – puntos esenciales 2.1.3 Preguntas de practicas

2.1.2 Proceso de prueba de penetración – puntos esenciales

El trabajo de un probador de penetración es extremadamente importante. Las computadoras y las redes están constantemente bajo ataque. Para combatir a estos piratas informáticos, las organizaciones contratan probadores de penetración.

Las pruebas de penetración son la práctica de encontrar vulnerabilidades y riesgos con el propósito de proteger una computadora o un sistema de red. Los términos pruebas de penetración y piratería ética a menudo se usan indistintamente. Sin embargo, la piratería ética es un término general que incluye todos los métodos de piratería. Las pruebas de penetración son parte de la piratería ética.

Esta lección cubre los siguientes temas:

- Equipo rojo contra equipo azul
- Metodología de piratería ética
- Ciclo de vida de las pruebas de penetración

- Marcos de prueba de penetración
- Tipos de pruebas de penetración

Equipo rojo vs. Equipo azul

Los especialistas en seguridad ofensiva se conocen como el equipo rojo o hackers éticos. Los especialistas en seguridad defensiva se conocen como el equipo azul.

Metodología de Ethical Hacking

Hay cinco fases en la metodología de piratería ética:

Fase	Descripción
Realización de reconocimiento	En esta fase, el pirata informático comienza a recopilar información sobre el objetivo. Esto puede incluir la recopilación de información disponible públicamente, el uso de técnicas de ingeniería social o incluso el buceo en basureros.
Escaneo y enumeración	El escaneo es una extensión natural del reconocimiento. El pirata informático utiliza varias herramientas para recopilar información detallada sobre la red, los sistemas informáticos, los sistemas en vivo, los puertos abiertos y otras funciones. La extracción de información como nombres de usuario, nombres de computadoras, recursos de red, recursos compartidos y servicios se conoce como enumeración. La enumeración es parte del paso de exploración.
Estableciendo acceso	En esta fase, el pirata informático utiliza toda la información recopilada a través del reconocimiento y el escaneo para explotar las vulnerabilidades encontradas y obtener acceso.
Mantener el acceso	Una vez que el hacker ha obtenido acceso, puede usar puertas traseras, rootkits o troyanos para establecer un acceso permanente al sistema.
Borrar pistas	El último paso en el proceso de piratería es limpiar pistas. El pirata informático sobrescribe los archivos de registro para ocultar el hecho de que alguna vez estuvieron allí.

Ciclo de vida de las pruebas de penetración

Otra metodología es el ciclo de vida de las pruebas de penetración. El ciclo de vida de las pruebas de penetración es casi idéntico al proceso de piratería ética. Los pasos son:

1. Realización de reconocimiento
2. Escaneo y enumeración
3. Estableciendo acceso
4. Mantener el acceso
5. Reportando

La única diferencia es el enfoque en la documentación de la prueba de penetración. Es importante un informe detallado de las pruebas realizadas y todo lo que se descubrió.

Marcos de prueba de penetración

Se han desarrollado múltiples marcos de prueba de penetración y se utilizan en situaciones apropiadas.

Marco de referencia	Descripción
Proyecto de seguridad de aplicaciones web abiertas (OWASP)	Describe técnicas para probar las aplicaciones web y los problemas de seguridad de servicios web más comunes.
Manual de metodología de pruebas de seguridad de código abierto (OSSTMM)	Intenta crear un método aceptado para una prueba de seguridad exhaustiva.
Publicación especial 800-115 del Instituto Nacional de Estándares y Tecnología (NIST SP 800-115)	Es una guía de los aspectos técnicos básicos de la realización de evaluaciones de seguridad de la información.

Tipos de pruebas de penetración

La siguiente tabla identifica los diferentes tipos de pruebas de penetración:

Tipo	Descripción
Caja negra	El hacker ético no tiene información sobre el objetivo o la red. Este tipo de prueba simula mejor un ataque externo e ignora las amenazas internas.
caja blanca	El hacker ético tiene pleno conocimiento del objetivo o la red. Esta prueba permite una prueba completa y exhaustiva, pero no es muy realista.
Caja gris	El hacker ético recibe información parcial del objetivo o la red, como configuraciones de IP o listas de correos electrónicos. Esta prueba simula una amenaza interna.

2.1.3 Preguntas de prácticas

1. Las pruebas de penetración son la práctica de encontrar vulnerabilidades y riesgos con el propósito de proteger un ordenador o una red. ¿Las pruebas de penetración están comprendidas en cuales de estos?

A. Escaneo de red

B. Equipo azul

C. Hacking ético

D. Equipo rojo

2. Heather está realizando una prueba de penetración. Ella ya ha reunido mucha información valiosa sobre su objetivo. Heather ha utilizado algunas herramientas de hackeo para determinar que, en su red objetivo, una computadora llamada Production Workstation tiene el puerto 445 abierto. ¿Qué paso en la metodología de hacking ético está realizando Heather?

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

3. ¿Cuál de los siguientes es el tercer paso en la metodología de piratería ética?

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

4. Miguel está realizando una prueba de penetración en la aplicación basada en web de su cliente. ¿Qué marcos de prueba de penetración debe utilizar Miguel?

A. ISO/IEC 27001
B. OSSTMM
C. NIST SP 800-115
D. OWASP

[Ir al inicio de página]