Hacking Ético Presencial y Remoto

Aprende Más

www.opensoftware.cl
+56976916042

Opensoftware, tu Socio en Hacking Ético y Seguridad Informática

Índice

Introducción al Hacking Ético

El hacking ético es la práctica de utilizar las mismas técnicas y herramientas que los hackers malintencionados, pero con un objetivo completamente distinto: identificar y corregir vulnerabilidades en sistemas informáticos antes de que puedan ser explotadas por cibercriminales.

Técnicas Comunes en Hacking Ético

Las técnicas incluye, escaneo de redes para detección de dispositivos y hacer sobre análisis, eliminación o mitigación de vulnerabilidades, y pruebas de penetración sobre ellos.

Herramientas Utilizadas por Hackers Éticos

Uso de Software

El software especializado ayuda en la identificación de debilidades en la seguridad. En Opensoftware usamos las heramientas TOP basada en OWASP.

Herramientas Popular

Herramientas como Nmap, Metasploit y muchas otras son comunes entre los hackers éticos.

Importancia del Hacking Ético en la Seguridad

Conciencia de Seguridad

Aumenta la conciencia sobre la seguridad cibernética en las empresas.

Prevención de Ataques

Al identificar las vulnerabilidades antes que los atacantes, se reduce el riesgo de sufrir un ciberataque exitoso.

Importancia del Hacking Ético en la Seguridad

Protección de Datos

* Protección de datos: El hacking ético ayuda a protegerlos de accesos no autorizados.

Otros

Cumplir con regulaciones de seguridad de datos.
Permite identificar áreas de mejora en la seguridad de los sistemas y promover una cultura de seguridad

Que más debe saber sobre Hacking Ético

Las diferencias entre un hacker ético y un hacker malintencionado.
Los tipos de pruebas de hacking ético.
Categorías de vulnerabilidades descubiertas por el hacking ético (según estandard OWASP).
En quién confiar para hacer hacking ético.
Cómo eliminar o mitigar las vulnerabilidades descubierta por al hacking ético.

Periodicidad Hacking Ético

La periodicidad ideal para realizar pruebas de hacking ético varía según varios factores:

* Tamaño y complejidad de la organización: Empresas más grandes y con sistemas más complejos suelen necesitar evaluaciones más frecuentes.

* Cambios en la infraestructura: Cada vez que se introducen nuevos sistemas, aplicaciones o se modifican los existentes, es recomendable realizar una nueva evaluación.

* Regulaciones y cumplimiento: Algunas industrias tienen requisitos legales específicos sobre la frecuencia de las pruebas de penetración.

* Nivel de amenaza: Si la organización opera en un sector con alto riesgo de ciberataques, las evaluaciones deben ser más frecuentes.

Generalmente, se recomienda realizar pruebas de hacking ético al menos una vez al año. Sin embargo, muchas organizaciones optan por realizarlas con mayor frecuencia, como cada seis meses o incluso cada trimestre, especialmente si manejan datos sensibles.

Otros factores a considerar:

* Tipo de prueba: Las pruebas de hacking ético pueden ser internas o externas, manuales o automatizadas. La combinación de estos tipos puede ofrecer una visión más completa de la seguridad.

* Alcance: Las pruebas pueden centrarse en sistemas específicos, aplicaciones o en toda la infraestructura de la organización.

* Presupuesto: Los recursos disponibles también influirán en la frecuencia de las evaluaciones.

Conclusiones

El hacking ético es esencial para la seguridad moderna, ayudando a las empresas a manejar y prevenir amenazas cibernéticas.
Recuerde que siempre es mejor prevenir que curar.

Nuestra Oferta

Experiencia

Solo personal especializado con más de 10 años en el tema de seguridad informática y expertos en TI.

Que ofrecemos

Escaneo de servidores, PC´s y otros dispositivos.
Eliminación o mitigación de vulnerabilidades
Escaneo de servidores, Pc´s y otros dispositivos para verificar eliminación o mitigación.
Generación de Politicas de Seguridad Informática para la no ocurrencia de las mismas vulnerabilidades.
Proceso de Hacking Ético dos veces al año por el precio de uno.

Póngase en Contacto

Asóciate con nosotros para crear un futuro más brillante juntos.

Correo Electrónico

cmoreno@opensoftware.cl

Número de Teléfono y Whatsapp

+569 76916042

Sitio Web

www.opensoftware.cl