Ethical Hacker Security Training

Objetivos

El objetivo final detrás del dictado de esta capacitación, es el de transmitir al alumno, el conjunto de conocimientos generales requeridos por el cuerpo común de conocimiento que soporta la certificación CEH (Certified Ethical Hacking) promovida por EC-Council.

El contenido vertido en nuestro ETHICAL HACKER SECURITY TRAINING, comprende un plan de entrenamiento NO OFICIAL, elaborado con el objeto que en él, no solo se encuentren alcanzados los principales objetivos requeridos de cara a la toma del examen oficial de CEH (Certified Ethical Hacker) propuesto por EC-Council, sino que a su vez, los asistentes puedan obtener el conocimiento necesario para planificar y ejecutar procesos de "Test de Intrusión Controlados" dentro de la organización o como servicio de valor agregado para terceros.

Este entrenamiento cuenta con una carga horaria de cuarenta (40) horas, la entrega de material digital, la realización de laboratorios a fin de fijar conocimientos, los cuales son impartidos por un equipo de profesionales, que no solo cuenta con experiencia comprobable en el dictado de cursos y carreras de similares características, sino también con la experiencia de campo necesaria, obtenida a partir del desarrollo de tareas de consultoría relacionada con la especialidad en empresas de primer nivel del ámbito Nacional e Internacional.

Prerrequisitos

Si bien no existen requerimientos específicos a ser cumplidos por los asistentes a este entrenamiento, se aconseja poseer conocimientos básicos de networking y administración de sistemas (Linux/Windows). Adicionalmente, es posible que para aquellas personas cuyo objetivo se encuentre fijado en la certificación oficial CEH (Certified Ethical Hacker), deban cumplir al momento de tomar el examen de certificación oficial con un conjunto de requisitos específicos, los cuales recomendamos se consulten en la siguiente URL: http://www.eccouncil.org/CEH.htm

Duración

40 Hs.

Ethical Hacker Security Training

Contenidos

1. **Introducción al Hacking Ético, Ética y Legalidad**
   a. Comprendiendo la Terminología
   b. Identificando las Diferentes Áreas de Explotación (Hacking Technologies)
   c. Comprendiendo los Pasos Involucrados en el Proceso de Ethical Hacking
      1) Etapas en el Proceso de Ethical Hacking:
         Paso 1: Reconocimiento (Pasivo / Activo)
         Paso 2: Escaneo
         Paso 3: Obtenciónde Acceso
         Paso 4: Mantenimiento de Acceso
         Paso 5: Eliminación de Rastros
   d. Hacktivismo
   e. Diferentes Clases de Hacker
      1) Ethical Hackers y Crackers
      2) Rol de Trabajo de un Hacker Ético
      3) Objetivos que persiguen los atacantes
   f. SFE Triangle
   g. Skills Requerido para convertirse en un Hacker Ético
   h. Vulnerability Research
   i. Formas de conducer un Proceso de Hacking Ético
      1) Creando un Plan de Evaluación de la Seguridad
      2) Tipos de Hacks Éticos
      3) Tipos de Testing
      4) Reportes relacionados con la tarea del Hacker Ético
   j. Implicancias Legales del Hacking
   k. Introducción a las Leyes Federales (18 U.S.C. § 1029 /1030)

2. **Footprinting ***
   a. Footprinting
      1) A que llamamos Footprinting?
      2) Proceso de Information Gathering
      3) Motores de Búsqueda
      4) Websites
      5) Network Footprinting
      6) Redes Sociales

7) Correo Electrónico
8) Metadatos
9) Buscadores Especializados
10) Complementos del Navegador
11) Maltego
12) Otros métodos de obtención de información
13) Inteligencia Competitiva

3. Introducción a Networking para Penetration Testers

a. Introducción a Networking
   1) Modelo OSI
   2) TCP/IP
   3) Direcciones MAC
   4) IP Protocol
   5) TCP Protocol
   6) UDP Protocol
   7) Puertos & Servicios
   8) 3 way Handshake

4. Escaneo y Enumeración *

b. Escaneo
   1) Introducción
   2) Identificación de Sistemas Vivos
   3) Identificación de Puertos Abiertos
   4) Identificación de Sistema Operativo
   5) Identificación de Aplicaciones
   6) Escaneo de Vulnerabilidades
   7) Identificación de Vectores de Ataque
   8) Técnicas de Ping Sweep
   9) Preparación del Ataque
c. Enumeración

5. Introducción a Criptografía para Penetration Testers

a. Tipos de Cifrado
b. Algorítmos Simétricos
c. Funciones de Hash
d. Algoritmos Asimétricos

6. **System Hacking ***
   a. Ataques a las Passwords
   b. Ataques a la Infraestructura
   c. Ataques de Denegación de Servicios
   d. Frameworks de Explotación

7. **Sniffers ***
   a. Protocolos susceptible a ser snifeados
   b. Sniffing Activo y Pasivo
   c. ARP Poisoning
   d. Ethereal: Filtros de Visualización y Captura
   e. MAC Flooding
   f. Técnicas de DNS Spoofing
   g. Sniffing: Contramedidas

8. **Ingeniería Social & Ataques del Lado del Cliente ***
   b. Ingeniería Social
      1) A que llamamos Ingeniería Social?
      2) Tipos communes de Ataque
      3) Ataques Internos
      4) Robo de Identidad
      5) Ataques de Phishing y su Relación con la Ingeniería Social
      6) Online Scams
      7) URL Obfuscation
      8) Contramedidas
   e. Ataques del Lado del Cliente

9. **Web Hacking ***
   a. Hacking Web Servers
      1) Introducción a la Problemática
      2) Ataques contra Web Servers: Generalidades
   b. Ataques a las Aplicaciones Web
      1) Cómo funcionan las aplicaciones Web?
      2) Objetivos detrás del Hacking de Aplicaciones Web
      3) Testeo de Aplicaciones
      4) Vulnerabilidades en Aplicaciones Web
      5) Web Application Penetration Test

6) OWASP / OWASP Top Ten
7) Recomendaciones Generales

10. SQL Injection *

a. SQL Injection
   1) A que llamamos SQL Injection?
   2) Pasos comprendidos en un ataque de SQL Injection
   3) SQL Injection: Contramedidas

11. Wireless Hacking

a. Introducción a las Redes Inalámbricas
b. Ataques a WEP
c. Ataques a WPA/WPA2
d. Rogue Access Points
e. MAC Spoofing
f. Rogue Access Points
g. Denegación de Servicio
h. Contramedidas

12. Test de Intrusión: Metodologías

a. Morivación, Justificación e Importancia
b. Una herramienta mas…
c. Periodicidad
d. Comercialización del Servicio
e. Contratación
f. Aspectos Legales, Autorizaciones
g. Evaluaciones de Seguridad
h. Como Conducir un Proceso de EH?
i. Componentes Principales en el Proceso de EH
j. Aspectos Generales
k. Entregables
l. Otras Guías y Marcos Metodológicos

**Áreas temáticas en los que se incluyen Laboratorios y/o Demostraciones a cargo del Instructor.*

Todo el material utilizado en el curso de capacitación para la exposición de los temas, se encuentra en castellano.