Project TI

DETECTA LAS VULNERABILIDADES EN TUS SISTEMAS

CURSO ETHICAL HACKING

Aprende a realizar pruebas, escaneos, ataques controlados y como implementar las defensas necesarias.

Presentación

Un Hacker Etico es un profesional dotado de habilidades para encontrar las debilidades o vulnerabilidades en los sistemas utilizando el mismo conocimiento y herramientas que un hacker malicioso, aprendiendo cómo escanear, probar, hackear y asegurar sus propios sistemas, entender cómo trabajan los perímetros de defensa para después analizar y atacar sus propias redes, procurando que ninguna red real resulte dañada.

Dentro de las políticas de seguridad que se deben desarrollar en las empresas, uno de los aspectos más importantes a considerar es cuan vulnerable es su red, si se han tomado las medidas adecuadas de prevención y si los mecanismos de protección actúan eficazmente sobre las mismas. Un sistema que permita evaluar las brechas de seguridad y debilidades de nuestro sistema es fundamental, para así robustecerlo y prepararlo para futuros ataques.

Teniendo en cuenta que cada vez más personas están conectadas a Internet desde sus empresas, y que por desconocimiento pueden poner en peligro a su red, se hace necesario identificar las fallas de seguridad que se presentan generadas por el personal de la organización.

Orientado para las empresas que requieran conocer las diversas técnicas que utilizan los hacker para acceder a las redes corporativas y que les permita tomar medidas correctivas para su neutralización. Profesionales que busquen la entrega de soluciones en el ámbito de la seguridad informática, combinando de forma integral productos y servicios del mercado, con el fin de proteger los activos informáticos de las empresas, facilitando el desarrollo y operación de sus actuales y futuros negocios.

¿Porqué formarte con nosotros?

- Se tiene un enfoque práctico, basado en distintos tipos de ataques y sobre diversos entornos.
- Se capacita a individuos en el área específica de seguridad en la disciplina de “Hackeo Ético”, creando conciencia de los riesgos y el uso adecuado del conocimiento adquirido.
- Contamos con docentes certificados y con experiencia laboral en los temas a impartir.
- Casos reales de discusión.
- Contamos con la mejor relación costo – beneficio, teniendo en cuenta todos los temas que se van a involucrar.

Fray. Juan Pérez No. 5968 Mitras
www. projectti.com
Teléfono: 83117258
Celular: 044811 272 5352

Project TI

Objetivos

- Alcanzar un amplio conocimiento y práctica sobre las herramientas y técnicas de ataque y metodologías disponibles para contrarrestarlas.
- Identificar y entender el entorno alrededor del Hacking y la ética profesional.
- Describir la utilidad del Ethical Hacking en un entorno de red. Comprender la importancia de este tipo de pruebas en un esquema de Seguridad de red.
- Conocer y usar en forma práctica Herramientas especializadas en la detección de vulnerabilidades.
- Aprender a desarrollar una prueba de PENTEST para una organización.

Dirigido a:

Profesionales carreras de Ingeniería de sistemas, o desempeñándose como Consultores de Tecnología, Gerentes de TI, Jefes de Informática, Auditores Internos y Externos de TI, Oficiales de Seguridad, Administradores de Seguridad, Administradores de Red, Jefes de proyecto o cualquier profesional de área TI que este interesado en conocer los métodos y técnicas de hacking y la manera de protegerse de ellos.

Duración: 52 Horas

Pre-requisitos: Manejo de entornos en ambiente Windows. Conocimientos en redes, Bases de datos e Internet. Conceptos básicos de infraestructura informática.

Metodología

Práctico.

Los talleres cuentan con una parte teórica dictados en forma de presentaciones con ejemplos concretos y talleres donde los participantes aplicaran los conceptos aprendidos durante las presentaciones teóricas. El curso es dirigido a realizar prácticas de los temas vistos en clase. Se incluyen material de apoyo así como videos ilustrativos.

Ayudas audiovisuales

Además de la presentación formal del material del curso - taller, se incluyen ejercicios, talleres y discusiones en grupo, con el propósito de facilitar el trabajo de las practicas reales que se desarrollen.

Fray. Juan Pérez No. 5968 Mitras
Teléfono: 83117258
www. projectti.com
Celular: 044811 272 5352

Project TI

CONTENIDO TEMÁTICO

- Etapas de Hackeo no ético.
  - Fases de Hackeo de sistemas
  - Triangulo de la seguridad
  - Legalidad del Hackeo ethico.
  - Sitios de internet para hackeo.

- Búsqueda de información útil del objetivo
  - Búsqueda de información útil en maquinas de búsqueda, sitos de empleos, proveedores, clientes, actividad financiera, Basura.
  - Whois, DNS, Direcciones publicas de red.
  - Caso especial hosting.

- Google hacking
  - Operadores Google.
  - Ejemplos de cómo usar operadores
  - Google hacking database.
  - Scanner de google hacking.

- Escaneo
  - Escaneo de red.
  - Escaneo de puertos
  - Escaneo de Vulnerabilidades
  - 4 formas de ocultar la dirección pública utilizada.

- Técnicas de Hackeo de contraseñas
  - Fisonomia de las contraseñas
  - Formas de atacar contraseñas
  - Fuerza Bruta, Diccionario, Hibrido
  - Tablas Precomputadas(Rainbow Tables)
  - Método Distribuido
  - Contraseñas en Windows
  - Linux
  - Contraseñas por defecto
  - Contramedidas
- EXploits.
  - Como son los exploits
  - Que Pueden hacer los exploits
  - Donde aplican los exploits
  - Cuales Herramientas aplican exploits.
  - Porque son necesarios los exploit en un análisis de seguridad.
  - Contramedidas

- Troyanos
  - Porque son una amenaza en nuestros días.
  - Características de los troyanos
  - Por usar uno si hay miles ya hechos.
  - Como evadir antivirus.

  - Como adherir el troyano a un ejecutable carnada.
  - Como detectar la actividad de estos.
  - Contramedidas

- Sniffers
  - Que hacen los sniffers
  - Diferencia en ambiente de Switch y de Hub
  - Métodos para hacer efectivo un sniffer en ambiente de switch
  - Y Wireless ¿cómo se comporta?
  - Protocolos que no cifran.
  - MITM
  - Contramedidas

- Técnicas de intrusión vía Web
  - Cross Site Script
  - Sql inyection
  - Cookie Poisoning
  - RFI
  - Contramedida

- Técnicas de intrusión vía SQL
  - Microsoft SQL con ASP
  - MySQL con Php
  - Contramedidas

- Intrusión vía Wireless
  - Fundamentos de Wireless
  - Debilidades comunes
  - Cracking WEP
  - Contramedidas

- Técnicas de ingeniería social, phising

- Voz sobre ip
  - Vulnerabilidades
  - Descifrar contraseñas
  - Capturar conversaciones.
- Pharming
  - Varias Tecnicas.

- Los pasos de un PENTEST usando metodología

- WARGAME