greenetics

Certificación en Ethical Hacking en Aplicativos Web

Greenetics Cybersecurity Academy

Es la primera academia de Seguridad Informática/Hacking Ético del país certificada por **CERT (Centro de Respuesta a Incidentes de Seguridad Informática).** Únete y conviértete en un Ethical Hacker desde cero o incrementa tus conocimientos en el mundo de la ciberseguridad. Nuestra compañía se complace en brindar todas las facilidades para entregarle un servicio de calidad y oportuno.

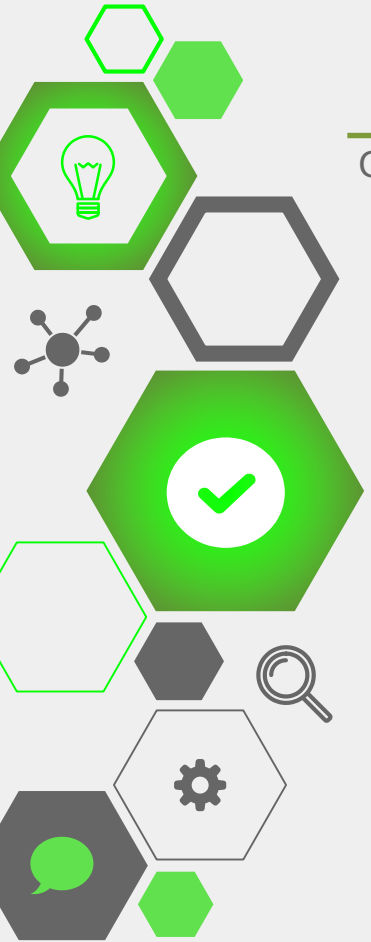
En Greenetics, nuestro objetivo es proporcionar sistemas seguros. Con las medidas necesarias, su empresa puede crecer más rápido y operar de manera más eficaz y, al mismo tiempo, preservar tanto la seguridad como la protección de los datos.

Auditoría de Sistemas	Informática Forense	Consultoría en Seguridad
Centro de respuesta de incidentes	Seguridad (Outsourcing)	Seguridad Perimetral
Capacitación Certificaciones	SGSI	Pentesting

CURSO DE ETHICAL HACKING EN APLICATIVOS WEB

- El **CURSO DE HACKING WEB** está orientado a toda persona que esté interesada en convertirse en un experto en las metodologías de hacking a sitios y aplicativos web; además de mejorar sus habilidades en seguridad informática y conocer las técnicas y herramientas más especializadas de ataque que utilizan los hackers en ambientes web e infiltraciones usando navegadores.
- Los portales Web son la imagen pública y garantizan la reputación de su Empresa ante sus clientes, socios e inversionistas. En este módulo entenderá cómo identificar y solucionar puntos de ataque, antes de que sean explotados por un agente malicioso. Aprenderá técnicas para medir la importancia de un sitio web y el impacto que tendría un ataque. Instalará y configurará un avanzado sistema de hackeo ético, incluyendo base de datos, servidor web y plataformas dinámicas para desarrollar ataques sobre las vulnerabilidades más frecuentes encontradas en websites.

Estructura del Curso



OBJETIVOS

En este curso se enseña a los participantes a entender las principales fallas en las aplicaciones web y su explotación; y más importante aún; aprender a realizar un proceso repetible y de prueba real para encontrar de manera consistente estas fallas en sus organizaciones.

El participante aprenderá una metodología de evaluación de cuatros fases, como configurar y utilizar las herramientas para realizar pruebas de seguridad Web satisfactorias. Comprender como se realiza la comunicación entre todas las partes involucradas en una aplicación web. Seleccionar y utilizar los diferentes métodos además de técnicas realizar los ataques más relevantes, como por ejemplo: Inyección de Comandos, Recorridos de Directorios, Inyección SQL, Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF), Hackear sitios Web e infiltrase en las organizaciones a través de sus páginas web.

Aval Internacional

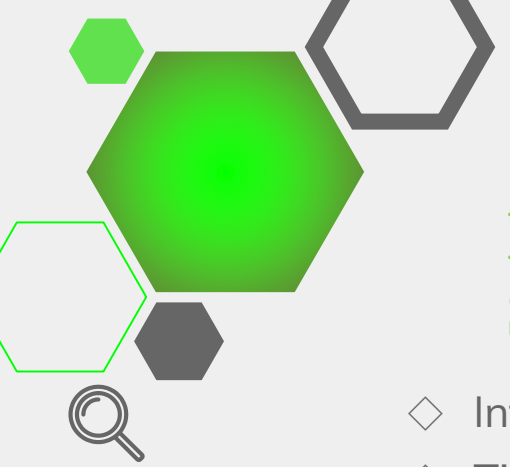
- Este curso es tipo certificación avalado internacionalmente por el **CERT Cyberseg** (Centro de Respuestas a Incidentes de Seguridad Informática de Guatemala, certificado por FIRST, OEA, ITU, Universidad Cernegie Mellon; con presencia y liderazgo internacional)

Aval Nacional

- Empresa y Capacitadores certificados como Operadores de Capacitación Profesional por la Secretaría Técnica de Capacitación y Formación Profesional del Ecuador - SETEC.

SECRETARÍA TÉCNICA
DEL **SISTEMA NACIONAL DE**
CUALIFICACIONES PROFESIONALES

CONTENIDOS



MÓDULO 1. FUNDAMENTOS DE SEGURIDAD WEB

- Introducción a la seguridad de las aplicaciones web
- Tipos de pruebas que se le pueden realizar a un sitio web
- Tipos de evaluación de seguridad que se le hace un sitio web
- OWASP-TOP 10
- Generalidades y Arquitectura de un sitio Web
- El protocolo HTTP
- Cookies
- Proyecto DVWA (Damn Vulnerable Web App).
- Vectores de ataque a aplicaciones web.

MÓDULO 2: ATAQUES WEB COMUNES PARTE 1

- Adquisición de información
- XSS Cross Site Scripting
- Cross Site Request Forgery (CSRF)
- SQL Injection y SQL ciega (SQLi)
- Inyección de comandos web

MÓDULO 3: ATAQUES WEB COMUNES PARTE 2

- File Inclusion
- Path Traversal
- Fuzzing de código
- Hacking Joomla

MÓDULO 4: HACKING WEB

- Session Hijacking
- SQL Injection extra
- Escaneo de Vulnerabilidades Web
- Herramientas para análisis de aplicaciones web
- Site Mirroring
- Criptografía
- Borrado de Logs

RETOS PRÁCTICOS – PLATAFORMA ONLINE – PARTE A

- Reto 1: Alterar código de Website de votos en línea
- Reto 2: Recuperación de Websites hackeados a través de formularios
- Reto 3: Hackear base de datos de un sitio web protegido con contraseña cifrada
- Reto 4: Hackear sitios web ganando acceso de administrador
- Reto 5: Hackear sistema de pagos de salario en línea
- Reto 6: Hackear un hosting para recuperar información almacenada
- Reto 7: Hackear plataforma de elecciones presidenciales en línea

RETOS PRÁCTICOS – PLATAFORMA ONLINE – PARTE B

- Reto 1: Recuperación de Websites hackeados
- Reto 2: Identificar usuarios (CUENTAS DE CORREO) de sitios usados para Cyberdelitos
- Reto 3: Descencriptar correos electrónicos cifrados
- Reto 4: Hackear website bancario
- Reto 5: Hackear website de un colegio y adulterar notas
- Reto 6: Hackear un servidor proxy y borrar las reglas de navegación
- Reto 7: Hackear hosting para obtener evidencia informática

INSTRUCTOR

- Ing. Galoget Latorre, Ingeniero en Sistemas Informáticos y de Computación de la Escuela Politécnica Nacional (EPN). Fundador & CEO del Grupo de Investigación en Software Libre y Seguridad Informática Hackem Research Group.

  Investigador y colaborador en Proyectos Internet of Things (IoT) con Technische Universiteit Delft (TU Delft) (Países Bajos) y Technische Universität München (TUM) (Alemania).

  Ex-Presidente IEEE Computer Society [EPN], Líder OWASP Ecuador [EPN], Embajador del Proyecto Fedora GNU Linux & Mozilla en Ecuador. Miembro ISACA Ecuador y Criptored.

  Docente/Instructor en el Centro de Educación Continua de la Escuela Politécnica Nacional (CEC-EPN).

Requisitos del Participante

- El alumno deberá tener conocimientos medios de redes, sistemas operativos, seguridad informática en infraestructura IT y Ethical Hacking.

Metodología

Luego de una exposición de los contenidos de cada capítulo, se llevará a cabo talleres participativos en grupos de trabajo para encontrar soluciones a escenarios planteados por el instructor promoviendo de esa forma la aplicación práctica de los conocimientos impartidos.

Evaluación

Se tomará en cuenta parámetros como:

- Participación en clase
- Presentación de resultados individuales o grupales
- Evaluación final online (Se deberá superar el 70% de la calificación total para la emisión de la certificación)

Recursos didácticos para el curso

Se dispondrá del contenido del curso en presentaciones y documentos con información complementaria actualizada y material para los talleres.

Recursos hardware para el curso

Se proveerá de los siguientes elementos de hardware y comunicaciones:

- Una estación de trabajo para cada estudiante con Windows 10 capacidad de operar máquinas virtuales.
- Interconexión de red entre las estaciones.
- Conexión a Internet controlada.
- Un servidor de mayor capacidad para colocar las máquinas virtuales comunes para los estudiantes.

Fechas y Horarios

27 al 31 de Mayo 2019

6pm a 9pm

Modalidad Presencial 16 horas

Inversión

Profesionales:
USD 280,00 + IVA

Descuento para Estudiantes:
USD 230,00 + IVA

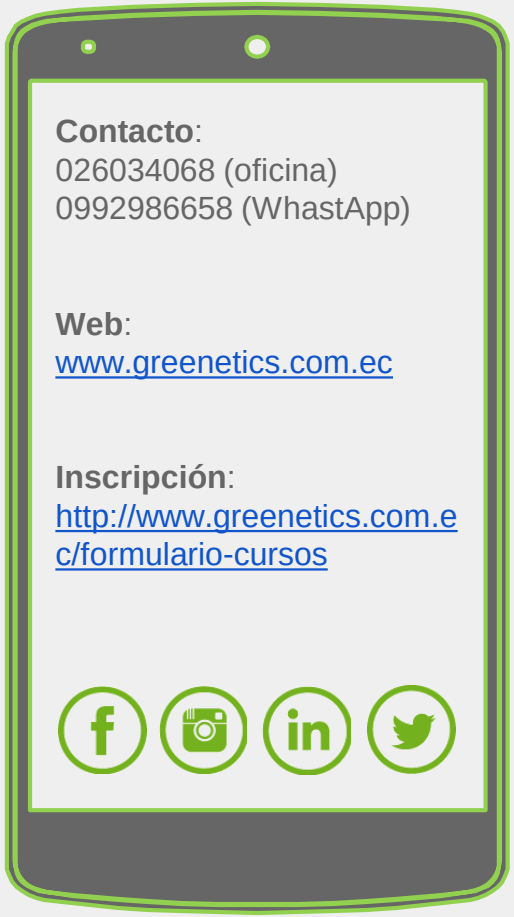
- Aceptamos todas las tarjetas, efectivo, o transferencia,
- Descuentos por grupo de interesados (más de 4),
- Para acceder al descuento estudiantil es necesario presentar documento de acreditación,
- Los precios no incluyen IVA

Incluye

- Material exclusivo y de uso confidencial.
- Un computador por participante (Curso Calendarizado).
- Refrigerios, almuerzos (Curso Calendarizado).

- **Certificado de aprobación del curso por 16 horas de duración**
- Certificado avalado por **CERT-CYBERSEG** (**Guatemala**).
- Contenidos, programa e instructores reconocidos por el **Ministerio de Trabajo**
- Empresa y Capacitadores certificados por la **Secretaría Técnica de Capacitación y Formación Profesional del Ecuador.**

Contacto



Dirección del Curso:
Av. Shyris N34-328 y Av. Portugal, Ed. SMERALD of 803. Junto a la sede de Alianza PAÍS.

Derechos Reservados