greenetics

Certificación en Ethical Hacking Módulo Básico

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.

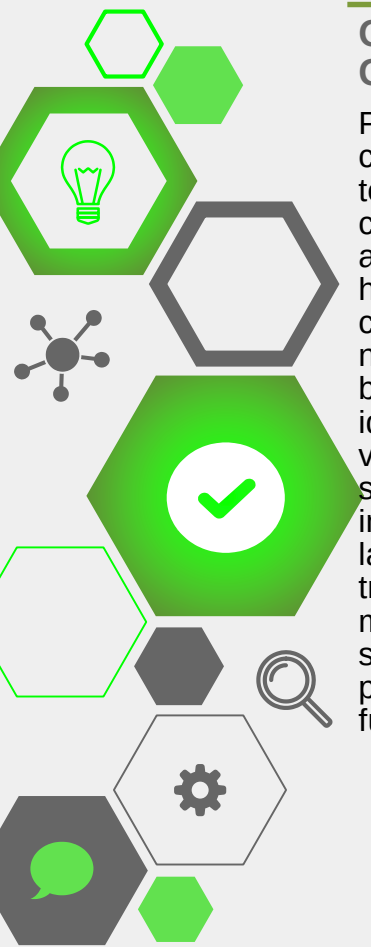
En Greenetics, nuestro objetivo es proporcionar sistemas seguros. Con las medidas necesarias, su empresa puede crecer más rápido y operar de manera más eficaz y, al mismo tiempo, preservar tanto la seguridad como la protección de los datos.

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 Y TEST DE PENETRACIÓN INFORMÁTICA BÁSICO

- El curso de ETHICAL HACKING Y TEST DE PENETRACIÓN INFORMÁTICA BÁSICO está orientado a toda persona que esté interesada en iniciarse en el mundo del Hacking Ético, de manera que pueda comprender las técnicas y herramientas básicas que utilizan los hackers actualmente para realizar un ataque.
- Durante las clases se realizarán ataques reales contra equipos y sistemas informáticos. Se atacará protocolos conocidos, redes sociales, computadores, dispositivos móviles, evadiendo sistemas de defensa en punto final, perimetrales, entre otros.

Estructura del Curso



Objetivo General

Proporcionar conocimientos teóricos y prácticos con la finalidad de adquirir las habilidades y conocimientos necesarios para buscar, detectar e identificar vulnerabilidades en sistemas informáticos sobre las cuales se trabajaran para mejorar la seguridad y evitar posibles ataques futuros.

En este curso aprenderás a:

Entender los fundamentos de Hacking y los diferentes tipos de hacking.

Dominar técnicas y usos del footprint.

Entender el funcionamiento de los robots utilizados por Google y otros buscadores

Crear un laboratorio de hacking desde cero.

Dominar el manejo de sistemas operativos utilizados para hacking.

Entender términos relacionados con networking.

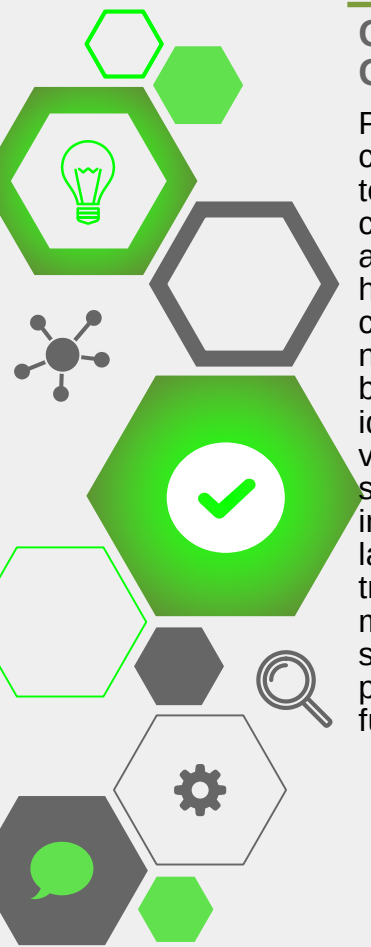
Dominar técnicas de búsqueda de información en fuentes abiertas y cerradas.

Aprender a escanear, enumerar, y hackear sistemas complejos de computación.

Entender los conceptos de Sniffing, Malware, y cómo identificarlos, evitarlos y enmendarlos en sistemas informáticos complejos.

Utilizar las herramientas para hackers

Qué es, cómo hacer, y cómo evitar que hagan Ingeniería Social tanto a individuos como a entornos corporativos. (Ejemplo: Phishing)



Objetivo General

Proporcionar conocimientos teóricos y prácticos con la finalidad de adquirir las habilidades y conocimientos necesarios para buscar, detectar e identificar vulnerabilidades en sistemas informáticos sobre las cuales se trabajaran para mejorar la seguridad y evitar posibles ataques futuros.

En este curso aprenderás a:

Conocer los ataques comunes

Introducción a la herramienta de explotación Metasploit

Hackear conexiones inalámbricas WiFi.

Aprender a crear software malicioso tanto para PC´s como para dispositivos móviles.

Comprender las metodologías de hacking

Determinar la ubicación de un equipo a través de su dirección IP

Identificar los servidores de eMail y DNS de una empresa

Identificar direcciones de eMail válidas de un dominio

Realizar escaneos de puertos TCP y UDP

Identificar versiones de software remotamente

Más de 20 demos y talleres prácticos de hacking y análisis de vulnerabilidades con diferentes herramientas.
Ejercicios de “CAPTURA LA BANDERA”

Certificación

- 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)

CONTENIDOS

MÓDULO 1. GENERAL

- Introducción al curso
- Contenido del curso
- Metodología del curso
- Advertencia del curso
- Requerimientos del curso

MÓDULO 2. ESCENARIO DE ATAQUE

- Laboratorios
- Virtualización y sistemas operativos para HACKING
- Manejo de Sistema Operativo orientado al HACKING
- Networking

MÓDULO 3. PENTESTING

- Introducción al pentesting
- Porqué es necesario un test de intrusión
- Qué buscamos en un test de intrusión
- Introducción al mundo del Hacker
- ¿Qué sabe un hacker?
- Tipos de hackers y por qué hackear
- Introducción a Metasploit y creación de códigos maliciosos
- Phishing de redes sociales – Obtener contraseñas

MÓDULO 4. HACKING

- Ciclo del Hacking
- Reconocimiento: Introducción a Google Hacking
- Escanear: Introducción a nmap
- Ganar acceso: Introducción a ataques de fuerza bruta y creación de diccionarios
- Mantener acceso: Introducción a backdoors
- Eliminar evidencia: Introducción a interpretación de logs

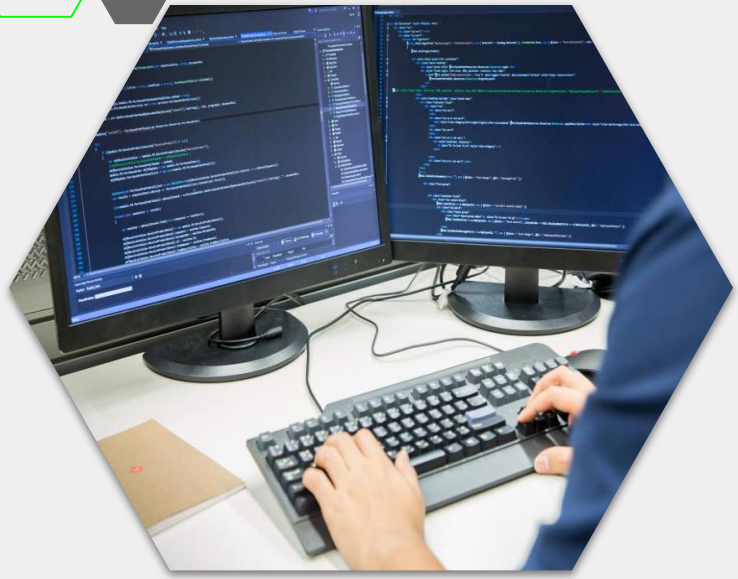
MÓDULO 5. ATAQUES

- Ataques y engaños más comunes
- Ataques a PC´s (creación de virus)
- Ingeniería social
- Ataques a dispositivos móviles – ANDROID (creación de APKs maliciosas)
- Wireless Pentesting

INSTRUCTORES

- Ing. Marco Rivadeneira, MBA, GCEH, GFI, Ingeniero en Electrónica y Redes de la Universidad Politécnica del Ecuador y Máster en Dirección de Empresas de la Universidad Complutense de Madrid – España. Ex Coordinador Nacional del *Computer Emergency Response Team* del Ecuador - ECUCERT, experto consultor de Ciberseguridad para el sector público y privado. Conferencista a nivel Nacional e Internacional en temas de Ciberseguridad. Ganador de varios juegos de Guerra Cibernética a nivel internacional.

- Ing. Diego Guacho, GCEH, GFI. Ingeniero en Electrónica y Redes de la Universidad Politécnica del Ecuador. Experto en seguridad informática, análisis de Malware e ingeniería reversa Analista Forense de Seguridad. Ganador de varios juegos de Guerra Cibernética a nivel internacional.
- **Apoyo**: Ing. Óscar Acevedo, CISSP, CISA, CEH. CEO Cyberseg (Guatemala) Remoto – virtual. Director y fundador del *Computer Emergency Response Team* de



Dirigido a

- Personas que quieren iniciarse en el mundo de la Ciberseguridad.
- Estudiantes técnicos que desean especializarse en Ciberseguridad.
- Profesionales y estudiantes técnicos vinculados a las áreas informáticas, redes de computadoras, bases de datos y telecomunicaciones.
- Administradores de redes de computadoras en general, y específicamente quienes tienen a su cargo un servidor Linux o Windows.
- Profesionales de Tecnología y otras áreas con interés en gestionar las áreas de Seguridad de la Información.

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

17 y 18 de Noviembre

8am a 5pm

Modalidad Presencial
20 horas académicas

Inversión

Profesionales:
USD 280,00 + IVA

Descuento para Estudiantes:
USD 230,00 + IVA

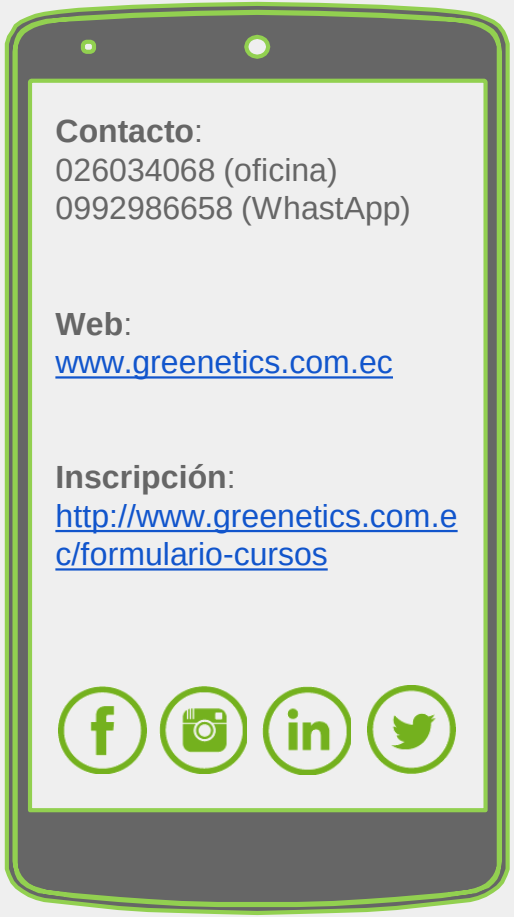
- Aceptamos todas las tarjetas, efectivo, o transferencia,
- Descuentos por grupo de interesados (más de 4),
- Para acceder al descuento estudiantil es necesario presentar documento de acreditación,
- Los precios no incluyen IVA
- Paypal por medio de nuestra página web www.greenetics.com.ec, sección de Inscripciones.

Incluye

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

- **Certificado de aprobación del curso por 20 horas de duración (20 créditos académicos)**
- 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.