greenetics
CUIDANDO TUS PASOS

CERTIFICACIÓN EN GUERRA CIBERNÉTICA CON MENCIÓN EN ETHICAL HACKING OFENSIVO AVANZADO

Greenetics Academy

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.

NUESTROS SERVICIOS

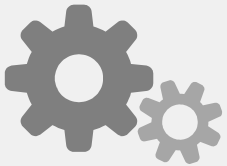
Auditoría de Sistemas	Informática Forense	Consultoría en Seguridad
Centro de respuesta de incidentes	Seguridad (Outsourcing)	Seguridad Perimetral
Capacitación Certificaciones	SGSI	Pentesting

greenetics
CUIDANDO TUS PASOS

Greenetics Academy

CURSO EN GUERRA CIBERNÉTICA CON MENCIÓN EN ETHICAL HACKING OFENSIVO BÁSICO

- El curso 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.
- Se enfoca en capacitar al alumno, para aprender y desarrollar, las distintas técnicas de hacking utilizadas por los atacantes informáticos, con el objetivo de comprometer la infraestructura de TIC de una organización y tener un conocimiento para prevenir estos incidentes, así como la capacidad de reaccionar en tiempo real cuando un ataque ocurre.
- Por otro lado también permite incorporar a los participantes, en el desarrollo de proyectos reales de Ethical Hacking ofensivo, pasando por las diferentes etapas, documentación requerida, y entregables de sustentación de este tipo de servicios.



Estructura del Curso

Objetivo General

Proporcionar conocimientos teóricos y prácticos con la finalidad de mejorar 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 avanzados de la Guerra Cibernética y el Hacking ofensivo.
Mejorar y ampliar el uso de un laboratorio de hacking y guerra cibernética.
Dominar el manejo de sistemas operativos utilizados para hacking.
Aprender a escanear, enumerar, y hackear sistemas complejos de computación.
Manejar técnicas avanzadas de Sniffing, creación de Malware, y cómo identificarlos, evitarlos y enmendarlos en sistemas informáticos complejos.
Utilizar las herramientas avanzadas para hackers.
Llevar a cabo los ataques más comúnes y utilizados en la actualidad.
Manejo avanzado de la herramienta de explotación Metasploit
Crear y ofuscar software malicioso tanto para PC´s como para dispositivos móviles.
Manejar los roles del Red Team y del Blue Team en una organización.
Mantener estrategias para prevenir ataques cibernéticos.
Desarrollar esquemas de respuesta inmediata frente a ataques cibernéticos.

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

greenetics
CUIDANDO TUS PASOS

Greenetics Academy

CONTENIDOS

MÓDULO 1. ESCANEO Y ANÁLISIS DE VULNERABILIDADES

- Manejo avanzado, escaneo de vulnerabilidades y scripting con NMAP.
- El Escáner de Vulnerabilidad OpenVAS
- Configuración inicial de OpenVAS
- El Escáner de Vulnerabilidad Nessus
- Uso de la herramienta Acunetix

MÓDULO 2: EXPLOTACIÓN DE VULNERABILIDADES

- Phising avanzado (Facebook, Hotmail, Paypal, Gmail)
- Uso de la herramienta Beef
- Trabajar con exploits
  - Búsqueda de explotaciones
  - Encontrar exploits en Kali Linux
  - Encontrar explotaciones en la web
- Escalada de privilegios.
  - Exploit de escalamiento de privilegios locales en Linux
  - Exploit de escalado de privilegios locales en el ejemplo de Windows

MÓDULO 3: HACKEO Y DEFENSA DE SERVIDORES

- Creación de diccionarios especializados
- Preparándose para la Fuerza Bruta
  - Archivos de diccionario
  - Fuerza bruta espacio-clave
  - Pwdump y Fgdump
  - Perfil de contraseña
- Ataques de contraseña en línea
  - Hydra, Medusa y Ncrack
- Contraseña Hash Attacks
  - Hashes de contraseña
  - Cracking de contraseña
  - Jhon de Ripper
- Manejo de RATS

MÓDULO 4: ATAQUES DE APLICACIONES WEB

- Cross Site Scripting (XSS)
  - Redirección del navegador e inyección de IFRAME
  - Robando cookies e información de sesión
- Vulnerabilidades de inclusión de archivos
  - Inclusión de archivos locales
  - Inclusión remota de archivos
- MySQL SQL Injection
  - Autenticación de bypass
  - Enumerar la base de datos
  - Enumeración del número de columna
  - Extraer datos de la base de datos
  - Aprovechar la inyección SQL para la ejecución de código
- Proxies de aplicaciones web
- Herramientas automatizadas de inyección SQL

MÓDULO 5: EL MARCO DE METASPLOIT

- Configuración de Metasploit Framework en Kali
- Explorando el marco de Metasploit
- Módulos auxiliares
  - Familiarizarse con la sintaxis de MSF
  - Acceso a la base de datos Metasploit
- Módulos de Explotación
- Metasploit Payloads
  - Meterpreter Payloads
  - Reverse HTTPS Meterpreter
  - Metasploit Exploit Multi Handler
- Post Explotación con Metasploit.
  - Características de la post-explotación del metro de prueba
  - Módulos posteriores a la explotación

MÓDULO 6: SOFTWARE BYPASSING ANTIVIRUS

- Codificación de cargas útiles con Metasploit
- Malware conocido cifrado con protectores de software
- Uso de herramientas personalizadas / no comunes y cargas útiles

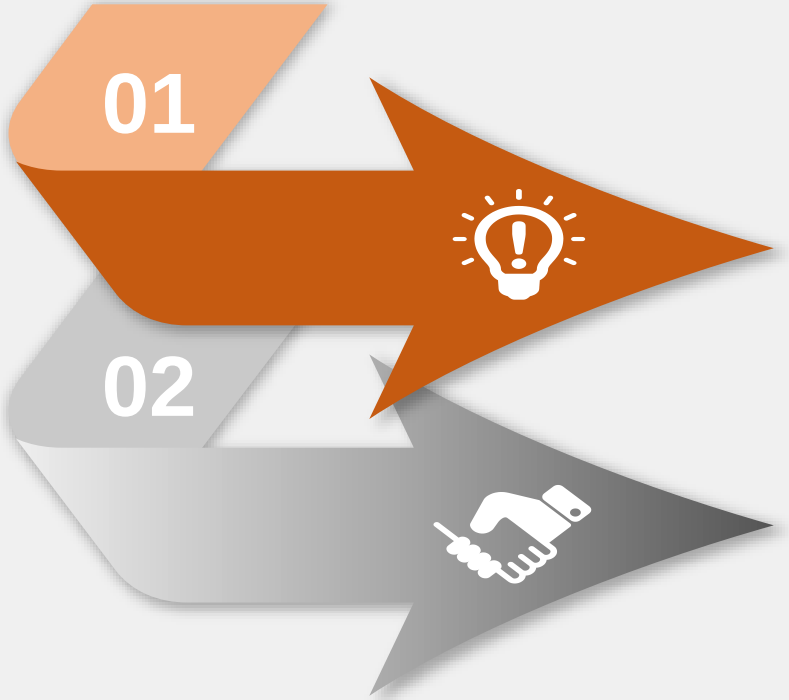
MÓDULO 7: ESCENARIOS DE GUERRA CIBERNÉTICA II

- Ejercicios de hacking web avanzados
- Modificación de parámetros WEB
- Criptografía
- Ejercicios tipo Capture de Flag.
- Ejercicios del tipo Cyberdrill.
- Manejo de plataformas de Guerra Cibernética
- Acciones de Blue Team
- Acciones de Red Team

Dirigido a

- 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.
- Gerentes de Sistema e Infraestructura
- Personal responsable de las áreas de Seguridad Informática o Seguridad de la Información.
- Profesionales de Tecnología y otras áreas con interés en gestionar las áreas de Seguridad de la Información.
- Oficiales de Seguridad de la Información designados.
- Personas responsables del área de Seguridad Informática
- Personas responsables del área de Seguridad de la Información

Requisitos del Participante



El alumno deberá tener conocimientos de redes, sistemas operativos (LINUX) y fundamentos básicos de seguridad informática en infraestructura IT.

Lenguajes de programación (de manera general)

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.

Inversión

USD 370,00 + IVA

- Aceptamos todas las tarjetas, efectivo, o transferencia,
- Descuentos por grupo de interesados (más de 4 personas),
- Los precios no incluyen IVA
- 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 24 horas de duración con AVAL NACIONAL. (SETEC).**
- **Certificado de aprobación del curso por 24 horas de duración avalado por CERT-CYBERSEG (Guatemala). AVAL INTERNACIONAL**
- 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.**

greenetics
CUIDANDO TUS PASOS

Greenetics Academy

Contactos

Contacto:
026034068 (oficina)
0992986658 (WhastApp)
0992795600 (WhastApp)

Web:
www.greenetics.com.ec

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

greenetics
CUIDANDO TUS PASOS

Greenetics Academy

Derechos Reservados

Se encuentra prohibida la copia y/o reproducción o en cualquier modo la explotación de este material sin la previa autorización legal escrita de la empresa GREENETICS SOLUCIONES S.A.
Sin embargo, usted podrá bajar el material a su computadora personal para uso exclusivamente personal o educacional y no comercial limitado a una copia por página.
De igual forma se prohíbe la publicación de este material en medios digitales y páginas web ajenas a la marca GREENETICS SOLUCIONES S.A.