ExecuTrain

Impulsamos tu talento tecnológico

MICROSOFT	RED HAT	VIRTUALIZACIÓN
CIBERSEGURIDAD	DESARROLLO	OFFICE
BIG DATA	BLOCK CHAIN	BASES DE DATOS
GESTIÓN DE SERVICIOS IT	CLOUD COMPUTING	METODOLOGÍAS EN PROYECTOS
SISTEMAS OPERATIVOS	Y MÁS...	

www.executrain.com.mx

¿Por qué ExecuTrain?

ExecuTrain es un proveedor de entrenamiento corporativo a nivel internacional y líder mundial en la capacitación empresarial. Contamos con más de 30 años de Experiencia y con más de 75 mil personas capacitadas a nivel Nacional.

Te guiamos en la definición de tus requerimientos de capacitación, en las diferentes etapas:

- ✓ Detección de necesidades, evaluación de conocimientos, plan de capacitación y seguimiento posterior para elegir el plan de capacitación como tú lo necesitas.
- ✓ El **más amplio catálogo de cursos**, desde un nivel básico hasta los niveles de conocimientos más especializados.
- ✓ En ExecuTrain el material y la **metodología están diseñados por expertos en aprendizaje humano**. Lo que te garantiza un mejor conocimiento en menor tiempo.
- ✓ Tú puedes confiar y estar seguro del aprendizaje porque nuestro **staff de instructores es de primer nivel**, algunos de los cuales son consultores en reconocidas empresas.
- ✓ No pierdas tu tiempo, los cursos están diseñados para un aprendizaje práctico.

Nuestro compromiso es que tú aprendas, si no quedas satisfecho con los resultados del programa, podrás volver a tomar los cursos hasta tu entera satisfacción o la devolución de tu dinero.

Modalidad de Servicio

Cursos en Fecha Calendario

Súmate a nuestros grupos en fechas públicas.

Cursos Privados

On site, en nuestras instalaciones o en línea con instructor en vivo.

Autoestudio con soporte de instructor

Cursos en modalidad autoestudio, con acceso 24/7 a la plataforma de estudio, con soporte de instructor y foros de ayuda

ExecuTrain
Impulsamos tu talento tecnológico

Duración: 40 horas

Seguridad / Certified Ethical Hacker (CEH v13 AI)

Al unirte a la Revolución de la IA como Certified Ethical Hacker, adquirirás la experiencia necesaria para desenvolverte en el mundo de la ciberseguridad de vanguardia. Los profesionales certificados en la última versión del CEH v13 están equipados con herramientas y técnicas impulsadas por inteligencia artificial para identificar, explotar y asegurar vulnerabilidades en sistemas y redes. Aprenderás a aprovechar la IA para automatizar la detección de amenazas, predecir brechas de seguridad y responder rápidamente a incidentes cibernéticos. Además, desarrollarás las habilidades necesarias para proteger tecnologías basadas en IA frente a amenazas potenciales. Esta combinación de hacking ético y capacidades en IA te posicionará a la vanguardia de la ciberseguridad, listo para defender a organizaciones de múltiples industrias frente a amenazas avanzadas y adaptarte a desafíos en constante evolución.

Potencia tu ventaja como Certified Ethical Hacker con capacidades impulsadas por IA:

- Conocimiento avanzado: Como Certified Ethical Hacker potenciado por IA, contarás con un conocimiento profundo de metodologías de hacking ético, mejorado con técnicas de inteligencia artificial de última generación.
- Integración de IA: Aplicarás la IA de forma efectiva en cada fase del hacking ético, desde el reconocimiento y escaneo, hasta la obtención y mantenimiento del acceso, así como el ocultamiento de huellas.
- Automatización y eficiencia: Utilizarás la IA para automatizar tareas, aumentar la eficiencia y detectar amenazas sofisticadas que los métodos tradicionales podrían no identificar.
- Defensa proactiva: Con el respaldo de la IA, estarás preparado para la búsqueda proactiva de amenazas, detección de anomalías y análisis predictivo para prevenir ciberataques antes de que ocurran.

Perfil de la audiencia

- ✓ Profesionales de TI y ciberseguridad con experiencia en redes, sistemas o seguridad de la información.
- ✓ Quienes buscan integrar IA a sus procesos de hacking ético, pentesting y defensa.
- ✓ Aquellos que desean adelantarse a las amenazas futuras y reforzar la postura defensiva en sus organizaciones.

Prerrequisitos

Se recomienda que los participantes cuenten con al menos dos años de experiencia laboral en seguridad de la información o tecnologías de la información. También es ideal que tengan familiaridad con entornos Windows y Linux, así como comprensión de protocolos de red, firewalls y herramientas de administración de sistemas, ya que el curso profundiza en técnicas prácticas de hacking ético y uso de herramientas avanzadas impulsadas por inteligencia artificial.

Módulos

Módulo 01 – Introducción al Hacking Ético

- Aprende los fundamentos y aspectos clave de la seguridad de la información, incluyendo los conceptos básicos del hacking ético, controles de seguridad, leyes relevantes y procedimientos estándar.

Módulo 02 – Footprinting y Reconocimiento

- Aprende a utilizar las técnicas y herramientas más recientes para realizar footprinting y reconocimiento, una fase crítica previa a un ataque en el hacking ético.

Módulo 03 – Escaneo de Redes

- Conoce las distintas técnicas de escaneo de redes y las contramedidas para protegerte contra ellas.

Módulo 04 – Enumeración

- Aprende diversas técnicas de enumeración, incluyendo exploits del Protocolo de Puerta de Enlace Fronteriza (BGP) y Compartición de Archivos en Red (NFS), así como las contramedidas asociadas.

Módulo 05 – Análisis de Vulnerabilidades

- Aprende a identificar brechas de seguridad en la red, la infraestructura de comunicación y los sistemas finales de una organización. También se cubren los tipos de evaluaciones de vulnerabilidades y las herramientas utilizadas.

Módulo 06 – Hacking de Sistemas

- Conoce las metodologías de hacking de sistemas empleadas para descubrir vulnerabilidades, incluyendo esteganografía, ataques de esteganálisis y técnicas para ocultar rastros.

Módulo 07 – Amenazas de Malware

- Estudia los distintos tipos de malware (troyanos, virus, gusanos, etc.), malware sin archivos y APTs, procedimientos de análisis de malware y contramedidas.

Módulo 08 – Sniffing (Escucha de Paquetes)

- Aprende sobre las técnicas de sniffing de paquetes, cómo se usan para detectar vulnerabilidades de red y las contramedidas para protegerse contra estos ataques.

Módulo 09 – Ingeniería Social

- Descubre los conceptos y técnicas de ingeniería social, cómo detectar intentos de robo de identidad, auditar vulnerabilidades humanas y aplicar contramedidas.

Módulo 10 – Denegación de Servicio (DoS)

- Estudia las técnicas de ataque de Denegación de Servicio (DoS) y Denegación Distribuida de Servicio (DDoS), las herramientas utilizadas para auditar un objetivo y las contramedidas aplicables.

Módulo 11 – Secuestro de Sesiones (Session Hijacking)

- Aprende sobre las técnicas de secuestro de sesiones para detectar debilidades en la gestión de sesiones, autenticación, autorización y criptografía, así como las contramedidas.

Módulo 12 – Evasión de IDS, Firewalls y Honeypots

- Conoce las técnicas para evadir sistemas de detección de intrusos (IDS), firewalls y honeypots, las herramientas utilizadas para auditar el perímetro de la red y las contramedidas.

Módulo 13 – Hacking de Servidores Web

- Aprende sobre los ataques a servidores web, incluyendo una metodología completa para auditar vulnerabilidades en la infraestructura de servidores web y sus contramedidas.

Módulo 14 – Hacking de Aplicaciones Web

- Explora los ataques a aplicaciones web y una metodología completa de hacking para auditar vulnerabilidades y aplicar contramedidas.

Módulo 15 – Inyección SQL (SQL Injection)

- Estudia las técnicas de ataque por inyección SQL, métodos de evasión y las contramedidas correspondientes.

Módulo 16 – Hacking de Redes Inalámbricas

- Aprende sobre los tipos de cifrado, amenazas, metodologías de ataque, herramientas de hacking y de seguridad, así como contramedidas para redes inalámbricas.

Módulo 17 – Hacking de Plataformas Móviles

- Explora los vectores de ataque en plataformas móviles, hacking en Android e iOS, gestión de dispositivos móviles, directrices de seguridad y herramientas.

Módulo 18 – Hacking de IoT

- Conoce los diferentes tipos de ataques a dispositivos de Internet de las Cosas (IoT) y tecnología operativa (OT), metodologías de hacking, herramientas utilizadas y contramedidas.

Módulo 19 – Computación en la Nube

- Aprende conceptos clave sobre la nube, incluyendo tecnologías de contenedores y cómputo sin servidor, amenazas, ataques y técnicas de seguridad en la nube.

Módulo 20 – Criptografía

- Estudia algoritmos de cifrado, herramientas criptográficas, infraestructura de clave pública (PKI), cifrado de correos y discos, ataques criptográficos y herramientas de criptoanálisis.

Examen de Conocimientos – CEH Knowledge-Based Exam

- El examen teórico de CEH es una evaluación de cuatro horas con 125 preguntas de opción múltiple, diseñada para poner a prueba tus habilidades en temas clave como: amenazas de seguridad de la información, vectores de ataque, detección y prevención de ataques, procedimientos, metodologías y más.
- Este examen es reconocido a nivel mundial como la certificación táctica de ciberseguridad más confiable y original.