



ExecuTrain

Impulsamos tu talento tecnológico

- Aplicaciones Móviles
- Colaboración
- Mejores Practicas
- Sistemas Operativos
- Bases de datos
- Cloud Computing
- Office
- Virtualización
- Big Data
- Desarrollo
- Seguridad

Tel: 33 3647 6622

ventas@executrain.com.mx

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 28 años y más de 62 mil personas capacitadas en zona occidente.

¿Por qué ExecuTrain?

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.
- Nuestra garantía: 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 de Calendario
- Cursos Privados: On site y en nuestras instalaciones.
- Cursos Personalizados: Adaptamos el contenido del curso y su duración dependiendo de la necesidad del cliente.
- E-Training: cursos a distancia de forma interactiva, mejorando la capacidad de aprendizaje de nuestros participantes guiados por un instructor en vivo.

Duración: 16 horas

Seguridad / Fundamentals of Ethical Hacking and Penetration

Con el Curso de Especialista en Seguridad Ofensiva, se busca proveer a los participantes con los conocimientos necesarios para realizar pruebas de Seguridad Ofensiva utilizando tácticas, técnicas y procedimientos para emular amenazas del mundo real con el fin de medir la efectividad de las personas, los procesos y la tecnología utilizada para proteger a las organizaciones. Al finalizar, el alumno realizará una práctica basada en un escenario realista donde podrá aplicar las habilidades adquiridas en este curso.

> Perfil de la audiencia

- Profesionales de tecnologías de la información que desean especializarse en seguridad
- Profesionales de seguridad interesados en incrementar sus conocimientos en el área ofensiva
- Profesionales dedicados a la seguridad defensiva y quieren conocer a profundidad las metodologías herramientas y técnicas que usan los atacantes
- Especialistas en computo forense que quieren entender mejor las técnicas ofensivas

> Prerrequisitos

- Conocimientos de TCP/IP y Redes
- Conocimientos básicos de Sistemas Operativos Linux y Windows
- Conocimientos básicos de scripting.

> Instructor

Roberto Martínez

Analista de Malware | Equipo Global de Investigación y Análisis (GReAT) | América Latina, Kaspersky Lab

Roberto forma parte del grupo de cerca de 800 investigadores a nivel mundial del “Equipo Global de Investigación y Análisis” (GREAT) asignado a la región de América Latina de Kaspersky Lab y es responsable de monitorear y detectar nuevas amenazas cibernéticas en la región.

Se desempeñó durante 5 años como consultor para ITelligent Security y como instructor de EC-Council para Latinoamérica y España, ganando durante 2 años consecutivos el premio como mejor Instructor del año en entrenamientos de Seguridad Informática.

Ha trabajado como Asesor Internacional de Gobiernos, Servicios de Inteligencia y Militares, así como de diversas Instituciones Financieras y Privadas en Latinoamérica.

Es miembro de la Asociación de Seguridad Informática Mexicana (AMSI), Mexico Security Professionals, Digital Forensics Association (DFA), Redteam: Association of Penetration Testers y también pertenece al grupo Cyberwar & Cybercrime.

Realizó estudios en la Universidad de Guadalajara y Universidad Tec Milenio del Tecnológico de Monterrey

> Esquema del curso

Módulos

- Offensive Security Fundamentals
- Penetration Testing vs. Red Teaming Concepts
- Social Engineering
- Offensive Security Arsenal: Kali
- Offensive Security Arsenal: NMAP
- Offensive Security Arsenal: Metasploit
- Offensive Security Arsenal: Burp Suite
- Attacking Network Protocols
- Bypassing Security Controls
- Penetration Testing in Web Environments
- Penetration Testing in Cloud Services
- Perimeter Penetration Testing
- Penetration Testing in Mobile Applications
- Penetration Testing DataBases
- Penetration Testing Desktop Applications
- Developing exploits
- Developing tools using C#, PowerShell, Python, Go