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 Penetration Testing Professional CPENT[AI]

El curso Certified Penetration Testing Professional (C | PENT) prepara a los profesionales para dominar las metodologías, herramientas y técnicas más avanzadas de penetration testing impulsadas por inteligencia artificial. A través de un enfoque completamente práctico, los participantes adquieren experiencia real en todos los fases del pentesting, desde la planeación y alcance de pruebas hasta la ejecución y elaboración de reportes. El programa incluye más de 110 laboratorios, rangos cibernéticos en vivo, y cinco entornos multidisciplinarios (Active Directory, Binaries, IoT, Web y CTF) que replican redes empresariales complejas. Además, enseña a aplicar técnicas de automatización y análisis con IA, desarrollar scripts personalizados, y utilizar marcos globales como MITRE ATT&CK y Cyber Kill Chain. Al finalizar, los participantes validan sus habilidades en un examen 100% práctico, obteniendo la certificación internacional C | PENT y, con puntuación destacada, la Licensed Penetration Tester (LPT), consolidándose como expertos en ofensiva y defensa cibernética de nivel profesional.

Perfil de la audiencia

El curso C | PENT está diseñado para profesionales de ciberseguridad y especialistas en pruebas de penetración que buscan llevar sus habilidades técnicas a un nivel avanzado mediante el uso de herramientas y metodologías impulsadas por inteligencia artificial. Está dirigido a quienes desempeñan o aspiran a desempeñar roles como:

- ✓ Penetration Tester o Ethical Hacker.
- ✓ Consultor o Ingeniero de Pruebas de Penetración.
- ✓ Analista o Especialista en Vulnerability Assessment y VAPT.
- ✓ Integrante o líder de Red Teams u Offensive Security.
- ✓ Ingeniero o asesor en seguridad aplicada a IA y aprendizaje automático.
- ✓ Desarrolladores o arquitectos de seguridad que deseen fortalecer su conocimiento en explotación, evasión y defensa avanzada.

Ideal para profesionales que desean validar su experiencia a nivel global y demostrar dominio práctico en entornos reales de ciberseguridad.

Prerrequisitos

Para aprovechar al máximo el curso C | PENT, se recomienda que los participantes:

- ✓ Cuenten con conocimientos sólidos en seguridad informática, redes y sistemas operativos (Windows y Linux).
- ✓ Tengan experiencia previa en pruebas de penetración, análisis de vulnerabilidades o administración de seguridad.
- ✓ Posean familiaridad con herramientas como Metasploit, Nmap, Burp Suite, Wireshark y entornos de scripting (Python, Bash, PowerShell, etc.).
- ✓ Hayan cursado o tengan el nivel equivalente de certificaciones como Certified Ethical Hacker (C | EH) o EC-Council Certified Security Analyst (ECSA).
- ✓ Comprendan los fundamentos de marcos globales de ciberseguridad como MITRE ATT&CK o Cyber Kill Chain.

Estos conocimientos previos permitirán desarrollar con éxito las habilidades avanzadas que exige el programa y obtener el máximo rendimiento del entrenamiento práctico y los laboratorios en vivo

Lo que aprenderás

- Aplicar una metodología completa de pruebas de penetración, desde la planeación, alcance y reglas de compromiso hasta la ejecución y presentación de resultados.
- Utilizar inteligencia artificial para potenciar el pentesting, automatizando tareas, detectando vulnerabilidades y simulando ataques reales con herramientas como ChatGPT, ShellGPT y PentestGPT.
- Recolectar y analizar inteligencia de fuentes abiertas (OSINT) para mapear la superficie de ataque y planificar estrategias ofensivas.
- Ejecutar pruebas de ingeniería social y evaluar la seguridad humana mediante técnicas de persuasión y manipulación ética.
- Identificar y explotar vulnerabilidades en aplicaciones web, APIs y sistemas IoT, abordando fallos comunes como inyección SQL, XSS o configuraciones inseguras.
- Superar mecanismos de defensa perimetral como firewalls, IDS/IPS y filtros de red mediante técnicas avanzadas de evasión.
- Explotar vulnerabilidades en entornos Windows, Linux y Active Directory, escalando privilegios y realizando movimientos laterales dentro de la red.
- Aplicar técnicas de ingeniería inversa, fuzzing y explotación binaria para detectar fallos en software y desarrollar exploits personalizados.
- Dominar el uso de scripting en Python, PowerShell, Bash y otros lenguajes para automatizar ataques, análisis y reportes.
- Realizar pruebas especializadas en entornos OT, SCADA, nube y dispositivos móviles, emulando escenarios empresariales reales.
- Acceder y pivotar en redes ocultas, aplicando técnicas únicas de doble pivoting y movimiento lateral.
- Documentar y presentar hallazgos profesionales mediante reportes técnicos claros y recomendaciones accionables para mitigar riesgos.
- Prepararte para un examen 100% práctico, demostrando tus capacidades ofensivas y defensivas en entornos reales de laboratorio.

Módulos

Módulos principales :

- Introducción a las pruebas de penetración y metodologías.
- Alcance y planeación de pruebas de penetración (Scoping and Engagement).
- Inteligencia de fuentes abiertas (OSINT) y mapeo de superficie de ataque.
- Pruebas de ingeniería social.
- Pruebas de penetración en aplicaciones web.
- Pruebas de penetración en API y JSON Web Tokens.
- Técnicas de evasión de defensa perimetral.
- Explotación y escalación de privilegios en Windows.
- Pruebas de penetración en Active Directory.
- Explotación y escalación de privilegios en Linux.
- Ingeniería inversa, fuzzing y explotación binaria.
- Movimiento lateral y pivoting.
- Pruebas de penetración en IoT.
- Elaboración de reportes y acciones posteriores a la prueba.

Módulos de autoestudio

- Conceptos esenciales de pruebas de penetración.
- Dominio del marco Metasploit Framework.
- Scripting en PowerShell.
- Entorno y scripting en Bash.
- Entorno y scripting en Python.
- Entorno y scripting en Perl.
- Entorno y scripting en Ruby.
- Pruebas de penetración inalámbrica.
- Pruebas de penetración en sistemas OT y SCADA.
- Pruebas de penetración en la nube.
- Pruebas de penetración en bases de datos.
- Pruebas de penetración en dispositivos móviles.

Certified Penetration Testing Professional (C | PENT)

- Código de examen: 312-39
- Duración: 24 horas continuas o dos sesiones de 12 horas cada una.
- Formato: 100% práctico y totalmente supervisado (proctored).
- Entrega de resultados: El participante deberá entregar un reporte profesional de pentesting dentro de los 7 días posteriores al examen.

Certificaciones obtenidas:

- Certified Penetration Testing Professional (C | PENT) — al aprobar el examen práctico.
- Licensed Penetration Tester (LPT) — al obtener una calificación superior al 90% en el examen C | PENT.

Características del examen:

- Incluye cinco rangos de práctica que replican entornos empresariales reales:
  - Active Directory Range
  - Binaries Range
  - IoT Range
  - Web Range
  - Capture the Flag (CTF) Range
- Evalúa tanto habilidades técnicas como no técnicas, incluyendo planeación, ejecución, documentación y presentación de resultados.
- Las pruebas se desarrollan en escenarios de redes segmentadas con DMZ, VPN, firewalls y defensas de endpoint.