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: 8 semanas

Seguridad / Curso Fundamentos de Pentesting

Este curso se imparte en modalidad online y consta de 7 unidades y actividades prácticas. La duración del curso es de 60 horas que se distribuyen entre el contenido y las herramientas de colaboración. A su finalización, el alumno recibirá un diploma acreditativo.

La formación se realiza a través de nuestro Campus Virtual, con esta modalidad dispondrás de todo el contenido didáctico en la plataforma del curso y estará accesible, desde el día de inicio de curso, las 24 horas todos los días de la semana. El alumno también dispondrá de foros de participación, así como una tutorización continua.

El curso se dicta en modalidad de teleformación (opción 100% de bonificación) y también se pueden realizar acciones formativas presenciales y telepresenciales bajo demanda.

Objetivos

Este curso tiene como objetivo proporcionar una introducción general al **Pentesting (Pruebas de Penetración)** para usuarios sin experiencia técnica. Se enfoca en explicar conceptos clave, la importancia de la seguridad informática, las fases del Pentesting y cómo los usuarios no técnicos pueden contribuir a mantener un entorno digital seguro.

Dirigido a:

Este curso ofrece una base sólida en Pentesting y ciberseguridad para usuarios no técnicos, fortaleciendo su papel en la protección de los entornos digitales. Curso Fundamentos de Pentesting para Usuarios No Técnicos.

Modalidad

Las tarifas del curso se aplican a la modalidad de teleformación.

- Duración: 60 horas con acceso a la plataforma durante 8 semanas
- Soporte individualizado

Requisitos Previos

Para aprovechar al máximo este curso introductorio de Pentesting y ciberseguridad para usuarios no técnicos, los alumnos deberían preferiblemente contar con los siguientes requisitos previos:

- **Conocimientos básicos de informática:**
  - Familiaridad con el uso de sistemas operativos (Windows, macOS, o Linux).
  - Comprensión básica de términos informáticos como redes, software y hardware.
- **Experiencia básica en el entorno digital:**
  - Habilidad para usar navegadores web y programas de correo electrónico.
  - Conocimientos básicos sobre el manejo de archivos y carpetas.
- **Conciencia sobre ciberseguridad:**
  - Experiencia previa enfrentando situaciones como correos sospechosos o problemas relacionados con contraseñas puede ser útil.
  - Interés por entender cómo proteger datos personales y corporativos.
- **Habilidad para trabajar en equipo y comunicarse:**
  - Dado el enfoque en la colaboración entre perfiles no técnicos, es útil que los alumnos tengan habilidades interpersonales y de comunicación.
- **Interés en la ciberseguridad y el Pentesting:**
  - Curiosidad o motivación por aprender conceptos relacionados con la protección de datos y la seguridad informática.
- **Apertura al aprendizaje práctico:**
  - Disposición para realizar actividades prácticas, como identificar vulnerabilidades en ejemplos simulados o analizar resultados ficticios generados por herramientas.

Aunque el curso está diseñado para usuarios sin experiencia técnica, estos requisitos básicos ayudarán a los participantes a integrar mejor los conceptos y actividades prácticas presentadas.

Módulos

Unidad 1: Introducción al Pentesting

Objetivo: Comprender qué es el Pentesting y su relevancia en la ciberseguridad.

Temas:

- Definición de Pentesting.
- Diferencia entre Pentesting y hacking ético.
- Importancia del Pentesting en las empresas.
- Casos famosos de ciberataques y cómo se podrían haber prevenido.
- Actividad práctica: Identificar vulnerabilidades comunes en ejemplos simulados.

Unidad 2: Conceptos Básicos de Ciberseguridad

Objetivo: Familiarizarse con los conceptos fundamentales relacionados con la seguridad digital.

Temas:

- Qué son las vulnerabilidades, amenazas y riesgos.
- Tipos de ciberataques más comunes (phishing, ransomware, etc.).
- Buenas prácticas de ciberseguridad para usuarios no técnicos.
- Actividad práctica: Detectar elementos sospechosos en un correo electrónico ficticio.

Unidad 3: Las Fases del Pentesting

Objetivo: Conocer las etapas básicas de un proceso de Pentesting.

Temas:

- Reconocimiento: qué es y cómo se realiza.
- Escaneo: identificación de posibles puntos débiles.
- Explotación: ejemplos sencillos de cómo los atacantes pueden aprovechar vulnerabilidades.
- Reporte: la importancia de documentar los hallazgos.
- Actividad práctica: Crear un mini-reporte ficticio de vulnerabilidades observadas en una simulación.

Unidad 4: Herramientas de Pentesting

Objetivo: Introducir herramientas comunes utilizadas en Pentesting (sin necesidad de operar con ellas).

Temas:

- ¿Qué son las herramientas de Pentesting? (Ejemplo: Nmap, Metasploit, etc.).
- Cómo funcionan de manera básica.
- Rol de los usuarios no técnicos en la interpretación de resultados.
- Actividad práctica: Analizar resultados ficticios generados por herramientas y discutirlos.

Unidad 5: Cómo Identificar Riesgos en tu Organización

Objetivo: Capacitar a los usuarios para identificar posibles áreas de riesgo en sus entornos laborales.

Temas:

- Señales de alerta de un entorno inseguro.
- Evaluación básica de seguridad en dispositivos y redes.
- Rol del usuario en la prevención de ataques.
- Actividad práctica: Checklist para autoevaluación de seguridad en el lugar de trabajo.

Unidad 6: Rol de los Usuarios No Técnicos en el Pentesting

Objetivo: Resaltar la importancia de la colaboración de usuarios no técnicos en procesos de seguridad.

Temas:

- Cómo informar incidentes de manera efectiva.
- Contribuir a la seguridad mediante hábitos digitales seguros.
- Importancia de la educación continua en ciberseguridad.
- Actividad práctica: Simulación de reporte de incidente con ejemplos prácticos.

Unidad 7: Implementando una Cultura de Seguridad

Objetivo: Fomentar la construcción de una mentalidad de seguridad en el entorno laboral y personal.

Temas:

- Sensibilización sobre la ciberseguridad como responsabilidad compartida.
- Cómo organizar talleres o campañas de concienciación en la empresa.
- La importancia de la actualización de conocimientos.
- Actividad práctica: Crear un plan básico para una campaña de concienciación en ciberseguridad.

Evaluación del Curso

Examen final: Preguntas de opción múltiple sobre los conceptos principales.

- Proyecto práctico: Crear un reporte ficticio de ciberseguridad basado en una simulación proporcionada.