FORMACIÓN E-LEARNING

Curso Online de

Seguridad Informática para Sistemas Operativos Windows y Linux en Empresas

→ Técnicas de preparación y desarrollo de planes para la protección de la información en entornos Windows y Linux en empresas.

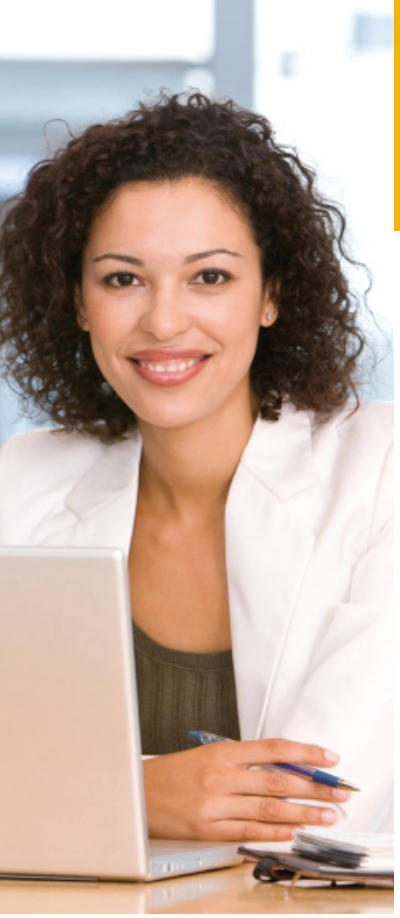
CURSO BONIFICABLE

Iniciativas Empresariales
estrategias de formación

MANAGER BUSINESS SCHOOL

Tel. 900 670 400 - attcliente@iniciativasempresariales.com
www.iniciativasempresariales.com

BARCELONA - BILBAO - MADRID - SEVILLA - VALENCIA - ZARAGOZA



Presentación

La información y su gestión han pasado a formar parte de la actividad cotidiana de las empresas. Los ordenadores almacenan información, la procesan y la transmiten a través de redes abriendo nuevas posibilidades, por ello cuanto mayor es el valor de la información gestionada, más importante es asegurarla.

Ante este reto, es necesario fortalecer la seguridad en las empresas con políticas y estrategias de seguridad destinadas a garantizar que toda implantación de nueva tecnología vaya acompañada de un adecuado entrenamiento y capacitación profesional y de un procedimiento de evaluación de los riesgos de seguridad para detectar vulnerabilidades y posibles amenazas de ataques.

El objetivo de este curso es aprender los aspectos teóricos y prácticos para asegurar un sistema informático haciendo uso de las últimas técnicas y tecnologías de seguridad. Para ello, una vez vistos los aspectos básicos sobre seguridad informática nos centraremos en sus diferentes etapas: prevención, detección de intrusos, copias de seguridad y análisis forense.

A lo largo del curso se utilizarán las diferentes herramientas que permiten asegurar los sistemas Windows y GNU/Linux.

La Educación On-line

Tras 15 años de experiencia formando a directivos y profesionales, Iniciativas Empresariales presenta sus cursos e-learning. Diseñados por profesionales en activo, expertos en las materias impartidas, son cursos de corta duración y eminentemente prácticos, orientados a ofrecer herramientas de análisis y ejecución de aplicación inmediata en el puesto de trabajo.

Los cursos e-learning de Iniciativas Empresariales le permitirán:

- **La posibilidad de escoger el momento y lugar más adecuado.**
- **Interactuar con otros estudiantes enriqueciendo la diversidad de visiones y opiniones y su aplicación en situaciones reales.**
- **Trabajar con más y diversos recursos que ofrece el entorno on-line.**
- **Aumentar sus capacidades y competencias en el puesto de trabajo en base al estudio de los casos reales planteados en este curso.**

Tel. 900 670 400 - attcliente@iniciativasempresariales.com - www.iniciativasempresariales.com

Método de Enseñanza

El curso se realiza on-line a través de la plataforma *e-learning* de Iniciativas Empresariales que permite, si así lo desea, descargarse los módulos didácticos junto con los ejercicios prácticos de forma que pueda servirle posteriormente como un efectivo manual de consulta.
A cada alumno se le asignará un tutor que le apoyará y dará seguimiento durante el curso, así como un consultor especializado que atenderá y resolverá todas las consultas que pueda tener sobre el material docente.
El curso incluye:

Aula Virtual | Tutor personal | Flexibilidad de horarios | Pruebas de Autoevaluación

Contenido y Duración del Curso

El curso tiene una duración de 80 horas y el material didáctico consta de:

Manual de Estudio
Corresponde a todas las materias que se imparten a lo largo de los 5 módulos de formación práctica de que consta el curso Seguridad Informática para Sistemas Operativos Windows y Linux en Empresas.

Material Complementario
Incluye ejemplos, casos reales, animaciones, presentaciones, etc. sobre la materia con el objetivo de ejemplificar y ofrecer recursos para la resolución de las problemáticas específicas de la seguridad informática.

Ejercicios de Seguimiento
Corresponden a ejercicios donde se plantean y solucionan determinados casos referentes a la seguridad informática.

Pruebas de Autoevaluación
Para la comprobación práctica de los conocimientos que Ud. va adquiriendo.

Curso Bonificable

Tel. 900 670 400 - attcliente@iniciativasempresariales.com - www.iniciativasempresariales.com

Este curso le permitirá saber y conocer:

- Cuáles son las mejores prácticas, los estándares y las recomendaciones más útiles sobre seguridad informática.
- Cuáles son los ataques informáticos más utilizados y su evolución en los últimos años.
- Qué metodologías utilizan más habitualmente los atacantes y cómo protegernos de ellas.
- Cómo analizar nuestro equipo para determinar sus posibles vulnerabilidades.
- Qué recomendaciones hay que seguir para asegurar un sistema informático a nivel físico y lógico.
- Qué diferentes topologías de red podemos utilizar para asegurar el sistema.
- Cuáles son las mejores tecnologías de cifrado que podemos utilizar para asegurar nuestras comunicaciones.
- Cómo instalar y configurar un cortafuegos y un servidor proxy.
- Cómo detectar intrusiones en un sistema informático y cómo instalar y configurar el sistema para detectarlos.
- Cómo recuperar la información perdida en un desastre informático cómo puede ser la información borrada de un sistema, etc.
- Cómo realizar un análisis forense de un equipo atacado para poder determinar las causas (competencia desleal, fugas de información, fraude económico, espionaje industrial) y determinar los mecanismos que ha seguido el atacante.

Domine los principios básicos y las herramientas necesarias para conseguir un sistema informático seguro y rentable.

Dirigido a:

Responsables, asistentes o miembros del departamento o servicio de informática que quieran mejorar la seguridad de su sistema informático.

Tel. 900 670 400 - attcliente@iniciativasempresariales.com - www.iniciativasempresariales.com

Contenido del curso

→ MÓDULO 1. Introducción a la seguridad informática

10 horas

En informática la seguridad se acerca más al concepto de fiabilidad; se entiende un sistema seguro como aquel que se comporta como se espera de él. Este módulo trata aquellos factores que pueden ayudar a mejorar la seguridad: detectar cuándo se produce una intrusión, poder restaurar el sistema e identificar las acciones que ha realizado un intruso.

1.1. Conceptos básicos sobre seguridad:
1.1.1. Amenazas de seguridad.
1.1.2. Tipos de ataques.

1.2. Buscar un vector de ataque:
1.2.1. Localizar el objetivo:
1.2.1.1. Bases de datos whois.
1.2.1.2. Consultas DNS inversas.
1.2.1.3. Transferencias de zonas DNS no autorizadas.
1.2.1.4. Barridos de pings.
1.2.1.5. Trazados de rutas.
1.2.2. Analizar el objetivo:
1.2.2.1. Identificar los servicios TCP y UDP.
1.2.2.2. Identificar el sistema operativo.
1.2.2.3. Identificar las versiones de los servicios.
1.2.3. Escaneo de vulnerabilidades.

1.3. Legislación y normativa sobre seguridad:
1.3.1. La legislación española sobre datos de carácter personal.
1.3.2. Ley de servicios de la sociedad de la información y del comercio electrónico.
1.3.3. La ley de firma electrónica.
1.3.4. La ley de propiedad intelectual.
1.3.5. El esquema nacional de seguridad.

Tel. 900 670 400 - attcliente@iniciativasempresariales.com - www.iniciativasempresariales.com

Contenido del curso

→ MÓDULO 2. Prevención

20 horas

Los mecanismos de seguridad preventivos son todas aquellas acciones que van encaminadas a prevenir cualquier tipo de ataque y a garantizar la confidencialidad, integridad, no repudio y disponibilidad de los elementos críticos del sistema.
En este módulo conoceremos los aspectos más importantes a nivel de seguridad física, equipos, red y comunicaciones.

2.1. Introducción:
2.1.1. Seguridad física.
2.1.2. Seguridad en los equipos.
2.1.3. Seguridad en la red.
2.1.4. Seguridad en las comunicaciones.

2.2. Windows 2008R2:
2.2.1. Firewall de Windows.
2.2.2. Microsoft Forefront:
2.2.2.1. Instalación.
2.2.2.2. Asistente de configuración inicial.
2.2.2.3. Configuración.
2.2.2.4. Directivas de firewall.
2.2.2.5. Publicar servidores.
2.2.2.6. Configuración del proxy.
2.2.2.7. Creación de redes privadas virtuales (VPN).
2.2.3. Windows Server Update Services.

2.3. GNU/Linux:
2.3.1. Iptables.
2.3.2. Squid:
2.3.2.1. Configuración básica.
2.3.2.2. Listas de acceso (ACL).
2.3.2.3. Filtrado de contenido.
2.3.2.4. Configuración de los clientes.
2.3.2.5. Configuración de proxy web transparente.
2.3.2.6. Squid Analysis Report Generator.

2.4. LiveCD:
2.4.1. IPCop.
2.4.2. Vyatta.

Tel. 900 670 400 - attcliente@iniciativasempresariales.com - www.iniciativasempresariales.com

Contenido del curso

→ MÓDULO 3. Sistemas de detección de intrusos

20 horas

Con la fuerte expansión de las TIC en las empresas e instituciones, cada vez se hace más necesario el uso de herramientas que permitan detectar cualquier incidente que se produzca y afecte al correcto funcionamiento de los diferentes recursos, servicios y equipos.
En este módulo conoceremos los aspectos más importantes sobre los sistemas de detección de intrusos.

3.1. Sistemas de detección de intrusos:
3.1.1. Honeypot.
3.1.2. Tipos de sistemas de detección de intrusos.
3.1.3. Colocación de un NIDS.

3.2. Instalación y configuración de un NIDS (Snort):
3.2.1. Elementos del sistema.
3.2.2. Instalación.
3.2.3. Modos de ejecución:
3.2.3.1. Sniffer Mode.
3.2.3.2. Packet Loger Mode.
3.2.3.3. Network Intrussion Detection System (NIDS).
3.2.4. Personalizando las reglas.
3.2.5. Actualización de reglas (OinkMaster).
3.2.6. BASE.

3.3. Instalación y configuración de un HIDS:
3.3.1. md5sum.
3.3.2. Tripwire.

3.4. Live CD – EASYIDS:
3.4.1. Instalación.
3.4.2. Configuración inicial.
3.4.3. Administración.

Tel. 900 670 400 - attcliente@iniciativasempresariales.com - www.iniciativasempresariales.com

Contenido del curso

→ MÓDULO 4. Copias de seguridad

20 horas

Tras detectar que la seguridad ha sido comprometida, una de las tareas del administrador del sistema afectado será recuperarlo y dejarlo tal y como estaba antes del incidente a partir de las copias de seguridad.
En este módulo veremos los aspectos más importantes que hay que tener en cuenta para realizar copias de seguridad y, posteriormente, se analizarán las copias de seguridad en los sistemas Windows y GNU/Linux.

4.1. Introducción:
4.1.1. Tipos de copias de seguridad.
4.1.2. Buenas costumbres.
4.1.3. Centralización de copias de seguridad.
4.1.4. Hardware para copias de seguridad.

4.2. Windows:
4.2.1. Realizar una copia de seguridad.
4.2.2. Recuperar una copia de seguridad.
4.2.3. Configurar opciones de rendimiento.

4.3. GNU/Linux:
4.3.1. Comandos básicos:
4.3.1.1. La orden TAR.
4.3.1.2. El comando DD.
4.3.1.3. RSYNC.
4.3.1.4. Backups sobre CD-Rom.
4.3.1.5. Programación de tareas.
4.3.1.6. Ejemplo de copias de seguridad.
4.3.2. Cifrado de sistemas de ficheros.
4.3.3. Herramientas gráficas.

4.4. Live CD:
4.4.1. FreeNAS.
4.4.2. Clonezilla.

Tel. 900 670 400 - attcliente@iniciativasempresariales.com - www.iniciativasempresariales.com

Contenido del curso

→ MÓDULO 5. Análisis forense

10 horas

Cuando un sistema informático ha sido atacado deben buscarse evidencias. Con este módulo conoceremos los principales pasos a dar para realizar un análisis forense así como las herramientas más utilizadas para hacerlo.

5.1. Análisis forense:
5.1.1. Recopilación de evidencias.
5.1.2. Análisis e investigación de las evidencias.
5.1.3. Documentación del análisis.

5.2. Live CD – SystemRescue CD:
5.2.1. Modo gráfico.
5.2.2. Modo terminal.

Tel. 900 670 400 - attcliente@iniciativasempresariales.com - www.iniciativasempresariales.com

Autor

El contenido y las herramientas pedagógicas del curso Seguridad Informática para Sistemas Operativos Windows y Linux en Empresas han sido elaboradas por un equipo de especialistas dirigidos por:

Julio Gómez

Doctor en Informática. Experto en Seguridad Informática. Director del Máster de Administración, Comunicaciones y Seguridad Informática de la Universidad de Almería, tiene en su haber más de 20 títulos publicados a escala nacional e internacional sobre la administración de sistemas operativos, comunicaciones y seguridad informática.

Consultor

Óscar Gómez

Doctorado en Tecnologías de la Información y la Comunicación. Máster de Profesorado de Educación Secundaria Obligatoria y Bachillerato, Formación Profesional y enseñanza de idiomas.
Máster Universitario Oficial en Ciencia de Datos e Ingeniería de Computadores.
Máster propio en Administración, Comunicaciones y Seguridad Informática.
Ingeniero en Informática.

El consultor y su equipo de colaboradores estarán a disposición de los alumnos para resolver sus dudas y ayudarles en el seguimiento del curso y el logro de objetivos.

Titulación

Una vez realizado el curso el alumno recibirá el diploma que le acredita como **experto en Seguridad Informática para Sistemas Operativos Windows y Linux en Empresas.** Para ello, deberá haber cumplimentado la totalidad de las pruebas de evaluación que constan en los diferentes apartados. Este sistema permite que los diplomas entregados por Iniciativas Empresariales y Manager Business School gocen de garantía y seriedad dentro del mundo empresarial.