EUROINNOVA FORMACION
INTERNATIONAL BUSINESS SCHOOL

Especialista TIC Internal Hacking Entorno Windows. Seguridad Informática

Especialista TIC Internal Hacking Entorno Windows. Seguridad Informática

Duración: 300 horas

Precio: 240 € *

Modalidad: Online

* Materiales didácticos, titulación y gastos de envío incluidos.

Descripción

Este Curso Especialista TIC Internal Hacking Entorno Windows. Seguridad Informática le ofrece una formación especializada para aprender a conocer mejor los riesgos de ataques internos, al alcance de usuarios simples, y por lo tanto favorecer la puesta en marcha de contramedidas que, obligatoriamente, aumentarán la seguridad frente a ataques externos.

A quién va dirigido

Este curso se dirige a Administradores de Sistemas Windows, Responsables de Seguridad o a Desarrolladores entusiastas con la seguridad informática.

Objetivos

- Aprender a conocer mejor los riesgos de ataques internos, al alcance de usuarios simples.
- Favorecer la puesta en marcha de contramedidas que, obligatoriamente, aumentarán la seguridad frente a ataques externos.
- Aprender todo lo necesario para convertirse en administrador en un puesto de trabajo o en un servidor (cuando se es un usuario con pocos o ningún privilegio), cómo apropiarse de una contraseña, coger el control remoto de un puesto, ejecutar una aplicación trampa, sobrepasar las restricciones software...
- Conocer las contramedidas técnicas que se deben poner en marcha e inicia también al lector en una buena gestión de los sistemas para darle los medios de proteger mejor sus sistemas de información.

Para que te prepara

Este Curso Online de Especialista TIC Internal Hacking Entorno Windows. Seguridad Informática le prepara para aprender a conocer mejor los riesgos de ataques internos, al alcance de usuarios simples, y por lo tanto favorecer la puesta en marcha de contramedidas que, obligatoriamente, aumentarán la seguridad frente a ataques externos.

Salidas laborales

Seguridad Informática.

Titulación

Una vez finalizado el curso, el alumno recibirá por parte de Euroinnova Formación vía correo postal, la titulación que acredita el haber superado con éxito todas las pruebas de conocimientos propuestas en el mismo.

Esta titulación incluirá el nombre del curso/master, la duración del mismo, el nombre y DNI del alumno, el nivel de aprovechamiento que acredita que el alumno superó las pruebas propuestas, las firmas del profesor y Director del centro, y los sellos de la instituciones que avalan la formación recibida (Euroinnova Formación, Instituto Europeo de Estudios Empresariales y Comisión Internacional para la Formación a Distancia de la UNESCO).

EUROINNOVA FORMACION

como centro de Formación acreditado para la impartición a nivel nacional de formación
EXPIDE EL PRESENTE TÍTULO PROPIO

NOMBRE DEL ALUMNO/A

con D.N.I. XXXXXXXXX ha superado los estudios correspondientes de

Nombre de la Acción Formativa

de XXX horas, perteneciente al Plan de Formación EUROINNOVA en la convocatoria de 2014
Y para que surtan los efectos pertinentes queda registrado con Número de Expediente XXXX/XXXX-XXXX-XXXX-XXXXXX

Con una calificación de SOBRESALIENTE

Y para que conste expido la presente TITULACIÓN en
Granada, a 23 de Abril de 2014

La direccion General

El/La interesado/a

Sello

Forma de financiación

- Contrarrembolso.
- Transferencia.
- Tarjeta de crédito.

Metodología

Entre el material entregado en este curso se adjunta un documento llamado Guía del Alumno dónde aparece un horario de tutorías telefónicas y una dirección de e-mail dónde podrá enviar sus consultas, dudas y ejercicios. También se adjunta en CDROM una guía de ayuda para utilizar el campus online.

La metodología a seguir es ir avanzando a lo largo del itinerario de aprendizaje online, que cuenta con una serie de temas y ejercicios. Para su evaluación, el alumno/a deberá completar todos los ejercicios propuestos en el curso. La titulación será remitida al alumno/a por correo una vez se haya comprobado que ha completado el itinerario de aprendizaje satisfactoriamente.

Materiales didácticos

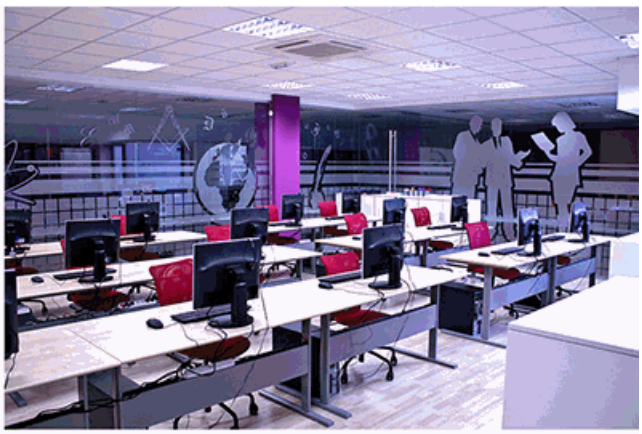
- CDROM 'Manual del Alumno de la Plataforma E-Learning. EUROINNOVA'

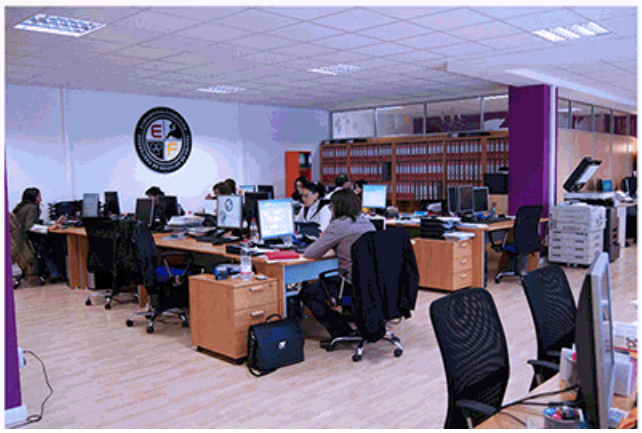
Profesorado y servicio de tutorías

Nuestro centro tiene su sede en el "Centro de Empresas Granada", un moderno complejo empresarial situado en uno de los centros de negocios con mayor proyección de Andalucía Oriental. Contamos con una extensa plantilla de profesores especializados en las distintas áreas formativas, con una amplia experiencia en el ámbito docente.

El alumno podrá contactar con los profesores y formular todo tipo de dudas y consultas, así como solicitar información complementaria, fuentes bibliográficas y asesoramiento profesional.
Podrá hacerlo de las siguientes formas:

- **Por e-mail:** El alumno podrá enviar sus dudas y consultas a cualquier hora y obtendrá respuesta en un plazo máximo de 48 horas.
- **Por teléfono:** Existe un horario para las tutorías telefónicas, dentro del cual el alumno podrá hablar directamente con su tutor.



Plazo de finalización

El alumno cuenta con un período máximo de 6 meses para la finalización del curso, a contar desde la fecha de recepción de las materiales del mismo.

Si una vez cumplido el plazo no se han cumplido los objetivos mínimos exigidos (entrega de ejercicios y evaluaciones correspondientes), el alumno podrá solicitar una prórroga con causa justificada de 3 meses.

Bolsa de empleo

El alumno tendrá la posibilidad de incluir su currículum en nuestra bolsa de empleo y prácticas, participando así en los distintos procesos de selección y empleo gestionados por más de 2000 empresas y organismos públicos colaboradores, en todo el territorio nacional.

Club de alumnos

Servicio gratuito que permitirá al alumno formar parte de una extensa comunidad virtual que ya disfruta de múltiples ventajas: becas, descuentos y promociones en formación, viajes al extranjero para aprender idiomas...

Revista digital

El alumno podrá descargar artículos sobre e-learning, publicaciones sobre formación a distancia, artículos de opinión, noticias sobre convocatorias de oposiciones, concursos públicos de la administración, ferias sobre formación, etc.

Programa formativo

UNIDAD DIDÁCTICA 1. INTRODUCCIÓN
Preámbulo
Desciframiento de un ataque conseguido
Descifrado de contramedidas eficaces
- Análisis de riesgos reales
- Consideraciones técnicas
- Consideraciones de gestión
¿Qué acciones, para qué roles?
- ¿Qué puede hacer un administrador local?
- ¿Qué puede hacer un administrador de dominio?
- ¿Qué puede hacer un usuario?

UNIDAD DIDÁCTICA 2. BÚSQUEDA DE INFORMACIÓn
¿Qué informaciones son interesantes?
- Tipos de búsquedas
- ¿Qué se debe anotar?
¿Cómo encontrar las informaciones locales útiles?
- Configuraciones del sistema
- Las políticas de grupo
- El cortafuegos
- Las carpetas y los ficheros
Las informaciones remotas
- Configuración de sistema
- Configuración de red
Contramedidas

UNIDAD DIDÁCTICA 3. TOMAR EL ROL DE ADMINISTRADOR O DE SISTEMA
Utilizar un medio de instalación de Windows oficial o una imagen de arranque PXE
- Arranque sobre el sistema
- Modificación del registro offline
- Utilización del hack sobre distintos sistemas
- Contramedidas
Trucar una aplicación con las herramientas integradas en Windows
- Tomar el rol de sistema en su puesto de trabajo o su servidor
- Tomar el rol de System en un servidor remoto o en un controlador de dominio
- Llegar a ser administrador del dominio
- Contramedidas
Engañar con un documento de Office
- Ejecutar un script o un programa
- Rodear la seguridad de las macros
- Contramedidas
Modificar un correo electrónico para arrancar una aplicación
- Enviar un PDF falso desde el exterior
- Enviar desde dentro un PowerPoint modificado
- Hacer descargar una aplicación oculta y ejecutarla

- Contramedidas

UNIDAD DIDÁCTICA 4. EXTRAER, ROMPER, CAMBIAR UNA CONTRASEÑA

Cómo extraer una contraseña en un equipo o un controlador de dominio
- Herramientas de extracción de contraseñas de sesión
- Herramientas de extracción de otras contraseñas
- Contramedidas

¿Cómo recuperar una contraseña desde la red?
- Utilización de un proxy
- Introducción a los certificados y a HTTPS
- Script que permite capturar el teclado en una página web
- Usar un sitio web falso copiado
- Redirección de puertos y escucha de la red
- ARP poisoning en Windows
- Software y herramientas para romper las contraseñas
- Contramedidas

UNIDAD DIDÁCTICA 5. DESARROLLAR SUS PROPIAS HERRAMIENTAS DE HACKING

Introducción a .NET
- ¿Cómo compilar su programa sin Visual Studio?

Forzar la ejecución de una aplicación
- Los medios clásicos
- Los medios no convencionales

Filtrar datos en diferencial
- Usar una carpeta compartida como destino
- Configurar un servidor con WebDAV como destino
- Configurar SharePoint como destino
- Crear la aplicación
- Compilar el programa

Crear una ventana de autenticación
- Principios básicos
- Crear el programa para Outlook
- Crear el programa para IE
- Crear el programa para una aplicación de gestión

Crear un keylogger
- Principios básicos
- Crear la aplicación
- Compilar la aplicación

Capturar la pantalla
- Principios básicos
- Crear la aplicación
- Compilar la aplicación

Grabar el sonido
- Principios básicos
- Crear la aplicación
- Compilar la aplicación

Romper una contraseña
- Principios básicos
- Crear la aplicación
- Compilar la aplicación
- Usar la GPU

Gobernar un equipo remoto
- Principios básicos
- Crear la aplicación
- Compilar la aplicación

Esquivar la seguridad de la UAC
- Principios básicos
- Extraer los iconos de una aplicación
- Firmar el código
- Trucar la aplicación para la víctima
- Probar las modificaciones

Cambiar el código PIN BitLocker con permisos de usuario
- Principios básicos
- Crear un servicio de Windows
- Compilar e instalar un servicio de Windows
- Crear la aplicación cliente
- Compilar la aplicación cliente

Contramedidas

UNIDAD DIDÁCTICA 6. HACER EJECUTAR SUS APLICACIONES TRAMPA

Entender a la persona, sus necesidades y sus deseos
- La toma de decisiones
- Entender al usuario

Las necesidades del usuario
- El modelo de Maslow
- El modelo de valor de inventario de Shalom Schwartz

Técnicas de manipulación
- Las sugestiones verbales

Creación de la fase de ataque
- Enviar un documento de Office trucado
- Enviar una aplicación trampa

Contramedidas

UNIDAD DIDÁCTICA 7. SUPERAR LAS RESTRICCIONES DE SOFTWARE

Superar las políticas de grupo
- Principio de las políticas de grupo
- Bloquear la ejecución de las GPO
- Contramedidas

Rodear las restricciones corrientes
- El explorador de Windows
- El registro
- El administrador de tareas
- Gestión de ficheros con FSRM
- Ejecutar otras aplicaciones que no sean las previstas en un Terminal Server
- Pasarela de mail
- Proxy Web

Contramedidas

UNIDAD DIDÁCTICA 8. TOMAR EL CONTROL REMOTAMENTE

Tomar el control de un equipo remoto
- Utilización de las herramientas de administración de Windows
- Usar una aplicación NetCommand en .NET
- Uso de una herramienta de escritorio remoto

- Contramedidas
Tomar el control mediante vulnerabilidades del sistema operativo o de las aplicaciones
- Las vulnerabilidades del sistema operativo y de las aplicaciones
- Metasploit y Armitage
- Contramedidas

UNIDAD DIDÁCTICA 9. GUARDAR UNA PUERTA ABIERTA

Introducción a las puertas traseras activas y pasivas
Conservar discretamente un acceso a un servidor o a un PC
- Puerto de escucha para Terminal Server
- Programa .NET

Conservar discretamente un acceso a un servidor web o de mensajería
- Tener acceso a todas las cuentas de correo electrónico de un servidor Exchange
- Modificar una aplicación web para conservar un acceso desde el exterior
- Contramedidas

Conservar discretamente un medio de tomar el control en un PC o un servidor
- Añadir un protocolo y trucar la navegación
- Añadir o modificar una extensión
- Añadir un certificado raíz
- Esconder una cuenta de usuario
- Contramedidas

UNIDAD DIDÁCTICA 10. ESCONDERSE Y ELIMINAR SUS HUELLAS

Usar la virtualización
- Hyper-V en Windows 8
- Otras herramientas de virtualización
- Contramedidas

Utilizar la cuenta de sistema
- Utilizar la cuenta de sistema directamente
- Utilizar la cuenta de sistema indirectamente
- Contramedidas

Eliminar los logs
- Los logs de eventos de Windows
- Los logs del cortafuegos local
- Los logs de los servicios web

UNIDAD DIDÁCTICA 11. LAS CONTRAMEDIDAS TÉCNICAS

Los medios integrados en los entornos Microsoft
- Impedir el arranque del sistema
- Instalar y configurar un controlador de dominio en modo de solo lectura
- Instalar y configurar una autoridad de certificación
- Instalar y configurar Network Access Protection
- Instalar y configurar WSUS (Windows Server Update Services)
- Las políticas de grupo
- Configurar la restricción de software
- La gestión de los ficheros y de los permisos
- Firmar las macros VBA y los scripts PowerShell
- Herramientas de auditoría y de seguridad de Microsoft

Otros medios
- La disociación
- Herramientas de monitoring y de vigilancia
- Herramientas de auditoría y de prueba de vulnerabilidades

UNIDAD DIDÁCTICA 12. LA GESTIÓN DE LOS SISTEMAS DE INFORMACIÓN

Los retos de la gestión

El impacto y las consecuencias del internal hacking en la gestión

Unas buenas prácticas que nos pueden ayudar

- Norma o buenas prácticas
- COBIT, Val IT y Risk IT

Poner en marcha la gestión de los SI con la ayuda de COBIT

- Marco general
- ¿Qué es un objetivo de control?
- El procedimiento «Puesta en marcha de la gestión de los SI»
- ¿Por dónde empezar?

Administrar y gestionar el riesgo

- Definiciones
- Estimación del riesgo
- Los factores de riesgo
- La clasificación del riesgo
- El tratamiento de un riesgo
- Los otros elementos de la gestión de riesgos

Tratar el internal hacking desde el punto de vista de la gestión

- La gestión de los administradores
- La gestión de los usuarios
- La gestión de los sistemas
- La gestión de las aplicaciones
- La gestión de la información
- La gestión de los problemas y de los incidentes