FICHA TÉCNICA DEL CURSO

Nombre del curso	Introducción al Hacking Ético
Rama	Ciberseguridad
Lengua en que se imparte	Castellano
Profesor/a responsable	Marcelo aka S4vitar
Datos de contacto	soporte@mastermind.ac
Modalidad	Online*
Metodología	La metodología empleada se basa en una combinación de: **Clases magistrales**, orientadas a la presentación de conceptos de la materia y a la definición de los objetivos y procedimiento de trabajo. **Tareas, retos y proyectos**, planteándose como técnica de aprendizaje individual tareas que exigen de una trabajo de investigación pretendiendo que el alumno sea autónomo en la resolución de problemas.
Método de aprendizaje	El proceso de enseñanza-aprendizaje se realizará mediante el método de ABP (Aprendizaje Basado en Proyectos) mediante el diseño, programación e implementación de un conjunto de tareas asociadas a una misma temática. Puede ser complejo y transversal. Culmina con una presentación, producto o ejecución de la solución, que refleja lo que el alumnado es capaz de hacer con los aprendizajes que ha adquirido durante el proyecto.
Accesibilidad	• SO: Windows® XP / Vista® / Windows® 7. • Procesador: 1.0 GHz. • Memoria: 512 MB de RAM. • Gráficos: Tarjeta compatible con DirectX y con 64 MB o mas • DirectX®: 8.1 o superior. • Sonido: Compatible con DirectX.

SITUACIÓN/SENTIDO DEL CURSO

Contextualización	Hacking ético se define a través de lo que hacen los profesionales que se dedican a ello, es decir, los piratas informáticos **éticos**. Estas personas son contratadas para hackear un sistema e identificar y reparar posibles vulnerabilidades, lo que previene eficazmente la explotación por ciberdelincuentes. Su tarea principal es la realización de pruebas de penetración de sistemas informáticos y de software con el fin de evaluar, fortalecer y mejorar la seguridad. Podemos decir que se encargan de implementar un hackeo ético para poner a prueba la seguridad del sistema.
Relación con otras ramas	
Prerrequisitos	Curso Cómo protegerse en la red

OBJETIVOS DEL CURSO

Generales	OG 1- Conocer el sistema de gestión de usuarios en sistemas Linux OG 2- Aprender los conceptos básicos del Pentesting
Específicos	OE 1- Realizar ataques y protección a usuarios en sistemas operativos tipo Linux OE 2- Usar herramientas para el mapeo y detección de servicios en la red OE 3- Utilizar WireShark para capturar el flujo de comunicaciones en una red OE 4- Saber proteger un servidor ante las vulnerabilidades más conocidas

DEDICACIÓN DEL ESTUDIANTE AL CURSO

Horas teóricas	8h
Horas prácticas (estimadas)	20h

BLOQUES TEMÁTICOS DEL CURSO

Módulo I: Introducción

Objetivos de aprendizaje	• Identificar la estructura de contenidos y los principales objetivos del curso
Número de lecciones	2
Plan de trabajo	Clases teóricas
Evaluación	
Recursos necesarios	Ordenador Acceso a Internet
Duración del módulo	<1h

Módulo II: Conceptos básicos

Objetivos de aprendizaje	• Aprender los conceptos básicos del Pentesting
Número de lecciones	12
Plan de trabajo	Clases combinadas teóricas y prácticas
Evaluación	3 tareas
Recursos necesarios	Ordenador Acceso a Internet
Duración del módulo	1h

Módulo III: Pentesting

Objetivos de aprendizaje	• Saber proteger un servidor ante las vulnerabilidades más conocidas • Realizar ataques y protección a usuarios en sistemas operativos tipo Linux • Utilizar herramientas para el mapeo y detección de servicios en la red
Número de lecciones	60
Plan de trabajo	Clases combinadas teóricas y práctica
Evaluación	3 Tareas
Recursos necesarios	Ordenador Acceso a Internet
Duración del módulo	8h

Módulo IV: Despedida

Objetivos de aprendizaje	• Reconocer todos los conocimientos impartidos a lo largo del curso
Número de lecciones	1
Plan de trabajo	Clase teórica
Evaluación	
Recursos necesarios	Ordenador Acceso a Internet
Duración del módulo	<1h

Módulo V: Examen Final

Objetivos de aprendizaje	• Evaluar los conocimientos adquiridos a lo largo del curso
Número de lecciones	1
Plan de trabajo	
Evaluación	Tipo test

Recursos necesarios	Ordenador Acceso a Internet
Duración del módulo	<1h

CONSIDERACIONES FINALES

Este curso no cuenta con ninguna consideración específica más allá de disfrutar aprendiendo.

CERTIFICACIÓN

Con la visualización del 100% del contenido del curso y la superación de un examen final se otorga un certificado de Finalización que consta de la siguiente información: nombre del alumno/a, nombre del curso, fecha de finalización e identificador de certificado.

*El 100% de la formación ofertada en Mastermind Academy es online