

## FICHA TÉCNICA DE LA ASIGNATURA

| Datos de la asignatura |   |
|------------------------|---|
| Nombre completo        | Optativa Complementaria: Test de Intrusión y Gestión de vulnerabilidades  |
| Código                 | DTC-MCS-516   |
| Impartido en           | Máster en Ciberseguridad [Primer Curso]   |
| Nivel                  | Master  |
| Cuatrimestre           | Semestral   |
| Créditos               | 3,0 ECTS  |
| Carácter               | Obligatoria   |
| Departamento / Área    | Departamento de Telemática y Computación  |
| Responsable            | Rafael Palacios   |
| Descriptor             | Los "Test de Intrusión" también conocidos como "Pentest" son un conjunto de pruebas utilizadas para que las empresas conozcan sus puntos débiles y puedan mitigar los mismos. Por otro lado, la "Gestión de Vulnerabilidades" permite conocer en que estado se encuentran las amenazas detectadas sobre una organización, sabiendo en cada momento el nivel de exposición de la misma y pudiendo llevar a cabo un seguimiento para hacer que se apliquen medidas que solventen las mismas. En esta materia se aprenderá de forma teórico-práctica todos los conceptos básicos para ejecutar pruebas que permitan analizar el nivel de exposición de una organización y como gestionar los hallazgos localizados para que se pongan en marcha aquellas acciones que sean necesarias. |

| Datos del profesorado |  |
|-----------------------|--|
| Profesor              |  |
| Nombre                | Antonio Pérez Sánchez                    |
| Departamento / Área   | Departamento de Telemática y Computación |
| Correo electrónico    | apsanchez@icai.comillas.edu              |

## DATOS ESPECÍFICOS DE LA ASIGNATURA

| Contextualización de la asignatura                       |  |
|--|--|
| Prerequisitos  |  |
| Manejo con máquinas virtuales tipo VMware o Virtual Box. |  |

| Competencias - Objetivos |
|--------------------------|
|--------------------------|

## BLOQUES TEMÁTICOS Y CONTENIDOS

| Contenidos – Bloques Temáticos |
|--------------------------------|
| Tema 1: Introducción           |

- Fases del test de intrusión
- Fase de Reconocimiento

### **Tema 2**

- Fases de test: Elección de herramientas, Envío, Ejecución
- Ejemplos de vulnerabilidades básicas

### **Tema 3: Vulnerabilidades avanzadas**

### **Tema 4**

- Fases de test: Instalación, C&C, Acciones sobre el objetivo
- Herramienta Metasploit Framework
- Técnicas de movimiento lateral y vertical.

### **Tema 5: Vulnerabilidades**

- Gestión de vulnerabilidades
- Herramientas de análisis automático

## **METODOLOGÍA DOCENTE**

### **Aspectos metodológicos generales de la asignatura**

## **EVALUACIÓN Y CRITERIOS DE CALIFICACIÓN**

### **Calificaciones**

1. **Prácticas (75%):** Se hará la media ponderada de las notas que obtenga el alumno en cada práctica, siendo el resultado el 75% de la nota final.
2. **Exámen tipo test 20 preguntas (25%):** El resultado del mismo supondrá el 25% de la nota final del alumno.

## **BIBLIOGRAFÍA Y RECURSOS**