FICHA DE LA ASIGNATURA: INGENIERÍA INVERSA Y ARQUITECTURAS SEGURAS			
CARÁCTER:	**Obligatorio**	**LENGUA/S EN LA/S QUE SE IMPARTE:**	**Español**
ECTS:	**4**	**CUATRIMESTRE**	**2**
Asignatura de la MATERIA TECNOLOGÍAS DE SEGURIDAD			
PROFESORES QUE IMPARTEN LA ASIGNATURA			
Mercedes Rodríguez García (coordinadora)			
COMPETENCIAS QUE SE ADQUIEREN: *(indicar código)*			
Comp. Básicas	**Comp. Generales**	**Comp. Específicas**	**Comp. Transversales**
CB6, CB7, CB8, CB9, CB10	**CG1, CG2, CG3, CG5**	**CE10, CE11**	**CT1**

RESULTADOS DE APRENDIZAJE:

Efectuar reconstrucción de código de ficheros ejecutables.

Conocer y detectar vulnerabilidades de bajo nivel.

Analizar ataques por desbordamiento de buffer y comprender los diferentes mecanismos de protección.

Realizar análisis de ficheros binarios.

Comprender el funcionamiento y las aplicaciones de los dispositivos de seguridad TPM.

CONTENIDOS:

TEMA 1. Introducción a la arquitectura del conjunto de instrucciones x86
- 1.1 Conjuntos de registros y tipos de datos
- 1.2 Conjuntos de instrucciones
- 1.3 Código máquina
- 1.4 Gestión física de la memoria

TEMA 2. Análisis de ficheros binarios
- 2.1 Ficheros ELF (Executable and Linkable Format)
- 2.2 Ficheros PE (Portable Executable)

TEMA 3. Reconstrucción de código
- 3.1 Procesos de compilación, enlazado y ensamblado
- 3.2 Herramientas de ingeniería inversa
- 3.3 Reconstrucción de código

TEMA 4. Ofuscación
- 4.1 Técnicas de ofuscación
- 4.2 Técnicas de desofuscación
- 4.3 Herramientas de desofuscación

TEMA 5. Vulnerabilidades de bajo nivel
- 5.1 Tipos de vulnerabilidades de bajo nivel
- 5.2 Detección de vulnerabilidades stack overflow
- 5.3 Framework para la creación de ataques stack overflow
- 5.4 Mecanismos de protección

TEMA 6. Trusted Platform Module (TPM)
- 6.1 Especificación TPM
- 6.2 Dispositivos de seguridad TPM
- 6.3 Casos de estudio y aplicaciones

OBSERVACIONES / REQUISITOS PREVIOS:

Se recomienda poseer conocimientos básicos de lenguaje ensamblador.

	Id de la Actividad Formativa	Nº de horas	Presencialidad (%)
ACTIVIDADES FORMATIVAS CON SUS CRÉDITOS ECTS:	Clases teórico-prácticas	32	100%
	Actividades académicas no presenciales	65	0%
	Evaluación	3	100%

METODOLOGÍAS DOCENTES:

Lección magistral expositiva
Resolución de problemas y casos prácticos
Prácticas de laboratorio
Realización de trabajos

SISTEMAS DE EVALUACIÓN DE ADQUISIÓN DE COMPETENCIAS:

Denominación Sistema Evaluación	Ponderación Mínima	Ponderación Máxima
Exposiciones de ejercicios, temas o trabajos	30%	70%
Pruebas escritas u orales	30%	70%

BIBLIOGRAFÍA RECOMENDADA:

Dennis Yurichev. Reverse Engineering for Beginners. Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) license, 2017.

Bruce Dang, Alexandre Gazet, Elias Bachaalany, Sebastien Josse (Contributions by). Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation. Wiley, 2014.