Ingeniería Inversa y Malware

Número total de créditos ECTS	6	
Tipología	Obligatoria	
Organización temporal	Semestre 2	
Modalidad	Virtual	
Idioma	Castellano	

Contenidos	• ARM para la ingeniería inversa.
	• Compiladores:
	  ○ Teoría de compiladores
	  ○ Fases de un compilador
	• Reconstrucción de código:
	  ○ Estructuras de datos
	  ○ Estructuras de código comunes
	  ○ Formatos de ficheros binarios y enlazadores
	• Análisis estático:
	  ○ Desensambladores
	  ○ Reconstructores de código
	• Análisis dinámico:
	  ○ Análisis de caja negra
	  ○ Análisis de caja blanca
	• Detección de técnicas de evasión
	  ○ Ofuscación
	  ○ Packing
	  ○ Técnicas de Evasión Avanzadas (AET).	

Resultados de aprendizaje TÍTULO	**Conocimientos y contenidos**	CC02 Identificar vulnerabilidades en sistemas clave de información y comunicación distinguiendo y categorizando las principales amenazas relacionadas con dichas vulnerabilidades CC04 Comprender el funcionamiento de los diferentes tipos de malware existentes, así como las partes de los sistemas informáticos a las que afectan. CC05 Identificar los diferentes tipos de malware existentes según las trazas de comportamiento de los mismos CC07 Identificar el comportamiento de códigos o ejecutables potencialmente maliciosos.
	Habilidades y destrezas	HD04 Extraer indicadores de compromiso (IOCs) de códigos o ejecutables potencialmente maliciosos para su futura clasificación y detección temprana. HD05 Evaluar diferentes ataques informáticos gracias a las trazas que dejan los mismos en los diferentes mecanismos de detección y registro de los sistemas.
Resultados de aprendizaje ASIGNATURA • Describir el comportamiento de un ejecutable binario con precisión. • Detectar los mecanismos más comunes usados en el desarrollo de malware en un ejecutable. • Diseñar/Aplicar mecanismos frente a las principales estrategias de evasión de detección por parte de sistemas IDS o IPS.		

Actividades formativas	Horas totales
Clases expositivas síncronas	6
Recursos didácticos audiovisuales	4
Seminarios síncronos	2
Clases prácticas síncronas	14
Resolución de ejercicios, casos y proyectos	4
Prácticas de laboratorio asíncronas	16
Trabajo autónomo	102
Prueba de evaluación final	2
Total	**150**

Sistemas de evaluación	MÍNIMO	MÁXIMO
Evaluación final: prueba o examen virtual	50	50
Resolución problemas	10	30
Estudio casos / Proyectos	10	30
Otras actividades de evaluación continua	0	10
Total	**70**	**120**