unie
Universidad

GUÍA DOCENTE

INGENIERÍA INVERSA Y MALWARE

Planeta Formación y Universidades

Ingeniería Inversa Y Malware

Número total de créditos ECTS		6
Tipología		Obligatoria
Organización temporal		Semestre 2
Modalidad		Presencial y virtual
Idioma		Castellano

Contenidos	• ARM para la ingeniería inversa.
	• Compiladores:
	  o Teoría de compiladores
	  o Fases de un compilador
	• Reconstrucción de código:
	  o Estructuras de datos
	  o Estructuras de código comunes
	  o Formatos de ficheros binarios y enlazadores
	• Análisis estático:
	  o Desensambladores
	  o Reconstructores de código
	• Análisis dinámico:
	  o Análisis de caja negra
	  o Análisis de caja blanca
	• Detección de Técnicas de evasión
	  o Ofuscación
	  o Packing
	  o 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.
	Competencias	
Resultados de aprendizaje MATERIA • 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.		

Modalidad Presencial	**Actividades formativas**	**Horas totales**	
	Clases Expositivas	14	
	Seminarios	2	
	Clases prácticas	14	
	Prácticas de laboratorio	16	
	Trabajo autónomo	**102**	
	Prueba de evaluación final	**2**	
	Total	**150**	
	Sistemas de evaluación	**MÍNIMO**	**MÁXIMO**
	Evaluación final: prueba o examen	40	40
	Resolución problemas	10	30
	Estudio casos - Proyectos	10	30
	Otras actividades de evaluación continua	0	10
	Total	**60**	**110**
Modalidad virtual	**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**
Observaciones			