Universidad Carlos III de Madrid

DENOMINACION DE ASIGNATURA: Técnicas de Ciberataque			
MÁSTER: Máster Universitario en Ciberseguridad		Curso: 2018/19	Cuatrimestre: 1º

PLANIFICACION SEMANAL DE LA ASIGNATURA

SEMANA	SESION	DESCRIPCION	GRUPO (marcar X)		ndicar espacio distinto de aula (aula informática, audiovisual, Etc.)	Indicar SI si la sesión requiere 2 profesores	TRABAJO SEMANAL DEL ALUMNO		
			GRANDE	PEQUEÑO			DESCRIPCIÓN	Horas presenciales	Horas de trabajo (Máx. 7h semana)
1	1	Bienvenida. Descripción del curso. Conceptos y definiciones.	X				Revisar y estudiar conceptos. Leer bibliografía	1.66	2
1	2	Pasos de una intrusión. Tipos de reconocimiento	X					1.66	
2	3	Técnicas de reconocimiento pasivo: inteligencia de fuentes abiertas.	X				Revisar y estudiar técnicas. Explorar distintas herramientas y fuentes abiertas.	1.66	4
2	4	Técnicas de escaneo activo(1/2).	X				Revisar y estudiar conceptos de redes. Aprender distintas técnicas de escaneado activo.	1.66	
3	5	Técnicas de escaneo activo (2/2). Práctica entregable 1: Reconocimiento		X	Lab	Si	Experimentar diferentes técnicas de escaneo. Trabajo entregable práctica 1.	1.66	7
3	6							1.66	
4	7	Pivoting. Meta herramientas de reconocimiento. Análisis de vulnerabilidades		X	Lab	Si	Experimentar con nuevas herramientas y preparar el examen.	1.66	7
4	8							1.66	
5	9	Examen parcial (1)	X				Revisar proxies web y técnicas de escaneo web.	1.66	4
5	10	Escaners web. Vectores de Ataque y estrategias de escaneo Web. Encoders.	X					1.66	
6	11	Practicando con escaners web.		X	Lab	Si	Experimentar con herramientas y trabajo entregable práctica 2.	1.66	7
6	12	Práctica entregable 2: escaners web.						1.66	

7	13	Explotación. Introducción, conceptos y técnicas básicas.		X	Lab		Revisar y estudiar técnicas y experimentar con herramientas Finalizar entregable.	1.66	7
7	14	Explotación de sistemas de autenticación y vulnerabilidades de software.						1.66	
8	15	Práctica con metasploit: Exploits, payloads, listeners, encoders.		X	Lab	Si	Experimentar con metasploit, herramientas de evasión y otros marcos.	1.66	4
8	16	Otros marcos de ataque.						1.66	
9	17	Técnicas de evasión. Consumo de recursos y DoS	X				Revisar y estudiar conceptos. Leer bibliografía	1.66	4
9	18	Ataques de ingeniería social. Herramientas web de control de campañas	X					1.66	
10	19	Práctica de ataques de ingeniería social. Técnicas de ocultación. Persistencia. Creando nuevos canales.		X	Lab		Revisar y estudiar conceptos. Expermientar con nuevas herramientas	1.66	4
10	20							1.66	
11	21	Escalada de privilegios y movimiento lateral		X	Lab	Si	Estudio conceptos de sesiones previas y preparar el examen.	1.66	7
11	22							1.66	
12	23	Examen parcial (2)		X	Lab	Si	Trabajo entregable práctica 3.	1.66	7
12	24	Práctica entregable 3: Ataque completo						1.66	
							Trabajo entregable práctica 3.		7
							Subtotal 1	**39.84**	**71**

TOTAL *(Total 1 + Total 2. Máximo 156 horas)*	**110.84**