Guia docente				
Datos Identificativos				2018/19
Asignatura (*)	Test de Intrusión		Código	614530008
Titulación	Máster Universitario en Ciberseguridade			
Descriptores				
Ciclo	Periodo	Curso	Tipo	Créditos
Máster Oficial	2º cuatrimestre	Primero	Obligatoria	5
Idioma	CastellanoGallego			
Modalidad docente	Presencial			
Prerrequisitos				
Departamento	Computación			
Coordinador/a	Carballal Mato, Adrián	Correo electrónico	adrian.carballal@udc.es	
Profesorado	Carballal Mato, Adrián	Correo electrónico	adrian.carballal@udc.es	
Web	www.munics.es			
Descripción general	No hay una mejor forma de probar la fortaleza de un sistema que atacarlo. Los Test de Intrusión sirven para reproducir intentos de acceso de un atacante valiéndose de las vulnerabilidades que puedan existir en una determinada infraestructura. En este curso se cubrirán los temas fundamentales orientados a los test de intrusión (pentesting) cubriendo las distintas fases de un ataque y explotación (desde el reconocimiento y el control de acceso hasta el borrado de huellas).			

Competencias / Resultados del título	
Código	Competencias / Resultados del título
A2	CE2 - Conocer en profundidad las técnicas de ciberataque y ciberdefensa
A3	CE3 - Conocer la normativa técnica y legal de aplicación en materia de ciberseguridad, sus implicaciones en el diseño de sistemas, en el uso de herramientas de seguridad y en la protección de la información
A4	CE4 - Conocer la normativa técnica y legal de aplicación en materia de ciberseguridad, sus implicaciones en el diseño de sistemas, en el uso de herramientas de seguridad y en la protección de la información
A7	CE7 - Tener capacidad para realizar la auditoría de seguridad de sistemas e instalaciones, el análisis de riesgos derivados de debilidades de ciberseguridad y desarrollar el proceso de certificación de sistemas seguros
B1	CB1 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y aplicación de ideas, a menudo en un contexto de investigación
B2	CB2 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio
B3	CB3 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formar juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios
B4	CB4 - Que los estudiantes sepan comunicar sus conclusiones, y los conocimientos y razones últimas que las sustentan, a públicos especializados y no especializados de un modo claro y sin ambigüedades
B5	CB5 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo
B6	CG1 - Tener capacidad de análisis y síntesis. Tener capacidad para proyectar, modelar, calcular y diseñar soluciones de seguridad de la información, las redes y/o los sistemas de comunicaciones en todos los ámbitos de aplicación
B7	CG2 - Resolución de problemas. Tener capacidad de resolver, con los conocimientos adquiridos, problemas específicos del ámbito técnico de la seguridad de la información, las redes y/o los sistemas de comunicaciones
B9	CG4 - Compromiso ético. Capacidad para diseñar e implantar soluciones técnicas y de gestión con criterios éticos de responsabilidad y deontología profesional en el ámbito de la seguridad de la información, las redes y/o los sistemas de comunicaciones
C4	CT4 - Valorar la importancia de la seguridad de la información en el avance socioeconómico de la sociedad

Resultados de aprendizaje

Resultados de aprendizaje	Competencias / Resultados del título		
Identificar los riesgos y vulnerabilidades de un sistema de información	AP2 AP4 AP7	BP6 BP9	
Identificar los mecanismos de seguridad y su integración en las organizaciones	AP2 AP3 AP4 AP7		
Utilizar herramientas de seguridad	AP2 AP4	BP2	
Enfrentarse a casos "reales" y "saber lo que hay que hacer" en el menor tiempo posible	AP4 AP7	BP4 BP7	
Capacidad de análisis y síntesis		BP1 BP3 BP5	CP4

Contenidos	
Tema	Subtema
Fundamentos	Hacking ético Vulnerabilidades Vectores de ataque Tipos de Test de Intrusión Alcance y objetivos
Estrategias de reconocimiento	Pasivo vs Activo Scapy P0f Netdiscover
Estrategias ofensivas	Análisis de vulnerabilidades Explotación de vulnerabilidades Elevación de privilegios Mantenimiento de acceso
Métodos de evasión	Contramedidas Borrado de huellas

Planificación				
Metodologías / pruebas	Competencias / Resultados	Horas lectivas (presenciales y virtuales)	Horas trabajo autónomo	Horas totales
Sesión magistral	A2 B9 C4	9	13.5	22.5
Análisis de fuentes documentales	A2 A3 A7 B6 B4	6	6	12
Prácticas de laboratorio	A4 B1 B6 B7	26	52	78
Prueba de respuesta múltiple	B5 B6 B7	1.5	0	1.5
Estudio de casos	B2 B3 B5 B7	5	6	11
Atención personalizada		0		0
(*)Los datos que aparecen en la tabla de planificación són de carácter orientativo, considerando la heterogeneidad de los alumnos				

Metodologías	
Metodologías	Descripción

Sesión magistral	Transmisión de información y conocimiento clave de cada uno de los temas. La participación de los estudiantes se fomenta en ciertos momentos. Como parte de la metodología, un enfoque crítico de la disciplina llevará a los estudiantes a reflexionar y descubrir las relaciones entre los diferentes conceptos, formar una mentalidad crítica para enfrentar los problemas y la existencia de un método, facilitando el proceso de aprendizaje en el alumno. Para luchar contra la posible pasividad del alumno, en pequeños momentos se presentan pequeñas preguntas, que reflexionan sobre el alumno, complementando esos aspectos con referencias bibliográficas que le permiten enriquecer el conocimiento adquirido. Este intercambio con el alumno, como parte de la lección magistral, nos permite controlar el grado de asimilación del conocimiento por parte de él. Las lecciones magisteriales incluyen, tanto conocimiento extraído de las referencias de la asginatura, como los resultantes de nuestras propias experiencias profesionales, fomentando la capacidad del análisis crítico. En todo momento se busca que una cierta parte de los contenidos no requiera que el alumno los memorice. Esta metodología intentará lograr un alto grado de motivación en el alumno.
Análisis de fuentes documentales	Lectura y examen crítico de los principales documentos éticos de la informática. Sirven como una introducción general a los temas. Proporcionan una explicación histórica y sistemática de su significado. Son de gran importancia en el contexto de las otras metodologías utilizadas en el tema.
Prácticas de laboratorio	Las prácticas de laboratorio permiten aprovechar al máximo la retroalimentación, el refuerzo y la asimilación de los objetivos. Los desarrollos prácticos comienzan con una práctica básica y su dificultad aumenta gradualmente. En todo momento, el alumno presenta el conjunto de ideas y técnicas que permiten el desarrollo práctico del conocimiento transmitido en las clases magistrales. En las prácticas se proponen varias secciones que exponen una batería de dificultades tratadas durante el estudio del tema. Se buscará la interrelación entre las diferentes secciones, proporcionando un contexto de ejercicio completo, con el fin de lograr la visión del estudiante como un todo, revelando los vínculos entre las preguntas que pueden parecer muy lejanas. En todas las clases prácticas, las máquinas virtuales se usan en las computadoras como una herramienta básica para la resolución de los ejercicios. El alumno podrá seleccionar e instalar las herramientas que considere más apropiadas en cada caso. De esta forma, se le exigirá, desde el comienzo, que se enfrente a la toma de decisiones, analizando las ventajas y desventajas en todos y cada uno de los casos. En este punto inicial, el asesoramiento personalizado será esencial, permitiendo un análisis realista de las decisiones tomadas, facilitando la retroalimentación de nuevos parámetros no considerados a priori.
Prueba de respuesta múltiple	Esta prueba estará orientada a determinar si el alumno ha asimilado los diferentes objetivos de la asignatura.
Estudio de casos	El análisis ético y legal de la tecnología de la información tiene características específicas. Con el estudio de caso, se pretende examinar la estructura y el contenido de los problemas presentes en los casos, tanto individualmente como en grupos. Es una forma de aprendizaje de contenido y también metodológica, en la cual el alumno aprende a analizar, deliberar y llegar a conclusiones razonables y razonables con los argumentos éticos y legales. Es muy útil para ejercitar las habilidades y las habilidades argumentativas.

Atención personalizada	
Metodologías	**Descripción**
Prácticas de laboratorio	Prácticas de laboratorio: se guía al alumno individualmente en el desarrollo de cada una de las prácticas de laboratorio. Aunque en el desarrollo de la primera práctica existen grandes diferencias en las necesidades de cada alumno, se están homogeneizando progresivamente en términos de sus necesidades de atención personalizada. Sin duda, la identificación de este parámetro es fundamental para determinar que la totalidad de los estudiantes avanza durante el desarrollo de la asignatura. También haremos que los grupos pequeños trabajen juntos en desarrollos prácticos. Atención personalizada: cualquier pregunta tecnológica expuesta por el alumno, en persona, tutoriales, correo electrónico, etc.

Evaluación			
Metodologías	Competencias / Resultados	Descripción	**Calificación**
Prácticas de laboratorio	A4 B1 B6 B7	Cada alumno de prácticas de laboratorio deberá pasar unha proba. Nela o profesor expón pequenas tarefas que os alumnos deberán resolver sobre as máquinas virtuais do laboratorio de prácticas.	30
Prueba de respuesta múltiple	B5 B6 B7	Esta proba inclúe os contidos e, en xeral, todo aspecto relacionado cos obxectivos da materia. Nela exponse diversas cuestións relacionadas tanto cos contidos das sesións maxistrais como das prácticas de laboratorio, dándolle un maior peso ás primeiras.	70

Observaciones evaluación

Fuentes de información	
Básica	- Pablo Gonzalez Perez, Germán Sánchez Garcés, Jose Miguel Soriano de la Cámara (2013). Pentesting con Kali. 0xWORD - Mike Schiffman (2001). Hacker's Challenge. Osborne - Julio Gomez López, Miguel Angel de Castro Simón, Pedro Guillén Núñez (2014). Hackers, Aprende a atacar y a defenderte. RA-MA - David Puente Castro (2013). Linux Exploiting. 0xWORD - Pablo Gonzalez Perez (2016). Metasploit para Pentesters. 0xWORD
Complementária	

Recomendaciones
Asignaturas que se recomienda haber cursado previamente
Seguridad de la Información/614530003 Redes Seguras/614530006
Asignaturas que se recomienda cursar simultáneamente
Conceptos y Leyes en Ciberseguridad/614530001 Ciberseguridad en Entornos Industriales/614530014
Asignaturas que continúan el temario
Trabajo Fin de Máster/614530017 Gestión de la Seguridad de la Información/614530002
Otros comentarios

(*) La Guía Docente es el documento donde se visualiza la propuesta académica de la UDC. Este documento es público y no se puede modificar, salvo cosas excepcionales bajo la revisión del órgano competente de acuerdo a la normativa vigente que establece el proceso de elaboración de guías