UNIVERSIDADE DA CORUÑA

Guía Docente				
Datos Identificativos				2019/20
Asignatura (*)	Test de Intrusión		Código	614530008
Titulación				

Descriptores				
Ciclo	Período	Curso	Tipo	Créditos
Mestrado Oficial	2º cuadrimestre	Primeiro	Obrigatoria	5

Idioma	CastelánGalego		
Modalidade docente	Presencial		
Prerrequisitos			
Departamento	Ciencias da Computación e Tecnoloxías da InformaciónComputación		
Coordinación	Carballal Mato, Adrián	Correo electrónico	adrian.carballal@udc.es
Profesorado	Carballal Mato, Adrián	Correo electrónico	adrian.carballal@udc.es
Web	faitic.uvigo.es		
Descrición xeral	Non hai mellor forma de probar a forza dun sistema que atacalo. As probas de intrusión serven para reproducir os intentos de acceso dun atacante usando as vulnerabilidades que poden existir nunha infraestrutura dada. Neste curso abordaranse os temas fundamentais orientados ás probas de intrusión (pentesting), que abarcan as diferentes fases dun ataque e explotación (desde o recoñecemento e control do acceso á eliminación de pistas).		

Competencias / Resultados do título	
Código	Competencias / Resultados do título

Resultados da aprendizaxe			
Resultados de aprendizaxe	Competencias / Resultados do título		
Identificar os riscos e vulnerabilidades dun sistema de información	AP2 AP4 AP7	BP6 BP9	
Identificar os mecanismos de seguridade e a súa integración nas organizacións	AP2 AP3 AP4 AP7		
Utilizar ferramentas de seguridade	AP2 AP4	BP2	
Enfrontrarse a casos "reais" e "saber o que hai que facer", no menor tempo posible	AP4 AP7	BP4 BP7	
Capacidade de análise e síntese		BP1 BP3 BP5	CP4

Contidos	
Temas	Subtemas
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				
Metodoloxías / probas	Competencias / Resultados	Horas lectivas (presenciais e virtuais)	Horas traballo autónomo	Horas totais
Sesión maxistral	A2 B9 C4	9	13.5	22.5
Análise de fontes documentais	A2 A3 A7 B4 B6	6	6	12
Prácticas de laboratorio	A4 B1 B6 B7	26	52	78
Proba de resposta múltiple	B5 B6 B7	1.5	0	1.5
Estudo de casos	B2 B3 B5 B7	5	6	11
Atención personalizada		0		0
*Os datos que aparecen na táboa de planificación son de carácter orientativo, considerando a heteroxeneidade do alumnado				

Metodoloxías	
Metodoloxías	Descrición
Sesión maxistral	Transmisión de información e coñecementos crave de cada un dos temas. Poténciase en certos momentos a participación do alumno. Como parte da metodoloxía, un enfoque crítico da disciplina levará aos alumnos a reflexionar e descubrir as relacións entre os diversos conceptos, formar unha mentalidade crítica para afrontar os problemas e a existencia dun método, facilitando o proceso de aprendizaxe no alumno. Para loitar contra a posible pasividade do alumno, en certos momentos exponse pequenas cuestións, que fagan reflexionar ao alumno, complementando devanditos aspectos con referencias bibliográficas que lle permitan enriquecer o coñecemento adquirido. Este intercambio co alumno, como parte da lección maxistral, permítenos controlar o grao de asimilación dos coñecementos por parte do mesmo. As leccións maxistrais inclúen, tanto coñecementos extraídos das referencias da asginatura, como os resultantes de nosas propias experiencias profesionais, fomentando a capacidade de análise crítica. En todo momento búscase que certa parte dos contidos achegados non requiran do alumno unha tarefa de memorización. Esta metodoloxía tratará de conseguir un alto grao de motivación no alumno.
Análise de fontes documentais	Lectura e exame crítico dos principais documentos éticos da informática. Serven de introdución xeral aos temas. Proporcionan unha explicación histórica e sistemática do seu significado. Son de gran importancia no contexto do resto de metoloxías utilizadas na materia.

Prácticas de laboratorio	As prácticas de laboratorio permiten sacar o máximo proveito na retroalimentación, reforzo e asimilación dos obxectivos. Os desenvolvementos prácticos iníciansе cunha práctica básica, e elévase a súa dificultade paulatinamente. En todo momento preséntase ao alumno o conxunto de ideas e técnicas que permiten o desenvolvemento práctico dos coñecementos transmitidos nas sesións maxistrais. Nas prácticas proponse diversos apartados que expoñen unha batería de dificultades tratadas durante o estudo do tema. Buscarase a interrelación entre os distintos apartados, achegando un contexto de exercicio completo, para lograr no alumno unha visión de conxunto, revelando os nexos existentes entre cuestións que poderían parecer afastadas. En todas as clases prácticas utilízanse máquinas virtuais sobre computadoras como ferramenta básica para a resolución dos exercicios. O alumno poderá seleccionar e instalar aquelas ferramentas que considere máis oportunas en cada caso. Desta forma, requiriráselle, desde un primeiro momento, que se enfronte a toma de decisións, analizando as vantaxes e desvantaxes en todos e cada un dos casos. Neste punto inicial, será fundamental un asesoramento personalizado, que permita unha análise realista sobre as decisións tomadas, facilitando a retroalimentación de novos parámetros non considerados a priori.
Proba de resposta múltiple	Esta proba estará orientada a determinar se o alumno asimilou os distintos obxectivos da materia.
Estudo de casos	A análise ética e xurídica da informática ten unhas características específicas. Co estudo de casos preténdese examinar a estrutura e os contidos dos problemas presentes nos casos, tanto de maneira individual como en grupo. É unha forma de aprendizaxe de contidos e tamén metodolóxica, na que o estudante aprende a analizar, deliberar e chegar a conclusións fundamentadas e razoables cos argumentos éticos e xurídicos. Resulta de gran utilidade para exercitar as destrezas e habilidades argumentativas.

Atención personalizada	
Metodoloxías	**Descrición**
Prácticas de laboratorio	Prácticas de laboratorio.: Se guía ao alumno de forma individualizada no desenvolvemento de cada unha das prácticas de laboratorio. Aínda que no desenvolvemento da primeira práctica existen grandes diferenzas nas necesidades de cada alumno, progresivamente vanse homoxeneizando en canto ás súas necesidades de atención personalizada. Sen ningunha dúbida, a identificación deste parámetro é fundamental para determinar que a totalidade dos alumnos progresa durante o desenvolvemento da materia. Tamén faremos pequenos grupos de traballo conxunto en desenvolvementos prácticos. Atención personalizada.: Toda cuestión tecnolóxica exposta polo alumno, en persoa, tutorías, email., etc. En caso de detección de plaxio en calquera das probas (probas curtas, exames parciais ou exame final), a cualificación final será de SUSPENSO (0) e o feito será comunicado á dirección do Centro para os efectos oportunos. En todas as convocatorias (primeira oportunidade, segunda oportunidade e convocatoria extraordinaria) realizarase unha avaliación única tanto na parte práctica como na teórica.

Avaliación			
Metodoloxías	**Competencias / Resultados**	**Descrición**	**Cualificación**
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
Proba de resposta 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

Observacións avaliación

Fontes de información	
Bibliografía 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
Bibliografía complementaria	

Recomendacións
Materias que se recomenda ter cursado previamente
Seguridade da Información/614530003 Redes Seguras/614530006
Materias que se recomenda cursar simultaneamente
Conceptos e Leis en Ciberseguridade/614530001 Ciberseguridade en Contornos Industriais/614530014
Materias que continúan o temario
Traballo Fin de Máster/614530017 Xestión da Seguridade da Información/614530002
Observacións