



Guía Docente				
Datos Identificativos			2020/21	
Asignatura (*)	Test de Intrusión		Código	614530008
Titulación				
Descriptor				
Ciclo	Período	Curso	Tipo	Créditos
Mestrado Oficial	2º cuatrimestre	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).			



Plan de continxencia	1. Modificacións nos contidos Non se farán cambios. 2. Metodoloxías *Metodoloxías docentes que se manteñen Mantemos todas as metodoloxías en liña. *Metodoloxías docentes que se modifican 3. Mecanismos de atención personalizada ao alumnado Utilizaranse diferentes ferramentas .: Micorosft Teams.: para sesións maxistrais con gravación de vídeo, titorías e prácticas de laboratorio. Máquinas virtuais.: para prácticas de laboratorio. Forms, FAITIC e moodle.: para probas de resposta múltiple e comunicacións varias. Correo electrónico.: para comunicacións varias. 4. Modificacións na avaliación Sen modificacións pasan a ser en liña. 5. Modificacións da bibliografía ou webgrafía A mesma e incorpórase ás sesións maxistrais dispoñibles en vídeo. En caso de docencia non presencial (por parte do alumnado ou total), e se procede: - Non se modificarán os contidos da materia. En todo caso, a oferta de recursos ampliarase mediante material de apoio nas plataformas telemáticas (FAITIC, MOODLE e EQUIPOS), pero sen que isto signifique un aumento na materia. - Nin o modelo nin o barómetro de avaliación serán modificados salvo a posterior resolución rectoral. No caso de que tanto a práctica como o exame non se poidan realizar de xeito persoal, ambos os dous faranse empregando as plataformas TIC dispoñibles. - No caso de que os números de matrícula non respecten a capacidade, hai que ter en conta que, os alumnos asistirán a clases presenciais na aula ata que se alcance a capacidade e o resto dos alumnos seguirán sincrónicamente a clase conectándose á aulas de videoconferencia aos sistemas de ensinanza en liña síncrona UVIGO e UDC. Asistencia presencial e non presencial articularanse semanalmente. - Acceso en liña ás fontes documentais do tema (libros, manuais, etc.).
-----------------------------	--



Código	Competencias do título
--------	------------------------

Resultados da aprendizaxe			
Resultados de aprendizaxe	Competencias 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	
Enfrontarse 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 e obxetivos
Estratexias de recoñecemento	Pasivo vs Activo Scapy P0f Netdiscover
Estratexias ofensivas	Análise de vulnerabilidades Explotación de vulnerabilidades Elevación de privilexios Mantemento de acceso
Métodos de evasión	Contramedidas Borrado de pegadas

Planificación				
Metodoloxías / probas	Competencias	Horas presenciais	Horas non presenciais / 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 expónse 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 materia, 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 metodoloxías 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 iníciase 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 propónse 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, requiríraselle, desde un primeiro momento, que se enfrente 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, titorías, 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	Descrición	Cualificación
Prácticas de laboratorio	A4 B1 B6 B7	Cada alumno de prácticas de laboratorio deberá pasar varias probas. Nela o profesor expón pequenas tarefas que os alumnos deberán resolver sobre as máquinas virtuais do laboratorio de prácticas. É necesario obter unha nota promedio entre todas as prácticas de laboratorio superior a 4 para facer media.	60
Proba de resposta múltiple	B5 B6 B7	Esta proba inclúe os contidos e, en xeral, todo aspecto relacionado cos obxectivos da materia. Nela expónse diversas cuestións relacionadas tanto cos contidos das sesións maxistras como das prácticas de laboratorio, dándolle un maior peso ás primeiras. É necesario obter unha nota promedio superior a 4 para facer media.	40

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

(*)A Guía docente é o documento onde se visualiza a proposta académica da UDC. Este documento é público e non se pode modificar, salvo casos excepcionais baixo a revisión do órgano competente dacordo coa normativa vixente que establece o proceso de elaboración de guías