UNIVERSIDADE DA CORUÑA

Guía Docente				
Datos Identificativos				2023/24
Asignatura (*)	Test de Intrusión		Código	614530110
Titulación	Máster Universitario en Ciberseguridade			
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 Vázquez Naya, José Manuel	Correo electrónico	adrian.carballal@udc.es jose.manuel.vazquez.naya@udc.es	
Web	moovi.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 do título	
Código	Competencias do título
A30	HD-10 - Identificar y aprovechar, de manera analítica y práctica, vulnerabilidades de los sistemas de información, así como identificar posibles vectores de ataque e innovar en técnicas y procesos referidos al hacking ético
B26	K-10 - Diferenciar los vectores y técnicas de ciberataque más comunes, así como comprender y aplicar los métodos y técnicas de detección de vulnerabilidades en equipos informáticos, redes de comunicaciones, bases de datos, programas y/o servicios de información
C11	C-06 - Identificar vulnerabilidades en un sistema real, así como variar sus parámetros y configurarlo para su protección frente a ellas; limitando así la exposición a amenazas conocidas
C13	C-08 - Realizar test de intrusión en entornos prácticos complejos para la identificación de vulnerabilidades, así como para realizar ataques en entornos controlados con juicio crítico y ético
C14	C-09 - Aplicar métodos de investigación forense para el análisis de incidentes o riesgos de ciberseguridad mediante técnicas científicas y analíticas para identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal
C15	C-10 - Diseñar y gestionar la seguridad de infraestructuras para realizar la auditoría de seguridad de la infraestructura y garantizar continuidad de negocio bajo normas y estándares de referencia

Resultados da aprendizaxe			
Resultados de aprendizaxe	Competencias do título		
Identificar os riscos e vulnerabilidades dun sistema de información	AP30		
Identificar os mecanismos de seguridade e a súa integración nas organizacións	AP30		CP11
Utilizar ferramentas de seguridade			CP13
Enfrontrarse a casos reais e saber o que hai que facer, no menor tempo posible			CP13 CP15
Capacidade de análise e síntese	AP30	BP26	CP14

Contidos	
Temas	Subtemas

Fundamentos	Hacking ético Vulnerabilidades Vectores de ataque Tipos de Test de Intrusión Alcance e obxetivos
Estratexias de recoñeceminto	Pasivo vs Activo Scapy P0f Netdiscover
Estratexias ofensivas	Análise de vulnerabilidades Explotación de vulnerabilidades Elevación de privilexios Mantemento de acceso Pivoting
Métodos de evasión	Contramedidas Borrado de pegadas

Planificación				
Metodoloxías / probas	Competencias	Horas presenciais	Horas non presenciais / traballo autónomo	Horas totais
Sesión maxistral	C15	9	13.5	22.5
Análise de fontes documentais	C11	6	6	12
Proba de resposta múltiple	B26	1.5	0	1.5
Prácticas de laboratorio	C11 C13 C14	6	12	18
Prácticas de laboratorio	C11 C13 C14	4	8	12
Prácticas de laboratorio	C11 C13 C14	4	8	12
Prácticas de laboratorio	C11 C13 C14	4	8	12
Prácticas de laboratorio	C11 C13 C14	4	8	12
Prácticas de laboratorio	C11 C13 C14	4	8	12
Estudo de casos	A30 C13	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 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.
Proba de resposta múltiple	Esta proba estará orientada a determinar se o alumno asimilou os distintos obxectivos da materia.
Prácticas de laboratorio	Cada alumno de prácticas de laboratorio deberá realizar unha proba de penetración sobre unha máquina virtual preconfigurada polo profesorado. O alumno deberá presentar un documento que acredite tódolos pasos realizados para o desempeño da práctica.
Prácticas de laboratorio	Cada alumno de prácticas de laboratorio deberá realizar unha proba de penetración sobre unha máquina virtual preconfigurada polo profesorado. O alumno deberá presentar un documento que acredite tódolos pasos realizados para o desempeño da práctica.
Prácticas de laboratorio	Cada alumno de prácticas de laboratorio deberá realizar unha proba de penetración sobre unha máquina virtual preconfigurada polo profesorado. O alumno deberá presentar un documento que acredite tódolos pasos realizados para o desempeño da práctica.
Prácticas de laboratorio	Cada alumno de prácticas de laboratorio deberá realizar unha proba de penetración sobre unha máquina virtual preconfigurada polo profesorado. O alumno deberá presentar un documento que acredite tódolos pasos realizados para o desempeño da práctica.
Prácticas de laboratorio	Cada alumno de prácticas de laboratorio deberá realizar unha proba de penetración sobre unha máquina virtual preconfigurada polo profesorado. O alumno deberá presentar un documento que acredite tódolos pasos realizados para o desempeño da práctica.
Prácticas de laboratorio	Cada alumno de prácticas de laboratorio deberá realizar unha proba de penetración sobre unha máquina virtual preconfigurada polo profesorado. O alumno deberá presentar un documento que acredite tódolos pasos realizados para o desempeño da práctica.
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 Prácticas de laboratorio Prácticas de laboratorio Prácticas de laboratorio 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	C11 C13 C14	Practica 2: Cada alumno de prácticas de laboratorio deberá realizar unha proba de penetración sobre unha máquina virtual preconfigurada polo profesorado. O alumno disporá dun calendario determinado para a resolución da mesma, e nos casos onde dito calendario non se cumpra a nota de dita practica será penalizada. O alumno deberá presentar un documento que acredite tódolos pasos realizados para o desempeño da práctica.	10
Prácticas de laboratorio	C11 C13 C14	Practica 3: Cada alumno de prácticas de laboratorio deberá realizar unha proba de penetración sobre unha máquina virtual preconfigurada polo profesorado. O alumno disporá dun calendario determinado para a resolución da mesma, e nos casos onde dito calendario non se cumpra a nota de dita practica será penalizada. O alumno deberá presentar un documento que acredite tódolos pasos realizados para o desempeño da práctica.	10
Prácticas de laboratorio	C11 C13 C14	Practica 4: Cada alumno de prácticas de laboratorio deberá realizar unha proba de penetración sobre unha máquina virtual preconfigurada polo profesorado. O alumno disporá dun calendario determinado para a resolución da mesma, e nos casos onde dito calendario non se cumpra a nota de dita practica será penalizada. O alumno deberá presentar un documento que acredite tódolos pasos realizados para o desempeño da práctica.	10
Prácticas de laboratorio	C11 C13 C14	Practica 5: Cada alumno de prácticas de laboratorio deberá realizar unha proba de penetración sobre unha máquina virtual preconfigurada polo profesorado. O alumno disporá dun calendario determinado para a resolución da mesma, e nos casos onde dito calendario non se cumpra a nota de dita practica será penalizada. O alumno deberá presentar un documento que acredite tódolos pasos realizados para o desempeño da práctica.	10
Prácticas de laboratorio	C11 C13 C14	Practica 6: Cada alumno de prácticas de laboratorio deberá realizar unha proba de penetración sobre unha máquina virtual preconfigurada polo profesorado. O alumno disporá dun calendario determinado para a resolución da mesma, e nos casos onde dito calendario non se cumpra a nota de dita practica será penalizada. O alumno deberá presentar un documento que acredite tódolos pasos realizados para o desempeño da práctica.	10
Proba de resposta múltiple	B26	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. É necesario obter unha nota promedio superior a 4 para facer media.	40
Prácticas de laboratorio	C11 C13 C14	Practica 1: Cada alumno de prácticas de laboratorio deberá realizar unha proba de penetración sobre unha máquina virtual preconfigurada polo profesorado. O alumno disporá dun calendario determinado para a resolución da mesma, e nos casos onde dito calendario non se cumpra a nota de dita practica será penalizada. O alumno deberá presentar un documento que acredite tódolos pasos realizados para o desempeño da práctica.	10

Observacións avaliación

Seguindo as directrices propias da titulación ofertarase a quen curse esta materia dous sistemas de avaliación: avaliación continua e avaliación global. Cando finalice o primeiro mes do curso, o estudantado deberán indicar ao profesorado da materia o sistema de avaliación elixido. Quen opte polo sistema de avaliación continua non poderá ser cualificado como "non presentado" se realiza unha entrega ou proba de avaliación con posterioridade á comunicación da súa decisión.

Sistema de avaliación continua

O estudantado que opte polo sistema de avaliación continua deberán:

-Realizar seis prácticas de laboratorio de probas de penetración. O alumno disporá dun calendario determinado para a resolución da mesma, e nos casos onde dito calendario non se cumpra a nota de dita practica será penalizada. Estas probas suporán un 60 % da cualificación global da materia, un 10% cada unha delas.

-Realizar unha proba de resposta múltiple sobre os contidos das sesións maxistrais e as prácticas de laboratorio. Esta proba suporá un 40 % da cualificación global da materia e é necesario sacar un mínimo de 4 sobre 10 para aprobar a materia.

A cualificación global da materia será igual á suma das tarefas indicadas. Para superar a materia a cualificación global debe ser maior ou igual que cinco.

Sistema de avaliación global

O estudantado que opte polo sistema de avaliación ao final do cuadrimestre deberán:

-Realizar unha proba de penetración dada nun tempo definido polos docentes. Esta proba suporá un 60 % da cualificación global da materia.

-Realizar unha proba de resposta múltiple sobre os contidos das sesións maxistrais e as prácticas de laboratorio. Esta proba suporá un 40 % da cualificación global da materia e é necesario sacar un mínimo de 4 sobre 10 para aprobar a materia.

A cualificación global da materia será igual á suma das tarefas indicadas. Para superar a materia a cualificación global debe ser maior ou igual que cinco.

OPORTUNIDADE EXTRAORDINARIA

Á avaliación en oportunidade extraordinaria só poderán presentarse aqueles estudantes que non se presentaron ou que suspenderon a materia na oportunidade ordinaria.

A avaliación consistirá en realizar unha ou dúas das seguintes tarefas, dependendo da cualificación obtida previamente nas probas equivalentes da oportunidade ordinaria:

-Realizar unha proba de penetración dada nun tempo definido polos docentes. Esta proba suporá un 60 % da cualificación global da materia.

-Realizar unha proba de resposta múltiple sobre os contidos das sesións maxistrais e as prácticas de laboratorio. Esta proba suporá un 40 % da cualificación global da materia e é necesario sacar un mínimo de 4 sobre 10 para aprobar a materia.

No caso de que a cualificación nas probas da oportunidade ordinaria, equivalentes a estas, sexa maior ou igual que cinco, o alumno pode optar por manter a súa nota da oportunidade ordinaria ou realizar a proba de novo.

OUTROS COMENTARIOS

-As puntuacións obtidas só son válidas para o curso académico en vigor.

-O uso de calquera material durante a realización dos exames e probas de avaliación terá que ser autorizado explicitamente polo profesorado da materia.

-En caso de detección de copia en calquera das probas (probas curtas, exames parciais ou exame final), cualificación final será de SUSPENSO (0) e o feito será comunicado á dirección do Centro para os efectos oportunos

Fontes de información	
Bibliografía básica	- Mike Schiffman (2001). Hacker's Challenge. Osborne - Pablo Gonzalez Perez, Germán Sánchez Garcés, Jose Miguel Soriano de la Cámara (2013). Pentesting con Kali. 0xWORD - 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 - Crystal Panek; Robb Tracy (2019). CompTIA pentest+ practice tests : exam PT0-001. Independiente - María Ángeles Caballero Velasco, Diego Cilleros Serrano (2022). El libro del Hacker. Edición 2022. Anaya
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
- Segundo se recolle nas distintas normativas de aplicación para a docencia universitaria deberase incorporar a perspectiva de xénero nesta materia (usarase linguaxe non sexista, utilizarase bibliografía de autores/as de ambos sexos, propiciarase a intervención en clase de alumnos e alumnas...)- Traballarase para identificar e modificar prexuízos e actitudes sexistas e influirase na contorna para modificalos e fomentar valores de respecto e igualdade.- Deberanse detectar situacións de discriminación por razón de xénero e proporanse accións e medidas para corrixilas.