



| Guía Docente | | | | |
|-----------------------|--|--------------------|-------------------------|----------|
| Datos Identificativos | | | | 2019/20 |
| Asignatura (*) | Test de Intrusión | Código | 614530008 | |
| Titulación | Máster Universitario en Ciberseguridade | | | |
| Descritores | | | | |
| 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). | | | |

| Competencias / Resultados do título | |
|-------------------------------------|---|
| Código | Competencias / Resultados do título |
| A2 | CE2 - Coñecer en profundidade as técnicas de ciberataque e ciberdefensa |
| A3 | CE3 - Coñecer a normativa técnica e legal de aplicación en materia de ciberseguridade, as súas implicacións no deseño de sistemas, no uso de ferramentas de seguridade e na protección da información |
| A4 | CE4 - Comprender e aplicar os métodos e técnicas de ciberseguridade aplicables ós datos, os equipos informáticos, as redes de comunicacións, as bases de datos, os programas e os servizos de información |
| A7 | CE7 - Ter capacidade para realizar a auditoría de seguridade de sistemas e instalacións, o análise de riscos derivados de debilidades de ciberseguridade e desenvolver o proceso de certificación de sistemas seguros |
| B1 | CB1 - Posuír e comprender coñecementos que aporten unha base ou oportunidade de ser orixinais no desenvolvemento e aplicación de ideas, a miúdo nun contexto de investigación |
| B2 | CB2 - Que os estudantes saiban aplicar os coñecementos adquiridos e a súa capacidade de resolución de problemas en contornas novas ou pouco coñecidas dentro de contextos máis amplos (ou multidisciplinares) relacionados coa súa área de estudo |
| B3 | CB3 - Que os estudantes sexan capaces de integrar coñecementos e enfrontarse á complexidade de formar xuízos a partir dunha información que, sendo incompleta ou limitada, inclúa reflexións sobre as responsabilidades sociais e éticas vinculadas á aplicación dos seus coñecementos e xuízos |
| B4 | CB4 - Que os estudantes saiban comunicar as súas conclusións ---e os coñecementos e razóns últimas que as sustentan--- a públicos especializados e non especializados de un modo claro e sen ambigüidades |
| B5 | CB5 - Que os estudantes posúan as habilidades de aprendizaxe que lles permitan continuar estudando dun modo que habrá de ser en gran medida autodirixido ou autónomo |
| B6 | CG1 - Ter capacidade de análise e síntesis. Ter capacidade para proxectar, modelar, calcular e diseñar solucións de seguridade da información, as redes e/ou os sistemas de comunicacións en todos os ámbitos de aplicación |
| B7 | CG2 - Resolución de problemas. Ter capacidade de resolver, cos coñecementos adquiridos, problemas específicos do ámbito técnico da seguridade da información, as redes e/ou os sistemas de comunicacións |
| B9 | CG4 - Compromiso ético. Capacidad para diseñar e implantar solucións 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 a importancia da seguridade da información no avance socioeconómico da sociedade |

| 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 | |
| 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 y objetivos |
| Estrategias de reconecimiento | Pasivo vs Activo Scapy P0f Netdiscover |
| Estrategias ofensivas | Análisis de vulnerabilidades Explotación de vulnerabilidades Elevación de privilegios Mantenimiento de acceso |
| Métodos de evasión | Contra medidas 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 | <p>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.</p> <p>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.</p> <p>As leccións maxistras inclúen, tanto coñecementos extraídos das referencias da asignatura, 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.</p> |
| Análise de fontes documentais | <p>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.</p> |
| Prácticas de laboratorio | <p>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 maxistras. 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, requiriráselle, 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.</p> |
| Proba de resposta múltiple | <p>Esta proba estará orientada a determinar se o alumno asimilou os distintos obxectivos da materia.</p> |
| Estudo de casos | <p>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.</p> |

Atención personalizada

| Metodoloxías | Descrición |
|--------------|------------|
|--------------|------------|



| | |
|--------------------------|---|
| Prácticas de laboratorio | <p>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.</p> <p>Atención personalizada.: Toda cuestión tecnolóxica exposta polo alumno, en persoa, tutorías, email., etc.</p> <p>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.</p> <p>En todas as convocatorias (primeira oportunidade, segunda oportunidade e convocatoria extraordinaria) realizarase unha avaliación única tanto na parte práctica como na teórica.</p> |
|--------------------------|---|

| 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 expone diversas cuestións relacionadas tanto cos contidos das sesións maxistras como das prácticas de laboratorio, dándolle un maior peso ás primeiras. | 70 |

| Observacións avaliación |
|-------------------------|
| |

| Fontes de información | |
|------------------------------------|--|
| Bibliografía básica | <ul style="list-style-type: none"> - 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