Teaching Guide				
Identifying Data				2023/24
Subject (*)	Penetration Testing		Code	614530110
Study programme	Máster Universitario en Ciberseguridade			
Descriptors				
Cycle	Period	Year	Type	Credits
Official Master's Degree	2nd four-month period	First	Obligatory	5
Language	SpanishGalician			
Teaching method	Face-to-face			
Prerequisites				
Department	Ciencias da Computación e Tecnoloxías da InformaciónComputación			
Coordinador	Carballal Mato, Adrián	E-mail	adrian.carballal@udc.es	
Lecturers	Carballal Mato, Adrián Vázquez Naya, José Manuel	E-mail	adrian.carballal@udc.es jose.manuel.vazquez.naya@udc.es	
Web	moovi.uvigo.es			
General description	There is no better way to prove the strength of a system than to attack it. The Intrusion Tests serve to reproduce access attempts of an attacker using the vulnerabilities that may exist in a given infrastructure. In this course the fundamental topics oriented to the intrusion tests (pentesting) will be covered, covering the different phases of an attack and exploitation (from the recognition and control of access to the erasure of tracks).			

Study programme competences / results	
Code	Study programme competences / results
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

Learning outcomes			
Learning outcomes	Study programme competences / results		
Identify the risks and vulnerabilities of an information system	AJ30		
Identify security mechanisms and their integration in organizations	AJ30		CJ11
Use security tools			CJ13
Facing real cases and knowing what to do in the shortest possible time			CJ13 CJ15
Capacity for analysis and synthesis	AJ30	BJ26	CJ14

Contents	
Topic	Sub-topic

Fundamentals	Ethical hacking Vulnerabilities Attack vectors Types of Intrusion Test Reach and objectives
Recognition strategies	Passive vs. Active Scapy P0f Netdiscover
Offensive strategies	Vulnerability analysis Exploitation of vulnerabilities Elevation of privileges Access maintenance Pivoting
Evasion methods	Countermeasures Erased footprints

Planning				
Methodologies / tests	Competencies / Results	Teaching hours (in-person & virtual)	Student?s personal work hours	Total hours
Guest lecture / keynote speech	C15	9	13.5	22.5
Document analysis	C11	6	6	12
Multiple-choice questions	B26	1.5	0	1.5
Laboratory practice	C11 C13 C14	6	12	18
Laboratory practice	C11 C13 C14	4	8	12
Laboratory practice	C11 C13 C14	4	8	12
Laboratory practice	C11 C13 C14	4	8	12
Laboratory practice	C11 C13 C14	4	8	12
Laboratory practice	C11 C13 C14	4	8	12
Case study	A30 C13	5	6	11
Personalized attention		0		0
(*)The information in the planning table is for guidance only and does not take into account the heterogeneity of the students.				

Methodologies	
Methodologies	Description
Guest lecture / keynote speech	Transmission of information and key knowledge of each one of the topics. The participation of students is encouraged at certain times. As part of the methodology, a critical approach to the discipline will lead students to reflect and discover the relationships between different concepts, form a critical mentality to face the problems and the existence of a method, facilitating the learning process in the student . To fight against the possible passivity of the student, in small moments small questions, that reflect on the student, are presented, complementing those aspects with bibliographical references that allow him to enrich the knowledge acquired. This exchange with the student, as part of the master class, allows us to control the degree of assimilation of knowledge on the part of him. The magisterial lessons include, as much knowledge extracted from the references of the course, as those resulting from our own professional experiences, fostering the capacity of the critical analysis. At all times it is sought that a certain part of the content does not require the student to memorize them. This methodology will attempt to achieve a high degree of motivation in the student.

Document analysis	Reading and critical examination of the main ethical documents of computer science. They serve as a general introduction to the topics. They provide a historical and systematic explanation of its meaning. They are of great importance in the context of the other methodologies used in the subject.
Multiple-choice questions	This test will be oriented to determine if the student has assimilated the different objectives of the subject.
Laboratory practice	Each student of laboratory practices must perform a penetration test on a virtual machine preconfigured by the teaching staff. The student must present a document that accredits the steps taken for the performance of the practice.
Laboratory practice	Each student of laboratory practices must perform a penetration test on a virtual machine preconfigured by the teaching staff. The student must present a document that accredits the steps taken for the performance of the practice.
Laboratory practice	Each student of laboratory practices must perform a penetration test on a virtual machine preconfigured by the teaching staff. The student must present a document that accredits the steps taken for the performance of the practice.
Laboratory practice	Each student of laboratory practices must perform a penetration test on a virtual machine preconfigured by the teaching staff. The student must present a document that accredits the steps taken for the performance of the practice.
Laboratory practice	Each student of laboratory practices must perform a penetration test on a virtual machine preconfigured by the teaching staff. The student must present a document that accredits the steps taken for the performance of the practice.
Laboratory practice	Each student of laboratory practices must perform a penetration test on a virtual machine preconfigured by the teaching staff. The student must present a document that accredits the steps taken for the performance of the practice.
Case study	The ethical and legal analysis of information technology has specific characteristics. With the case study, it is intended to examine the structure and content of the problems present in the cases, both individually and in groups. It is a form of content learning and also methodological, in which the student learns to analyze, deliberate and reach reasonable and reasonable conclusions with ethical and legal arguments. It is very useful for exercising the abilities and argumentative abilities.

Personalized attention	
Methodologies	**Description**
Laboratory practice Laboratory practice Laboratory practice Laboratory practice Laboratory practice Laboratory practice	Laboratory practices: If you guide the student individually in the development of each of the laboratory practices. Although in the development of the first practice there are large differences in the needs of each student, they are progressively homogenizing in terms of their personalized attention needs. Without a doubt, the identification of this parameter is fundamental to determine that the totality of the students progresses during the development of the subject. We will also make small groups work together in practical developments. Personalized attention: Any technological question exposed by the student, in person, tutorials, email, etc. Plagiarism is regarded as serious dishonest behavior. If any form of plagiarism is detected in any of the tests or exams, the final grade will be FAIL (0), and the incident will be reported to the corresponding academic authorities for prosecution. All calls (first call, second call and end-of-program call) will perform an unique final assessment for both practical and theoretical.

Assessment			
Methodologies	**Competencies / Results**	**Description**	**Qualification**
Laboratory practice	C11 C13 C14	Practice 2: Each student of laboratory practices must perform a penetration test on a virtual machine preconfigured by the teaching staff. The student will have a specific calendar for the resolution of the same, and in cases where said calendar is not fulfilled the note of said practice will be penalized. The student must present a document that accredits the steps taken for the performance of the practice.	10

Laboratory practice	C11 C13 C14	Practice 3: Each student of laboratory practices must perform a penetration test on a virtual machine preconfigured by the teaching staff. The student will have a specific calendar for the resolution of the same, and in cases where said calendar is not fulfilled the note of said practice will be penalized. The student must present a document that accredits the steps taken for the performance of the practice.	10
Laboratory practice	C11 C13 C14	Practice 4: Each student of laboratory practices must perform a penetration test on a virtual machine preconfigured by the teaching staff. The student will have a specific calendar for the resolution of the same, and in cases where said calendar is not fulfilled the note of said practice will be penalized. The student must present a document that accredits the steps taken for the performance of the practice.	10
Laboratory practice	C11 C13 C14	Practice 5: Each student of laboratory practices must perform a penetration test on a virtual machine preconfigured by the teaching staff. The student will have a specific calendar for the resolution of the same, and in cases where said calendar is not fulfilled the note of said practice will be penalized. The student must present a document that accredits the steps taken for the performance of the practice.	10
Laboratory practice	C11 C13 C14	Practice 6: Each student of laboratory practices must perform a penetration test on a virtual machine preconfigured by the teaching staff. The student will have a specific calendar for the resolution of the same, and in cases where said calendar is not fulfilled the note of said practice will be penalized. The student must present a document that accredits the steps taken for the performance of the practice.	10
Multiple-choice questions	B26	This test includes the contents and, in general, all aspects related to the objectives of the subject. It establishes several topics related both to the content of the master sessions and to the laboratory practices, giving more weight to the first one. It is necessary to obtain an average grade higher than 4 to do average.	40
Laboratory practice	C11 C13 C14	Practice 1: Each student of laboratory practices must perform a penetration test on a virtual machine preconfigured by the teaching staff. The student will have a specific calendar for the resolution of the same, and in cases where said calendar is not fulfilled the note of said practice will be penalized. The student must present a document that accredits the steps taken for the performance of the practice.	10

Assessment comments

ORDINARY OPPORTUNITY

Following the guidelines of the degree, those taking this course will be offered two evaluation systems: continuous evaluation and global evaluation. At the end of the first month of the course, students must indicate the chosen evaluation system to the professors of the course. Those who choose the continuous evaluation system will not be graded as "no-shows" if they take a delivery or evaluation test after the notification of their decision.

Continuous evaluation system

Students who opt for the continuous evaluation system must:

-Perform six laboratory practices of penetration tests. The student will have a specific calendar for the resolution of the same ones, and in the cases in which this calendar is not fulfilled, the grade of the above mentioned practice will be penalized. These tests will account for 60% of the overall grade of the course, 10% each.

- To take a multiple-choice test on the contents of the lectures and laboratory practices. This test will represent 40% of the overall grade of the course and it is necessary to get a minimum of 4 out of 10 to pass the course.

The overall grade for the course will be equal to the sum of the indicated assignments. In order to pass the course, the overall grade must be greater or equal to five.

Overall evaluation system

Students who opt for the evaluation system at the end of the semester must:

- Take a penetration test given at a time defined by the professors. This test will account for 60% of the overall grade of the course.

- Take a multiple-choice test on the contents of the lectures and laboratory practices. This test will represent 40% of the overall grade of the course and it is necessary to get a minimum of 4 out of 10 to pass the course.

The overall grade of the course will be equal to the sum of the indicated tasks. In order to pass the course, the overall grade must be greater or equal to five.

EXTRAORDINARY OPPORTUNITY

Only those students who did not present themselves or failed the subject in the ordinary opportunity will be able to present themselves for the evaluation in the extraordinary opportunity.

The evaluation will consist of the completion of one or two of the following tasks, depending on the grade previously obtained in the equivalent tests of the ordinary opportunity:

- Performing a given penetration test in a time defined by the teachers. This test will account for 60% of the overall grade of the subject.

- To take a multiple-choice test on the contents of the lectures and laboratory practices. This test will represent 40% of the overall grade of the course and it is necessary to get a minimum of 4 out of 10 to pass the course.

In the case that the grade in the ordinary opportunity tests, equivalent to these, is higher or equal to five, the student may choose to keep his ordinary opportunity grade or retake the test.

OTHER COMMENTS

-The scores obtained are only valid for the current academic year.

- The use of any material during exams and evaluation tests must be expressly authorized by the faculty of the subject.

-In case of detection of copying in any of the tests (short tests, partial exams or final exam), the final grade will be SUSPENSION (0) and the fact will be communicated to the direction of the Center for the appropriate effects

.

Sources of information	
Basic	- 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
Complementary	

Recommendations
Subjects that it is recommended to have taken before
Information Security/614530003 Secure Networks/614530006
Subjects that are recommended to be taken simultaneously
Cibersecurity Concepts and Laws/614530001 Cybersecurity in Industrial Environments /614530014
Subjects that continue the syllabus
Final Year Dissertation/614530017 Information Security Mangement/614530002
Other comments
- As stated in the different regulations of application for university teaching, the gender perspective must be incorporated in this subject (non-sexist language will be used, bibliography of authors of both sexes will be used, intervention in class of students will be encouraged...)- Work to identify and modify sexist prejudices and attitudes and influence the environment to modify them and promote values of respect and equality.- Situations of discrimination on the basis of gender should be detected and actions and measures will be proposed to correct them.