UNIVERSIDADE DA CORUÑA

Teaching Guide				
Identifying Data				2020/21
Subject (*)	Penetration Testing		Code	614530008
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	E-mail	adrian.carballal@udc.es	
Web	faitic.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).			

Contingency plan	1. Modifications in the contents. No changes will be made. 2. Methodologies * Teaching methodologies that are maintained We keep all methodologies online. * Teaching methodologies that change 3. Mechanisms for personalised attention to students. Different tools will be used: Micorosft equipment: For master sessions with video recording, tutorials and laboratory practices. Virtual machines: For laboratory practices. Forms, FAITIC and moodle: For multiple choice tests and several communications. E-mail: For several communications. 4. Modifications in the evaluation. No modifications. 5. Modifications to the bibliography or webography. The master sessions will be available on video. In case of non-attendance teaching (either for part of the students or the whole), and if applicable: - The contents of the subject will not be modified. In any case, the offer of resources will be extended by means of support material in the telematic platforms (FAITIC, MOODLE and TEAMS), but without meaning an increase in the subject. - Neither the model nor the evaluation barometer will be modified except for subsequent rectoral resolution. In the case that both the practice and the exam cannot be done in person, both will be done using the available ICT platforms. - In the case that the registration numbers do not respect the capacity, it must be taken into account that the students will attend classes in the classroom until the capacity is full and the rest of the students will follow the class synchronously by connecting the videoconference rooms to the synchronous online teaching systems of UVIGO and UDC. Attendance and non-attendance will be articulated on a weekly basis. - Online access to the documentary sources of the subject (books, manuals, etc.).

Study programme competences / results	
Code	Study programme competences / results
A2	CE2 - Deep knowledge of cyberattack and cyberdefense techniques

A3	CE3 - Knowledge of the legal and technical standards used in cybersecurity, their implications in systems design, in the use of security tools and in the protection of information
A4	CE4 - To understand and to apply the methods and tools of cybersecurity to protect data and computers, communication networks, databases, computer programs and information services
A7	CE7 - To demonstrate ability for doing the security audit of systems, equipment, the risk analysis related to security weaknesses, and for developing de procedures for certification of secure systems
B1	CB1 - To possess and understand the knowledge that provides the foundations and the opportunity to be original in the development and application of ideas, frequently in a research context
B2	CB2 - Students will be able to apply their knowledge and their problem-solving ability in new or less familiar situations, within a broader context (or in multi-discipline contexts) related to their field of specialization
B3	CB3 - Students will be able to integrate diverse knowledge areas, and address the complexity of making statements on the basis of information which, notwithstanding incomplete or limited, may include thoughts about the ethical and social responsibilities entailed to the application of their professional capabilities and judgements
B4	CB4 - Students will learn to communicate their conclusions ---and the hypotheses and ultimate reasoning in their support--- to expert and nonexpert audiences in a clear and unambiguous way
B5	CB5 - Students will apprehend the learning skills enabling them to study in a style that will be selfdriven and autonomous to a large extent
B6	CG1 - To have skills for analysis and synthesis. To have ability to project, model, calculate and design solutions in the area of information, network or system security in every application area
B7	CG2 - Ability for problem-solving. Ability to solve, using the acquired knowledge, specific problems in the technical field of information, network or system security
B9	CG4 - Ethical commitment. Ability to design and deploy engineering systems and management systems with ethical and responsible criteria, based on deontological behaviour, in the field of information, network or communications security
C4	CT4 - Ability to ponder the importance of information security in the economic progress of society

Learning outcomes			
Learning outcomes	Study programme competences / results		
Identify the risks and vulnerabilities of an information system	AJ2 AJ4 AJ7	BJ6 BJ9	
Identify security mechanisms and their integration in organizations	AJ2 AJ3 AJ4 AJ7		
Use security tools	AJ2 AJ4	BJ2	
Facing real cases and knowing what to do in the shortest possible time	AJ4 AJ7	BJ4 BJ7	
Capacity for analysis and synthesis		BJ1 BJ3 BJ5	CJ4

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
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	A2 B9 C4	9	13.5	22.5
Document analysis	A2 A3 A7 B4 B6	6	6	12
Laboratory practice	A4 B1 B6 B7	26	52	78
Multiple-choice questions	B5 B6 B7	1.5	0	1.5
Case study	B2 B3 B5 B7	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.

Laboratory practice	The laboratory practices allow to maximize the feedback, reinforcement and assimilation of the objectives. Practical developments begin with a basic practice and their difficulty increases gradually. At all times, the student presents the set of ideas and techniques that allow the practical development of the knowledge transmitted in master classes. In the practices several sections are proposed that expose a battery of difficulties treated during the study of the subject. The interrelation between the different sections will be sought, providing a context of full exercise, in order to achieve the student's vision as a whole, revealing the links between the questions that may seem very distant. In all practical classes, virtual machines are used on computers as a basic tool for solving exercises. The student can select and install the tools that he deems most appropriate in each case. In this way, you will be required, from the beginning, to face the decision making, analyzing the advantages and disadvantages in each and every one of the cases. At this initial point, personalized advice will be essential, allowing a realistic analysis of the decisions made, facilitating the feedback of new parameters not considered a priori.
Multiple-choice questions	This test will be oriented to determine if the student has assimilated the different objectives of the subject.
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 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	A4 B1 B6 B7	Each student of laboratory practices will have to pass several tests. In it, the teacher explains small tasks that students must solve in the virtual machines of the practice laboratory. It is necessary to obtain an average grade among all the laboratory practices greater than 4 to make average.	60
Multiple-choice questions	B5 B6 B7	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

Assessment comments

Contingency plan In case of non-attendance teaching (either for part of the students or the whole), and if applicable: - The contents of the subject will not be modified. In any case, the offer of resources will be extended by means of support material in the telematic platforms (FAITIC, MOODLE and TEAMS), but without meaning an increase in the subject. - Neither the model nor the evaluation barometer will be modified except for subsequent rectoral resolution. In the case that both the practice and the exam cannot be done in person, both will be done using the available ICT platforms. - In the case that the registration numbers do not respect the capacity, it must be taken into account that the students will attend classes in the classroom until the capacity is full and the rest of the students will follow the class synchronously by connecting the videoconference rooms to the synchronous online teaching systems of UVIGO and UDC. Attendance and non-attendance will be articulated on a weekly basis. - Online access to the documentary sources of the subject (books, manuals, etc.).

Sources of information	
Basic	- 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
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

(*)The teaching guide is the document in which the URV publishes the information about all its courses. It is a public document and cannot be modified. Only in exceptional cases can it be revised by the competent agent or duly revised so that it is in line with current legislation.