Teaching Guide				
Identifying Data				2019/20
Subject (*)	Operating Systems Hardening		Code	614530007
Study programme	Máster Universitario en Ciberseguridade			
Descriptors				
Cycle	Period	Year	Type	Credits
Official Master's Degree	2nd four-month period	First	Obligatory	5
Language	SpanishGalicianEnglish			
Teaching method	Face-to-face			
Prerequisites				
Department	Ciencias da Computación e Tecnoloxías da InformaciónComputación			
Coordinador	Yañez Izquierdo, Antonio Fermin	E-mail	antonio.yanez@udc.es	
Lecturers	Yañez Izquierdo, Antonio Fermin	E-mail	antonio.yanez@udc.es	
Web	faitic.uvigo.es			
General description	A newly installed Operating system is inherently insecure. It has a certain number of vulnerabilities, depending on such things such as the age of the O.S., the amount of services it provides, the existence of initial backdoors not already patched, and the use of default policies designed without security in mind By Hardening Operating Systems we refer to the act of configuring an operating system with the aim of making it as secure as possible, so that we minimize the risk of getting it compromised. This usually implies applying patches, changing default O.S. policies, and removing (or disabling) non-essential aplications and/or services. In this course we'll try to identify common O.S. vulnerabilities and how to defend the O.S. against them. Both UNIX (linux) and Windows type O.S. will be considered.			

Study programme competences	
Code	Study programme competences
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
A5	CE5 - To design, deploy and operate a security management information system based on a referenced methodology
A8	CE8 - Skills for conceive, design, deploy and operate cybersecurity systems
A9	CE9 - Ability to write clear, concise and motivated projects and work plans in the field of cybersecurity
A11	CE11 - Ability to collect and interpret relevant data the field of computer and communications security
A13	CE13 - Ability for analysing, detecting and eliminating software vulnerabilities and malware capable to exploit those in systems or networks
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
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
B8	CG3 - Capacity for critical thinking and critical evaluation of any system designed for protecting information, any information security system, any system for network security or system for secure communication
B10	CG5 - Students will have ability to apply theoretical knowledge to practical situations, within the scope of infrastructures, equipment or specific application domains, and designed for precise operating requirements
C3	CT3 - Ability to include sustainability principles and environmental concerns in the professional practice. To integrate into projects the principle of efficient, responsible and equitable use of resources
C4	CT4 - Ability to ponder the importance of information security in the economic progress of society

Learning outcomes			
Learning outcomes	Study programme competences		
To identify the different vulnerabilities that affect an operating system		BJ2 BJ5 BJ6 BJ7 BJ10	
To understand how the vulnerabilities work and how the O.S. can be protected from them	AJ8	BJ2 BJ5 BJ6 BJ7 BJ10	
To configure an O.S so that we minimize its exposure to threats, minimizing the risk of getting it compromised	AJ3 AJ4 AJ5 AJ8 AJ9 AJ11 AJ13	BJ2 BJ5 BJ6 BJ7 BJ8	CJ3 CJ4

Contents	
Topic	Sub-topic
Introduction to H.O.S.	The concept of hardening an operating system. Vulnerabilities. Hardening during installation, post installation and maintenance.
Boot procedure hardening	Physycal system security. Hardening the Firmware (BIOS, UEFI). Hardening the Boot Loader
Hardening user acounts	Identifying and eliminating non used accounts. Limiting user privileges. Group Policies. Hardening authentification. Forcing Password policies
Hardening File Systems	File system permissions and protections. Quotas. Locking system directories. Encryption. Limiting access to devices
Hardening applications	Identifying and eliminating non used applications. Identifying connections and eliminating apps/packeges providing unwanted connections. Limiting applications provileges. Excuting in secure enviroments: container based execution, SELinux...
Hardening network	Identify and eliminate unwanted connections/services. Packet filetring
Monitoring and maintenance	System monitoring. Logs. Securing logs. Identifying possible threats. Security patches.

Planning				
Methodologies / tests	Competencies	Ordinary class hours	Student?s personal work hours	Total hours
Introductory activities	A8 A11 A13 B6	1	2	3
Guest lecture / keynote speech	A3 A4 A11 A13 B5 B6 B8 B10 C3	16	32	48
Problem solving	A3 A4 A5 B2 B5 B7 B8 B10 C3	5	15	20
Laboratory practice	A4 A5 A8 A9 A11 A13 B2 B5 B6 B7 B8 B10 C3	16	16	32

Objective test	A3 A4 A5 A8 A9 A11 A13 B2 B5 B6 B7 B8 B10 C3 C4	2	20	22
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**
Introductory activities	Introductory activities to get the students acquainted with O.S. vulnerabilities and their defence against them
Guest lecture / keynote speech	The student will attend to the lectures given by the teacher about how to minimize the chance of having usable vulnerabilities in the different parts of an O.S.: boot procedure, user accounts, network connections,,,
Problem solving	Problems and short practical questions to consolidate the contents presented in the master classes.
Laboratory practice	Lab assignments diealing with securing the different parts of real world operating systems. Both UNIX (linux) and windows types will be considered
Objective test	Test about the fundamental contents of the subject

Personalized attention	
Methodologies	**Description**
Guest lecture / keynote speech Problem solving Laboratory practice	Although lab assignments,and problem solving will be dealt with mostly in the allocated lab/room hours, the teacher will be available to help with any question arising from these items in a individualized basis. The same will stand for the concepts exposed during the keynote speeches

Assessment			
Methodologies	**Competencies**	**Description**	**Qualification**
Objective test	A3 A4 A5 A8 A9 A11 A13 B2 B5 B6 B7 B8 B10 C3 C4	Questions related to the knowledge acquired. Questions that involve reasoning over the knowledge acquired Questions that involve practical problem-solving on real world O.S. Hardening Both the objective test and the laboratory practice must be passed indepently in order to pass the subject	50
Laboratory practice	A4 A5 A8 A9 A11 A13 B2 B5 B6 B7 B8 B10 C3	Control of the labs assignments and evaluation of the results achieved. Work done during lab time will represent 60% of the total lab score A practical test, consisting of the reolution of some exercises on a physical equipment (real or virtualized machine) would yield a score up to 40% of the total lab score. This practical test will take place either the last day of lab time or the same day of the Objective test (after it). Both the objective test and the laboratory practice must be passed indepently in order to pass the subject .	50

Assessment comments

To pass the subject, it is necessary to pass both parts separately: objective test and laboratory practices (that is, 2.5 in each part)FIRST OPPORTUNITYStudents who do not participate in any part of the evaluation at the first opportunity will have 0 in each non-participated part. If the objective test is the final grade will be No PresentedSECOND OPPORTUNITY The option of repeating the objective test and/or the practical test will be given at the student's choice PLAGIARISM: Plagiarism is regarded as serious dishonest behavior. If any form of plagiarism is detected in any of the exams or provided material, the final grade will be FAIL (0), and the incident will be reported to the corresponding academic authorities for prosecution.

Sources of information	
Basic	- Donald A. Tevault (2018). Mastering Linux Security and Hardening. Packt Publishing - James Turnbull (2008). Hardening Linux . Apress - Carlos Álvarez Martín y Pablo González Pérez 0xWord (2016). Hardening de servidores GNU / Linux (3a Edicion). 0xWord - Tajinder Kalsi (2018). Practical Linux Security Cookbook: Secure your Linux environment from modern-day attacks with practical recipes, 2nd Edition. Packt Publishing - Gris, Myriam (2017). Windows 10. ENI - Aprea, Jean-François (2017). Windows Server 2016 : Arquitectura y Administración de los servicios de dominio Active Directory. ENI - Bonnet, Nicolas (2017). Windows Server 2016 : las bases imprescindibles para administrar y configurar su servido. ENI - De los Santos, Sergio (). Máxima Seguridad en Windows: Secretos Técnico. 0xWord - Núñez, Ángel (). Windows Server 2016: Administración, seguridad y operaciones. 0xWord - Yuri Diogenes, Erdal Ozkaya (2018). Cybersecurity - Attack and Defense Strategies. Packt Publishing - Salvy, Pierre (2017). Windows 10 : despliegue y gestión a través de los servicios de empresa. ENI - Deman, Thierry (2018). Windows Server 2016 : Administración avanzada. ENI - García, Carlos. González, Pablo (). Hacking Windows: Ataques a sistemas y redes Microsoft. 0xWord
Complementary	

Recommendations
Subjects that it is recommended to have taken before
Subjects that are recommended to be taken simultaneously
Subjects that continue the syllabus
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.