Teaching Guide					
Identifying Data					2020/21
Subject (*)	Secure Networks			Code	614530006
Study programme	Máster Universitario en Ciberseguridade				
Descriptors					
Cycle	Period		Year	Type	Credits
Official Master's Degree	1st four-month period		First	Obligatory	6
Language	SpanishGalician				
Teaching method	Face-to-face				
Prerequisites					
Department	Ciencias da Computación e Tecnoloxías da InformaciónComputaciónTecnoloxías da Información e as Comunicacións				
Coordinador	Novoa De Manuel, Francisco Javier		E-mail	francisco.javier.novoa@udc.es	
Lecturers	Novoa De Manuel, Francisco Javier		E-mail	francisco.javier.novoa@udc.es	
Web	faitic.uvigo.es				
General description	The main objective of Secure Networks is for students to learn how to design and implement network infrastructures that are capable of providing the necessary security services in a modern corporate environment. They must know the reference security architectures and be able to configure and manage them, using technologies such as IDS / IPS and Firewalls, among others. The subject is conceived so that laboratory practices, with physical and virtual equipment, have a major importance in the learning process.				

Contingency plan	Contingency Plan A: total or partial confinement of students and / or professors 1. Modifications to the contents None 2. Methodologies *Teaching methodologies that are modified - Master Session: will be taught through videoconference - ICT practices are maintained through the use of simulators and / or remote access to classroom equipment - Objective test, by means of Faitic, Moodle or other tool provided by UVigo and / or UDC. - Practical test is maintained using simulators, remote access and video conferencing tools. 3. Mechanisms for personalized attention to students - Moodle: always. All teaching resources (slides, practice statement, announcements, software, etc.) are available through Faitic. - Teams or other video conferencing tool: weekly. The tutorial sessions will be given through Teams in the official schedules of each teacher. - Email: always. To answer any question 4. Modifications in the evaluation None *Evaluation observations: In the event that it cannot be done in person, the following will be carried out: - Objective test: through Faitic and Remote Campus or Teams - Practical test: using simulators and / or remote access mechanisms 5. Modifications to the bibliography or webgraphy None Contingency Plan B: number of students exceed the classroom capacity 1. Modifications to the contents None 2. Methodologies *Teaching methodologies that are modified - Master Session: two groups will be established that will attend face-to-face in alternate weeks. A video conferencing solution (Remote Campus or Teams) will be enabled to access the sessions - ICT Practices, two groups will be established that will attend in person every other week. Simulators or remote access mechanisms will be used for the group that cannot attend in person. - Objective test, an alternative classroom will be sought, with sufficient capacity. - Practical test, shifts will be established to carry it out 3. Mechanisms for personalized attention to students - Moodle: always. All teaching resources (slides, practice statement, announcements, software, etc.) are available through Faitic. - Teams or other video conferencing tool: weekly. The tutorial sessions will be given through by Teams in the official schedules of each teacher. - Email: always. To answer any question 4. Modifications in the evaluation None

*Evaluation observations:

- Objective test, an alternative classroom will be sought, with sufficient capacity.
- Practical test, shifts will be established to carry it out

5. Modifications to the bibliography or webgraphy

None

Study programme competences	
Code	Study programme competences
A2	CE2 - Deep knowledge of cyberattack and cyberdefense techniques
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
A8	CE8 - Skills for conceive, design, deploy and operate cybersecurity systems
A12	CE12 - Knowledge of the role of cybersecurity in the design of new industrial processes, as well as of the singularities and restrictions to be addressed in order to build a secure industrial infrastructure
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
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
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
C4	CT4 - Ability to ponder the importance of information security in the economic progress of society

Learning outcomes			
Learning outcomes	Study programme competences		
They will understand the role of a firewall in the security strategy of a final device or the network it protects.	AJ2 AJ8	BJ2 BJ6	
They will be able to describe what the access policies are and to design / specify the set of them that a scenario or particular case requires.	AJ8 AJ12	BJ2 BJ4 BJ6 BJ8	CJ4
They will know the different types of packet filtering (stateful/stateless) and application-level firewalls, and they will know how to configure them on different platforms.	AJ2	BJ6 BJ8	
They can design and describe, for a specific scenario / topology, alternative configurations to place the firewall within the corporate network (bastion, DMZ, distributed firewall)	AJ8	BJ2 BJ6 BJ8	
They will be able to describe the basic principles that underlie intrusion detection, the common sensors they use for information collection, and the analysis techniques (anomaly detection versus heuristic detection) that decide when to trigger an alarm. They will know possible technical solutions (HIDS / NIDS, IPS, SIEM, honeypot), which they will know how to install and configure for some platforms and particular implementations	AJ2 AJ8	BJ6 BJ8	
They will be familiar with the concepts of tunneling and network virtualization, and will be able to choose and implement the most appropriate virtual private network technology for different scenarios	AJ2 AJ4	BJ6	
They can explain the principles on which anonymous networks are built	AJ2	BJ4 BJ5	CJ4

Contents	
Topic	Sub-topic
1. Secure Networks Design	1.1. Enterprise Network Architectures 1.2. Design Patterns 1.3. Perimetral Security Approaches

2.- IPv6 Fundamentals	2.1. IPv6 addresses 2.2. IPv6 addresses configuration 2.3. IPv6 multicast addresses 2.4. ICMPv6 2.5. IPv6 routing protocols
3.- Network Devices Hardening	3.1. Internal Architecture of Network Devices 3.2. Protecting the Data Plane 3.3. Protecting the Control Plane 3.4. Protecting the Management Plane
4. Firewalls	4.1. Static Packet Filtering 4.2. Dynamic Packet Filtering 4.3. Application-level Filtering 4.4. Zone-based Firewalls 4.5. Next-Generation Firewalls 4.6. NAT/NATP
5. IDS/IPS	5.1 Network-based Systems 5.2 Host-based Systems
6. Monitoring	6.1 Syslog 6.2 SNMP 6.3 Netflow 6.4 SIEM
7. VPNs over MPLS	7.1 MPLS fundamentals 7.2 VPNs over MPLS

Planning				
Methodologies / tests	Competencies	Ordinary class hours	Student?s personal work hours	Total hours
ICT practicals	A2 A8 B2 B5 B6	21	60	81
Objective test	A8 B2 B4 B6 B8	2	0	2
Practical test:	A8 B2 B6	2	0	2
Guest lecture / keynote speech	A2 A4 A8 A12 B8 C4	21	42	63
Personalized attention		2	0	2
(*)The information in the planning table is for guidance only and does not take into account the heterogeneity of the students.				

Methodologies	
Methodologies	Description
ICT practicals	In which the student will observe the operation in practice of some of the theoretical contents explained in the lectures. In these practices, the student will use different tools (network equipment, network simulators, monitoring tools, etc.) proposed by the professors, which will allow them to deepen and strengthen their knowledge on different aspects of network security. In addition to the basic practices that all students will have to do, additional practices that interested students can do optionally will be proposed.
Objective test	At the end of the exposition of the subject, a test type exam will be carried out that will allow to assess the theoretical knowledge and the practical skills acquired during the evolution of the course.
Practical test:	At the end of the ICT lab sessions, there will be an exam in which the student must demonstrate the acquired skills. Starting from an initial scenario (non-secure network), the student will be asked to protect it using the strategies and techniques discussed in the subject, especially in the practical laboratories.

Guest lecture / keynote speech	In which the theoretical content of the syllabus will be exposed, including illustrative examples and with the support of audiovisual media. The student will have the support material (notes, copies of the slides, articles, etc.) beforehand and the teacher will promote an active attitude, recommending the previous reading of the topics to be discussed each day in class, as well as asking questions that allow to clarify concrete aspects and leaving open questions for the reflection of the student. The master sessions will be complemented with conferences that will bring an external expert to discuss a topic in greater depth.

Personalized attention	
Methodologies	**Description**
ICT practicals	Personalized attention during the practices will be used to guide and verify the work that students are doing according to the instructions given to them, depending on the specific practice in question. All the professors of the subject will also propose a tutorial schedule in which the students can solve any doubt related to the development of the same. Recommendations for the study of the subject The tutorials will be recommended as a fundamental part of the learning support.

Assessment			
Methodologies	**Competencies**	**Description**	**Qualification**
Practical test:	A8 B2 B6	At the end of the ICT lab sessions, there will be an exam in which the student must demonstrate the acquired skills. Starting from an initial scenario (non-secure network), the student will be asked to protect it using the strategies and techniques discussed in the subject, especially in the practical laboratories.	30
ICT practicals	A2 A8 B2 B5 B6	The subject's practices will consist of different activities related to the design and implementation of Secure Networks. A report of the practices will be carried out to assess the level of understanding and the work developed by the student	20
Objective test	A8 B2 B4 B6 B8	At the end of the exposition of the subject, there will be an objective test type test on the contents, both in the theoretical sessions and in the practical sessions.	50

Assessment comments

It will be necessary to obtain at least 50% of the grade to pass the subject. In addition to pass the subject, it will be necessary (at any opportunity) that the student obtains a minimum of 40% of the final mark in the objective test and in the practices (ICT lab sessions and report). Otherwise, the maximum grade that can be obtained is 4.5.

FIRST CALL

The evaluation of the laboratory practices will be carried out by means of the realization of four practical reports related to the laboratory exercises and will have a total weight of 20% of the final mark. There will also be a practical exam that will have a weight of 30% on the final grade It will be necessary to obtain a minimum of 40% in practices (ICT lab sessions and exam) to pass the subject.

50% of the remaining grade of the first call can be achieved by conducting an objective test (exam), which may contain questions related to the concepts developed in theory classes, practices, tutorials and basic bibliographic matherials.

SECOND CALL

The students may retain the mark obtained in the practices or the objective test of the first opportunity provided they have obtained an assessment equal to or greater than 50% of their weight in the final grade.

The evaluation of the practices in the second call will be carried out by means of the practical test in the laboratory.

50% of the remaining grade of the second call can be obtained through the take of an objective test (exam), which may contain questions related to the concepts developed in theory classes, practices, tutorials and basic bibliographic matherials.

END-OF-PROGRAM CALL

The evaluation of the practices will be carried out by means of a practical exam in the laboratory, at the end of the objective test of the extraordinary call.

50% of the remaining grade may be obtained by taking an objective test (exam), which may contain questions related to the concepts developed in the theory class, practices, tutorials and basic bibliographic matherials.

STUDENTS WITH PARTIAL REGISTRATION OR WITH ACADEMIC DISPENSE OF TEACHING EXEMPTION: They should contact professors of the subject to enable the completion of tasks outside the usual organization of the subject.

Sources of information	
Basic	- Anthony Bruno; Steve Jordan (2020). CCNP Enterprise Design ENSLD 300-420 Official Cert Guide: Designing Cisco Enterprise Networks. Cisco Press - Omar Santos (2020). CCNP and CCIE Security Core SCOR 350-701 Official Cert Guide. Cisco Press - Brad Edgeworth, Kevin Wallace, Jason Gooley, David Hucaby, Ramiro Garza Rios (2019). CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide. Cisco Press - Wendell Odom (2019). CCNA 200-301 Official Cert Guide Library. Cisco Press
Complementary	- Kulbir Saini (2011). Squid Proxy Server 3.1 Beginner's Guide. Packt Publishing

Recommendations
Subjects that it is recommended to have taken before
Subjects that are recommended to be taken simultaneously
Subjects that continue the syllabus
Penetration Testing/614530008 Communications Security/614530004
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.