UNIVERSIDADE DA CORUÑA

Teaching Guide			
Identifying Data			2023/24
Subject (*)	Secure Networks	Code	614530105
Study programme	Máster Universitario en Ciberseguridade		

Descriptors				
Cycle	Period	Year	Type	Credits
Official Master's Degree	1st four-month period	First	Obligatory	5

Language	SpanishGalician		
Teaching method	Face-to-face		
Prerequisites			
Department	Ciencias da Computación e Tecnoloxías da InformaciónComputaciónTecnoloxías da Información e as Comunicacións		
Coordinador	Nóvoa Manuel, Francisco Javier	E-mail	francisco.javier.novoa@udc.es
Lecturers	Nóvoa Manuel, Francisco Javier	E-mail	francisco.javier.novoa@udc.es
Web	moovi.uvigo.gal		
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.		

Study programme competences	
Code	Study programme competences
A25	HD-05 - Diseñar e implementar redes seguras, seleccionando y configurando los dispositivos adecuados para cada sección de la red y utilizando proactivamente la monitorización de red como de modo que se implemente correctamente la política de seguridad de la organización
B21	K-05 - Conocer de las vulnerabilidades en los dispositivos y tecnologías de acceso de red, las herramientas para explorarlas y las medidas de protección para obtener redes de comunicaciones seguras, así como comprender el concepto de política de seguridad aplicado a redes, la seguridad perimetral y los cortafuegos
C7	C-02 - Demostrar autonomía e iniciativa para resolver problemas complejos que involucren múltiples tecnologías en el ámbito de las redes o los sistemas de comunicaciones, y desarrollar soluciones innovadoras en el campo de las comunicaciones y la computación distribuida privadas.
C10	C-05 - Analizar la seguridad de los protocolos de comunicación en la capa física; de enlace; de red y de transporte, así como evaluar en una red corporativa las medidas de seguridad que es necesario implantar para la protección de sus activos internos y sus comunicaciones
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		
They will understand the role of a firewall in the security strategy of a final device or the network it protects.	AJ25	BJ21	
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.			CJ7 CJ15
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.	AJ25		
They can design and describe, for a specific scenario / topology, alternative configurations to place the firewall within the corporate network (bastion, DMZ, distributed firewall)	AJ25		CJ7 CJ10

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	AJ25		CJ15
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	AJ25	BJ21	CJ15
They can explain the principles on which anonymous networks are built			CJ7

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	C10 C15	21	39	60
Objective test	A25 B21 C7 C10	1	0	1
Practical test:	A25 B21 C7	2	0	2
Long answer / essay questions	C7	1	0	1
Guest lecture / keynote speech	A25 B21 C15	21	38	59
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.
Long answer / essay questions	At the end of the exposition of subject and ICT lab sessions, there will be an exam in which the student in which he/she have to develop one or two themes, where the student must show an advanced comprenhesion about them or he/she must be able to solve a complex problem.
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. Individual office hours schedule is available at https://pdi.udc.es/es/File/Pdi/HB9HJ for Francisco Javier Nóvoa and https://www.uvigo.gal/es/universidad/administracion-personal/pdi/raul-fernando-rodriguez-rubio for Raúl Rodríguez Rubio 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:	A25 B21 C7	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
Long answer / essay questions	C7	At the end of the exposition of subject and ICT lab sessions, there will be an exam in which the student in which he/she have to develop one or two themes, where the student must show an advanced comprenhesion about them or he/she must be able to solve a complex problem.	10
ICT practicals	C10 C15	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	A25 B21 C7 C10	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.	40

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, essay questions and in the practices (ICT lab sessions and report). Otherwise, the maximum grade that can be obtained is 4.5.

FIRST CALL - ORDINARY 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.

40% of the 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.

10% of the remaining grade of the first call can be achieved by conducting an essay questions, which may contain questions related to the concepts developed in theory classes, practices, tutorials and basic bibliographic matherials.

SECOND CALL - EXTRAORDINARY 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.

40% of the 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.

10% of the remaining grade of the first call can be achieved by conducting an essay questions, 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.

40% of the 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.

10% of the remaining grade of the first call can be achieved by conducting an essay questions, which may contain questions related to the concepts developed in theory classes, 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.