VNIVERSITAT DE VALÈNCIA

Course Guide
43861 Network security

COURSE DATA

Data Subject	
Code	43861
Name	Network security
Cycle	Master's degree
ECTS Credits	5.0
Academic year	2022 - 2023

Study (s)

Degree	Center	Acad. year	Period
2174 - M.U. en Ingeniería de Telecomunicación 13-V.2	School of Engineering	2	First term

Subject-matter

Degree	Subject-matter	Character
2174 - M.U. en Ingeniería de Telecomunicación 13-V.2	15 - Network security	Obligatory

Coordination

Name	Department
GARCIA PINEDA, MIGUEL	240 - Computer Science

SUMMARY

This course focuses on the study, from the theoretical and practical point of view, of several mechanisms and tools to ensure the safety of a corporate intranet, against external and internal attacks, in wired and wireless networks.

The course prepares students for official certifications related to security, that have a great professional demand in the telecommunications sector. The certification opens the door to a strategic sector such as Internet in the business world.

The course is designed following a methodology adapted to the new European Higher Education Area (EHEA), and it intends to focus on student's learning. This method improves student involvement and helps your assessment continuously, reinforcing and complementing the knowledge acquired in lectures.

PREVIOUS KNOWLEDGE

Relationship to other subjects of the same degree

There are no specified enrollment restrictions with other subjects of the curriculum.

Other requirements

Being able to handle network commands of Linux and Windows, as well as understand the basics of IP, TCP / IP, UDP / IP, DHCP, access points and routers required to set up a small LAN.

OUTCOMES

2174 - M.U. en Ingeniería de Telecomunicación 13-V.2

- To have critical thinking capabilities to investigate independently and self-critically, and to search and utilize information for documenting ideas.
- Students should apply acquired knowledge to solve problems in unfamiliar contexts within their field of study, including multidisciplinary scenarios.
- Students should demonstrate self-directed learning skills for continued academic growth.
- Students should possess and understand foundational knowledge that enables original thinking and research in the field.
- Be able to access to information tools in other areas of knowledge and use them properly.
- To be able to assess the need to complete the scientific, historical, language, informatics, literature, ethics, social and human background in general, attending conferences, courses or doing complementary activities, self-assessing the contribution of these activities towards a comprehensive development.
- Ability to model, design, implement, manage and maintain networks, services and contents.
- Ability to plan, take decisions and design networks, services and applications considering quality of service, direct costs, implantation plans, supervision, security protocols, scaling and maintenance, as well as managing and assuring the required quality in the development process.
- Ability to understand the organization of the Internet, applying new-generation technologies and protocols, component models, intermediate software and services.

LEARNING OUTCOMES

After finishing this course, students will have acquired the knowledge to:

- Describe common network security concepts

- Ensure routing and switching infrastructure

- Develop basic services of authentication, authorization and accounting

- Develop basic firewall services

- Basic deployment from site to site and remote access VPN services

- Describe the use of the most advanced, such as intrusion protection, content security and identity management security services.

DESCRIPTION OF CONTENTS

1. Threats of network security

1.1. Fundamental Principles of secure networks
1.2. Worms, viruses and Trojans
1.3. Attack methodologies

2. Secure network devices

2.1. Ensuring access files and devices
2.2. Role-based CLI
2.3. Monitoring devices
2.4. Using automated features

3. Authentication, authorization and accounting

3.1. Purpose AAA
3.2. AAA locale
3.3. Configuring AAA server based

4. Implementing firewall technologies

4.1. Access Control Lists
4.2. Firewall technologies
4.3. Access control based on context
4.4. Firewall policies

5. Implementation of intrusion prevention

5.1. IPS technology
5.2. Implementation of IPS

6. Ensuring local area network

6.1. Final considerations Security
6.2. Security Considerations layer 2
6.3. Wireless, VoIP and security considerations SAN
6.4. Security settings switch

7. Cryptography

7.1. cryptographic service
7.2. Abstracts, digital signatures and authentication
7.3. symmetric and asymmetric encryption

8. Implementation of Virtual Private Networks

8.1. VPNs
8.2. Components and operations of IPSEC VPNs
8.3. Deploying VPNs site-to-site.
8.4. Deploying Remote Access VPNs
8.5. Implementation SSLVPNs

9. Manage a secure network

9.1. Life cycle of a secure network
9.2. Self-Defending Network
9.3. Construction of a comprehensive security policy

WORKLOAD

ACTIVITY	Hours	% To be attended
Theory classes	21,00	100
Classroom practices	18,00	100
Laboratory practices	9,00	100
Tutorials	2,00	100
Development of individual work	30,00	0
Study and independent work	30,00	0
Preparation of evaluation activities	5,00	0
Preparing lectures	5,00	0
Preparation of practical classes and problem	5,00	0
TOTAL	**125,00**	

TEACHING METHODOLOGY

The training activities are conducted in accordance with the following distribution:

40% of the hours of ECTS credits (1 credit is 25 hours) will go to the following sessions:

-MD1.- Activities theory.

Description: The lectures will develop the issues by providing a global and inclusive vision, analyzing in detail the key issues and more complex, encouraging at all times, participation / student.

- MD2.- Practical activities.

Description: Complementing theoretical activities in order to apply the basics and expand the knowledge and experience to be acquired in the course of the work proposed. They include the following types of classroom activities: Classes of problems and issues in classroom discussion sessions and problem-solving exercises and previously worked by students laboratory practice oral presentations, conferences, tutorials scheduled (individualized or group)

- Evaluation.

Description: Implementation of individual evaluation questionnaires in the classroom with the presence of teachers.

60% of the hours of ECTS (25 hours per ECTS) will be devoted to the following non-contact activities:

- Working staff / student.

Description: Realization (outside the classroom) of monographs, literature search directed, issues and problems as well as the preparation of classes and exams (study). This is done individually and tries to promote self-employment.

The platform of e-learning (virtual classroom) of the University of Valencia will be used in support of communication with students. Through it you will have access to course materials used in class as well as solve problems and exercises.

EVALUATION

The subject is assessed as follows in a continuous assessment:

1. SE1.- Theoretical final exam (35%). Minimum grade 5. As an alternative to continuous assessment will be conducted averaged written.

2. SE2.- Part laboratory (50%)

   1. Assistance, preparation and conduct of the practice assessed in the same laboratory (10%).
   2. Written test configuration commands (40%). Minimum grade 5. As an alternative averaged practical examinations will be conducted.

3. SE3.- Exercises proposed by the professor (15%).

On second call, it will be apply the same than the first one.

In any case, the system of evaluation will be ruled by the established in the Regulation of Evaluation and Qualification of the University of Valencia for Degrees and Masters. (http://www.uv.es/graus/normatives/2017_108_Reglament_avaluacio_qualificacio.pdf).

REFERENCES

Basic

- Stallings, Network Security Essential (5th edition), 2013
- Mark Rhodes-Ousley, Roberta Bragg, Keith Strassberg. Network Security: The Complete Reference
- Cisco Press: Designing Network Security
- Omar Santos, John Stuppi. CCNA Security 210-260 Official Cert Guide. Cisco Press, 2015