Course guide
230617 - NS - Network Security

Last modified: 26/05/2023

Unit in charge: Barcelona School of Telecommunications Engineering
Teaching unit: 744 - ENTEL - Department of Network Engineering.

Degree: MASTER'S DEGREE IN TELECOMMUNICATIONS ENGINEERING (Syllabus 2013). (Optional subject).
MASTER'S DEGREE IN ADVANCED TELECOMMUNICATION TECHNOLOGIES (Syllabus 2019). (Optional subject).
MASTER'S DEGREE IN CYBERSECURITY (Syllabus 2020). (Compulsory subject).

Academic year: 2023 **ECTS Credits:** 5.0 **Languages:** English

LECTURER

Coordinating lecturer: Consultar aquí / See here:
https://telecos.upc.edu/ca/estudis/curs-actual/professorat-responsables-coordinadors/responsables-assignatura

Others: Consultar aquí / See here:
https://telecos.upc.edu/ca/estudis/curs-actual/professorat-responsables-coordinadors/professorat-assignat-idioma

PRIOR SKILLS

Internetworking skills are mandatory and basic administration linux knowledge.
Is is recommended a previous course in introduction to cryptography

DEGREE COMPETENCES TO WHICH THE SUBJECT CONTRIBUTES

Specific:
1. Ability to model, design, implement, manage, operate, administrate and maintain networks, services and contents
2. Ability to plan networks and decision-making about services and applications taking into account: quality of service, operational and direct costs, implementation plan, supervision, security processes, scalability and maintenance. Ability to manage and assure the quality during the development process
3. Ability to understand and to know how to apply the functioning and organization of the Internet, new generation Internet technologies and protocols, component models, middleware and services

Transversal:
4. TEAMWORK: Being able to work in an interdisciplinary team, whether as a member or as a leader, with the aim of contributing to projects pragmatically and responsibly and making commitments in view of the resources that are available.

5. EFFECTIVE USE OF INFORMATION RESOURCES: Managing the acquisition, structuring, analysis and display of data and information in the chosen area of specialisation and critically assessing the results obtained.

6. FOREIGN LANGUAGE: Achieving a level of spoken and written proficiency in a foreign language, preferably English, that meets the needs of the profession and the labour market.

TEACHING METHODOLOGY

- Lectures
- Laboratory practical work
- Group work (distance)
- Individual work (distance)
- Oral presentations
- Short answer test (Control)
- Extended answer test (Final Exam)

LEARNING OBJECTIVES OF THE SUBJECT

Learning objectives of the subject:

The aim of this course is to train students in methods of designing, evaluating and understanding the basic mechanisms for securing a data communications networks. We propose a practical approach where the different concepts introduced in the lectures are deployed in the lab in real networks.

Learning results of the subject:

- Ability to specify, design networks, services, processes and applications of telecommunications in both a fixed, mobile, personal, local or long distance, with different bandwidths in multicast networks, including voice and data.
- Ability to apply both traffic engineering tools as planning tools, dimensioning and network analysis.
- Ability to analyse, model and implement new architectures, network protocols and communication interfaces and new network services and applications.
- Ability to analyse, model and apply advanced techniques both security, including cryptographic protocols, firewalls, and collection mechanisms, authentication and content protection.

STUDY LOAD

Type	Hours	Percentage
Self study	86,0	68.80
Hours large group	19,5	15.60
Hours small group	19,5	15.60

Total learning time: 125 h

CONTENTS

1. Introduction

Description:
- Fundamental principles of secure networks
- Worms, viruses, and trojans
- Botnets
- Attack Methodologies
- Monitoring devices

Full-or-part-time: 8h
Theory classes: 2h
Self study : 6h

2. Authentication, authorization and accounting (AAA)

Description:
- Purpose of AAA Protocols AAA: Radius and Diameter
- AAA server based configuration

Full-or-part-time: 21h
Theory classes: 4h
Laboratory classes: 3h
Self study : 14h

3. Perimeter Security

Description:
- Introduction to firewalls
- Firewall technologies
- Access Control based on firewall policy context
- Detection systems and intrusion prevention (IDPS)
- Fundamentals of IDPS technologies
- HIDPS, NIDPS and Honeypots

Full-or-part-time: 26h
Theory classes: 6h
Laboratory classes: 2h
Self study : 18h

4. LAN protection

Description:
- Security Considerations Layer 2
- Wireless, VoIP and SAN security considerations
- Configuring Switch Security SPAN and RSPAN

Full-or-part-time: 14h
Theory classes: 2h
Laboratory classes: 2h
Self study : 10h

5. Virtual Private Networks VPNs

Description:
- Introduction. Requirements and types of VPNs: remote access, point to point and internal
- Components and operations of IPSec VPNs
- SSL VPNs: architecture and fundamentals

Full-or-part-time: 18h
Theory classes: 4h
Laboratory classes: 2h
Self study : 12h

6. Manage a secure network

Description:
- Life cycle of a secure Self-Defending Network
- Construction of a comprehensive security policy

Full-or-part-time: 18h
Theory classes: 4h
Laboratory classes: 2h
Self study : 12h

7. Network Forensics

Description:
- Forensics phases. Digital Evidence. Common occurrences
- Collection of information. Toolbox. Procedures.
- Timeline. Data search. Recovering deleted files
- Analysis of evidence. Event audit

Full-or-part-time: 20h
Theory classes: 4h
Laboratory classes: 2h
Self study : 14h

ACTIVITIES

LABORATORY

Description:
- Radius/Diameter lab
- Firewall lab
- WiFi Security lab
- VPN lab
- Network management lab
- Forensics lab

EXERCISES

Description:
Exercises to strengthen the theoretical knowledge.

ORAL PRESENTATION

Description:
Presentation of Use Case: Network Security Management.

SHORT ANSWER TEST (CONTROL)

Description:
Mid term control.

SHORT ANSWER TEST (TEST)

Description:
Partial evaluation test with theoretical questions and short exercises.

EXTENDED ANSWER TEST (FINAL EXAMINATION)

Description:
Final examination.

GRADING SYSTEM

Midterm exam: 30%
Final exam: 40%
Attendance and class performance: 10%
Assigments: 20%

EXAMINATION RULES.

Laboratory exercises are done in groups of 4 people (5 max)
2 laptops per group are required

BIBLIOGRAPHY

Basic:

- Anderson, R.J. Security engineering : a guide to building dependable distributed systems [on line]. 3rd ed. Indianapolis, Indiana: John Wiley & Sons, Inc., 2020 [Consultation: 25/01/2021]. Available on: https://ebookcentral-proquest-com.recursos.biblioteca.upc.edu/lib/upcatalunya-ebooks/detail.action?docID=6412239. ISBN 9781119642831.

Complementary:

- Bosworth, S.; Kabay, M.E.; Whyne, E. Computer security handbook [on line]. 5th ed. New York: John Wiley & Sons, 2012 [Consultation: 08/06/2022]. Available on: https://ebookcentral-proquest-com.recursos.biblioteca.upc.edu/lib/upcatalunya-ebooks/reader.action?docID=707226. ISBN 9780470413746.