Last update: 06-05-2019

230617 - NS - Network Security

Coordinating unit: 230 - ETSETB - Barcelona School of Telecommunications Engineering

Teaching unit: 744 - ENTEL - Department of Network Engineering

Academic year: 2019

Degree: MASTER'S DEGREE IN ADVANCED TELECOMMUNICATION TECHNOLOGIES (Syllabus 2019). (Teaching unit Optional)
MASTER'S DEGREE IN TELECOMMUNICATIONS ENGINEERING (Syllabus 2013). (Teaching unit Optional)
MASTER'S DEGREE IN INFORMATION AND COMMUNICATION TECHNOLOGIES (Syllabus 2009). (Teaching unit Optional)
MASTER'S DEGREE IN NETWORK ENGINEERING (Syllabus 2009). (Teaching unit Optional)

ECTS credits: 5 Teaching languages: English

Teaching staff

Coordinator: JOSEP PEGUEROLES VALLÉS

Others: JUAN HERNANDEZ SERRANO, MIGUEL SORIANO IBAÑEZ

Opening hours

Timetable: Office hours will be published every semester in ETSETB's intranet

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.

Last update: 06-05-2019

230617 - NS - Network Security

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

Total learning time: 125h	Hours large group:	13h	10.40%
	Hours medium group:	0h	0.00%
	Hours small group:	26h	20.80%
	Guided activities:	0h	0.00%
	Self study:	86h	68.80%

Last update: 06-05-2019

230617 - NS - Network Security

Content

1. Introduction

Learning time: 8h

Theory classes: 2h
Self study : 6h

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

2. Authentication, authorization and accounting (AAA)

Learning time: 21h

Theory classes: 4h
Laboratory classes: 3h
Self study : 14h

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

3. Perimeter Security

Learning time: 26h

Theory classes: 6h
Laboratory classes: 2h
Self study : 18h

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

Last update: 06-05-2019

230617 - NS - Network Security

4. LAN protection

Learning time: 14h

Theory classes: 2h
Laboratory classes: 2h
Self study : 10h

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

5. Virtual Private Networks VPNs

Learning time: 18h

Theory classes: 4h
Laboratory classes: 2h
Self study : 12h

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

6. Manage a secure network

Learning time: 18h

Theory classes: 4h
Laboratory classes: 2h
Self study : 12h

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

7. Network Forensics

Learning time: 20h

Theory classes: 4h
Laboratory classes: 2h
Self study : 14h

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

Last update: 06-05-2019

230617 - NS - Network Security

Planning of 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.

Qualification system

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

230617 - NS - Network Security

Regulations for carrying out activities

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. 2nd ed. New York: John Wiley & Sons, 2008. ISBN 978-0-470-06852-6.

Complementary:

Bosworth, S.; Kabay, M.E.; Whyne, E. Computer security handbook [on line]. 5th ed. New York: John Wiley & Sons, 2012 [Consultation: 28/09/2015]. Available on: <http://site.ebrary.com/lib/upcatalunya/docDetail.action?docID=10582597>. ISBN 9780470413746.