230617 - NS - Network Security

Coordinating unit: 230 - ETSETB - Barcelona School of Telecommunications Engineering
Teaching unit: 744 - ENTEL - Department of Network Engineering
Academic year: 2017

Degree: MASTER'S DEGREE IN NETWORK ENGINEERING (Syllabus 2009). (Teaching unit Optional)
MASTER'S DEGREE IN INFORMATION AND COMMUNICATION TECHNOLOGIES (Syllabus 2009).
(Teaching unit Optional)
DEGREE IN TELECOMMUNICATIONS ENGINEERING (Syllabus 1992). (Teaching unit Optional)
DEGREE IN ELECTRONIC ENGINEERING (Syllabus 1992). (Teaching unit Optional)
MASTER'S DEGREE IN TELECOMMUNICATIONS ENGINEERING (Syllabus 2013). (Teaching unit Optional)

ECTS credits: 5
Teaching languages: English

Teaching staff
Coordinator: JOSEP PEGUEROLES VALLES
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.
It 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.
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

<table>
<thead>
<tr>
<th>Total learning time: 125h</th>
<th>Hours large group:</th>
<th>13h</th>
<th>10.40%</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Hours medium group:</td>
<td>0h</td>
<td>0.00%</td>
</tr>
<tr>
<td></td>
<td>Hours small group:</td>
<td>26h</td>
<td>20.80%</td>
</tr>
<tr>
<td></td>
<td>Guided activities:</td>
<td>0h</td>
<td>0.00%</td>
</tr>
<tr>
<td></td>
<td>Self study:</td>
<td>86h</td>
<td>68.80%</td>
</tr>
</tbody>
</table>
## Content

<table>
<thead>
<tr>
<th>1. Introduction</th>
<th>Learning time: 8h</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Theory classes: 2h</td>
</tr>
<tr>
<td></td>
<td>Self study: 6h</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>2. Authentication, authorization and accounting (AAA)</th>
<th>Learning time: 21h</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Theory classes: 4h</td>
</tr>
<tr>
<td></td>
<td>Laboratory classes: 3h</td>
</tr>
<tr>
<td></td>
<td>Self study: 14h</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>3. Perimeter Security</th>
<th>Learning time: 26h</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Theory classes: 6h</td>
</tr>
<tr>
<td></td>
<td>Laboratory classes: 2h</td>
</tr>
<tr>
<td></td>
<td>Self study: 18h</td>
</tr>
</tbody>
</table>

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
## 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  
- Timeline. Data search. Recovering deleted files  
- Analysis of evidence. Event audit
## 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%
Assignments: 20%
Regulations for carrying out activities

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

Bibliography

Basic:


Complementary: