Course guide
230714 - NSAA - Network Security - Authentication and Authorization

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: 2022  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

Basic knowledge of Linux OS.
Understanding of security-related topics; for instance: cryptography, network security protocols, etc.
Medium-average computer programming skills.

TEACHING METHODOLOGY

Theoretical classes encouraging the students to participate in the class discussion
Lab sessions that reinforce the contents learnt during the theoretical classes and put them into practice.

LEARNING OBJECTIVES OF THE SUBJECT

Upon finishing this course, students should be able to understand how authentication and authorization methods and protocols work at the different OSI layer, to identify the potential threats, and to know best practises and countermeasures.

STUDY LOAD

<table>
<thead>
<tr>
<th>Type</th>
<th>Hours</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self study</td>
<td>86.0</td>
<td>68.80</td>
</tr>
<tr>
<td>Hours small group</td>
<td>39.0</td>
<td>31.20</td>
</tr>
</tbody>
</table>

Total learning time: 125 h
## CONTENTS

<table>
<thead>
<tr>
<th>Course</th>
<th>Description</th>
<th>Full-or-part-time</th>
<th>Laboratory classes</th>
<th>Self study</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Crypto Background</strong></td>
<td>An overview of the necessary cryptographic background</td>
<td>19h</td>
<td>6h</td>
<td>13h</td>
</tr>
<tr>
<td><strong>Authentication Protocols</strong></td>
<td>Understanding authentication protocols based on something you have, something you are and/or something you know. It includes replay attacks, nonces, SK authentication, PK authentication, DS authentication, passwords, hashed passwords, password cracking, biometrics, 2-factor authentication.</td>
<td>48h</td>
<td>15h</td>
<td>33h</td>
</tr>
<tr>
<td><strong>Access Authentication</strong></td>
<td>Access Authentication, PAP; CHAP, MSCHAP, EAP, RADIUS, DIAMETER, WPA-Enterprise</td>
<td>19h</td>
<td>6h</td>
<td>13h</td>
</tr>
<tr>
<td><strong>Web Authentication</strong></td>
<td>Sessions, Tokens, OAuth, OpenID connect</td>
<td>19h</td>
<td>6h</td>
<td>13h</td>
</tr>
<tr>
<td><strong>Mid-term exam</strong></td>
<td>Theory and lab</td>
<td>10h</td>
<td>3h</td>
<td>7h</td>
</tr>
</tbody>
</table>
Final exam

Description:
Final exam: theory and lab

Full-or-part-time: 10h
Laboratory classes: 3h
Self study : 7h

GRADING SYSTEM

Mid-term exam: 30%
Final exam: 40%
Assignments: 20%
Attitude: 10%