Course guide
270123 - SI - Computer Security

Unit in charge: Barcelona School of Informatics
Teaching unit: 701 - DAC - Department of Computer Architecture.
Degree: BACHELOR'S DEGREE IN INFORMATICS ENGINEERING (Syllabus 2010). (Optional subject).
Academic year: 2022  ECTS Credits: 6.0  Languages: Catalan, Spanish

LECTURER
Coordinating lecturer: DAVIDE CAREGLIO
Others: Primer quadrimestre:
ROBERTO BARREDA ORENGA - 11, 12
DAVIDE CAREGLIO - 11, 12, 13

PRIOR SKILLS
Those obtained at the Operating Systems and Computer Networks subjects.
Knowledge of technical English.

REQUIREMENTS
- Pre-Corequisite SO
- Pre-Corequisite XC

DEGREE COMPETENCES TO WHICH THE SUBJECT CONTRIBUTES

Specific:
CT6.4. To demonstrate knowledge and capacity to apply the characteristics, functionalities and structure of the Distributed Systems and Computer and Internet Networks guaranteeing its use and management, as well as the design and implementation of application based on them.
CT7.1. To demonstrate knowledge about metrics of quality and be able to use them.
CT7.2. To evaluate hardware/software systems in function of a determined criteria of quality.
CT7.3. To determine the factors that affect negatively the security and reliability of a hardware/software system, and minimize its effects.
CT8.1. To identify current and emerging technologies and evaluate if they are applicable, to satisfy the users needs.
CT11.1. To demonstrate understanding the environment of an organization and its needs in the field of the information and communication technologies.
CT11.2. To select, design, deploy, integrate and manage communication networks and infrastructures in a organization.
CT11.3. To select, deploy, integrate and manage information system which satisfy the organization needs with the identified cost and quality criteria.
CT12.3. To demonstrate comprehension, apply and manage the reliability and security of the computer systems (CEI C6).
CT13.1. To conceive systems, applications and services based on network technologies, taking into account Internet, web, electronic commerce, multimedia, interactive services and ubiquitous computation.

Generical:
G6. SOLVENT USE OF THE INFORMATION RESOURCES: To manage the acquisition, structuring, analysis and visualization of data and information of the field of the informatics engineering, and value in a critical way the results of this management.
TEACHING METHODOLOGY

This course should give an overview and a technical view of the problems and possible solutions to computer systems and networks security. For this reason, it covers many topics and has a great descriptive component.

However, the teaching methodology will use examples and problems for introducing the concepts to which students attain the necessary skills. Also, we will try to encourage interactivity with students considering real situations in class to discuss possible solutions.

Moreover, the laboratory will complete the skills and knowledge acquired in theory / problems class.

LEARNING OBJECTIVES OF THE SUBJECT

1. Being able to understand the threats and security risks of computer systems.
2. Being able to analyze malicious code such as viruses, Trojans, etc..
3. Being able to understand and identify mechanisms for access control of an operating system.
4. Knowing the problems of security in computer networks and be able to find solutions to protect them.
5. Being able to design protection mechanisms for distributed applications.
6. Being able to understand the need and operation of forensic computer security mechanisms.
7. Being able to use cryptographic mechanisms to protect resources.
8. Being able to understand, design and implement public key infrastructure (PKI).
9. Being able to understand the mechanisms of protection and security policies.
10. Being able to manage the acquisition, structuring, analysis and visualization of data and information in the field of computer engineering, critically evaluating the results of this management.

STUDY LOAD

<table>
<thead>
<tr>
<th>Type</th>
<th>Hours</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hours large group</td>
<td>45,0</td>
<td>30.00</td>
</tr>
<tr>
<td>Self study</td>
<td>84,0</td>
<td>56.00</td>
</tr>
<tr>
<td>Hours small group</td>
<td>15,0</td>
<td>10.00</td>
</tr>
<tr>
<td>Guided activities</td>
<td>6,0</td>
<td>4.00</td>
</tr>
</tbody>
</table>

Total learning time: 150 h

CONTENTS

Introduction

Description:
Threats, risk analysis, protection mechanisms, security of communications, security forensics, polities, recovery, legal aspects, ...

Cryptography

Description:

PKI Infrastructure

Description:
### Network security

**Description:**

### Security in applications

**Description:**

### Security in operating systems

**Description:**

### Forensic analysis

**Description:**
Collection of evidence. Analysis.

## ACTIVITIES

### Development of theme 1. Introduction.

**Description:**
Learning the concepts and objectives associated with this item.

**Specific objectives:**
1, 10

**Full-or-part-time:** 6h
- Theory classes: 2h
- Self study: 4h

### Development Topic 2. Cryptography.

**Description:**
Learning the concepts and objectives associated with this item.

**Specific objectives:**
7

**Full-or-part-time:** 18h
- Theory classes: 6h
- Practical classes: 4h
- Self study: 8h
Development of item 3. Infrastructure PKI.

**Description:**
Learning the concepts and objectives associated with this item.

**Specific objectives:**
8

**Full-or-part-time:** 9h
Theory classes: 3h
Practical classes: 1h
Self study: 5h

Lab 1. Using digital certificates and apache (HTTPS)

**Description:**
Being able to create a X.509 certificate with openssl and install it on an Apache web server to configure HTTPS

**Specific objectives:**
8

**Full-or-part-time:** 7h
Laboratory classes: 2h
Guided activities: 1h
Self study: 4h

First theory exam

**Description:**
Theory exam of the following topics: Introduction, Criptography, PKI infrastructure.

**Specific objectives:**
1, 7, 8, 10

**Full-or-part-time:** 5h
Guided activities: 1h
Self study: 4h

Development of item 4. Internet security

**Description:**
Learning the concepts and objectives associated with this item.

**Specific objectives:**
4

**Full-or-part-time:** 16h
Theory classes: 4h
Practical classes: 3h
Self study: 9h
### Lab 2 and 3. Iptables i snort

**Description:**
Understanding how the iptables command works as well as its internal operations based on tables and chains. Being able to create snort rules

**Specific objectives:**
1, 10

**Full-or-part-time:** 13h
Laboratory classes: 4h
Guided activities: 1h
Self study: 8h

### Development of item 5. Security applications.

**Description:**
Learning the concepts and objectives associated with this item.

**Specific objectives:**
5

**Related competencies:**
G6. SOLVENT USE OF THE INFORMATION RESOURCES: To manage the acquisition, structuring, analysis and visualization of data and information of the field of the informatics engineering, and value in a critical way the results of this management.

**Full-or-part-time:** 12h
Theory classes: 4h
Practical classes: 2h
Self study: 6h

### Lab 4. Vulnerabilities in web applications

**Description:**
Understanding the secure programming techniques described in the session. Understanding the webscarab and webgoat applications included in the OWASP linux distribution

**Specific objectives:**
1, 5

**Related competencies:**
G6. SOLVENT USE OF THE INFORMATION RESOURCES: To manage the acquisition, structuring, analysis and visualization of data and information of the field of the informatics engineering, and value in a critical way the results of this management.

**Full-or-part-time:** 7h
Laboratory classes: 2h
Guided activities: 1h
Self study: 4h
Second theory exam

Description:
Theory exam of the following topics: Security in operating systems and Security in computer networks

Specific objectives:
2, 3, 4, 5

Related competencies:
G6. SOLVENT USE OF THE INFORMATION RESOURCES: To manage the acquisition, structuring, analysis and visualization of data and information of the field of the informatics engineering, and value in a critical way the results of this management.

Full-or-part-time: 5h
Guided activities: 1h
Self study: 4h


Description:
Learning the concepts and objectives associated with this item.

Specific objectives:
2, 3

Related competencies:
G6. SOLVENT USE OF THE INFORMATION RESOURCES: To manage the acquisition, structuring, analysis and visualization of data and information of the field of the informatics engineering, and value in a critical way the results of this management.

Full-or-part-time: 13h
Theory classes: 5h
Practical classes: 3h
Self study: 5h

Lab 5. Malware analysis

Description:
Understanding the different forms to analyze a malicious code. Being able to properly use the analysis tool IDAPro

Specific objectives:
1, 2

Related competencies:
G6. SOLVENT USE OF THE INFORMATION RESOURCES: To manage the acquisition, structuring, analysis and visualization of data and information of the field of the informatics engineering, and value in a critical way the results of this management.

Full-or-part-time: 7h
Laboratory classes: 2h
Guided activities: 1h
Self study: 4h
Development issue 7. Security forensics.

Description:
Learning the concepts and objectives associated with this item.

Specific objectives:
6

Related competencies:
G6. SOLVENT USE OF THE INFORMATION RESOURCES: To manage the acquisition, structuring, analysis and visualization of data and information of the field of the informatics engineering, and value in a critical way the results of this management.

Full-or-part-time: 8h
Theory classes: 3h
Practical classes: 2h
Self study: 3h

Lab 6. Investigation of a forensic case

Description:
Students will learn the basic procedures and methodologies that must be taken into account when performing a forensic analysis. It is also expected that after the lab you will increase your understanding of the forensic tools and applications needed to solve most of the security incidents where a digital evidence is involved.

Specific objectives:
6

Related competencies:
G6. SOLVENT USE OF THE INFORMATION RESOURCES: To manage the acquisition, structuring, analysis and visualization of data and information of the field of the informatics engineering, and value in a critical way the results of this management.

Full-or-part-time: 7h
Laboratory classes: 2h
Guided activities: 1h
Self study: 4h

Lab CT. Solvent use of bibliographic resources

Description:
Manage the acquisition, structuring, analysis and visualization of data and information in the field of computer engineering, and critically evaluate the results of this management.
- Plan and use the information needed for an academic project (for example, for the final degree project) based on a critical reflection on the information resources used.
- Manage information competently, independently and autonomously.
- Evaluate the information found and identify the gaps.

Specific objectives:
11

Related competencies:
G6. SOLVENT USE OF THE INFORMATION RESOURCES: To manage the acquisition, structuring, analysis and visualization of data and information of the field of the informatics engineering, and value in a critical way the results of this management.

Full-or-part-time: 4h
Laboratory classes: 2h
Self study: 2h
Final exam lab

Description:
Review on all laboratory practices carried out throughout the course.

Specific objectives:
2, 3, 4, 5, 7, 8

Related competencies:
G6. SOLVENT USE OF THE INFORMATION RESOURCES: To manage the acquisition, structuring, analysis and visualization of data and information of the field of the informatics engineering, and value in a critical way the results of this management.

Full-or-part-time: 5h
Guided activities: 1h
Self study: 4h

Third theory Exam

Description:
Theory exam of the following topics: Computer Forensics and Security in computer networks

Specific objectives:
4, 5, 6

Related competencies:
G6. SOLVENT USE OF THE INFORMATION RESOURCES: To manage the acquisition, structuring, analysis and visualization of data and information of the field of the informatics engineering, and value in a critical way the results of this management.

Full-or-part-time: 5h
Guided activities: 1h
Self study: 4h

Questionnaire on the solvent use of bibliographic resources

Description:
Questionnaire on the solvent use of bibliographic resources

Specific objectives:
11

Related competencies:
G6. SOLVENT USE OF THE INFORMATION RESOURCES: To manage the acquisition, structuring, analysis and visualization of data and information of the field of the informatics engineering, and value in a critical way the results of this management.

Full-or-part-time: 3h
Guided activities: 1h
Self study: 2h

GRADING SYSTEM

Theory (70%) - Laboratory (25%) - Generic competence (5%).
The laboratory mark is obtained from the grades of each practice (50%) and the laboratory final exam (50%), but taking into account that the practices, which can be done either at the lab or at home, are mandatory in order to do the laboratory exam.
The theory grade will be the average of three course exams (ET1, ET2 and ET3). In other words, the theory grade will be NT = (ET1+ET2+ET3)/3.
The grade for the generic competence is obtained from the evaluation of the activity "Bibliographic Internet Research and analysis".
BIBLIOGRAPHY

Basic:

Complementary: