

Academic Year: ( 2019 / 2020 )

Review date: 20/04/2020 15:25:57

Department assigned to the subject: Computer Science and Engineering Department

Coordinating teacher: GONZALEZ MANZANO, LORENA

Type: Compulsory ECTS Credits : 3.0

Year : 1 Semester : 1

## REQUIREMENTS (SUBJECTS THAT ARE ASSUMED TO BE KNOWN)

None

## OBJECTIVES

Master the knowledge required to propose original designs or developments, often in a research process within the area of cyber security.

Ability to apply acquired knowledge to solve problems under novel or almost novel situations or within broader (multidisciplinary) contexts related with cyber security.

Ability to state critical opinions and judgements having incomplete or limited information in the field of cyber security. These judgements must take into account include considerations about social and ethical responsibilities

Discuss in a public audience about their acquired knowledge, and the conclusions from the work. Students will be able to give their foundational and most convincing reasons to a specialized and non specialized audience in a clear way, without ambiguities.

Students should have the learning skills required to continue studying in a autonomous or self-directed way.

Understand and apply methods and techniques to investigate vulnerabilities of a given site.

Create and refine concise and comprehensively documents, plans and projects in the scope of cyber security.

Knowledge of trends in the cyber attacks techniques and knowledge about learned experiences in real cases.

Know and apply the cryptographic and steganographic mechanisms required to protect data stored in a system or data transiting a network

## DESCRIPTION OF CONTENTS: PROGRAMME

System Software Exploitation:

1. Introduction
  - 1.1. Vulnerabilities in Software Components
  - 1.2. Exploitation mechanisms
  - 1.3. Exploitation Laboratory and Tools
2. Software Exploitation
  - 2.1. Segmentation Faults
  - 2.2. Input validation and code injection
  - 2.3. Race conditions
  - 2.4. Privilege-confusion

- 2.5. User interface exploitation
- 2.6. Configuration and functionality abuse
- 2.7. Cache exploitation
  
- 3. Web system exploitation
  - 3.1. Channel vulnerabilities
  - 3.2. Server vulnerabilities
  - 3.3. Browser vulnerabilities
  
- 4. Vulnerability and exploitation information sources
  - 4.1. Repositories
  - 4.2. Representation standards and information exchange languages

## LEARNING ACTIVITIES AND METHODOLOGY

### TRAINING ACTIVITIES

Theoretical classes  
 Laboratory classes  
 Tutorial sessions  
 Individual work

### TEACHING METHODOLOGIES

Teachers use computer and audiovisual media to explain the main concepts of the subject. Literature is provided to support students' learning.

Reading recommended texts: newspaper articles , reports, manuals and / or academic papers, either to expand or to consolidate the knowledge of the subject.

Preparation of laboratory reports individually or in groups.

## ASSESSMENT SYSTEM

<b>% end-of-term-examination/test:</b>	40
<b>% of continuous assessment (assignments, laboratory, practicals...):</b>	60

Continuous evaluation:

- Lab assignments (60%)
- Final Exam (40%)

Both marks are added when the mark of the final exam is equal or higher than 50% (20% out of 40%)

Non-continuous evaluation:

Students who do not follow the continuous evaluation should do a final exam composed of questions related to theory (50%) and lab assignments (50%). Both parts have to be passed separately (more than 25% each of them) to pass the subject. The result of this exam (both parts) corresponds to 100% of the final mark.

The evaluation of the extraordinary exam follows the same criteria as aforementioned.

## BASIC BIBLIOGRAPHY

- Eagle, C The IDA pro book: the unofficial guide to the world's most popular disassembler, No Starch Press, 2008
  
- Klein, T A Bug Hunter's Diary, No Starch Press, 2011
  
- Ross Anderson Security engineering, John Wiley & Sons, 2008
  
- Stuttard, D., & Pinto, M. The web application hacker's handbook: discovering and exploiting security flaws, John Wiley & Sons, 2008

## ADDITIONAL BIBLIOGRAPHY

- Anley, C., Heasman, J., Lindner, F., & Richarte, G. The Shellcoder's Handbook: Discovering and Exploiting Security Holes, John Wiley & Sons., 2011
- Dhanjani, N., Rios, B., & Hardin, B. Hacking: The next generation, O'Reilly Media, Inc., 2009
- Drake, J. J., Lanier, Z., Mulliner, C., Fora, P. O., Ridley, S. A., & Wicherski, G. Android Hacker's Handbook, John Wiley & Sons, 2014
- Hope, P., & Walther, B. Web Security Testing Cookbook: Systematic Techniques to Find Problems Fast, O'Reilly Media, Inc, 2008
- Miller, C., Blazakis, D., DaiZovi, D., Esser, S., Iozzo, V., & Weinmann, R. P IOS Hacker's Handbook, John Wiley & Sons, 2012

#### BASIC ELECTRONIC RESOURCES

- OWASP . OWASP: <https://www.owasp.org/>
- Safari Books . Safari Books: <http://proquest.safaribooksonline.com>