[MNB002] OFFENSIVE SECURITY

GENERAL INFORMATION

Studies	MASTER DEGREE IN DATA ANALYSIS, CYBERSECURITY AND CLOUD COMPUTING			**Subject**	Cybersecurity
Semester	2	**Course**	1	**Mention / Field of specialisation**	
Character	COMPULSORY				
Plan	2019	**Modality**	Adapted Face-to-face	**Language**	ENGLISH
Credits	3	**Hours/week**	0	**Total hours**	32 class hours + 43 non-class hours = **75 total hours**

PROFESSORS

EZPELETA GALLASTEGI, ENAITZ

REQUIRED PREVIOUS KNOWLEDGE

Subjects	Knowledge
(No specific previous subjects required)	*(No previous knowledge required)*

SKILLS

VERIFICA SKILLS

SPECIFIC

MNCE07 - Defining, designing and conducting offensive security audits on target networks and infrastructure, exploiting existing vulnerabilities, so that it can identify different attack vectors.

CROSS

MNCTR1 - Ability to work in multidisciplinary teams and in a multilingual environment (Basque/Spanish/English) and to communicate, both orally and in writing, knowledge, procedures, results and ideas related to the life cycle of the data, cybersecurity, and development and operations.

BASIC

M_CB10 - To have learning skills and the capacity for self-guided or independent subsequent learning.

LEARNING RESULTS

RA221 The student knows how to recognize different possible attack vectors in one or several targets based on the analysis of information sources and performing reconnaissance, individually or in a coordinated manner in groups

LEARNING ACTIVITIES	CH	NCH	TH
Development and writing of records, reports, presentations, audiovisual material, etc. on projects/work experience/challenges/case studies/experimental investigations carried out individually and/or in teams	7 h.	15 h.	22 h.
Conducting tests, giving presentations, presenting defences, taking examinations and/or doing checkpoints	2 h.	8 h.	10 h.
Presentation by the teacher in the classroom, in participatory classes, of concepts and procedures associated with the subjects	6 h.		6 h.
Carrying out exercises and solving problems individually and/or in teams	3 h.	4 h.	7 h.

EVALUATION SYSTEM	W
Presentation and defence of exercises, case studies, computer practical work, simulation practical work, laboratory practical work, term projects, end of degree project, master's thesis, challenges and problems	17%
Individual written and/or oral tests or individual coding/programming tests	83%

MAKE-UP MECHANISMS

Individual written and/or oral tests or individual coding/programming tests

CH - Class hours: 18 h.
NCH - Non-class hours: 27 h.
TH - Total hours: 45 h.

RA222 The student knows how to exploit vulnerabilities that may compromise the targets, minimizing the exposure to possible security countermeasures that they may have

LEARNING ACTIVITIES	CH	NCH	TH
Development and writing of records, reports, presentations, audiovisual material, etc. on projects/work experience/challenges/case studies/experimental investigations carried out individually and/or in teams	2 h.	6 h.	8 h.
Presentation by the teacher in the classroom, in participatory classes, of concepts and procedures associated with the subjects	8 h.		8 h.
Carrying out exercises and solving problems individually and/or in teams	4 h.	10 h.	14 h.

EVALUATION SYSTEM	W	MAKE-UP MECHANISMS
Reports on the completion of exercises, case studies, computer exercises, simulation exercises, laboratory exercises, term projects, challenges and problems	100%	Reports on the completion of exercises, case studies, computer exercises, simulation exercises, laboratory exercises, term projects, challenges and problems

CH - Class hours: 14 h.
NCH - Non-class hours: 16 h.
TH - Total hours: 30 h.

CONTENTS

- Security audit overview

- Asset recoinnassance

- Asset exploitation

- Post exploitation

- Audit reports

LEARNING RESOURCES AND BIBLIOGRAPHY

Learning resources	Bibliography
Subject notes Topic related web quires Moodle Platform Class presentations Computer practical training Slides of the subject	http://katalogoa.mondragon.edu/janium-bin/janium_login_opac_re_lnk.pl?grupo=MASTERDATUANALISIA12&ejecuta=15&