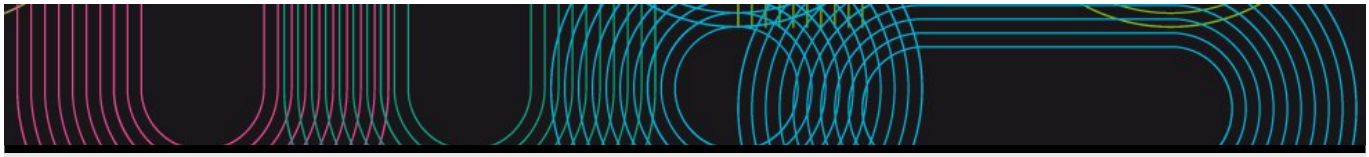

IDENTIFYING DATA				
Malware Analysis				
Subject	Malware Analysis			
Code	V05M175V01204			
Study programme	(*)Máster Universitario en Ciberseguridade			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	5	Mandatory	1st	2nd
Teaching language	English			
Department	Telematics Engineering			
Coordinator	Burguillo Rial, Juan Carlos			
Lecturers	Burguillo Rial, Juan Carlos			
E-mail	jrial@uvigo.es			
Web				
General description	Malware uses the systems and the communication networks to disseminate virus, hijack devices or steal confidential data. The aim of this subject is to provide the student the capability to analyze, detect and erase malware. To achieve that, we will explore and evaluate, practically and with case studies, the techniques used nowadays to hide malware, together with the new tendencies to detect it and eliminate it.			

Competencies	
Code	
A1	To possess and understand the knowledge that provides the foundations and the opportunity to be original in the development and application of ideas, frequently in a research context.
B1	To have skills for analysis and synthesis. To have ability to project, model, calculate and design solutions in the area of information, network or system security in every application area.
C8	Skills for conceive, design, deploy and operate cybersecurity systems.
C11	Ability to collect and interpret relevant data in the field of computer and communications security.
C13	Ability for analysing, detecting and eliminating software vulnerabilities and malware capable to exploit those in systems or networks.
D4	Ability to ponder the importance of information security in the economic progress of society.
D5	Ability for oral and written communication in English.

Learning outcomes	
Expected results from this subject	Training and Learning Results
The student will learn to analyze, detect and erase malware in systems and networks.	B1 C11 C13 D5
The student will learn to detect and fight against techniques used to hide and to provide persistence to malware in systems and networks.	A1 B1 C8 C11 C13 D5
The student will analyze systems and networks to detect and correct vulnerabilities that can be used by malware.	B1 C8 C11 C13 D5
The student will learn the malware nowadays trends and the experience obtained from relevant case studies.	A1 B1 D4 D5

Contents	
Topic	
Introduction to malware analysis and engineering.	a) What is malware? b) How to detect and erase it? c) What is malware engineering?
Malware types and definitions.	a) Estructure. b) Components. c) Infection vectors.
Malware Engineering.	a) Propagation techniques. b) Infection processes. c) Malware persistence. d) Hiding techniques.
Reverse malware engineering.	a) How to analyze and infer malware behavior? b) Understanding how new malware types work.
Tools for malware analysis.	a) Tools for malware detection. b) Tools for malware erasing.

Planning	Class hours	Hours outside the classroom	Total hours
Introductory activities	1	0	1
Lecturing	13	36	49
Laboratory practices	15	45	60
Discussion Forum	0	1	1
Case studies	4	4	8
Objective questions exam	1	4	5
Short answer tests	1	0	1
*The information in the planning table is for guidance only and does not take into account the heterogeneity of the students.			

Methodologies	Description
Introductory activities	We start doing a general introduction to the aims, the global contents of the subject and the expected outcomes. This activity will be performed individually.
Lecturing	We describe the different subject topics, giving the teaching material needed to follow them. Through this methodology the competencies CB1, CG1, CE8, CE11, CE13, CT4 and CT5 are developed. This activity will be performed individually.
Laboratory practices	Students must perform a set of practices in the lab to better understand the contents explained along the master lessons. Through this methodology the competencies CG1, CE8, CE11, CE13 and CT5 are developed. Some practices will be performed individually and others in groups (depending on the number of students).
Discussion Forum	Students must participate in the subject forum within TEMA at FAITIC. Through this methodology the competencies CE8, CE11, CE13 and CT5 are developed. This activity will be performed individually.
Case studies	Along master lessons and/or lab practices, students will review typical case studies for security problems already known. Through this methodology the competencies CG1, CE11, CE13 and CT5 are developed. This activity will be performed in group.

Personalized attention	
Methodologies	**Description**
Introductory activities	In the practical formative activities and tutoring, the professors of the subject will offer personal guidance to each student in the tasks to be performed, with the aim to orient the approach and the methodology. Also they will offer coordination information with other contents and subjects of the study program. It is recommended to consult the doubts with the teachers along the course in order to improve the understanding of the basic concepts, and for performing the tasks and activities to be evaluated.

Lecturing	In the practical formative activities and tutoring, the professors of the subject will offer personal guidance to each student in the tasks to be performed, with the aim to orient the approach and the methodology. Also they will offer coordination information with other contents and subjects of the study program. It is recommended to consult the doubts with the teachers along the course in order to improve the understanding of the basic concepts, and for performing the tasks and activities to be evaluated.
Case studies	In the practical formative activities and tutoring, the professors of the subject will offer personal guidance to each student in the tasks to be performed, with the aim to orient the approach and the methodology. Also they will offer coordination information with other contents and subjects of the study program. It is recommended to consult the doubts with the teachers along the course in order to improve the understanding of the basic concepts, and for performing the tasks and activities to be evaluated.
Laboratory practices	In the practical formative activities and tutoring, the professors of the subject will offer personal guidance to each student in the tasks to be performed, with the aim to orient the approach and the methodology. Also they will offer coordination information with other contents and subjects of the study program. It is recommended to consult the doubts with the teachers along the course in order to improve the understanding of the basic concepts, and for performing the tasks and activities to be evaluated.
Discussion Forum	In the practical formative activities and tutoring, the professors of the subject will offer personal guidance to each student in the tasks to be performed, with the aim to orient the approach and the methodology. Also they will offer coordination information with other contents and subjects of the study program. It is recommended to consult the doubts with the teachers along the course in order to improve the understanding of the basic concepts, and for performing the tasks and activities to be evaluated.

Assessment

	Description	Qualification	Training and Learning Results			
Laboratory practices	Students will perform a set of practices at the lab, where they work with the concepts studied along the master lessons.	45	A1	B1	C8 C11 C13	D5
Discussion Forum	Students must participate in the subject forum available at TEMA in FAITIC.	5	A1	B1	C11 C13	D4 D5
Objective questions exam	Three evaluation tests will be performed along the subject for the partial contents provided in the subject. Tests will be filled individually and time limited	45	A1	B1	C11 C13	D5
Short answer tests	Along master lessons, the teacher will ask questions to the students to test their knowledge level in the discussed topics.	5	A1		C11 C13	D5

Other comments on the Evaluation

The elements that are part of the evaluation of the subject are the following:

- **Questionnaires**: along the course the student will fill 3 questionnaires that will contribute 15% to the final mark (each one).

- **Laboratory practice**: each student will have to perform a set of practical tasks in the laboratory that will contribute 45% to the final mark.

- **Class participation**: students will discuss in class about expositions done by the professor, and this contributes up to a 5% to the final mark.

- **Forum participation**: students should interact individually in the forum of the subject to achieve up to a 5% to the final mark. To achieve such percentage the student should provide at least two relevant contributions.

Therefore, we have:

Final Mark = Questionnaires (3*x15% = 45%) + Lab. practice (45%) + Class participation (5%) + Forum (5%) = 100%.

The students need to pass the questionnaires and the practical task with at least 4 points over 10 to calculate the average final mark. If any of the marks is below 4, then the final mark will never be higher than 4 points over 10.

The schedule of the midterm/intermediate exams will be approved in the Comisión Académica de Grado (CAG) and will be available at the beginning of each academic semester.

Plagiarism is regarded as serious dishonest behavior. If any form of plagiarism is detected in any of the tests or exams, the

final grade will be FAIL (0), and the incident will be reported to the corresponding academic authorities for prosecution.

Following the degree guidelines, the students that will follow this subject can choose between two possibilities: continuous evaluation and final evaluation at the end of the semester.

Continuous assessment (CA): the student follows the continuous evaluation since the moment he/she fulfills two questionnaires. From that moment we assume that he/she will participate in the subject, independently of the assistance to the first call.

First Call: if the continuous evaluation is not performed, then the student will have to perform a final exam that substitutes the questionnaires done along the course, in addition to provide the practical tasks and the equivalent work to be done as part of the CA.

Second Call: the student will have to perform the part not passed previously.

The questionnaires and tasks, proposed and performed along the module, are only valid for the current course.

Sources of information

Basic Bibliography

Michael Hale Ligh, Andrew Case, Jamie Levy, Aaron Walters, **The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory**, 1, John Wiley & Sons Inc, 2014

Complementary Bibliography

Michael Sikorski / Andrew Honig, **Practical Malware Analysis**, 1, William Pollock, 2012

Recommendations

Subjects that are recommended to be taken simultaneously

Forensic Analysis/V05M175V01207
Hardening of Operating Systems/V05M175V01202
Security in Mobile Devices/V05M175V01206

Subjects that it is recommended to have taken before

Applications Security/V05M175V01104