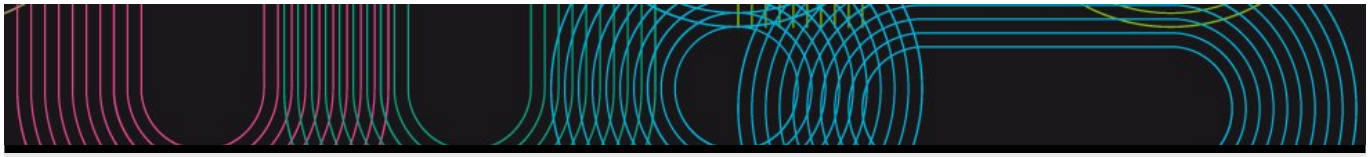

IDENTIFYING DATA				
Malware Analysis				
Subject	Malware Analysis			
Code	V05M175V01204			
Study programme	Máster Universitario en Ciberseguridad			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	5	Mandatory	1st	2nd
Teaching language	English			
Department				
Coordinator	Burguillo Rial, Juan Carlos			
Lecturers	Burguillo Rial, Juan Carlos Hernández Pereira, Elena María Rivas López, Jose Luis			
E-mail	jrial@uvigo.es			
Web	http://moovi.uvigo.gal/			
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. This course will be taught in English. However, students have the possibility to interact with teachers in Spanish or Galician if necessary. All the documentation needed for the course will be provided in English.			

Skills	
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) Structure. 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	2	2	4
Lecturing	10	30	40
Laboratory practical	15	40	55
Discussion Forum	0	2	2
Case studies	5	4	9
Objective questions exam	2	4	6
Problem and/or exercise solving	3	6	9

*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 practical	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 the MOOVI platform. Through this methodology the competencies CE8, CE11, CE13 and CT5 are developed. This activity will be performed individually.
Case studies	Along master lessons students will present case studies about threats, security problems already known and nowadays technologies. Through this methodology the competencies CG1, CE11, CE13 and CT5 are developed. This activity can be performed individually or in groups of two people.

Personalized assistance

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 practical	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 practical	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 Moovi.	5	A1	B1	C11 C13	D4 D5
Case studies	Students will provide presentations about case studies, selected by them, in order to analyze nowadays threads.	15		B1	C11 C13	D5
Objective questions exam	Two evaluation tests will be performed along the subject for the partial contents provided in the subject. Tests will be filled individually and time limited	30	A1	B1	C11 C13	D5
Problem and/or exercise solving	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 two questionnaires that will contribute 15% to the final mark (each one).

- **Presentation of case studies**: each student has to provide an original presentation, which contributes with a 15% to the final mark.

- **Laboratory practice**: each student will have to perform a set of practical tasks/quizzes 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 (2*x15% = 30%) + Case Study Presentation (15%) + Lab. Tasks (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 Máster (CAM) 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 or final assessment (at the end of the semester).

Continuous assessment: the student follows the continuous assessment since the moment he/she fulfills the two questionnaires. From that moment we assume that he/she will participate in the subject, independently of the presentation at the first call.

Exam-only assessment: if the continuous assessment 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 continuous assessment.

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

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

Complementary Bibliography

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