



IDENTIFYING DATA

Hardening of Operating Systems

Subject	Hardening of Operating Systems			
Code	V05M175V01202			
Study programme	Master's Degree in Cybersecurity			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	5	Mandatory	1st	1st
Teaching language	Spanish			
Department				
Coordinator	Blanco Fernández, Yolanda			
Lecturers	Blanco Fernández, Yolanda Yáñez Izquierdo, Antonio Fermín			
E-mail	yolanda@det.uvigo.es			
Web	http://guiadocente.udc.es/guia_docent/index.php?centre=614&ensenyament=614530&assignatura=614530007&any_academic=2021_22&idioma_assig=eng			
General description	A newly installed Operating system is inherently insecure. It has a certain number of vulnerabilities, depending on such things such as the age of the O.S., the amount of services it provides, the existence of initial backdoors not already patched, and the use of default policies designed without security in mind. By Hardening Operating Systems we refer to the act of configuring an operating system with the aim of making it as secure as possible, so that we minimize the risk of getting it compromised. This usually implies applying patches, changing default O.S. policies, and removing (or disabling) non-essential applications and/or services. In this course we'll try to identify common O.S. vulnerabilities and how to defend the O.S. against them. Both UNIX (linux) and Windows type O.S. will be considered.			

Skills

Code

Learning outcomes

Expected results from this subject	Training and Learning Results
------------------------------------	-------------------------------

Contents

Topic

Planning

	Class hours	Hours outside the classroom	Total hours
*The information in the planning table is for guidance only and does not take into account the heterogeneity of the students.			

Methodologies

Description

Personalized assistance

Assessment

Description	Qualification	Training and Learning Results
-------------	---------------	-------------------------------

Other comments on the Evaluation

Sources of information

Basic Bibliography

Recommendations

Contingency plan

Description

=== EXCEPTIONAL PLANNING ===

Given the uncertain and unpredictable evolution of the health alert caused by COVID-19, the University of Vigo establishes an extraordinary planning that will be activated when the administrations and the institution itself determine it, considering safety, health and responsibility criteria both in distance and blended learning. These already planned measures guarantee, at the required time, the development of teaching in a more agile and effective way, as it is known in advance (or well in advance) by the students and teachers through the standardized tool.

=== ADAPTATION OF THE METHODOLOGIES ===

- * Teaching methodologies maintained
- * Teaching methodologies modified
- * Non-attendance mechanisms for student attention (tutoring)
- * Modifications (if applicable) of the contents
- * Additional bibliography to facilitate self-learning
- * Other modifications

=== ADAPTATION OF THE TESTS ===

* Tests already carried out
Test XX: [Previous Weight 00%] [Proposed Weight 00%]
...

* Pending tests that are maintained
Test XX: [Previous Weight 00%] [Proposed Weight 00%]
...

* Tests that are modified
[Previous test] => [New test]

* New tests

* Additional Information
