



Teaching Guide

Identifying Data					2023/24
Subject (*)	Operating Systems Hardening		Code	614530108	
Study programme	Máster Universitario en Ciberseguridade				
Descriptors					
Cycle	Period	Year	Type	Credits	
Official Master's Degree	2nd four-month period	First	Obligatory	5	
Language	SpanishGalicianEnglish				
Teaching method	Face-to-face				
Prerequisites					
Department	Ciencias da Computación e Tecnoloxías da InformaciónComputación				
Coordinador	Yañez Izquierdo, Antonio Fermin	E-mail	antonio.yanez@udc.es		
Lecturers	Yañez Izquierdo, Antonio Fermin	E-mail	antonio.yanez@udc.es		
Web	faitic.uvigo.es				
General description	<p>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</p> <p>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.</p> <p>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.</p>				

Study programme competences / results

Code	Study programme competences / results
A28	HD-08 - Identificar las vulnerabilidades de un SO en un entorno de uso concreto, modificar la configuración para minimizar su exposición y comprobar su nivel de seguridad
B24	K-08 - Distinguir los distintos tipos de vulnerabilidades de los SO, su funcionamiento y configuración, así como la forma que limitan la exposición del SO
C11	C-06 - Identificar vulnerabilidades en un sistema real, así como variar sus parámetros y configurarlo para su protección frente a ellas; limitando así la exposición a amenazas conocidas
C15	C-10 - Diseñar y gestionar la seguridad de infraestructuras para realizar la auditoría de seguridad de la infraestructura y garantizar continuidad de negocio bajo normas y estándares de referencia

Learning outcomes

Learning outcomes	Study programme competences / results		
To identify the different vulnerabilities that affect an operating system	AJ28		
To understand how the vulnerabilities work and how the O.S. can be protected from them		BJ24	
To configure an O.S so that we minimize its exposure to threats, minimizing the risk of getting it compromised			CJ11 CJ15

Contents

Topic	Sub-topic
Introduction to H.O.S.	The concept of hardening an operating system. Vulnerabilities. Hardening during installation, post installation and maintenance.



Boot procedure hardening	Physical system security. Hardening the Firmware (BIOS, UEFI). Hardening the Boot Loader
Hardening user accounts	Identifying and eliminating non used accounts. Limiting user privileges. Group Policies. Hardening authentication. Forcing Password policies
Hardening File Systems	File system permissions and protections. Quotas. Locking system directories. Encryption. Limiting access to devices
Hardening applications	Identifying and eliminating non used applications. Identifying connections and eliminating apps/packages providing unwanted connections. Limiting applications privileges. Executing in secure environments: container based execution, SELinux...
Hardening network	Identify and eliminate unwanted connections/services. Packet filtering
Monitoring and maintenance	System monitoring. Logs. Securing logs. Identifying possible threats. Security patches.

Planning				
Methodologies / tests	Competencies / Results	Teaching hours (in-person & virtual)	Student's personal work hours	Total hours
Guest lecture / keynote speech	A28 B24 C11 C15	16	32	48
Laboratory practice	A28 B24 C11 C15	26	0	26
Practical test:	A28 B24 C11	4	14	18
Objective test	A28 B24 C11	3	30	33
Personalized attention		0	0	0

(*The information in the planning table is for guidance only and does not take into account the heterogeneity of the students.

Methodologies	
Methodologies	Description
Guest lecture / keynote speech	The student will attend to the lectures given by the teacher about how to minimize the chance of having usable vulnerabilities in the different parts of an O.S.: boot procedure, user accounts, network connections,,
Laboratory practice	Lab assignments dealing with securing the different parts of real world operating systems. Both UNIX (linux) and windows types will be considered
Practical test:	Solving problems similar to those carried out in practice on a physical machine (real or virtualized) with the sole help of the documentation available on the machine itself.
Objective test	Test about the fundamental contents of the subject

Personalized attention	
Methodologies	Description
Guest lecture / keynote speech Practical test: Objective test Laboratory practice	<p>Although the laboratory practices and the solution of problems will be carried out for the most part during class hours, the teacher will be available to help individually with any doubt or question that arises from the completion of these tasks.</p> <p>The professor will also be available to help with the concepts presented during the master sessions.</p> <p>The udc tutorial schedules can be found here</p> <p>https://www.udc.es/es/centros_departamentos_servizos/centros/titorias/?codigo=614</p>

Assessment			
Methodologies	Competencies / Results	Description	Qualification



Practical test:	A28 B24 C11	<p>There will also be a practical test where the student will perform some exercises on a physical computer (real or virtualized machine) without the help of additional material.</p> <p>This test will be carried out in practice sessions, after each part (linux and windows). It represents 40% of the subject's score (20% for Linux and 20% for Windows).</p> <p>Non-face-to-face students who want to have an continuous evaluation must take these tests. For them they represent 60% (30% for Linux and 30% for Windows)</p>	40
Objective test	A28 B24 C11	<p>Questions related to the knowledge acquired.</p> <p>Questions that involve reasoning over the knowledge acquired</p> <p>Questions that involve practical problem-solving on real world O.S. Hardening</p> <p>Both the objective test and the laboratory practice must be passed indepently in order to pass the subject</p>	40
Laboratory practice	A28 B24 C11 C15	<p>Control of the practices carried out and evaluation of the results obtained:</p> <p>The practices carried out during the practical sessions will yield 20% of the score for the subject (10% for Linux and 10% for Windows)</p>	20

Assessment comments

Nas oportunidades ordinaria e extraordinaria farase so a proba obxectiva.

Os alumnos que renuncien á avaliación continua e se decidan acollerse á global, terán que realizar este mesmo día una proba que terá un valor do 100% da cualificación da asignatura.

Dita proba consistirá nunha proba obxectiva, unha proba práctica ou unha combinación de ambas.

Para renunciar a avaliación continua e acollerse a avaliación global deberá enviarse un correo a antonio.yanez@udc.es

antes dunha semana da data da oportunidade ordinaria ou, no seu caso, extraordinaria.

Sources of information

Basic	<ul style="list-style-type: none"> - Donald A. Tevault (2018). Mastering Linux Security and Hardening. Packt Publishing - James Turnbull (2008). Hardening Linux . Apress - Carlos Álvarez Martín y Pablo González Pérez 0xWord (2016). Hardening de servidores GNU / Linux (3a Edición). 0xWord - Tajinder Kalsi (2018). Practical Linux Security Cookbook: Secure your Linux environment from modern-day attacks with practical recipes, 2nd Edition. Packt Publishing - Yuri Diogenes, Erdal Ozkaya (2018). Cybersecurity - Attack and Defense Strategies. Packt Publishing - Gris, Myriam (2017). Windows 10. ENI - Aprea, Jean-François (2017). Windows Server 2016 : Arquitectura y Administración de los servicios de dominio Active Directory. ENI - Bonnet, Nicolas (2017). Windows Server 2016 : las bases imprescindibles para administrar y configurar su servidor. ENI - De los Santos, Sergio (). Máxima Seguridad en Windows: Secretos Técnico. 0xWord - Núñez, Ángel (). Windows Server 2016: Administración, seguridad y operaciones. 0xWord - Salvy, Pierre (2017). Windows 10 : despliegue y gestión a través de los servicios de empresa. ENI - Deman, Thierry (2018). Windows Server 2016 : Administración avanzada. ENI - García, Carlos. González, Pablo (). Hacking Windows: Ataques a sistemas y redes Microsoft. 0xWord
--------------	--



Complementary	
---------------	--

Recommendations

Subjects that it is recommended to have taken before
--

Subjects that are recommended to be taken simultaneously
--

Subjects that continue the syllabus

Other comments

(*)The teaching guide is the document in which the URV publishes the information about all its courses. It is a public document and cannot be modified. Only in exceptional cases can it be revised by the competent agent or duly revised so that it is in line with current legislation.