COURSE PROGRAM: System Security Architecture

CODE: 503236

ACADEMIC YEAR: **2024/2025**

COURSE PROGRAM

Academic Year: 2024/2025

Identification and characteristics of the course

Code	503236	ECTS Credits	6
Course name (English)	System security architecture		
Course name (Spanish)	Arquitectura de seguridad en los sistemas		
Degree programs	Bachelor’s degree in computer engineering in Information Technologies		
Faculty/School	Mérida University Center http://www.unex.es/conoce-la-uex/estructura-academica/centros/cum		
Semester	7	Type of course	elective
Module	Elective contents module in Information Technologies		
Matter	Cybersecurity		
Lecturer/s			
Name	Office	E-mail	Web page
Josefa Díaz Álvarez	17	mjdiaz@unex.es	http://campusvirtual.unex.es
Subject Area	Computer architecture and technology http://www.unex.es/conoce-la-uex/estructura-academica/centros/cum/centro/departamentos		
Department	Computer and communication technology		
Coordinating Lecturer (If more than one)			

Competencies*

CG3 Ability to design, develop, assess, and guarantee the availability, ergonomics, usability, and security of computer systems, services, and applications and the information they manage.
CG4 – Ability to define, assess and select hardware and software platforms for the development and execution of systems, services, and computer applications, according to the acquired knowledge, as established in annex-2 of the Resolution of June 8, 2009, of the General Secretariat of Universities (BOE of August 4, 2009) in the field of Information Technology
CG8 –Knowledge of the base subjects and technologies that qualify them to learn and develop new methods and technologies, as well as those that provide them with great versatility to adapt to new situations.
CG9 – Ability to solve problems with initiative, decision-making, autonomy, and creativity. Ability to know how to communicate and transmit the knowledge, skills, and abilities of the Computer Engineering profession.

* The sections concerning competencies, course outline, educational activities, teaching methodologies, learning outcomes and assessment systems must conform to that included in the ANECA verified document of the degree program.

Basic competencies

CB1 – Students have demonstrated knowledge and understanding in a study area that builds on the foundation of general secondary education and it is usually at a level that, while relying on advanced textbooks, also includes some aspects that involve knowledge from the cutting edge of their study area.

CB2 – Students know how to apply their knowledge to their work or vocation in a professional way and have the skills that are usually evidenced by developing and presenting arguments and solving problems within their study area.

CB3 – Students have the ability of gather and interpret relevant data (generally in their study area) to make judgement that include a thought about relevant topics of social, scientific or ethical issues.

CB4 – Students can communicate information, ideas, problems and solutions to both specialized and non-specialized audiences.

CB5 – Students have developed those learning skills required to undertake further studies with a high level of autonomy.

Specific competencies

CEO2: Implementing systems and using tools to minimize an organization's risks in the cyberspace in the fase of security threats. Apply standards and procedures to protect the privacy, integrity and availability of information system. (ASS)

Transversal competencies

CT12 – Diversity and interculturalism

CT15 – Interpersonal communication

Contents

Course outline*

System setup and administration and its implications in security issues. Identification of computer system components and their relationship with security risks. Know the types of virtualizations, hypervisor architectures, virtualization taxonomies and security in virtual environments. Identify the main operating system vulnerabilities and hacking techniques. Apply analysis techniques to storage systems. Know the main tools applied to forensic research in local and remote environments. Cloud security

Course syllabus

Name of lesson 1: Setup and administration of Linux operating system

Contents of lesson 1:

1. Introduction
2. System startup and shutdown
3. User and group management
4. Filesystems
5. System monitoring and assessment
6. Software installation and upgrades
7. Backups
8. Task automatization and scheduling

Description of the practical activities of lesson 1: a case study is proposed that includes setup and administration tasks (startup management, uses, filesystems, storage, backups and system evaluation).

Name of lesson 2: Virtualization.

Contents of lesson 2:

1. Introduction to virtualization
   1.1. Virtualization and high availability
2. Virtualization taxonomies.
   2.1. Access virtualization
   2.2. Application virtualization
   2.3. Processing virtualization
   2.4. Network virtualization

   2.5. Storage virtualization
3. Hypervisor architectures.
   3.1. Partial virtualization
   3.2. Emulation
   3.3. Paravirtualization
   3.4. Full virtualization
   3.5. Virtual environments security

Description of the practical activities of lesson 2: The practical section Works with several virtualization hypervisors widely used in professional environments.

Name of lesson 3: Operating system vulnerabilities
Contents of lesson 3:

1. Introduction
2. Case studies on Windows, Linux y Mac
3. Virtualization attacks
4. Logs, upgrades and backups
5. Confidentiality in Big Data

Description of the practical activities of lesson 3: study with password recovery tools, priviledge escalation and hooking

Name of lesson 4: Hacking
Contents of lesson 4:

1. Introduction
2. Information systems
3. Social engineering
4. Ethical hacking
5. Hacking techniques
6. Types of attackers and audits

Description of the practical activities of lesson 4: work with tools used

Name of lesson 5: Forensic analysis
Contents of lesson 5:

1. Introduction
2. Methods
3. Analysis tools
   a. Network
   b. Memory
   c. Binary
   d. System

Description of the practical activities of lesson 5: study of tools used in

Educational activities *

Student workload in hours by lesson		Lectures	Practical activities				Monitoring activity	Homework
Lesson	**Total**	**L**	**HI**	**LAB**	**COM**	**SEM**	**SGT**	**PS**
1	36	10			6		1	19
2	23,5	6			3,5		0	14
3	25,5	5,5			4		0	16
4	27	6			4		1	16
5	30	8			4		1	17
Assessment **	8	2			1		0	5
TOTAL	150	37,5			22,5		3	87

L: Lectures (85 students)
HI: Hospital internships (7 students)

** Indicate the total number of evaluation hours of this subject.

LAB: Laboratory or field practices (15 students)
COM: Computer room or language laboratory practices (20 students)
SEM: Problem classes or seminars or case studies (40 students)
SGT: Scheduled group tutorials (educational monitoring, ECTS type tutorials)
PS: Personal study, individual or group work and reading of bibliography

Teaching Methodologies*

1. Lectures on theory and problems: Presentation of the contents of the subject and planning the participation of all students in the different tasks. Discussion of theoretical aspects. In addition, informative talks will be given by experts and/or companies in the field.

2. Participative teaching: Practical work in small or medium-sized groups.

3. Monitoring activity: Follow-up activity for supervised work, queries, and advice in small or individual groups.

4. Autonomous learning through the analysis of written documents, reports elaboration, the study of the taught subject, and the development of the proposed practical cases.

5. Virtual learning. Use of virtual communication tools between teacher and student and even between students themselves.

Learning outcomes *

Know how to safely configure and manage computer systems. Understanding system architectures to identify their vulnerabilities. Know and use security and forensic analysis tools in local and remote environments.

Linked to transversal competencies:

Demonstrate conviction that cultural diversity, consubstantial to coexistence generates social cohesion and inclusion. (CT12, 3rd level of mastery).

Encourage empathetic and sincere communication aimed at constructive dialogue (CT15, 3rd level of mastery).

Assessment systems *

Continuous assessment model

Assessment systems	Percentage
Exam	(Between 0 and 70%) 20%
Oral presentation of the works carried out	(Between 0 and 40%) 10%
Implementation of supervised Works (reports, case studies, exercices and problems).	(Entre el 0 y el 80%) 60%
Attendance and/or participation in classroom, virtual classroom, monitoring activities, etc.	(Entre el 0 y el 30%) 10%

Assessment criteria explanation:

1. Demonstrate the acquisition, comprehension of the main concepts of the subject.
2. Solve cases through the application of theoretical and experimental knowledge.
3. Clearly exhibit the theorical/practical works developed.

4. Critically and rigorously analyze the outcomes of the practical training.
5. Actively participate in the activities to be developed in both practical and theoretical sessions.

For continuous assessment, the implementation of the proposed case studies represents 60 % of the grade. Classroom attendance and participation are 10% of the grade. The oral presentation of the carried-out works constitutes 10% of the grade. The remaining 20% is for test exams that will be done during the semester.

If a student is found to commit plagiarism (presenting practical works from others as their own, cheating during the exam, presenting downloaded works from internet, etc.), in the practical part, work presentation, written exam, etc, a zero mark will be applied.

Students who pass one of the parts in the ordinary exam will keep that mark until the extraordinary exam in November of the following academic year.

Transversal Competences

Transversal competences will be continuously evaluated during practical, theoretical and ECTS sessions.
During the theoretical and practical sessions, students must solve problems that allow them to acquire the subject learning outcomes, providing quality solutions. The activities both in the interaction between students and in the documentation to be produced will be oriented towards guaranteeing respect and coexistence, taking care of the language, and promoting interaction between students.
In general, special emphasis will be given to constructive communication both during the learning process and in the work environment.
The milestones in the ECTS monitoring activities are a reference to check the degree of achievement and thus to detect deviations and facilitate improvement for each kind of competence.

Global asssessment model

For students taking the single final exam option, the following procedure will be applied:

1. At the end of the semester, students must take a final exam corresponding to the theoretical part. In this exam, the student will have to answer theoretical questions, either topic to be developed and/or multiple-choice questions. This part represents 50% of the mark for the course.
2. Attendance to the laboratory sessions and oral presentation of work is compulsory. This part accounts for 40% of the mark for the subject.

The remaining 10% of the grade is obtained from attendance and work during the compulsory sessions.

Bibliography (basic and complementary)

Basic Bibliography

1. “Essential System Administration, 2nd Edition Revised & Updated” Æleen Frisch. Ed O'Reilly & associates, Inc.
2. Ciberseguridad : hacking ético. Maíllo Fernández, J. (2020). Ra-Ma.

3. Computer Security Fundamentals Fourth Edition. Dr. Chuck Easttorn. Pearson
4. Learn Computer Forensics: A beginner's guide to searching, analyzing, and securing digital evidence. William Oettinger. 2020. Packt.

Complementary Bibliography

1. Administración de Sistemas Operativos Windows y Linux. Un enfoque práctico. Julio Gómez, Nicolás Padilla y Juan Antonio Gil. Ed. Rama.
2. Pentesting con Kali. David Santo Orcero
3. Learn Ethical Hacking from Scratch. Zaid Sabih. 2018. ISBN: 9781788622059
4. National Institute of Standards and Technology (NIST).
5. Josef Pieprzyk, Thomas Hardjono, and Jennifer Seberry. Fundamentals of Computer Security. Springer, 2003.
6. Oakley, J. (2019). Professional Red Teaming Conducting Successful Cybersecurity Engagements (1st ed. 2019.). Apress.
7. Roussev, V. (2017). Digital forensic science : issues, methods, and challenges . Morgan & Claypool Publishers
8. Oettinger, W. (2020). Learn Computer Forensics (1st edition). Packt Publishing.

Other resources and complementary educational materials

1. http://campusvirtual.unex.es
2. https://books.google.es/
   - "The Linux System Administrator's Guide" Lars Wirzenius, Joanna Oja, Stephen Stafford. Disponible en http://www.tldp.org/LDP/sag/index.html
   - Cyber Security and Digital Forensics: Challenges and Future Trends. Wiley. 2022
   - Introduction to cyber security: stay safe online. The open university. 2016.