DESCRIPCIÓN DE LA ASIGNATURA

Grado/Máster en:	Master Universitario en INGENIERÍA INFORMÁTICA por la Universidad de Málaga
Centro:	Escuela Técnica Superior de Ingeniería Informática
Asignatura:	DISEÑO Y CONFIGURACIÓN DE SISTEMAS SEGUROS EN RED
Código:	103
Tipo:	Obligatoria
Materia:	CIBERSEGURIDAD DE SISTEMAS Y APLICACIONES
Módulo:	TECNOLOGÍAS INFORMÁTICAS
Experimentalidad:	
Idioma en el que se imparte:	Español
Curso:	1
Semestre:	1
Nº Créditos	6
Nº Horas de dedicación del estudiante:	150
Nº Horas presenciales:	45
Tamaño del Grupo Grande:	
Tamaño del Grupo Reducido:	
Página web de la asignatura:	

EQUIPO DOCENTE

Departamento: LENGUAJES Y CIENCIAS DE LA COMPUTACIÓN

Área: INGENIERÍA TELEMÁTICA

Nombre y Apellidos	Mail	Teléfono Laboral	Despacho	Horario Tutorías
Coordinador/a: FRANCISCO JAVIER LOPEZ MUÑOZ	fjlopezm@uma.es	952131327	3.2.14 - E.T.S.I. INFORMÁTICA	

RECOMENDACIONES Y ORIENTACIONES

Although it is not a strictly essential requirement for taking this course, it is recommended that the student has basic knowledge on information security and networking, maybe by having taken previous course(s) on those topics at BSc level (Grado).

CONTEXTO

This course is divided into three main blocks. The first block provides the basis for the students to understand the structure and motivation of the course, its purpose and the fundamental principles on which to support and develop their learning. In the second block, the students will acquire in-deep knowledge of attacks at different network levels, the security requirements that are required to mitigate these attacks, as well as an overview of the countermeasures to be taken in order to hardening the network system. The last block is designed to make the student understand how to take decisions regarding the configuration of secure network systems at a higher level. With this aim, the student will learn to identify and solve possible vulnerabilities in the operating systems, and will learn the main characteristics of the systems for the comprehensive management of security on large scale networks.

COMPETENCIAS

1 Competencias generales y básicas.

Competencias básicas

1.1 CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación

1.2 CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio

1.3 CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios

1.4 CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades

1.5 CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo

2 Competencias específicas.

2.1 ETI1 - Capacidad para modelar, diseñar, definir la arquitectura, implantar, gestionar, operar, administrar y mantener aplicaciones, redes, sistemas, servicios y contenidos informáticos.

2.2 ETI2 - Capacidad de comprender y saber aplicar el funcionamiento y organización de Internet, las tecnologías y protocolos de redes de nueva generación, los modelos de componentes, software intermediario y servicios.

2.3 ETI3 - Capacidad para asegurar, gestionar, auditar y certificar la calidad de los desarrollos, procesos, sistemas,

2 Competencias específicas.

servicios, aplicaciones y productos informáticos.

3 Competencias transversales.

3.2 CT2 - Capacidad para identificar estrategias, herramientas y métodos que responden a situaciones de éxito que pueden ser abordadas con los recursos disponibles.

CONTENIDOS DE LA ASIGNATURA

PART I - FOUNDATIONS

Chapter 1. Introduction to Cyber-Security

- Sources and Motives of Cybersecurity Threats
- Sources of Vulnerabilities
- Types of Threats in Network Security

Chapter 2. Network perimeter Basics

- Network elements
- Protocols
- Attacks landscape

PART II - NETWORK HARDENING

Chapter 3. Switches & Routers Hardening

- Attacks to Switches and Countermeasures
- Attacks to Routers and Countermeasures
- Wireless Hardening

Chapter 4. Firewalls Hardening

- Firewall features
- Type of (Network) Firewalls and Checklists
- Firewalls Configuration and Location

Chapter 5. Intrusion Detection and Prevention Systems (IDPS)

- IDPS Fundamentals
- IDPS Categories and Deployment Architectures
- Honeypots
- Tools for testing IDSs

PART III - HARDENING INFRASTRUCTURE SYSTEMS

Chapter 6. Harden the Operating System

- Linux Security
- Windows Security
- Vulnerability analysis

Chapter 7. Security information and event management (SIEMs) systems

- Characteristics and purpose of a SIEM
- Basic steps and requirements to configure a SIEM
- Security Operations Center (SOC)

ACTIVIDADES FORMATIVAS

Actividades presenciales

Actividades expositivas

Lección magistral

ACTIVIDADES DE EVALUACIÓN

Actividades de evaluación presenciales

Actividades de evaluación del estudiante

Realización de trabajos y/o proyectos

Otras actividades eval.del estudiante

RESULTADOS DE APRENDIZAJE / CRITERIOS DE EVALUACIÓN

It is expected that, at the end of this course, the student has acquired the following skills:

- The student will be able to understand and classify new emerging attacks. This will be possible because, during the course, the student will learn the characteristics of the attacks to identify not only the already known attacks, but to identify the existence of new ones.

- Be aware of the limitations of network elements and potential advantages to stop specific threats if they are configured properly.

- Understand the specific characteristics of the network elements used for security and why their location is very important.

- Learn to identify vulnerabilities in operating systems and to apply countermeasures to solve them.

- Be able to understand the concept of "trustworthy computing" and the current solutions that can be used to build a trustworthy platform.

- Learn what is a Security information and event management (SIEM) and a Security Operations Center (SOC) and when should be used.

- Be critical and skilled in the performance of his/her functions, able to demonstrate in a comfortable way that will be able to face the new security challenges that are about to appear.

PROCEDIMIENTO DE EVALUACIÓN

Evaluation of the contents of the course will be mainly based on projects and practical assignments developed by the student along the semester.
More precisely, up to 80% of the final grade will be based on incremental lab projects and corresponding practical assignments, that student will perform individually and for which will provide activity reports.

An additional 20% of the final grade will be based on up to two individual essays for different works proposed to students.

Should the student need to pass the course in September or further, he/she will have to obtain 5 out of 10 points in the exam.

BIBLIOGRAFÍA Y OTROS RECURSOS

Básica

Chayapathi, R., Hassan, S. F., & Shah, P. (2016). Network Functions Virtualization (NFV) with a Touch of SDN. Addison-Wesley Professional.

Dieterle, D.W. (2015). Intermediate Security Testing with Kali Linux 2.

Halton, W., & Weaver, B. (2016). Kali Linux 2: Windows Penetration Testing. Packt Publishing Ltd.

Kizza, J. M. (2017). Guide to computer network security. Springer.

Miller, D. R., Harris, S., Harper, A., VanDyke, S., & Blask, C. (2010). Security Information and Event Management (SIEM) Implementation (Network Pro Library). McGraw Hill

Noonan, W. J. (2004). Hardening network infrastructure. McGraw-Hill/Osborne.

Rao, U. H., & Nayak, U. (2014). The InfoSec Handbook. Apress.

Rhodes-Ousley, M. (2013). Information security: the complete reference. McGraw Hill Education.

Stallings, W. (2013). Network security essentials: applications and standards. Pearson Education.

DISTRIBUCIÓN DEL TRABAJO DEL ESTUDIANTE

ACTIVIDAD FORMATIVA PRESENCIAL

Descripción	Horas	Grupo grande	Grupos reducidos
Lección magistral	45	☑	☐
TOTAL HORAS ACTIVIDAD FORMATIVA PRESENCIAL	**45**		
TOTAL HORAS ACTIVIDAD FORMATIVA NO PRESENCIAL	**90**		

TOTAL HORAS ACTIVIDAD EVALUACIÓN	15 horas	Grupo grande	Grupos reducidos
TOTAL HORAS DE TRABAJO DEL ESTUDIANTE	150		