UNIVERSIDAD COMPLUTENSE DE MADRID

FACULTAD DE INFORMATICA

Ficha del curso: 2020-2021

Debido la situación especial del curso 2020-2021, para conocer el régimen de presencialidad de las asignaturas se debe comprobar la información que se encuentra publicada en https://informatica.ucm.es/marco-docente-2020-2021

Grado: GRADO EN INGENIERÍA INFORMÁTICA	**Curso**: Optativas itinerario 3º **(** 1C **)**	Idioma: **Español**
Asignatura: 805359 - Redes y seguridad I **Asignatura en Inglés**: Network Security I	**Abrev:** RS1 **Carácter:** Optativa	4,5 **ECTS**
Materia: Redes y seguridad	9 **ECTS**	
Otras asignaturas en la misma materia: Redes y seguridad II	4,5 ECTS	
Módulo: Tecnología específica: Tecnologías de la información		
Departamento: Arquitectura de Computadores y Automática	**Coordinador:** Sánchez-Elez Martín, Marcos	

Descripción de contenidos mínimos:

Conceptos básicos sobre seguridad.
Técnicas de cifrado, firmas, certificados digitales y PKI.
Comunicaciones seguras.
Conceptos básicos sobre políticas y auditorías de seguridad.

Programa detallado:

==TEORÍA==

Módulo 1. Introducción a la seguridad de sistemas
1.1. Introducción
1.2 Tendencias en seguridad
1.3 Anatomía de un ataque
1.4 Introducción a la gestión de la seguridad
1.5 Marco Legal

Módulo 2. Comunicaciones seguras
2.1. Introducción
2.2. Técnicas de cifrado: clave secreta, clave pública y funciones resumen
2.3. Firmas digitales
2.4. Certificados digitales y autoridades de certificación
2.5. Aplicaciones para comunicaciones seguras

Módulo 3. Seguridad de sistemas
3.1 Seguridad de usuarios y grupos
3.2 Seguridad del sistema de archivos
3.3 Seguridad de los programas
3.3 Troyanos, puertas traseras y virus
3.5 Otros aspectos de seguridad del sistema

==PRÁCTICAS==

Módulo 0
0.1 Comandos básicos de Linux. Usuarios y permisos (primer cuatrimestre)

Módulo 2
2.1 Cifrado de clave secreta y funciones resumen
2.2 Cifrado de clave pública
2.3 Certificados digitales, autoridades de certificación y
fortificación de un servidor web mediante SSL

Módulo 3
3.1 ACLs en GNU-Linux
3.2 Fuzzing de aplicaciones
3.3 Programación de Buffer overflows (pila y montículo), shellcodes
3.4 Malware
3.4.1 Vulnerabilidades y ataques comunes en Windows (troyanos, cracking de aplicaciones)
3.4.2 Vulnerabilidads y ataques comunes en Linux (rootkits)

Fecha: ____ de _____ de _____

Firma del Director del Departamento:

Programa detallado en inglés:

==THEORY==

Module 1. Introduction to system security
1.1 Introduction
1.2 Security trends
1.3 Anatomy of an attack
1.4 Introduction to Security Operations
1.5 Legal aspects

Module 2. Communications Security
2.1 Introduction
2.2 Encryption techniques: Secret keys, Public keys, hash functions
2.3 Digital signatures
2.4 Public Key Infrastructure
2.5 Secure communications applications

Module 3. System Security
3.1 Users and groups security
3.2 File system security
3.3 Application security
3.4 Trojans, backdoors and virus

==LABORATORY==

Module 0
0.1 Basic Linux console commands. Linux users. File permissions (first semester)

Module 2
2.1 Secret key and hash functions
2.2 Public key
2.3 Digital certificates, certification authorities and web server hardening with SSL

Module 3
3.1 ACLs in GNU-Linux
3.2 Application fuzzing
3.3 Buffer (stack and heap) overflow coding, shellcodes
3.4 Malware:
3.4.1 Windows trojans and application cracking
3.4.2 Linux rootkit deployment and detection

Competencias de la asignatura:

Generales:

CG14-Capacidad de conocer, comprender y evaluar la estructura y arquitectura de los computadores, así como los componentes básicos que los conforman.

Específicas:

CE_TI1-Capacidad para comprender el entorno de una organización y sus necesidades en el ámbito de las tecnologías de la información y las comunicaciones.

CE_TI4-Capacidad para seleccionar, diseñar, desplegar, integrar y gestionar redes e infraestructuras de comunicaciones en una organización.

CE_TI7-Capacidad para comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos.

Básicas y Transversales:

Fecha: ____ de _____ de _____

Firma del Director del Departamento:

CT1-Capacidad de comunicación oral y escrita, en inglés y español utilizando los medios audiovisuales habituales, y para trabajar en equipos multidisciplinares y en contextos internacionales.

CT2-Capacidad de análisis y síntesis en la resolución de problemas.

CT3-Capacidad para gestionar adecuadamente la información disponible integrando creativamente conocimientos y aplicándolos a la resolución de problemas informáticos utilizando el método científico.

CT4-Capacidad de organización, planificación, ejecución y dirección de recursos humanos.

CT5-Capacidad para valorar la repercusión social y medioambiental de las soluciones de la ingeniería, y para perseguir objetivos de calidad en el desarrollo de su actividad profesional.

Resultados de aprendizaje:

Analizar vulnerabilidades de sistemas y explotarlos. (CG14, CT2, CT3, CE_TI1, CE_TI4, CE_TI7)

Describir temas relacionados con la asignatura al resto de los compañeros (CG14, CT1, CT4, CT5, CE_TI1, CE_TI4)

Intercambiar información con el resto de compañeros. (CT1, CT4, CT5, CE_TI1, CE_TI4)

Relacionar paradigmas de ataques con su aplicación en diversas tecnologías. (CG14, CT2, CT3, CE_TI1, CE_TI4, CE_TI7)

Resolver retos que requieren conocimientos adquiridos en la asignatura e ingenio. (CG14, CT1, CT2, CT3, CT4, CE_TI1, CE_TI4)

Evaluación:

Todas las pruebas realizadas en cada asignatura serán comunes a todos los grupos de la misma.
La calificación final tendrá en cuenta:
Exámenes sobre la materia: 70-90%
Otras actividades: 10-30%
En el apartado "Otras actividades" se podrá valorar la participación activa en el proceso de aprendizaje, la realización de prácticas y ejercicios y la realización de otras actividades dirigidas. La realización de las prácticas de laboratorio y del resto de las actividades evaluables será obligatoria.
Antes del comienzo de cada curso escolar se concretarán en las fichas docentes los porcentajes exactos que se utilizarán durante ese curso para la evaluación de la materia, siendo comunes estos criterios para todos los grupos de una misma asignatura.
La calificación reflejará los resultados de aprendizaje de las diferentes competencias que se adquieren en el módulo o materia.

Evaluación detallada:

La asignatura consta de una parte práctica (que no se recupera en la convocatoria extraordinaria) y una parte teórica.

La calificación será:
1) 70% (examen teórico) + 30% (prácticas y otras actividades)
2) 90% (examen teórico-práctico)

El estudiante podrá ser calificado siguiendo la opción marcada como 1 tanto en la convocatoria ordinaria como extraordinaria si ha realizado todas las prácticas y al menos el 66% de las actividades de evaluación continua.

En caso contrario el estudiante será calificado siguiendo la opción 2, este examen se realizará el mismo día y hora que el examen de la opción 1.

La asistencia a la tutorización para la realización de las prácticas durante las 2h reservadas para ello por la asignatura es obligatoria (asistencia virtual/presencial al laboratorio), en caso de que para una práctica particular el estudiante no asista a esta, esa práctica puntuará un 66% de su nota.

Actividades docentes:

Reparto de créditos:
- Teoría: 2,00
- Problemas: 0,00
- Laboratorios: 2,50

Otras actividades:
- Actividades presenciales: enseñanza teórica y realización de prácticas.
- Trabajo personal: realización de las prácticas, preparación del examen, participación activa en clase.
- Participación activa en clase: propuesta de mejoras (teoría y prácticas), propuesta y discusión de temas relacionados con la temática de la asignatura, propuesta y defensa en el aula de un tema consensuado con el profesor.

Fecha: ____ de _____ de _____

Firma del Director del Departamento:

Bibliografía:

- E. Cole. Network Security Bible, 2nd Edition. Ed. John Wiley & Sons. 2009
- J. Vacca. Computer and Information Security Handbook. Ed. Morgan Kaufmann. 2009
- B. Burns y otros. Security Power Tools. Ed. O'Reilly. 2007
- S. MacClure y otros. Hacking exposed 6. Ed. MacGraw Hill. 2009
- R. Johnson and M. Merkow. Security Policies and Implementation Issues. Ed. Jones & Bartlett Learning. 2010
- S. Harris, F. Maymí, Mc Graw Hill, All in one CISSP, exam guide, 7ª edición 2016
- William Stallings Network Security Essentials: Applications and Standards, Prentice Hall, 2013
- J. Michael Stewart, Jones & Bartlett Learning, Network Security, Firewalls, and VPNs, 2014
- Ruby B. Lee, Security Basics for Computer Architects, Synthesis Lectures on Computer Architecture, 2013

Ficha docente guardada por última vez el **21/07/2020 9:53:00** por el departamento: **Arquitectura de Computadores y Automática**

Fecha: ____ de _____ de _____

Firma del Director del Departamento: