Comunicaciones Seguras

Curso Académico: (2022 / 2023) **Fecha de revisión: 19-01-2023**

Departamento asignado a la asignatura: Departamento de Ingeniería Telemática

Coordinador/a: PASTOR PERALES, ANTONIO AGUSTIN

Tipo: Obligatoria Créditos ECTS : 6.0

Curso : 1 Cuatrimestre : 1

REQUISITOS (ASIGNATURAS O MATERIAS CUYO CONOCIMIENTO SE PRESUPONE)

Esta asignatura asume conocimientos previos sobre redes de comunicaciones TCP/IP y criptografía.

OBJETIVOS

COMPETENCIAS
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.

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.

Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando.

Elaborar concisa, clara y razonadamente documentos, planes y proyectos de trabajo en el ámbito de la Ciberseguridad.

Aplicar los servicios, mecanismos y protocolos de seguridad oportunos en un caso concreto.

Diseñar y evaluar arquitecturas de seguridad de sistemas y redes.

Conocer y aplicar los mecanismos de cifrado y esteganografia pertinentes para proteger los datos residentes en un sistema o en tránsito por una red.

RESULTADOS DE APRENDIZAJE
Esta asignatura contribuye a los siguientes resultados de aprendizaje:

Identificado un ataque y su fuente, proponer las contramedidas para contrarrestarlo explicando la medida de su eficacia. Evaluar estrategias de zonificación de redes y diseñar políticas de filtrado de tráfico.

Dado un sistema con unos requisitos de seguridad establecidos, proponer mecanismos y protocolos necesarios para proporcionar algunos de los servicios básicos de seguridad: autenticación, autorización, privacidad y control de acceso. Dar una medida de su eficacia y limitaciones.

Evaluar la arquitectura de seguridad de un sistema vulnerable dado y proponer mejoras.

DESCRIPCIÓN DE CONTENIDOS: PROGRAMA

1. Principios de seguridad de redes de comunicaciones
   1.1. Definiciones y conceptos. Servicios de seguridad vs. Mecanismos de seguridad
   1.2. Ataques más comunes a las redes de comunicaciones
   1.3. Contramedidas. Costes de la seguridad.

2. Seguridad en el nivel físico y de enlace. Ataques y defensas.
   2.1. Redes Ethernet. Ataques y defensas
   2.2. Los protocolos PPP y EAP. Autenticación, Autorización y Contabilidad (AAA)
   2.3. Seguridad en familia IEEE 802.11

3. Seguridad en el nivel de red.
   3.1. Seguridad en IPv4 e IPv6.

3.2. Protocolos auxiliares (ICMP, DHCP). Ataques y defensas
3.3. Protocolos de encaminamiento. Ataques y defensas.
3.4. IPsec

4. Seguridad en el nivel de transporte.
4.1. TLS/SSL.
4.2. Redes privadas virtuales SSL

5. Seguridad en el nivel de aplicación.
5.1. Seguridad en DNS
5.2. Seguridad en HTTP
5.3. Seguridad en correo electrónico
5.4. Seguridad en otras aplicaciones: ejecución remota, transferencia de ficheros, ficheros en red.

ACTIVIDADES FORMATIVAS, METODOLOGÍA A UTILIZAR Y RÉGIMEN DE TUTORÍAS

ACTIVIDADES FORMATIVAS
Clase teórica
Prácticas de laboratorio
Tutorías
Trabajo en grupo
Trabajo individual del estudiante

METODOLOGÍAS DOCENTES
Exposiciones en clase del profesor, con soporte de medios informáticos y audiovisuales, en las que se desarrollan los conceptos principales de la materia y se proporciona la bibliografía para complementar el aprendizaje de los alumnos.
Lectura crítica de textos recomendados por el profesor de la asignatura: Artículos de prensa, informes, manuales y/o artículos académicos, bien para su posterior discusión en clase, bien para ampliar y consolidar los conocimientos de la asignatura.
Resolución de casos prácticos, problemas, etc. planteados por el profesor de manera individual o en grupo
Elaboración de trabajos e informes de manera individual o en grupo

SISTEMA DE EVALUACIÓN

Evaluación continua:
Práctica de WLAN: 10%
Laboratorio de MitM: 10%
Laboratorio de TLS: 10%
Examen parcial: 35%
Examen final (conv. ord.): 35%

En los exámenes es necesario obtener una nota mínima de 3,5 sobre 10 puntos.

Evaluación no continua:
Examen final (conv. extr.): 100%

Peso porcentual del Examen Final:	35
Peso porcentual del resto de la evaluación:	65

BIBLIOGRAFÍA BÁSICA

- Charlie Kaufman, Radia Perlman, Mike Speciner Network Security: Private Communication in a Public World, Second Edition, 2002
- William Stallings Cryptography and Network Security: Principles and Practice, Prentice Hall, 2013

BIBLIOGRAFÍA COMPLEMENTARIA

- Jon Edney, William A. Arbaugh Real 802.11 Security: Wi-Fi Protected Access and 802.11i, Addison-Wesley Professional, 2003
- Sheila E. Frankel, Paul Hoffman, Angela Orebaugh, Richard Park Guide to SSL VPNs, NIST, 2008
- Stephen Thomas SSL & TLS essentials: securing the Web, John Wiley & Sons, 2000
- Yago Fernández Hansen, Antonio Angel Ramos Varón, Jean Paul García-Moran Maglaya RADIUS / AAA / 802.1x, RA-MA Editorial, 2008