2822 – REDES DE COMPUTADORAS Y SEGURIDAD

UASLP
Universidad Autónoma de San Luis Potosí

FACULTAD DE INGENIERÍA
Área de Ciencias de la Computación

Clave de la materia: 2822
Clave Facultad: 2822
Clave U.A.S.L.P.: ----
Clave CACEI: CI
Nivel del Plan de Estudios: I.S.I.: 5
No. de créditos: 8
Horas/Clase/Semana: 4
Horas totales/Semestre: 64
Horas/Práctica (y/o Laboratorio): 0
Prácticas complementarias: 0
Trabajo extra-clase Horas/Semana: 4
Carrera/Tipo de materia: I.S.I./Obligatoria
No. de créditos aprobados: ----
Fecha última de Revisión Curricular: 26-junio-2019
Materia y clave de la materia requisito: Ninguna

OBJETIVO DEL CURSO

Aplicar los protocolos necesarios para la operación y funcionamiento de redes de computadoras, además de conocer e implementar los principios de la seguridad informática para dichas redes.

CONTENIDO TEMÁTICO

1. INTRODUCCIÓN A REDES

Tiempo Estimado: 3 hrs.

Objetivo: Analizar los conceptos básicos de las redes de computadoras.

1.1. Estructura del Internet
1.2. Conmutación de circuitos y de paquetes
1.3. El sistema de capas para redes
1.4. Principales equipos físicos de red

2. APLICACIONES DE REDES

Tiempo Estimado: 7 hrs.

Objetivo: Analizar e implementar aplicaciones que se comuniquen a través del Internet.

2.1. Principios de aplicaciones para redes
2.2. El caso de HTTP
2.3. Programación de sockets

3. CAPA DE TRANSPORTE

Tiempo estimado: 6 hrs.

Objetivo: Analizar y aplicar las funciones básicas de la capa de transporte: Transmisión confiable y control del flujo de la información.

3.1. La capa de transporte, TCP y UDP
3.2. Principios de transmisión confiable
3.3. Principios de control de flujos

4. CAPA DE RED

Tiempo estimado: 9 hrs.

Objetivo: Realizar configuración básica de redes IPv4, IPv6, y analizar los protocolos de ruteo que se emplean en Internet.

4.1. IPv4 e IPv6
4.2. Ruteo estático y ruteo dinámico
4.3. Protocolos de ruteos en el Internet

5. CAPAS DE ACCESO AL MEDIO Y FÍSICA

Tiempo estimado: 7 hrs.

Objetivo: Comprender las funciones principales y las implementaciones de las capas de acceso al medio y física.

5.1. El problema de acceso a un medio compartido
5.2. LANs
5.3. Ethernet
5.4. Partición y multiplexación de canales físicos

6. PRINCIPIOS DE SEGURIDAD

Tiempo estimado: 11 hrs.

Objetivo: Analizar y aplicar los conceptos básicos de seguridad informática.

6.1. Integridad, confidencialidad y disponibilidad
6.2. Riesgo, amenaza, vulnerabilidad
6.3. Autorización, autenticación y control de acceso
6.4. Ética de seguridad informática

7. AMENAZAS Y ATAQUES

Tiempo estimado: 11 hrs.

Objetivo: Identificar los riesgos, vulnerabilidades y amenazas en los sistemas informáticos, así como los ataques más comunes.

7.1. Motivación y objetivos del atacante
7.2. Malware: virus, gusanos, caballo de Troya, rootkit, spyware
7.3. Denial of service (DoS) y Distributed Denial of Service (DDoS)
7.4. Ingeniería social

8. SEGURIDAD DE REDES

Tiempo estimado: 10 hrs.

Objetivo: Analizar los mecanismos de seguridad en redes y sus principales vulnerabilidades, y aplicar las contramedidas adecuadas.

8.1. Ataques específicos para redes
8.2. Empleando criptografía para comunicación segura
8.3. Arquitectura para redes seguras
8.4. Mecanismos de defensa y contención

METODOLOGÍA

Explicación de los temas por parte del profesor y desarrollo de ejercicios por parte de los alumnos siguiendo el método de aprendizaje basado en problemas. Se espera que el alumno investigue ciertos temas, siguiendo el método de aula invertida. Implementar estrategias de trabajo en equipo cuando sea conveniente (aprendizaje colaborativo).

EVALUACIÓN

Se realizarán cuatro exámenes parciales de forma colegiada en las fechas establecidas por la Facultad, de acuerdo al Reglamento de Exámenes. La calificación de los exámenes parciales estará compuesta en 80% por el examen parcial, y el otro 20% por otras actividades, como tareas e investigaciones. La calificación del examen ordinario es el promedio de los cuatro parciales.

BIBLIOGRAFÍA

Bibliografía Básica

Kurose, J.F., Ross, K.W. *Computer Networking: A Top-Down Approach Featuring the Internet*. 7th Edition, Addison-Wesley, 2016.

Stallings, W. *Data and Computer Communications*. 10th Edition, Prentice Hall, 2013.

Grimes, R. *Hacking the Hacker: Learn from the Experts Who Take Down Hackers*, 1st Edition, Wiley, 2017.

Whitman, M., Mattord H., *Principles of Information Security*. 6ª Edición, Cengage Learning, 2017.

Bibliografía Complementaria

Kenneth, C., Mansfield, J., James, L., Antonakos. *Computer Networking from LANs to WANs: Hardware, Software and Security*. Course Technology, 1st Edition, 2010.

Nastase, R. *Cisco CCNA Command Guide: An Introductory Guide for CCNA & Computer Network Beginners*. Cisco Press, 2017.

Astudillo, K. *Hacking Ético*. 3ª Edición, Ra-Ma, 2018.

Ozkaya, E. *Learn Social Engineering: Learn the Art of Human Hacking with an Internationally Renowned Expert*, 1st Edition, Packt Publishing, 2018.