Proyecto Docente de la asignatura de Seguridad Informática

Asignatura	Seguridad Informática		
Materia	Planificación y Explotación de Sistemas Informáticos		
Módulo			
Titulación	Grado en Ingeniería Informática de Servicios y Aplicaciones		
Plan	413	**Código**	40823
Periodo de impartición	Semestre 4	**Tipo/Carácter**	OB
Nivel/Ciclo	Grado	**Curso**	2
Créditos ECTS	6 ECTS		
Lengua en que se imparte	Español		
Profesor/es responsable/s	Juan José Álvarez Sánchez		
Datos de contacto (E-mail, teléfono…)	E. I. de Informática Plaza de la Universidad, 1. 40005 Segovia Tel.: +34 921 112430 Fax: +34 921 112401 e-mail: jjalvarez@infor.uva.es http://www.infor.uva.es/~jjalvarez/		
Horario de tutorías	Disponible en http://www.uva.es/ (UVa → Campus de Segovia → E. I. de Informática → Tutorías)		
Departamento	Informática (ATC, CCIA, LSI)		

Objetivos Generales

- Dominar los principios básicos de la criptografía así como su implementación a las arquitecturas OSI y TCP/IP.
- Comprender los problemas derivados de la seguridad informática en el diseño de configuraciones diferentes de redes y sus capas.
- Dominar las tecnologías profesionales para la de gestión y administración de seguridad en redes y hosts.
- Dominar y desarrollar la gestión de servicios de red y su protección.
- Capacidad para supervisar problemas de intrusión que afecten al rendimiento y la privacidad de las redes de computadores.

Competencias a desarrollar

Competencias genéricas:

G01, G02, G03, G04, G05, G07, G08, G09, G10, G11, G12, G13, G14, G16, G17, G18, G19, G20, G21 y G22. G06 opcional (si se elige la modalidad bilingüe español-inglés).

Competencias específicas:

- E07-Capacidad para diseñar, desarrollar, seleccionar y evaluar aplicaciones y sistemas informáticos, asegurando su fiabilidad, seguridad y calidad, conforme a principios éticos y a la legislación y normativa vigente.
- E09- Capacidad para elaborar el pliego de condiciones técnicas de una instalación informática que cumpla los estándares y normativas vigentes
- E10-Conocimiento, administración y mantenimiento sistemas, servicios y aplicaciones informáticas.
- E13-Capacidad para analizar, diseñar, construir y mantener aplicaciones de forma robusta, segura y eficiente, eligiendo el paradigma y los lenguajes de programación más adecuados.
- E16-Conocimiento y aplicación de las características, funcionalidades y estructura de los Sistemas Distribuidos, las Redes de Computadores e Internet y diseñar e implementar aplicaciones basadas en ellas.
- E22-Capacidad para comprender la importancia de la negociación, v los hábitos de trabajo efectivos, el liderazgo y las habilidades de comunicación en todos los entornos de desarrollo de software.
- E25-Capacidad para comprender el entorno de una organización y sus necesidades en el ámbito de las tecnologías de la información y las comunicaciones.
- E31-Capacidad para comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos.

Bloque 1: Redes de computadoras e Internet. Principios de Criptografía

Carga de trabajo en créditos ECTS: 1

a. Contextualización y justificación

Introducción del vocabulario y los términos específicos para el estudio pormenorizado de la seguridad en los niveles OSI y TCP/IP.

b. Objetivos de aprendizaje

- Internet y sus protocolos
- Arquitecturas cliente-servidor.
- Conceptos básicos de criptografía

c. Contenidos

1.1 ¿Qué es Internet?
1.1.1 Descripción de los componentes esenciales
1.1.2 Descripción de los servicios
1.1.3 ¿ Qué es un protocolo ?

1.2 La frontera de la red
1.2.1 Programas cliente y servidor
1.2.2 Redes de acceso
1.2.3 Medios físicos

1.3 Capas de protocolos y sus modelos de servicio
1.3.1 Arquitectura en capas
1.3.2 Mensajes, segmentos, datagramas y tramas

1.4 Fundamentos de criptografía
1.4.1 Criptografía de clave privada
1.4.2 Criptografía de clave pública

Bloque 2: La capa de aplicación

Carga de trabajo en créditos ECTS: 1,2

a. Contextualización y justificación

Esta es la capa con la que se encuentra el usuario y por tanto es muy importante conocer de primera mano sus funcionalidades para dar un servicio apropiado de seguridad en la red.

b. Objetivos de aprendizaje

- Dominar los protocolos de seguridad de los servicios HTTP, Correo electrónico y aplicaciones P2P.

c. Contenidos

2.1 La Web y HTTP
2.1.1 Introducción a HTTP
2.1.2 Conexiones persistentes y no persistentes
2.1.3 Formato de los mensajes HTTP
2.1.4 Interacción usuario-servidor: cookies
2.1.5 Almacenamiento en caché web
2.1.6 GET condicional

2.2 Transferencia de archivos: FTP
2.2.1 Comandos y respuestas de FTP

2.3 Correo electrónico en Internet
2.3.1 SMTP
2.3.2 Comparación con HTTP
2.3.3 Formatos de los mensajes de correo
2.3.4 Protocolos de acceso para correo electrónico

2.4 DNS: servicio de directorio de Internet
2.4.1 Servicios proporcionados por DNS
2.4.2 Cómo funciona DNS

2.4.3 Registros y mensajes DNS

2.5 Seguridad en la capa de aplicación

Bloque 3: Seguridad en la capa de transporte

Carga de trabajo en créditos ECTS: 1,25

a. Contextualización y justificación

Esta capa gestiona los protocolos más usados para las comunicaciones síncronas y asíncronas en Internet; de ahí la importacia del estudio de la seguridad en este ámbito.

b. Objetivos de aprendizaje

- Entender los proceso de cifrado SSL.
- Manejarse con el entorno Openssl

c. Contenidos

3.1 Transporte sin conexión: UDP
3.1.1 Estructura de los segmentos UDP
3.1.2 Suma de comprobación de UDP

3.2 Transporte orientado a la conexión: TCP
3.2.1 La conexión TCP
3.2.2 Estructura del segmento TCP
3.2.3 Estimación del tiempo de ida y vuelta y fin de temporización
3.2.6 Gestión de la conexión TCP

3.3 Seguridad en el protocolo TCP: SSL

Bloque 4: Seguridad en la capa de red

Carga de trabajo en créditos ECTS: 1,25

a. Contextualización y justificación

Esta es la capa básica de conexión en red de Internet por lo que sus protocolos y los dispositivos que los implementan son de capital importancia para implantar seguridad a nivel de conexión de red.

b. Objetivos de aprendizaje

- Conocer los modelos de servicio de red
- Implementación de seguridad VPN
- Familiarizarse con el protocolo de red seguro IPSec

c. Contenidos

4. Protocolo de Internet (IP): reenvío y direccionamiento en Internet
4.1 Formato de los datagramas
4.2 Direccionamiento IPv4
4.3 Protocolo de mensajes de control de Internet (ICMP)
4.4 Seguridad en la capa de red: IPSec

Bloque 5: Seguridad en la capa de enlace y las redes de área local

Carga de trabajo en créditos ECTS: 1,3

a. Contextualización y justificación

No solo de Internet vive el hombre. También hemos de estudiar las redes locales y los protocolos con que se implementa la comunicación de hosts en las mismas y la integridad de los mensajes.

b. Objetivos de aprendizaje

- Conocer la capa de enlace de datos y los servicios de integridad de datos que presta
- Entender el funcionamiento básico de la corrección de errores en la transmisión de información
- Entender el funcionamiento de los dispositivos electrónicos que trabajan en este nivel.

c. Contenidos

5.1 Direccionamiento de la capa de enlace
5.1.1 Direcciones MAC
5.1.2 Protocolo de resolución de direcciones (ARP)

5.2 Ethernet
5.2.1 Estructura de la trama de-Ethernet
5.2.2 CSMA/CD: protocolo de acceso múltiple de Ethernet

5.3 Seguridad en la capa de enlace (Ethernet)

l. Bibliografía básica

Autor	Kurose, James F.
Título	**Redes de computadoras : un enfoque descendente / James F. Kurose, Keith W. Ross**
Publicac	Madrid [etc.] : Pearson, 2010
Edición	5th ed.
Descr. Física	XXV, 817 p. ; 24 cm
Nota	Bibliografía p. 767-792. Indices
Materia	Redes de ordenadores
ISBN	978-84-7829-119-9
Otro Autor	Ross, Keith W., coaut

II. Bibliografía complementaria

Autor	Tanenbaum, Andrew S.
Título	**Redes de computadoras / Andrew S. Tanenbaum**
Publicac	México [etc.] : Prentice-Hall, 2003
Edición	4ª ed.
Descr. Física	XX, 891 p. ; 24 cm
Nota	Bibliografía p. 848-868. Indices
Materia	Redes de ordenadores
ISBN	9702601622

III. Temporalización (por bloques temáticos)

BLOQUE TEMÁTICO	CARGA ECTS	PERIODO PREVISTO DE DESARROLLO
Bloque 1: Redes de computadoras e Internet. Principios de Criptografía	1	Teoría: semanas 1-2 Lab.: semanas 1-2 Expo o repaso.: semanas 14-15
Bloque 2: Seguridad en la capa de aplicación	1,2	Teoría: semanas 3-4 Lab.: semanas 3-5 Expo o repaso.: semanas 14-15
Bloque 3: Seguridad en la capa de transporte	1,25	Teoría: semanas 5-7 Lab.: semanas 6-9 Expo o repaso.: semanas 14-15
Bloque 4: Seguridad en la capa de red	1,25	Teoría: semanas 8-9 Lab.: semanas 10-12 Expo o repaso.: semanas 14-15
Bloque 5: Seguridad en la capa de enlace y las redes de área local	1,3	Teoría: semanas 10-13 Lab.: semanas 12-15 Expo o repaso.: semanas 14-15

IV. Tabla resumen de los instrumentos, procedimientos y sistemas de evaluación/calificación

INSTRUMENTO/PROCEDIMIENTO	PESO EN LA NOTA FINAL	OBSERVACIONES
1. Examen escrito sobre los contenidos teóricos con cuestiones cortas y problemas	60%	Se realizará un examen para evaluar los conocimientos de la parte teórica de los alumnos. A este examen deberán acudir todos los alumnos y abarcará todos los contenidos vistos en la parte teórica de la asignatura.
2. Prácticas de laboratorio	40%	Se realizará un examen para evaluar los conocimientos de la parte práctica de los alumnos. A este examen deberán acudir todos los alumnos y abarcará todos los contenidos vistos en la parte de laboratorio de la asignatura.

Otros comentarios y segunda convocatoria

En principio se entiende que todos los alumnos siguen la asignatura de forma presencial. Si un alumno desea cursar la asignatura de forma no presencial deberá comunicarlo al profesor al inicio del semestre. En ese caso:

- Los alumnos no tienen obligación de asistir a prácticas. La evaluación de las mismas se realizará por medio de un examen escrito que, en su caso, se podrá hacer el mismo día que la prueba sobre los contenidos teóricos.

V. Consideraciones finales

Todos los recursos docentes de la asignatura estarán disponibles en el Aula Virtual de la E. I. de Informática. http://campusvirtual2015.uva.es/