

ANX-PR/CL/001-01
GUÍA DE APRENDIZAJE

ASIGNATURA

Seguridad en sistemas y redes

CURSO ACADÉMICO - SEMESTRE

2016-17 - Segundo semestre

Datos Descriptivos

Nombre de la Asignatura	Seguridad en sistemas y redes
Titulación	61AC - Master Universitario en Software de Sistemas Distribuidos y Empotrados
Centro responsable de la titulación	Escuela Técnica Superior de Ingeniería de Sistemas Informáticos
Semestre/s de impartición	Segundo semestre
Materias	Seguridad en sistemas y redes
Carácter	Obligatoria
Código UPM	613000046
Nombre en inglés	Seguridad en sistemas y redes

Datos Generales

Créditos	6	Curso	1
Curso Académico	2016-17	Período de impartición	Febrero-Junio
Idioma de impartición	Castellano	Otros idiomas de impartición	

Requisitos Previos Obligatorios

Asignaturas Previas Requeridas

El plan de estudios Master Universitario en Software de Sistemas Distribuidos y Empotrados no tiene definidas asignaturas previas superadas para esta asignatura.

Otros Requisitos

El plan de estudios Master Universitario en Software de Sistemas Distribuidos y Empotrados no tiene definidos otros requisitos para esta asignatura.

Conocimientos Previos

Asignaturas Previas Recomendadas

Servicios y protocolos de aplicaciones en internet

Redes inalámbricas

Otros Conocimientos Previos Recomendados

Conocimientos de redes en sentido amplio

Conocimientos de criptografía anivel de usuario

Competencias

CG5 - Gestión de la información.

CG9 - Capacidad de análisis y síntesis.

Resultados de Aprendizaje

RA84 - Aplicar técnicas, principios y métodos para identificar información relevante y sintetizarla de manera autónoma, flexible, efectiva y con criterio

RA6 - Genera y crea todas las estructuras de una PKI.

RA12 - Comprende las características de seguridad de un sistema cortafuegos.

RA10 - Audita, con criterios de seguridad, redes WIFI.

RA7 - Configura adecuadamente servidores web seguros con soporte de cifrado con el protocolo SSL/TLS.

RA11 - Comprende, instala y configura mecanismos de seguridad en dispositivos móviles.

RA13 - Diseña un sistema de defensa de barrera, incorporando herramientas de detección de intrusos.

RA8 - Comprende los mecanismos de seguridad en redes WIFI.

RA78 - RAG5 -Saber buscar la documentación necesaria y la normativa. Elabora la información y la publica adecuadamente.

RA17 - Conoce y aplica las técnicas de defensa frente a ataques hacking.

RA9 - Dimensiona y configura adecuadamente el sistema de seguridad de una red WIFI.

RA14 - Instala y configura adecuadamente sistemas complejos cortafuegos. Ejemplo pfSense

RA15 - Configura y dimensiona redes privadas virtuales.

RA5 - Entiende y aplica los diferentes sistemas de cifrado.

RA16 - Establece la mejor solución para un diseño de sistemas de túneles para interconectar usuarios o redes.

RA18 - Audita redes desde el punto de vista de la defensa y seguridad frente ataques, tanto internos como externos.

Profesorado

Profesorado

Nombre	Despacho	e-mail	Tutorías
Calzada Del Fresno, Daniel (Coordinador/a)	4303	daniel.calzada@upm.es	M - 10:00 - 13:00 X - 10:00 - 13:00

Nota.- Las horas de tutoría son orientativas y pueden sufrir modificaciones. Se deberá confirmar los horarios de tutorías con el profesorado.

Descripción de la Asignatura

La asignatura Seguridad en Sistemas y Redes está encuadrada en el núcleo del máster de Software de Sistemas Distribuidos y Empotrados. En esta asignatura se adquieren los conocimientos tópicos de la seguridad en redes y sistemas, en sentido amplio, con adaptación a la parte de seguridad en dispositivos móviles. La asignatura empieza con una introducción a la criptografía aplicada haciendo incidencia en certificados digitales, y PKI's. Después se estudian los protocolos de comunicaciones seguros y sus aplicaciones en las comunicaciones e Internet. En cuanto a la parte clásica de seguridad se estudian los sistemas de protección de barrera, filtros de paquetes, cortafuegos y sus topologías y sistemas de detección y prevención de intrusiones. La interconexión segura de redes queda cubierta con el estudio de las redes privadas virtuales. El hacking y la defensa contra ataques forman la parte final del programa. Es parte importante la seguridad en dispositivos móviles, haciendo fuerte incidencia en la seguridad en redes wifi, en modo infraestructura y adhoc y también en las comunicaciones por bluetooth.

Temario

1. Criptografía Aplicada. Protocolo TLS.
 - 1.1. Funciones HASH. Funciones HMAC.
 - 1.2. Criptografía básica. Simétrica. Asimétrica.
 - 1.3. Certificados digitales. tipos. Formatos.
 - 1.4. Autoridades de certificación.
 - 1.5. Firma digital.
 - 1.6. Cifrado de las comunicaciones. Protocolos de cifrado.
 - 1.7. TLS y SSL en Internet. aplicación para el WEB.
 - 1.8. Autenticación del servidor web. Autenticación del cliente web.
2. Seguridad en Redes WIFI y dispositivos Móviles
 - 2.1. Seguridad en redes wireless: Autenticación y confidencialidad.
 - 2.2. Asociación abierta. Asociación con WEP.
 - 2.3. Portal cautivo.
 - 2.4. WEP. Ataques al WEP.
 - 2.5. 802.11i. Fase 1. Acuerdo de política de seguridad.
 - 2.6. 802.11i. Fase 2. Autenticación.
 - 2.7. 802.11i. Fase 3. Derivación y distribución de clave. Four Way Handshake.
 - 2.8. 802.11i. Fase 4. Confidencialidad e integridad de datos. RSNA. Cifrado con TKIP. Cifrado con CCMP (AES modo contador).
 - 2.9. Definiciones de WPA. WPA_PSK. WPA2. WPA^_PSK.
 - 2.10. Seguridad en redes AD-HOC.
 - 2.11. Seguridad en Bluetooth: especificación, protocolos, conexión.
 - 2.12. Seguridad en dispositivos móviles: Debilidades inherentes a la tecnología.
 - 2.13. Seguridad en dispositivos móviles: Seguridad en las comunicaciones. Seguridad en las aplicaciones.

3. Seguridad en la Red y en el acceso. Cortafuegos y topologías.
 - 3.1. Filtros de paquetes de datos.
 - 3.2. Filtros de aplicación. Proxys. Filtros de kernel.
 - 3.3. Ejemplos de proxys, ejemplos de filtros de kernel: iptables.
 - 3.4. Cortafuegos. topologías de cortafuegos.
 - 3.5. Dual homed host. Screened Subnet. Backbone.
 - 3.6. Sistemas de detección de intrusos. IDS'S
 - 3.7. Sistemas de Prevención de intrusos. IPS'S
 - 3.8. Casos de uso: Dispositivos cortafuegos con pfSense
 - 3.9. Gestores de información de seguridad en redes. ejemplo: OSSIM.
4. Túneles y redes privadas virtuales
 - 4.1. Túneles. Concepto. Tipos: transporte y red.
 - 4.2. Túneles sobre SSH, Túneles sobre http.
 - 4.3. Túneles de red.
 - 4.4. IPsec. Protocolos AH y ESP. Modos transporte y tunel.
 - 4.5. OpenVPN
 - 4.6. Casos de uso: instalación de túneles sobre openVPN
5. Hacking y prevención de ataques
 - 5.1. Concepto de hacking. Método para hackear un sistema.
 - 5.2. Sniffers y Scanners de red. Sniffers especiales.
 - 5.3. Detección del sistema operativo.
 - 5.4. Ataques DoS (Denied of Service)
 - 5.5. Hacking de linux. Exploits. Telnet inverso. Desbordamiento de buffers.
 - 5.6. Hijacking de sesión.
 - 5.7. Redirección ARP. Redirección de puertos TCP.
 - 5.8. Rootkits. Defensa.
 - 5.9. Defensa y prevención de ataques en máquinas.

Cronograma

Horas totales: 60 horas

Horas presenciales: 60 horas (38.5%)

Peso total de actividades de evaluación continua:
100%

Peso total de actividades de evaluación sólo prueba final:
100%

Semana	Actividad Presencial en Aula	Actividad Presencial en Laboratorio	Otra Actividad Presencial	Actividades Evaluación
Semana 1	Exposición de conceptos teóricos y/o casos prácticos Duración: 02:00 LM: Actividad del tipo Lección Magistral	Realización de actividades prácticas. Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio	Resolución de supuestos prácticos Duración: 03:00 PL: Actividad del tipo Prácticas de Laboratorio	Resolución de configuraciones, puesta en funcionamiento y pruebas. (RA5, RA6, RA7, RA84) Duración: 03:00 TI: Técnica del tipo Trabajo Individual Evaluación continua Actividad presencial
Semana 2	Exposición de conceptos teóricos y/o casos prácticos Duración: 02:00 LM: Actividad del tipo Lección Magistral	Realización de actividades prácticas. Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio	Resolución de supuestos prácticos Duración: 03:00 PL: Actividad del tipo Prácticas de Laboratorio	Resolución de configuraciones, puesta en funcionamiento y pruebas. (RA8, RA9, RA10, RA11, RG5, RA78, RA84) Duración: 03:00 TI: Técnica del tipo Trabajo Individual Evaluación continua Actividad presencial
Semana 3	Exposición de conceptos teóricos y/o casos prácticos Duración: 02:00 LM: Actividad del tipo Lección Magistral	Realización de actividades prácticas. Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio	Resolución de supuestos prácticos Duración: 03:00 PL: Actividad del tipo Prácticas de Laboratorio	Resolución de configuraciones, puesta en funcionamiento y pruebas. (RA12, RA13, RA14, RA78, RA84) Duración: 03:00 TI: Técnica del tipo Trabajo Individual Evaluación continua Actividad presencial
Semana 4	Exposición de conceptos teóricos y/o casos prácticos Duración: 02:00 LM: Actividad del tipo Lección Magistral	Realización de actividades prácticas. Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio	Resolución de supuestos prácticos Duración: 03:00 PL: Actividad del tipo Prácticas de Laboratorio	Resolución de configuraciones, puesta en funcionamiento y pruebas. (RA15, RA16, RA78, RA84) Duración: 03:00 TI: Técnica del tipo Trabajo Individual Evaluación continua Actividad presencial
Semana 5	Exposición de conceptos teóricos y/o casos prácticos Duración: 02:00 LM: Actividad del tipo Lección Magistral	Realización de actividades prácticas. Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio	Resolución de supuestos prácticos Duración: 03:00 PL: Actividad del tipo Prácticas de Laboratorio	Resolución de configuraciones, puesta en funcionamiento y pruebas. (RA7, RA17, RA18, RA78, RA84) Duración: 03:00 TI: Técnica del tipo Trabajo Individual Evaluación continua Actividad presencial
Semana 6	Exposición de conceptos teóricos y/o casos prácticos Duración: 02:00 LM: Actividad del tipo Lección Magistral	Realización de actividades prácticas. Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio	Resolución de supuestos prácticos Duración: 03:00 PL: Actividad del tipo Prácticas de Laboratorio	Resolución de configuraciones, puesta en funcionamiento y pruebas. (RA17, RA18, RA78, RA84) Duración: 03:00 TI: Técnica del tipo Trabajo Individual Evaluación continua Actividad presencial

Semana 7				<p>Prueba de evaluación final por examen escrito. (RA5, RA6, RA7, RA8, RA9, RA10, RA11, RA12, RA13, RA14, RA15, RA16, RA17, RA18, RA78, RA84)</p> <p>Duración: 02:00</p> <p>EX: Técnica del tipo Examen Escrito</p> <p>Evaluación sólo prueba final</p> <p>Actividad presencial</p> <p>Prueba de evaluación final ejercicios prácticos. (RA5, RA6, RA7, RA8, RA9, RA10, RA78, RA84)</p> <p>Duración: 03:00</p> <p>EP: Técnica del tipo Examen de Prácticas</p> <p>Evaluación sólo prueba final</p> <p>Actividad presencial</p> <p>Prueba de evaluación final ejercicios prácticos. (RA11, RA12, RA13, RA14, RA15, RA16, RA17, RA18, RA78, RA84)</p> <p>Duración: 05:00</p> <p>EP: Técnica del tipo Examen de Prácticas</p> <p>Evaluación sólo prueba final</p> <p>Actividad presencial</p>
Semana 8				
Semana 9				
Semana 10				
Semana 11				
Semana 12				
Semana 13				
Semana 14				
Semana 15				
Semana 16				
Semana 17				

Nota.- El cronograma sigue una planificación teórica de la asignatura que puede sufrir modificaciones durante el curso.

Nota 2.- Para poder calcular correctamente la dedicación de un alumno, la duración de las actividades que se repiten en el tiempo (por ejemplo, subgrupos de prácticas") únicamente se indican la primera vez que se definen.

Actividades de Evaluación

Semana	Descripción	Duración	Tipo evaluación	Técnica evaluativa	Presencial	Peso	Nota mínima	Competencias evaluadas
1	Resolución de configuraciones, puesta en funcionamiento y pruebas. (RA5, RA6, RA78, RA84)	03:00	Evaluación continua	TI: Técnica del tipo Trabajo Individual	Sí	15%	5 / 10	CG5, CG9
2	Resolución de configuraciones, puesta en funcionamiento y pruebas. (RA8, RA9, RA10, RA11, RG5, RA78, RA84)	03:00	Evaluación continua	TI: Técnica del tipo Trabajo Individual	Sí	18%	5 / 10	CG5, CG9
3	Resolución de configuraciones, puesta en funcionamiento y pruebas. (RA12, RA13, RA14, RA78, RA84)	03:00	Evaluación continua	TI: Técnica del tipo Trabajo Individual	Sí	18%	5 / 10	CG5, CG9
4	Resolución de configuraciones, puesta en funcionamiento y pruebas. (RA15, RA16, RA78, RA84)	03:00	Evaluación continua	TI: Técnica del tipo Trabajo Individual	Sí	18%	5 / 10	CG5, CG9
5	Resolución de configuraciones, puesta en funcionamiento y pruebas. (RA7, RA17, RA18, RA78, RA84)	03:00	Evaluación continua	TI: Técnica del tipo Trabajo Individual	Sí	16%	5 / 10	CG5, CG9
6	Resolución de configuraciones, puesta en funcionamiento y pruebas. (RA17, RA18, RA78, RA84)	03:00	Evaluación continua	TI: Técnica del tipo Trabajo Individual	Sí	15%	5 / 10	CG5, CG9
7	Prueba de evaluación final por examen escrito. (RA5, RA6, RA7, RA8, RA9, RA10, RA11, RA12, RA13, RA14, RA15, RA16, RA17, RA18, RA78, RA84)	02:00	Evaluación sólo prueba final	EX: Técnica del tipo Examen Escrito	Sí	30%	5 / 10	CG5, CG9
7	Prueba de evaluación final ejercicios prácticos. (RA5, RA6, RA7, RA8, RA9, RA10, RA78, RA84)	03:00	Evaluación sólo prueba final	EP: Técnica del tipo Examen de Prácticas	Sí	30%	5 / 10	CG5, CG9
7	Prueba de evaluación final ejercicios prácticos. (RA11, RA12, RA13, RA14, RA15, RA16, RA17, RA18, RA78, RA84)	05:00	Evaluación sólo prueba final	EP: Técnica del tipo Examen de Prácticas	Sí	40%	5 / 10	CG5, CG9

Criterios de Evaluación

EVALUACIÓN CONTINUA:

La calificación final corresponderá a la suma de las calificaciones obtenidas por el alumno en la realización de los cuestionarios y todas y cada una de las tareas a realizar en cada tema. Para que la evaluación sea continua hay que cumplir los siguientes requisitos:

Haber entregado en tiempo y forma el 98% de las tareas y cuestionarios propuestos.

En caso contrario el alumno deberá realizar un examen final teórico-práctico que incluirá todos los contenidos de la asignatura. El examen se realizará en la siguiente convocatoria, a aquella en la que ha seguido la evaluación continua.

EVALUACIÓN mediante SOLO EXAMEN FINAL:

Los alumnos que deseen ser evaluados SOLO mediante examen final y no seguir la evaluación continua, deberán solicitarlo, por escrito, antes de que finalice la segunda semana de clase. Una vez finalizado el plazo no se admitirán peticiones excepto por motivos de enfermedad y justificada con certificado médico.

El examen final consistirá en una prueba tipo examen escrito sobre los contenidos teóricos de la asignatura (2 horas) y una prueba sobre los contenidos y realización práctica de las prácticas, cuestionarios y demás tareas de la asignatura (Se realizará en dos sesiones de 3 horas la primera y 4 horas la segunda). Cada prueba se calificará sobre 10 puntos siendo necesario

obtener una nota igual o superior a 5 en cada una para superar la asignatura. La calificación final será la nota media de las calificaciones obtenidas en la prueba teórica, la primera sesión práctica y la segunda sesión práctica.

Recursos Didácticos

Descripción	Tipo	Observaciones
Bibliografía	Bibliografía	Colección de diapositivas realizadas por el profesor para cada tema.
Recursos web	Recursos web	Plataforma moodle de la asignatura
Equipamiento	Equipamiento	Software de libre distribución aplicable al contenido de la asignatura: Dsitribución Kali Linux.Distribución pfSense.
Aula	Otros	Aula equipada con ordenador proyector de video y pizarra.
Laboratorio	Equipamiento	Laboratorio con ordenadores con software adecuado para la realización de las prácticas. Plataforma PKI. Plataforma servidora RADIUS. Routes WIFI.
Articulos1	Bibliografía	Artículos de la revista haking9, especificados en el moodle de la asignatura.
Artículos2	Bibliografía	FAQ'S de criptografía Especificacion TLS Tutorial de manejo de OpenSSL
Norma IEEE802.11i	Bibliografía	Norma IEEE802.11i
Página web de netfilter	Bibliografía	Descripción del funcionamiento del netfilter de linux
Documentación IPSec	Bibliografía	Página wen IPSec, especificación de la norma.
Página web de OpenVPN	Bibliografía	Página web de OpenVPN.
Herramientas hacking	Bibliografía	Página de dsniff Página de knockd Herramientas DOS Lista de fuzzers

Otra Información

La competencia transversal CG5 (Gestión de la Información), se evalúa en base a los resultados de análisis de documentación y la síntesis de conceptos presente en la normativa, que debe realizar el alumno al realizar las instalaciones y las configuraciones de servicios seguros.

La competencia CG9 (Capacidad de Análisis y Síntesis) se evalúa en base a la habilidad del alumno para integrar conocimientos de diferentes partes de la asignatura para resolver problemas de instalación configuración y aseguramiento de sistemas y servicios.