ANX-PR/CL/001-01
GUÍA DE APRENDIZAJE

ASIGNATURA

613000046 - Seguridad en sistemas y redes

PLAN DE ESTUDIOS

61AC - Master Universitario En Software De Sistemas Distribuidos Y Empotrados

CURSO ACADÉMICO Y SEMESTRE

2018/19 - Segundo semestre

Índice

Guía de Aprendizaje

1. Datos descriptivos

1.1. Datos de la asignatura

Nombre de la asignatura	613000046 - Seguridad en sistemas y redes
No de créditos	6 ECTS
Carácter	Obligatoria
Curso	Primer curso
Semestre	Segundo semestre
Período de impartición	Febrero-Junio
Idioma de impartición	Castellano
Titulación	61AC - Master universitario en software de sistemas distribuidos y empotrados
Centro responsable de la titulación	61 - Escuela Tecnica Superior de Ingenieria de Sistemas Informaticos
Curso académico	2018-19

2. Profesorado

2.1. Profesorado implicado en la docencia

Nombre	Despacho	Correo electrónico	Horario de tutorías *
Jesus Sanchez Lopez (Coordinador/a)		jesus.sanchezl@upm.es	- -
Eduardo Garcia Pardo	4305	eduardo.pardo@upm.es	Sin horario. El horario de tutorías se publicará en la web de la ETSISI al comienzo del cuatrimestre

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

3. Conocimientos previos recomendados

3.1. Asignaturas previas que se recomienda haber cursado

- Servicios y protocolos de aplicaciones en internet

- Redes inalambricas

3.2. Otros conocimientos previos recomendados para cursar la asignatura

- Conocimientos de criptografía anivel de usuario

- Conocimientos de redes en sentido amplio

4. Competencias y resultados de aprendizaje

4.1. Competencias

CG5 - Gestión de la información.

CG9 - Capacidad de análisis y síntesis.

4.2. Resultados del aprendizaje

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.

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

RA15 - Configura y dimensiona redes privadas virtuales.

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.

5. Descripción de la asignatura y temario

5.1. 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 su 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 tambien en las comunicaciones por bluetooth.

5.2. Temario de la asignatura

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. Autentificación del servidor web. Autentificación del cliente web.
2. Seguridad en Redes WIFI y dispositivos Móviles
    2.1. Seguridad en redes wireless: Autentificación 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. Autentificación.

2.7. 802.11i. Fase 3. Derivación y distribución de clave. Four Way Handsake.

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 accesso. 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 intrusoss. 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. Caos de uso: instalación de túneles obre 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. Telner 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.

6. Cronograma

6.1. Cronograma de la asignatura *

Sem	Actividad presencial en aula	Actividad presencial en laboratorio	Otra actividad presencial	Actividades de evaluación
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. RA78, RA84)** TI: Técnica del tipo Trabajo Individual Evaluación continua Duración: 03:00
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)** TI: Técnica del tipo Trabajo Individual Evaluación continua Duración: 03:00
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)** TI: Técnica del tipo Trabajo Individual Evaluación continua Duración: 03:00
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)** TI: Técnica del tipo Trabajo Individual Evaluación continua Duración: 03:00
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)** TI: Técnica del tipo Trabajo Individual Evaluación continua Duración: 03:00
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)** TI: Técnica del tipo Trabajo Individual Evaluación continua Duración: 03:00
7				**Prueba de evaluación final por examen escrito. (RA5, RA6, RA7, RA8, RA9, RA10, RA11, RA12, RA13,RA14,RA15,RA16,RA17, RA18, RA78, RA84)** EX: Técnica del tipo Examen Escrito Evaluación sólo prueba final Duración: 02:00 **Prueba de evaluación final ejercicios prácticos. (RA5, RA6, RA7, RA8, RA9, RA10, RA78, RA84)** EP: Técnica del tipo Examen de Prácticas Evaluación sólo prueba final

				Duración: 03:00 **Prueba de evaluación final ejercicios prácticos. (RA11, RA12, RA13, RA14, RA15, RA16, RA17, RA18, RA78, RA84)** EP: Técnica del tipo Examen de Prácticas Evaluación sólo prueba final Duración: 05:00
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				

Las horas de actividades formativas no presenciales son aquellas que el estudiante debe dedicar al estudio o al trabajo personal.

Para el cálculo de los valores totales, se estima que por cada crédito ECTS el alumno dedicará dependiendo del plan de estudios, entre 26 y 27 horas de trabajo presencial y no presencial.

* El cronograma sigue una planificación teórica de la asignatura y puede sufrir modificaciones durante el curso.

7. Actividades y criterios de evaluación

7.1. Actividades de evaluación de la asignatura

7.1.1. Evaluación continua

Sem.	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
1	Resolución de configuraciones, puesta en funcionamiento y pruebas. (RA5, RA6. RA78, RA84)	TI: Técnica del tipo Trabajo Individual	Presencial	03:00	15%	5 / 10	CG5 CG9
2	Resolución de configuraciones, puesta en funcionamiento y pruebas. (RA8, RA9, RA10, RA11, RG5, RA78, RA84)	TI: Técnica del tipo Trabajo Individual	Presencial	03:00	18%	5 / 10	CG5 CG9
3	Resolución de configuraciones, puesta en funcionamiento y pruebas. (RA12, RA13, RA14, RA78, RA84)	TI: Técnica del tipo Trabajo Individual	Presencial	03:00	18%	5 / 10	CG5 CG9
4	Resolución de configuraciones, puesta en funcionamiento y pruebas. (RA15, RA16, RA78, RA84)	TI: Técnica del tipo Trabajo Individual	Presencial	03:00	18%	5 / 10	CG5 CG9
5	Resolución de configuraciones, puesta en funcionamiento y pruebas. (RA7, RA17, RA18, RA78, RA84)	TI: Técnica del tipo Trabajo Individual	Presencial	03:00	16%	5 / 10	CG5 CG9
6	Resolución de configuraciones, puesta en funcionamiento y pruebas. (RA17, RA18, RA78, RA84)	TI: Técnica del tipo Trabajo Individual	Presencial	03:00	15%	5 / 10	CG5 CG9

7.1.2. Evaluación sólo prueba final

Sem	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
7	Prueba de evaluación final por examen escrito. (RA5, RA6, RA7, RA8, RA9, RA10, RA11, RA12, RA13,RA14,RA15,RA16,RA17, RA18, RA78, RA84)	EX: Técnica del tipo Examen Escrito	Presencial	02:00	30%	5 / 10	CG5 CG9

7	Prueba de evaluación final ejercicios prácticos. (RA5, RA6, RA7, RA8, RA9, RA10, RA78, RA84)	EP: Técnica del tipo Examen de Prácticas	Presencial	03:00	30%	5 / 10	CG5 CG9
7	Prueba de evaluación final ejercicios prácticos. (RA11, RA12, RA13, RA14, RA15, RA16, RA17, RA18, RA78, RA84)	EP: Técnica del tipo Examen de Prácticas	Presencial	05:00	40%	5 / 10	CG5 CG9

7.1.3. Evaluación convocatoria extraordinaria

No se ha definido la evaluación extraordinaria.

7.2. Criterios de evaluación

EVALUACIÓN CONTÍNUA:

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 100% de las tareas y cuestionarios propuestos.

No haber tenido ninguna falta de asistencia las clases presenciales.

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 finalize 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 2 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.

8. Recursos didácticos

8.1. Recursos didácticos de la asignatura

Nombre	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

9. Otra información

9.1. Otra información sobre la asignatura

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 (Capácidad 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.