17-18

GRADO EN INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN
TERCER CURSO

GUÍA DE ESTUDIO PÚBLICA

PROCESOS Y HERRAMIENTAS DE GESTIÓN DE LA SEGURIDAD DE REDES

CÓDIGO 71023074

UNED

17-18

PROCESOS Y HERRAMIENTAS DE GESTIÓN DE LA SEGURIDAD DE REDES

CÓDIGO 71023074

ÍNDICE

Nombre de la asignatura	PROCESOS Y HERRAMIENTAS DE GESTIÓN DE LA SEGURIDAD DE REDES
Código	71023074
Curso académico	2017/2018
Departamento	SISTEMAS DE COMUNICACIÓN Y CONTROL, INGENIERÍA ELÉCTRICA, ELECTRÓNICA, CONTROL, TELEMÁTICA Y QUÍMICA APLICADA A LA INGENIERÍA
Título en que se imparte	GRADO EN INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN
Curso	TERCER CURSO
Tipo	OBLIGATORIAS
Nº ETCS	6
Horas	150.0
Periodo	SEMESTRE 2
Idiomas en que se imparte	CASTELLANO

PRESENTACIÓN Y CONTEXTUALIZACIÓN

Esta guía presenta las orientaciones básicas que requiere el alumno para el estudio de la asignatura Procesos y Herramientas de Gestión de la Seguridad de Redes. Por esta razón es muy recomendable leer con atención esta guía antes de iniciar el estudio, para adquirir una idea general de la asignatura y de los trabajos, actividades y prácticas que se van a desarrollar a lo largo del curso.

Procesos y Herramientas de Gestión de la Seguridad de Redes es una asignatura de seis créditos ECTS de carácter obligatorio que se imparte en el segundo semestre del tercer curso de la carrera en la titulación de Grado en Ingeniería en Tecnologías de la Información. Esta asignatura inicia el contacto del alumno con el mundo real de la seguridad informática de sistemas, datos y comunicaciones.

El objetivo esencial de la asignatura es adquirir los conocimientos asociados a todos los aspectos del problema de la seguridad en sistemas y redes de ordenadores, orientándolos a la consecución de la creación de una política de seguridad informática general y, en particular, de la de las redes de una organización. En ese sentido, se analizan los problemas de seguridad física y lógica asociados con los componentes hardware (cableado, repetidores, encaminadores, etc.) así como software (sistemas operativos, aplicaciones y protocolos). Se estudian los distintos tipos de ataques por la red, haciendo una taxonomía lo más exhaustiva posible, así como los distintos tipos de defensas posibles. Se estudian las distintas herramientas de defensa habituales como cortafuegos, analizadores de vulnerabilidades, sistemas de detección de intrusiones, analizadores de protocolos y otros. Se hace especial énfasis en las aplicaciones de la criptografía al problema de la seguridad informática en las comunicaciones, empezando por una aproximación básica, siguiendo con la clasificación de los distintos tipos de algoritmos criptográficos, su aplicación en protocolos (incluyendo los de redes inalámbricas) y aplicaciones de uso habitual (y experimental) hoy en día, y finalizando con una discusión de cómo todo lo anteriormente expuesto se está utilizando para construir lo que llamamos redes privadas virtuales.

Esta asignatura requiere de los conocimientos y competencias adquiridas en materias de segundo curso, concretamente en las asignaturas de Sistemas Operativos y Redes y Comunicaciones.

El nivel de conocimientos alcanzado de la materia está entre bajo y medio, un nivel considerado suficiente para poder integrar con éxito la seguridad informática de las redes como un criterio más, y esencial, en cualquier proyecto de ingeniería informática.

REQUISITOS Y/O RECOMENDACIONES PARA CURSAR LA ASIGNATURA

Como se ha descrito previamente, esta asignatura, que inicia el estudio de una nueva materia, se apoya fuertemente en los conocimientos y competencias adquiridos en asignaturas de segundo curso. Sin esta base de conocimientos la asignatura presentará un nivel alto de dificultad al alumno que la aborde por primera vez.

EQUIPO DOCENTE

Nombre y Apellidos	GABRIEL DIAZ ORUETA
Correo Electrónico	gdiaz@ieec.uned.es
Teléfono	91398-8255
Facultad	ESCUELA TÉCN.SUP INGENIEROS INDUSTRIALES
Departamento	ING.ELÉCT., ELECTRÓN., CONTROL, TELEMÁT.

Nombre y Apellidos	ELIO SAN CRISTOBAL RUIZ
Correo Electrónico	elio@ieec.uned.es
Teléfono	91398-7769
Facultad	ESCUELA TÉCN.SUP INGENIEROS INDUSTRIALES
Departamento	ING.ELÉCT., ELECTRÓN., CONTROL, TELEMÁT.

Nombre y Apellidos	MANUEL ALONSO CASTRO GIL
Correo Electrónico	mcastro@ieec.uned.es
Teléfono	91398-6476
Facultad	ESCUELA TÉCN.SUP INGENIEROS INDUSTRIALES
Departamento	ING.ELÉCT., ELECTRÓN., CONTROL, TELEMÁT.

Nombre y Apellidos	ROBERTO HERNANDEZ BERLINCHES
Correo Electrónico	roberto@scc.uned.es
Teléfono	91398-7196
Facultad	ESCUELA TÉCN.SUP INGENIERÍA INFORMÁTICA
Departamento	SISTEMAS DE COMUNICACIÓN Y CONTROL

HORARIO DE ATENCIÓN AL ESTUDIANTE

La enseñanza a distancia utilizada para el seguimiento de esta asignatura, que garantiza la ayuda al alumno, dispone de los siguientes recursos:

1. **Tutores** virtuales. Los tutores serán los encargados del seguimiento y control de las pruebas que constituyen la evaluación continua del alumno.
2. **Entorno Virtual**. A través de CiberUNED el equipo docente de la asignatura pondrá a disposición de los alumnos diverso material de apoyo al estudio, así como el enunciado del trabajo de prácticas. Se dispone además de foros donde los alumnos podrán plantear sus dudas para que sean respondidas por los tutores o por el propio equipo docente. Es el

SOPORTE FUNDAMENTAL de la asignatura, y supone la principal herramienta de comunicación entre el equipo docente, los tutores y los alumnos, así como de los alumnos entre sí.

3. **Tutorías con el equipo docente**: los martes de 14:00 a 18:00 h para el periodo durante el que se desarrolla la asignatura, en los teléfonos 913988255 o 913989381 , o presencialmente. También en cualquier momento del curso en el entorno CiberUNED.

TUTORIZACIÓN EN CENTROS ASOCIADOS

COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE

- Competencias cognitivas superiores: selección y manejo adecuado de conocimientos, recursos y estrategias cognitivas de nivel superior apropiados para el afrontamiento y resolución de d diversos tipos de tareas/problemas con distinto nivel de complejidad y novedad: Análisis y Síntesis.
- Aplicación de los conocimientos a la práctica Resolución de problemas en entornos nuevos o poco conocidos. Pensamiento creativo. Razonamiento crítico. Toma de decisiones
- Capacidad para diseñar, desarrollar, seleccionar y evaluar, aplicaciones y sistemas informáticos, asegurando su fiabilidad, seguridad y calidad, conforme a los principios éticos y a la legislación y normativa vigente.
- Capacidad para planificar, implantar, dirigir y peritar proyectos, servicios y sistemas informáticos en todos los ámbitos, liderando su puesta en marcha y mejora continua y valorando su impacto económico y social.
- Capacidad para comprender el entorno de una organización y sus necesidades en el ámbito de las tecnologías de la información y las comunicaciones
- Capacidad de comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos
- Capacidad para determinar los requisitos de los sistemas de información y comunicación de una organización atendiendo a aspectos de seguridad y cumplimiento de la normativa y la legislación vigente

RESULTADOS DE APRENDIZAJE

El objetivo básico de la asignatura Procesos y Herramientas de Gestión de la Seguridad de Redes es dar una visión completa y clara de los fundamentos básicos de la seguridad informática aplicada a redes y sistemas. Como resultado del estudio y aprendizaje de los contenidos de esta asignatura el estudiante será capaz de:

- Comprender la trascendencia de introducir (o no) la seguridad como un criterio de diseño en cualquier sistema o aplicación informática.
- Comprender los problemas más habituales actuales que implica la falta de seguridad en sistemas, aplicaciones y redes
- Clasificar los diferentes ataques a la seguridad de redes, desde el punto de vista de

peligrosidad, organización y necesidad de recursos.
- Entender, y saber implantar, las defensas básicas en sistemas operativos, aplicaciones y dispositivos de comunicaciones.
- Comprender la necesidad de la puesta en marcha de una política de seguridad informática en cualquier organización.
- Entender la trascendencia para las organizaciones de una correcta implementación de la LOPD (Ley Orgánica de Protección de Datos).
- Aplicar los conceptos más elementales aprendidos, relacionados con la seguridad en redes, sistemas y datos, a una organización concreta.
- Comprender las diferencias de conceptos, seguridad y complejidad entre los diferentes tipos de cortafuegos.
- Implantar una seguridad básica en cortafuegos de tipo filtro de paquetes.
- Comprender qué son los analizadores de vulnerabilidades de seguridad y cómo se usan.
- Comprender qué son las herramientas de scanning de seguridad y cómo se usan.
- Usar las características básicas de una herramienta de scanning como nmap.
- Comprender qué son los sistemas de detección de intrusiones (IDS) y qué papel juegan en una política de seguridad.
- Usar las características básicas de un IDS como snort.
- Comprender, y ser capaz de explicar, las diferencias entre las principales familias de algoritmos criptográficos.
- Decidir qué tipo de algoritmo criptográfico usar para las distintas necesidades de seguridad en redes: privacidad, integridad y autenticación.
- Comprender el funcionamiento básico interno de protocolos criptográficos como IPSec, SSL o PGP.
- Hacer una configuración básica de una infraestructura de clave pública.
- Explicar las ventajas e inconvenientes del uso de certificados X.509 y de sistemas basados en firma digital.
- Comprender el funcionamiento básico de las diferentes tipos de redes privadas virtuales.
- Entender los problemas asociados con la inseguridad de las redes inalámbricas.
- Entender las diferencias entre los distintos protocolos criptográficos usados en redes inalámbricas: WEP, WPA y WPA-2.

CONTENIDOS

TEMA 1. Descripción del problema de la seguridad en las comunicaciones y en la información

TEMA 2.- Seguridad en los elementos físicos existentes en una red

TEMA 3.- Seguridad en los elementos software existentes en una red

TEMA 4.- Métodos de ataque a equipos y redes

TEMA 5.- Defensas básicas ante ataques

TEMA 6.- La política de seguridad como respuesta razonable a los problemas de seguridad en redes

TEMA 7.- Métodos no criptográficos en la implantación de la política de seguridad

TEMA 8.- Los cortafuegos y sus aplicaciones

TEMA 9.- Tecnologías de última generación en cortafuegos

TEMA 10.- Herramientas de análisis de vulnerabilidades para la auditoría de seguridad en redes

TEMA 11.- Herramientas de detección de intrusiones en red para monitorización de seguridad en redes

TEMA 12.- Diseño seguro de redes. Conceptos de alta disponibilidad y sistemas redundantes

TEMA 13.- Introducción a la criptografía aplicada en Informática

TEMA 14.- Métodos criptográficos: Sistemas de clave privada, sistemas de clave pública y sistemas de una sola vía (one-way hash)

TEMA 15.- Certificación, autenticación e integridad de la información. Firma digital y PKI

TEMA 16.- Protocolos criptográficos: SSL, PGP, IPSec y otros

TEMA 17.- Introducción a las Redes Privadas Virtuales

TEMA 18.- Introducción a los protocolos criptográficos en redes inalámbricas

METODOLOGÍA

La metodología de estudio utiliza la tecnología actual para la formación a distancia en aulas virtuales, con la participación del Equipo Docente, los Profesores Tutores y todos los alumnos matriculados. En este entorno se trabajaran los contenidos teórico-prácticos cuya herramienta fundamental de comunicación será el curso virtual, utilizando la bibliografía básica y el material complementario. Esta actividad del alumno en el aula virtual corresponde aproximadamente a un 10% del tiempo total asignado al estudio de la asignatura.
El trabajo autónomo de estudio, junto con las actividades de ejercicios y pruebas de autoevaluación disponibles, bajo la supervisión del tutor, con las herramientas y directrices preparadas por el equipo docente, completará aproximadamente un 70% del tiempo de preparación de la asignatura.
Por último esta asignatura tiene además programadas unas prácticas a distancia. Esta actividad formativa representa aproximadamente el 20% del tiempo dedicado a la asignatura.

SISTEMA DE EVALUACIÓN

TIPO DE PRUEBA PRESENCIAL

Tipo de examen	Examen mixto
Preguntas test	5
Preguntas desarrollo	4
Duración del examen	120 (minutos)
Material permitido en el examen	
Calculadora no programable	
Criterios de evaluación	

DE LAS PREGUNTAS TEST:

- Cada respuesta correcta es 1 punto

- Cada respuesta incorrecta resta 0,5 puntos

DE LAS PREGUNTAS DE DESARROLLO:

- Cada respuesta se puntua hasta un máximo de 1,25 puntos

NOTA: En el curos virtual residen exámenes y respuestas correctas de los cursos anteriores

% del examen sobre la nota final	60
Nota del examen para aprobar sin PEC	0

Nota máxima que aporta el examen a la calificación final sin PEC	0
Nota mínima en el examen para sumar la PEC	5

Comentarios y observaciones

NOTA IMPORTANTE:

Para aprobar esta asignatura hay que aprobar la prueba presencial y las prácticas obligatorias. Las PEC son evaluables pero opcionales.

Como consecuencia, no tienen sentido los apartados anteriores "Nota del examen para aprobar sin PEC" y "Nota máxima que aporta el examen a la calificación final sin PEC "

PRUEBAS DE EVALUACIÓN CONTINUA (PEC)

¿Hay PEC?

Descripción

Estos ejercicios tienen como objetivo:

Aclaración y consolidación de los conocimientos adquiridos en el estudio de los contenidos

Comprobación del nivel de conocimientos

Resolución de ejercicios simulares a los de la prueba presencial.

Características:

Ejercicios **no obligatorios**, de realización voluntaria

Serán dos pruebas a distancia, al final de los temas 6 y 12

Criterios de evaluación

Constituyen un 10% de la nota de la asignatura (junto con el informe tutorial) que se sumará a la nota final si la nota en la prueba presencial es igual o superior a 5 (en cualquier caso la nota máxima de la asignatura será un 10). La evaluación la llevará a cabo el tutor de la asignatura.

Ponderación de la PEC en la nota final	Un 10%
Fecha aproximada de entrega	PEC/fecha 30/04/2018; PEC/fecha 30/05/2018

Comentarios y observaciones

OTRAS ACTIVIDADES EVALUABLES

¿Hay otra/s actividad/es evaluable/s?

Descripción

Prácticas obligatorias a distancia

Estas prácticas tienen como objetivos:

Adquisición de destreza y rapidez en la resolución de las prácticas de la asignatura

Familiarizarse con los sistemas de seguridad reales y sus interfases

Aclaración y consolidación de los conocimientos adquiridos en el estudio

Características:

Serán dos ejercicios separados, hacia el final de los temas 12 y 16

Es **obligatoria** la realización de al menos una de las dos, que habrá de ser superada para aprobar la asignatura.

Criterios de evaluación

Son **evaluables** y constituyen, entre las dos, un 30% de la nota de la asignatura. Esta nota se sumará a la nota final si la nota en la prueba presencial es igual o superior a 5 (en cualquier caso la nota máxima de la asignatura será un 10). La evaluación la llevarán a cabo los tutores y el equipo docente de la asignatura.

Ponderación en la nota final	Un 30%
Fecha aproximada de entrega	actividad/fecha 30/04/2018; actividad/fecha 30/05/2018

Comentarios y observaciones

¿CÓMO SE OBTIENE LA NOTA FINAL?

La nota final de la asignatura tiene la siguiente composición:

NOTA FINAL = 60%(nota prueba presencial) + 30%(nota prácticas obligatorias) + 10%(nota PECs)

- Si se aprueban las prácticas pero no la prueba presencial, se guarda la nota de prácticas para el curso siguiente

- Si se aprueba la prueba presencial, pero no las prácticas, se guarda la nota de la prueba presencial para el curso siguiente

BIBLIOGRAFÍA BÁSICA

ISBN(13):9788436267167
Título:PROCESOS Y HERRAMIENTAS PARA LA SEGURIDAD DE REDES (2013)
Autor/es:Castro Gil, Manuel Alonso ; Ignacio Alzórriz ; San Cristóbal Ruiz, Elio ; Díaz Orueta, Gabriel ;
Editorial:UN.E.D.

La bibliografía básica esta constituida por un libro siguiendo el formato de las Unidades Didácticas de la UNED, denominado "PROCESOS Y HERRAMIENTAS PARA LA SEGURIDAD DE REDES", editado por la UNED, en el que se recoge y desarrolla de forma completa y suficiente el contenido de la asignatura.

Los siguientes libros forman parte también de la bibliografía básica:

- Título: LA PROTECCIÓN DE DATOS PERSONALES, SOLUCIONES EN ENTORNOS MICROSOFT, VERSIÓN 2.0, Autor/es: Alonso J.M. y otros. Disponible gratuitamente

en formato pdf dentro del curso virtual.

- Título: THE CODE BOOK, Autor/es: Singh, Simon. Libro virtual con ejercicios disponible gratuitamente dentro del curso virtual.

El texto citado de la UNED comprende el 90% del desarrollo teórico de la asignatura. Contiene múltiples ejemplos y ejercicios resueltos, que ayudan mucho al estudio de la asignatura.

La primera parte (legal) del texto de Alonso y otros complementa con mucho detalle el apartado del libro básico sobre la LOPD (Ley Orgánica de Protección de Datos). Aunque no será objeto de evaluación, su segunda parte (técnica) es una muy buena presentación de cómo usar una tecnología concreta para implementar correctamente la LOPD.

Finalmente, el libro de Simon Singh es un gran complemento formativo para la Unidad Didáctica 3, que, además de hacer un repaso completo a la historia de la criptografía aplicada, dispone de numerosos ejemplos y programas que pueden usarse para comprobar la adquisición correcta de conocimientos y competencias en torno a la criptografía.

BIBLIOGRAFÍA COMPLEMENTARIA

ISBN(13):9780201634662
Título:FIREWALLS AND INTERNET SECURITY: REPELLING THE WILY HACKER (2ND EDITION) (2º)
Autor/es:Steven M. Bellovin ; William Cheswick ;
Editorial:Addisson-Wesley

ISBN(13):9780979958717
Título:NMAP NETWORK SCANNING: THE OFFICIAL NMAP PROJECT GUIDE TO NETWORK DISCOVERY AND SECURITY SCANNING
Autor/es:Gordon F. Lyon ;
Editorial:Nmap Project

ISBN(13):9788420541105
Título:COMUNICACIONES Y REDES DE COMPUTADORES (7ª)
Autor/es:Stallings, William ;
Editorial:PRENTICE-HALL

ISBN(13):9789688805411
Título:REDES GLOBALES DE INFORMACIÓN CON INTERNET Y TCP/IP
Autor/es:D. E. Comer ;
Editorial:PEARSON-PRENTICE HALL

Los libros de Stalling y Comer son un gran complemento para repasar toda una serie de conceptos, estándares y protocolos de comunicación (especialmente TCP/IP) necesarios

como base para la adquisición correcta de conocimientos y capacidades asociadas con los contenidos de la asignatura.
El libro de Cheswick y otros es una muy buena aproximación a los conceptos e implementaciones más inteligentes de los cortafuegos, herramientas con poco más de 20 años de historia, pero que se han convertido en una herramienta imprescindible para la puesta en marcha de cualquier política de seguridad informática para cualquier tipo de organización.
La característica principal del libro de Gordon Fyodor es la extensión, profundidad y practicidad con la que trata un tema tan relevante hoy en día como el de las herramientas de scanning en redes, usadas lo mismo como herramientas de ataque a sistemas y redes o como herramientas de puesta en marcha de defensas activas frente a tales ataques.
Finalmente hemos decidido incluir un libro actualizado sobre la seguridad en sistemas operativos UNIX:
Título: SEGURIDAD EN UNIX Y REDES v2.1, Autor: Antonio Villalón Huertas
e incluirlo gratuitamente en el curso virtual de la asignatura
En este caso, el libro de Villalón une la facilidad de lectura a la profundidad en conceptos de seguridad especialmente relevantes para el mundo de los sistemas operativos UNIX.

RECURSOS DE APOYO Y WEBGRAFÍA

Como materiales adicionales para el estudio de la asignatura se ofrece en el curso virtual:
- Distintos libros electrónicos gratuitos, algunos interactivos.
- Diferentes videolecciones grabadas por los tutores intercampus y el equipo docente
- Material desarrollado ex-profeso para el curso por el equipo docente
- Pruebas prácticas de evaluación a distancia.
- Enunciados y soluciones de ejercicios teórico-prácticos que el alumno puede usar como ejercicios de autoevaluación.
- Lista de preguntas frecuentes.

IGUALDAD DE GÉNERO

En coherencia con el valor asumido de la igualdad de género, todas las denominaciones que en esta Guía hacen referencia a órganos de gobierno unipersonales, de representación, o miembros de la comunidad universitaria y se efectúan en género masculino, cuando no hayan sido sustituido por términos genéricos, se entenderán hechas indistintamente en género femenino o masculino, según el sexo del titular que los desempeñe.