26-27

GUÍA DE ESTUDIO PÚBLICA

PROCESOS Y HERRAMIENTAS DE GESTIÓN DE LA SEGURIDAD DE REDES

CÓDIGO 71023074

UNED

26-27

PROCESOS Y HERRAMIENTAS DE GESTIÓN DE LA SEGURIDAD DE REDES

CÓDIGO 71023074

ÍNDICE

PRESENTACIÓN Y CONTEXTUALIZACIÓN
REQUISITOS Y/O RECOMENDACIONES PARA CURSAR LA ASIGNATURA
EQUIPO DOCENTE
HORARIO DE ATENCIÓN AL ESTUDIANTE
TUTORIZACIÓN EN CENTROS ASOCIADOS
COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE
RESULTADOS DE APRENDIZAJE
CONTENIDOS
METODOLOGÍA
SISTEMA DE EVALUACIÓN
BIBLIOGRAFÍA BÁSICA
BIBLIOGRAFÍA COMPLEMENTARIA
RECURSOS DE APOYO Y WEBGRAFÍA
IGUALDAD DE GÉNERO

NOMBRE DE LA ASIGNATURA	PROCESOS Y HERRAMIENTAS DE GESTIÓN DE LA SEGURIDAD DE REDES
CÓDIGO	71023074
CURSO ACADÉMICO	2026/2027
TÍTULO EN QUE SE IMPARTE	GRADO EN INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN
CURSO - PERIODO - TIPO	- TERCER - SEMESTRE 2 - OBLIGATORIAS
TÍTULO EN QUE SE IMPARTE	MÁSTER UNIVERSITARIO EN INDUSTRIA CONECTADA (COMPLEMENTO)
Nº ETCS	6
HORAS	150.0
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, que se inserta en la Materia de Seguridad y Auditoría de la Información, 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.
La asignatura contribuye de manera fundamental a conseguir los conocimientos y competencias básicas asociadas a la seguridad de la información, y a una correcta gestión de los problemas asociados con la misma, para cualquier profesional del mundo de la 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, concretamente en las asignaturas de Sistemas Operativos y Redes y Comunicaciones. 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	ELIO SAN CRISTOBAL RUIZ (Coordinador/a de asignatura)
Correo Electrónico	elio@ieec.uned.es
Teléfono	91398-9381
Facultad	ESCUELA TÉCN.SUP INGENIEROS INDUSTRIALES
Departamento	INGENIERÍA ELÉCTRICA, ELECTRÓNICA, CONTROL, TELEMÁTICA Y QUÍMICA APLICADA A LA INGENIERÍA

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 atención a los alumnos por el equipo docente se llevará a cabo:
1- A través del curso virtual de la asignatura en la plataforma de e-Learning aLF
2- En cualquier momento, por correo electrónico con el equipo docente:
Elio Sancristobal Ruiz - elio@ieec.uned.es, ETSI Industriales, C/Juan del Rosal, 12, 28040 Madrid
Roberto Hernández Berlinches - roberto@scc.uned.es, ETSI Informática, C/Juan del Rosal, 16, 28040 Madrid
3- En el horario de guardia del equipo docente, los martes de 10:00 a 14:00 en el Telf. 91-3989381

TUTORIZACIÓN EN CENTROS ASOCIADOS

En el enlace que aparece a continuación se muestran los centros asociados y extensiones en las que se imparten tutorías de la asignatura. Estas pueden ser:

•**Tutorías de centro o presenciales**: se puede asistir físicamente en un aula o despacho del centro asociado.

•**Tutorías campus/intercampus**: se puede acceder vía internet.

Consultar horarios de tutorización de la asignatura 71023074

COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE

CG.1 - Competencias de gestión y planificación: Iniciativa y motivación. Planificación y organización (establecimiento de objetivos y prioridades, secuenciación y organización del tiempo de realización, etc.). Manejo adecuado del tiempo.
CG.2- 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.
CG.7 - Compromiso ético. Compromiso ético, especialmente relacionado con la deontología profesional. El tratamiento y funcionamiento ético individual es un valor indiscutible para la construcción de sociedades más justas y comprometidas.
BC.1- 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.
BC.4- Capacidad para elaborar el pliego de condiciones técnicas de una instalación informática que cumpla los estándares y normativas vigentes.
BC.6 - Conocimiento y aplicación de los procedimientos algorítmicos básicos de las tecnologías informáticas para diseñar soluciones a problemas, analizando la idoneidad y complejidad de los algoritmos propuestos.
BTEti.1- Capacidad para comprender el entorno de una organización y sus necesidades en el ámbito de las tecnologías de la información y las comunicaciones
BTEti.7- Capacidad de comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos
BTEsi.2- 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 el entorno operativo de modelo de seguridad de red (NSM, Net work Security Model) y las buenas prácticas asociadas a la implementación de dicho modelo.
- Proporcionar un conjunto de prácticas recomendables para la realización e implementación de un modelo de seguridad de red, y evaluar a fabricantes de productos de monitorización y despliegue de una arquitectura de seguridad de red.
- Desarrollar y aplicar conocimientos relativos a armas, tácticas, telecomunicaciones, administradores de sistemas, guiones y programación de un modelo de seguridad de red.
- Comprender las técnicas básicas sobre los procedimientos de difuminación de la información mediante cifrado mediante una revisión histórica de los diferentes métodos empleados hasta nuestro tiempo.
- Analizar el funcionamiento de los algoritmos de secreto compartido (clave privada) y cifrado público, y
las implicaciones más importantes de su utilización como por ejemplo la distribución segura de la clave compartida.
- Desarrollar proyectos de uso de las técnicas criptográficas mediante la arquitectura de seguridad cripto- gráfica de Java e implementar procedimientos de seguridad basadas en los algoritmos criptográficos más co- munes.
- Comprender el concepto de auditoría informática, y los diferentes ámbitos de aplicación de los procesos auditores: redes, seguridad y calidad.
- Ser capaz de aplicar e implantar el conjunto de buenas prácticas recomendadas por ITIL en los procesos software de las organizaciones, con especial relevancia en los procesos de gestión de la seguridad, redes y cali- dad de la organización

Asociados con estos resultados de aprendizaje se busca que los estudiantes sean capaces de:

- Comprender la trascendencia de introducir (o no) la seguridad como un criterio de diseño en cualquier sistema o aplicación informática y 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, así como 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
- Comprender las diferencias de conceptos, seguridad y complejidad entre los diferentes tipos de cortafuegos, sistemas de detección de intrusiones y analizadores de vulnerabilidades de seguridad
- Implantar una seguridad básica en cortafuegos de tipo filtro de paquetes y usar las

características básicas de una herramienta de scanning como nmap.
- 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 y 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

Este es un tema de introducción a la materia, por tanto no requiere de conocimientos previos de la misma. Sin embargo si es importante tener conocimientos sólidos de asignaturas que se imparten en cursos anteriores de la carrera. En este capítulo se sitúa el problema de la seguridad en redes en su ámbito actual y se presenta una panorámica global del mismo, exponiéndose una introducción general al problema de la gestión de la seguridad de la información.

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

En este capítulo se trata de los problemas de seguridad asociados con los dispositivos físicos existentes en una red, desde los inalámbricos hasta los hosts y dispositivos especializados.

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

En este capítulo, y de manera básica, se trata de los problemas de seguridad asociados con todo el software residente en los dispositivos físicos existentes en una red, desde los sistemas operativos hasta las mejoras de seguridad en protocolos.

TEMA 4.- Métodos de ataque a equipos y redes

En este capítulo se analizan los métodos de ataque a redes más extendidos, tratándolos desde diferentes puntos de vista, intentando hacer una clasificación según diferentes criterios. Es éste claramente uno de los temas que más tiempo y reflexión necesitarán,

formando la base que servirá como ejemplos para la mayor parte del resto de la asignatura, en la que se tratará de muchas y muy diferentes formas y herramientas de defensa ante ataques.

TEMA 5.- Defensas básicas ante ataques

En este capítulo se trata de los elementos de defensa básicos, existentes en el software básico de los dispositivos en la red

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

En este capítulo se trata del concepto de política de seguridad aplicable a las redes informáticas de cualquier organización, desde muy diferentes puntos de vista. Es éste un concepto fundamental para la gestión de la seguridad en cualquier tipo de organización. Por ello, es muy importante entender la aplicación práctica de los conceptos que se estudian en este tema, que exigirá de una mayor reflexión y dedicación.

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

En este tema se presenta una panorámica de los métodos más habituales de defensa en redes, no basados en algoritmos criptográficos. Es claramente un capítulo de introducción para el resto de la unidad didáctica.

TEMA 8.- Los cortafuegos y sus aplicaciones

En este tema se presenta tanto el concepto básico de cortafuegos, como las diferentes arquitecturas básicas de los mismos.

TEMA 9.- Tecnologías de última generación en cortafuegos

Para ilustrarlas con casos reales se presentan dos aproximaciones de la industria diferentes: la de Cisco Systems y la de IPTables. Aunque la información no está completamente actualizada, al ser éste un sector sujeto a cambios continuos, la presentación básica sigue siendo suficiente. Se tratará, además, de añadir información actualizada en el curso virtual sobre los modelos nuevos durante el curso académico. Es éste un capítulo que necesitará de más tiempo, reflexión y contextualización por parte del estudiante.

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

Este tema presenta una introducción práctica a las aplicaciones básicas utilizadas para realizar análisis de vulnerabilidades y auditorías de seguridad en redes a diferentes niveles

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

Este tema presenta una introducción a los sistemas y aplicaciones básicas que permiten monitorizar la seguridad en redes, buscando ataques a cualquier dispositivo en las mismas, los conocidos como sistemas de detección de intrusiones o, en sus siglas en inglés, IDS. Igualmente se estudian dos casos prácticos. Este capítulo abre un campo nuevo, así que requerirá un mayor esfuerzo de reflexión y comprensión de los contenidos.

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

En este tema se presenta una introducción a las diferentes soluciones para el problema de la disponibilidad de sistemas y dispositivos, incluyendo los dedicados a la seguridad, en redes.

TEMA 13.- Introducción a la criptografía aplicada en Informática

En este tema se hace una introducción básica a la criptografía, caracterizando los asuntos principales que tienen que ver con su uso aplicado a la seguridad de sistemas y redes. Se trata de un capítulo introductorio a la tercera, y última, unidad didáctica.

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

Para el estudio de este tema es necesario haber comprendido los conceptos y contenidos del tema 13. Este tema analiza las características más importantes de las principales familias de algoritmos criptográficos, resaltando las características más importantes de cada una para su aplicación en la seguridad en redes. No profundiza en el aparato matemático, pero si intenta que el estudiante vea las aplicaciones prácticas. Requiere de un mayor detenimiento y reflexión pues el resto de los capítulos se basan en los contenidos de éste.

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

Este tema presenta y analiza algunos conceptos y mecanismos fundamentales hoy en día para asegurar la autenticación e integridad de las operaciones en redes de ordenadores, como las autoridades de certificación o la firma digital, por lo que es fundamental entender correctamente los contenidos básicos del mismo.

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

Este tema presenta y analiza algunos de los principales protocolos criptográficos usados actualmente en redes de ordenadores. Empieza presentando el concepto de “protocolo criptográfico”, relacionándolo con el de protocolo de comunicaciones, más conocido por los estudiantes a estas alturas, para pasar después a analizar cada uno de ellos.

TEMA 17.- Introducción a las Redes Privadas Virtuales

Este tema presenta una introducción conceptual, que puede hacerse más práctica complementándolo con los protocolos IPsec del tema anterior, a las Redes Privadas Virtuales, conexiones seguras creadas a través de redes públicas.

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

Este último tema presenta una introducción a los principales problemas de seguridad en redes inalámbricas. Aunque son los mismos en esencia que para cualquier otra red, es cierto que la forma de los ataques y los protocolos usados hacen necesario un trato diferenciado

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, pruebas de evaluación continua y pruebas de autoevaluación disponibles al final de cada capítulo del libro de la Bibliografía básica, 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? Si

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

Comentarios y observaciones

No hay una segunda fecha de entrega en Septiembre

OTRAS ACTIVIDADES EVALUABLES

¿Hay otra/s actividad/es evaluable/s? Si

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

Comentarios y observaciones

No hay una segunda fecha de entrega en Septiembre

¿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 y/o las PEC pero no la prueba presencial, se guarda la nota de prácticas y/o PEC para septiembre

- Si se aprueban las prácticas y/o las PEC pero no la prueba presencial, se guarda la nota de prácticas y/o PEC 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 REDES2013
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 SCANNINGnull

Autor/es:Gordon F. Lyon ;
Editorial:Nmap Project

ISBN(13):9788420541105
Título:COMUNICACIONES Y REDES DE COMPUTADORES7ª
Autor/es:Stallings, William ;
Editorial:PRENTICE-HALL

ISBN(13):9789688805411
Título:REDES GLOBALES DE INFORMACIÓN CON INTERNET Y TCP/IPnull
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 se hayan sustituido por términos genéricos, se entenderán hechas indistintamente en género femenino o masculino, según el sexo del titular que los desempeñe.