ASIGNATURA DE GRADO:

PROCESOS Y HERRAMIENTAS DE GESTIÓN DE LA SEGURIDAD DE REDES

Curso 2012/2013

(Código:71023074)

1.PRESENTACIÓN DE LA ASIGNATURA

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 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.

2.CONTEXTUALIZACIÓN EN EL PLAN DE ESTUDIOS

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.

Resultados de Aprendizaje/Competencias que se adquieren:

- Comprender el entorno operativo de modelo de seguridad de red (NSM, Network 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.

- 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.

3.REQUISITOS PREVIOS REQUERIDOS 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.

4.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.

5.CONTENIDOS DE LA ASIGNATURA

Los contenidos de la asignatura se dividen en tres bloques o Unidades Didácticas:

Unidad didáctica 1, en la que se presenta una introducción a los problemas de seguridad en las comunicaciones y en sistemas y datos. Se hace asimismo un examen de los principales problemas de seguridad tanto en los elementos hardware como en los elementos software, tanto en medios y dispositivos como en sistemas operativos, aplicaciones y protocolos. Igualmente se clasifican los ataques más habituales mediante distintos criterios, tratando de ser más didácticos que extensivos, como corresponde a un curso de estas características. Después de una primera aproximación a las defensas más elementales y básicas, se discute el concepto de la política de seguridad y las necesidades fundamentales para hacer una buena implementación. Se abordan los siguientes temas:

- Descripción del problema de la seguridad en las comunicaciones y en la información. Tipos de ataques.

- Seguridad en los elementos físicos existentes en una red: canales de comunicación, cableado, repetidores, conmutadores, encaminadores, servidores, etc.
- Seguridad en los elementos software existentes en una red: sistemas operativos, aplicaciones, protocolos de red IP (e IPv6).
- Métodos de ataque a equipos y redes. Taxonomía de los ataques.
- Defensas básicas ante ataques.
- La política de seguridad como la respuesta razonable a los problemas de seguridad en las comunicaciones y en la información.

Unidad didáctica 2, en la que se estudian los métodos no criptográficos utilizados para la implantación de diversas normas de seguridad. Se analizan las distintas tecnologías de cortafuegos, desde las más sencillas, como los filtros de paquetes, hasta las más sofisticadas basadas en filtros dinámicos de conexiones (stateful inspection). Se presentan igualmente las técnicas más habituales de análisis de vulnerabilidades y los sistemas de detección de intrusiones. Finalmente se analizan brevemente las técnicas de creación de redes seguras mediante diseños de alta disponibilidad. Se abordan los siguientes temas:

- Introducción a los métodos no criptográficos en la implantación de la política de seguridad.
- Los cortafuegos (firewalls) y sus aplicaciones como elemento básico de una política de seguridad de redes.
- Tecnologías de última generación en cortafuegos.
- Herramientas de análisis de vulnerabilidades para la auditoría de seguridad en las comunicaciones.
- Herramientas de detección de intrusiones para la monitorización de la seguridad en las comunicaciones.
- Diseño seguro de redes. Conceptos de alta disponibilidad y diseños redundantes.

Unidad Didáctica 3, en la que se tratan los diversos métodos criptográficos de obtención de seguridad informática en redes. Se inicia asociando la criptografía tradicional con sus usos informáticos, analizando los distintos algoritmos utilizados y qué propiedades de seguridad proporcionan. Se analizan conceptos y técnicas que ya son utilizados ampliamente como los certificados digitales, la firma electrónica y sus aplicaciones y problemas. Igualmente se analizan algunos de los principales problemas criptográficos de uso en sistemas de seguridad actuales, como IPSec o SSL. Finalmente, a la luz de estos protocolos, se discuten las propiedades y problemas de las redes privadas virtuales o de las redes inalámbricas seguras. Se abordan los siguientes temas:

- Introducción a la Criptografía como herramienta de obtención de una mayor seguridad en las comunicaciones.
- Métodos criptográficos: sistemas de clave privada, sistemas de clave pública y sistemas de una sola via (one-way hash).
- Certificación, autenticación e integridad de la información. Firma digital. Protección de datos
- Protocolos criptográficos: S.S.L., P.G.P., IPSec, PKI, etc.
- Redes Privadas Virtuales. Túneles IP.
- Introducción a los protocolos criptográficos en redes inalámbricas

6.EQUIPO DOCENTE

- GABRIEL DIAZ ORUETA
- ELIO SAN CRISTOBAL RUIZ
- MANUEL ALONSO CASTRO GIL
- ROBERTO HERNANDEZ BERLINCHES

7.METODOLOGÍA Y ACTIVIDADES DE APRENDIZAJE

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.

8.EVALUACIÓN

En esta asignatura se utilizan las siguientes modalidades de evaluación

Evaluación continua:

- Autoevaluación, de carácter voluntario: En esta asignatura se plantea a los alumnos un proceso de autoevaluación, basado en la realización de pruebas de test. Estos ejercicios no serán evaluables. En el módulo de contenidos dentro del entorno virtual CiberUNED los alumnos podrán encontrar el apartado de "Autoevaluación" donde se alojarán tanto las pruebas como sus soluciones, con las que el alumno podrá autoevaluar sus conocimientos.

- Pruebas prácticas obligatorias de evaluación a distancia: En el módulo de contenidos dentro del entorno virtual CiberUNED los alumnos encontrarán el apartado de "Evaluación a distancia" donde se alojarán las pruebas que serán evaluadas por los profesores tutores de los centros, con la ayuda del equipo docente. Consistirán en tests y/o pequeños trabajos prácticos que permitirán comprobar la correcta asimilación de contenidos y la adquisición real de competencias relacionadas.

Evaluación final de la asignatura que se llevará a cabo a partir de las siguientes pruebas:

- Realización de un examen teórico/práctico, que es indispensable aprobar para la superación de la asignatura, y que contará como el 70% de la nota final.

- Calificación de las prácticas obligatorias, que es indispensable aprobar para la superación de la asignatura y que contarán como el 30% de la nota final.

9.BIBLIOGRAFÍA BÁSICA

ISBN(13): 9788436249750
Título: SEGURIDAD EN LAS COMUNICACIONES Y EN LA INFORMACIÓN (1ª)
Autor/es: Castro Gil, Manuel Alonso ; Díaz Orueta, Gabriel ; Peire Arroba, Juan ; Mur Pérez, Francisco ;
Editorial: UNED

Buscarlo en Editorial UNED

Buscarlo en libreria virtual UNED

Buscarlo en bibliotecas UNED

Buscarlo en la Biblioteca de Educación

Comentarios y anexos:

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.

Igualmente, el equipo docente ha desarrollado a medida un documento cuyo contenido estará relacionado con seguridad en redes inalámbricas, que se distribuirá en el curso virtual de la asignatura en formato electrónico bajo licencia Creative Commons.

El texto de Díaz Orueta y otros 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.

10.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

Buscarlo en libreria virtual UNED

Buscarlo en bibliotecas UNED

Buscarlo en la Biblioteca de Educación

Buscarlo en Catálogo del Patrimonio Bibliográfico

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

Buscarlo en libreria virtual UNED

Buscarlo en bibliotecas UNED

Buscarlo en la Biblioteca de Educación

Buscarlo en Catálogo del Patrimonio Bibliográfico

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

Buscarlo en libreria virtual UNED

Buscarlo en bibliotecas UNED

Buscarlo en la Biblioteca de Educación

Buscarlo en Catálogo del Patrimonio Bibliográfico

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

Buscarlo en libreria virtual UNED

Buscarlo en bibliotecas UNED

Buscarlo en la Biblioteca de Educación

Buscarlo en Catálogo del Patrimonio Bibliográfico

Comentarios y anexos:

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.

11.RECURSOS DE APOYO

Como materiales adicionales para el estudio de la asignatura se ofrece en el curso virtual:

- Esta guía de estudio y la guía didáctica de estudio de la asignatura.

- Distintos libros electrónicos gratuitos, algunos interactivos.

- Material desarrollado exprofeso para el curso por el equipo docente

- Apartado de noticias y enlaces interesantes, relacionados con el desarrollo de la asignatura

- 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.

12.TUTORIZACIÓN

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

1. Tutores en los centros asociados. Los tutores serán los encargados del seguimiento y control de las pruebas que constituyen la evaluación continua del alumno.

2. Tutorías presenciales o virtuales en el centro asociado correspondiente.

3. 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.

4. Tutor de Apoyo en Red (TAR).

5. Tutorías con el equipo docente: los martes de 15:00 a 19:00 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 por correo electrónico a gdiaz@ieec.uned.es, mcastro@ieec.uned.es o elio@ieec.uned.es o en el entorno CiberUNED.

13.Revisión de calificaciones

Se podrá solicitar revisión de las calificaciones en el plazo y forma establecidos por la UNED.