UNIVERSIDAD DE LAS PALMAS DE GRAN CANARIA

GUÍA DOCENTE *CURSO: 2009/10*

12736 - GESTIÓN Y ADMIN. DE REDES DE COMPUTADORES

ASIGNATURA: *12736 - GESTIÓN Y ADMIN. DE REDES DE COMPUTADORES*
Vinculado a : (Titulación - Asignatura - Especialidad)
1801-Ingeniería en Informática - 12736-GESTIÓN Y ADMIN. DE REDES DE COMPUTADOR - 00

CENTRO: *Escuela de Ingeniería Informática*

TITULACIÓN: *Ingeniero en Informática*

DEPARTAMENTO: *INFORMÁTICA Y SISTEMAS*

ÁREA: *Ciencia De La Comp. E Intel. Artificial*

PLAN: *10 - Año 199* **ESPECIALIDAD:**

CURSO: *Cr. comunes cic* **IMPARTIDA:** *Primer semestre* **TIPO:** *Optativa*

CRÉDITOS: *6* **TEÓRICOS:** *3* **PRÁCTICOS:** *3*

Descriptores B.O.E.

Control, Planificación, Monitorización y Administración.

Temario

MODULO 1:FUNDAMENTOS DE GESTIÓN DE REDES

CAPÍTULO 1: INTRODUCCIÓN A LA GESTIÓN DE REDES

Horas Estimadas: 1
Bibliografía: Stallings, Heinz-Gerd

TEMA 1: Introducción a la Gestión de Redes

MODULO 2: GESTIÓN SNMP

CAPÍTULO 1: LA MIB. PROTOCOLO SNMPv1

Horas Estimadas: 4
Bibliografía: Stallings

TEMA 1: Conceptos de Gestión de SNMP
TEMA 2: Información para la Gestión SNMP
TEMA 3: Base de Información de Gestión (MIB)
TEMA 4: Protocolo SNMP

CAPÍTULO 2:PROTOCOLO DE GESTIÓN DE REDES SIMPLE (SNMPv2)

Horas Estimadas: 2
Bibliografía: Stallings

TEMA 1: Informaciópn para la Gestión SNMPv2
TEMA 2: Protocolo SNMPv2
TEMA 3: Base de Información de Gestión (MIB) y Conformidad

CAPÍTULO 3:PROTOCOLO DE GESTIÓN DE REDES SIMPLE (SNMPv3)

Horas Estimadas: 2
Bibliografía: Stallings, Zeltserman

TEMA 1: Algoritmos Criptográficos
TEMA 2: Arquitectura y Aplicaciones
TEMA 3: Procesamiento del Mensaje y Modelo de Seguridad basado en el Usuario
TEMA 4: Modelo de Control de Acceso Basado en la Vista

CAPÍTULO 4: MONITORIZACIÓN REMOTA DE REDES (RMON)

Horas Estimadas: 3
Bibliografía: Stallings, Heinz-Gerd

TEMA 1: Examen Estadístico
TEMA 2: Alarmas y Filtros
TEMA 3: Monitorización Remota de Redes (RMON2)

MODULO 3: TÉCNICAS DE INTRUSIÓN

CAPÍTULO 1: INTRODUCCIÓN A LAS TÉCNICAS DE INTRUSIÓN
Horas Estimadas: 9
Bibliografía: Muñoz

Tema 1: Ingeniería Social
Tema 2: Análisis de las máquinas objetivos
Tema 3: Software inseguro
Tema 4: Suplantación de identidad
Tema 5: Control de los sistemas comprometidos

MODULO 4: MONITORIZACIÓN DE SEGURIDAD EN REDES

CAPÍTULO 1: INTRODUCCIÓN A LA MONITORIZACIÓN EN REDES
Horas Estimadas: 9
Bibliografía: Bejtlich

Tema 1: El proceso de seguridad
Tema 2: ¿Qué es la monitorización de seguridad de redes?
Tema 3: Consideraciones de depliegue
Tema 4: Productos

Requisitos Previos

Se recomienda que el alumno tenga unos conocimientos básicos de redes de ordenadores tanto en lo referente a la arquitectura de interconexión como a las diferentes tecnologías de redes, LAN y WAN. Estos conocimientos se cubren en las asignaturas de Redes de Computadores y Arquitectura de Sistemas y Aplicaciones Distribuidas impartidas en cuarto curso de Ingeniería Informática

Objetivos

Las Redes y los sistemas de procesamiento distribuidos tienen una gran importancia y son cruciales en el mundo de los negocios. Dentro de una cierta organización la tendencia es al aumento de redes complejas soportando muchas aplicaciones y a muchos usuarios. La complejidad de estos sistemas conduce a la utilización de herramientas para la gestión de redes automatizadas. Uno de los objetivos de esta asignatura es que el alumno conozca y maneje diferentes herramientas para la gestión y administración de redes.

Por otro lado, la seguridad en entornos distribuidos se ha revelado hoy día como uno de los aspectos fundamentales a considerar, sobre todo en aquellas actividades donde la información almacenada es altamente sensible (datos personales, económicos, clínicos, etc.). Por ello, otro de los objetivos es que el alumno conozca y maneje diferentes herramientas para la monitorización de seguridad en redes de computadores.

Metodología

La metodología a seguir en la asignatura consistirá de un conjunto de clases magistrales impartidas en el aula durante el horario correspondiente a las clases teóricas de la asignatura. Así mismo, y durante dicho horario, se impartirán un conjunto de clases abiertas donde se irán verificando la adquisición de conocimientos teóricos del alumno.

Para la realización de las prácticas se hará entrega al alumno del enunciado de la misma donde se le expondrá el trabajo a realizar, la documentación necesaria para su realización así como las fuentes de las mismas. Con dicha información el alumno tendrá que plantear una solución teórica para la realización de dicha tarea y deberá implementar dicha solución en el laboratorio.

Criterios de Evaluación

Para superar la asignatura es necesario superar tanto la parte teórica como la práctica, siendo la nota final una ponderación entre ambas

Nota Final = 0,4 * Nota Teoría + 0,6 * Nota de Prácticas

Teoría

La teoría se evaluará por parciales de forma que para superar la parte teórica de la asignatura, el alumno deberá superar cada uno de los parciales. Para superar un parcial habrá que obtener en el mismo una nota superior o igual a 5.

Prácticas

Para superar las prácticas hay que superar cada una de ellas en los plazos establecidos al efecto para la Convocatoria Ordinaria, evaluándose individualmente cada una de ellas.

Habrá una convocatoria especial de defensa de prácticas en la Convocatoria Extraordinaria de Septiembre para aquellos alumnos que no las hayan superado durante el curso.

La nota de prácticas se establecerá valorando los siguientes apartados:

1. Asistencia y participación en clases prácticas
2. Memorias
3. Defensa

Descripción de las Prácticas

1.- M.I.B.. Estudio en detalle de los objetos del grupo iso.org.dod.internet.mgmt.mib mediante la interrogación de la Management Information Base (MIB).

Nº horas estimadas en Laboratorio: 6

2.- Estudio de las técnicas de intrusión actuales, en sistemas en red, más comunes, tales como ingeniería social, escaneo de sistemas, exploits, etc.

Nº horas estimadas en Laboratorio: 12

3.- Monitorización de Seguridad en red.

Estudio de herramientas de software libre que nos permiten llevar a cabo una monitorización de seguridad en red desde la perspectivas de:

- Datos de contenido completo.

- Datos de Sesión

- Datos Estadísticos

Nº horas estimadas en Laboratorio: 12

Bibliografía

[1 Básico] Request for comments [

Internet Engineering Task Force.

[2 Básico] Seguridad de sistemas en red /

José Antonio Muñoz Blanco, Víctor Manuel Henríquez Henríquez.
Universidad de Las Palmas de Gran Canaria, Servicio de Publicaciones,, Las Palmas de Gran Canaria : (2007)
97884969710305

[3 Básico] El Tao de la monitorización de seguridad en redes /

Richard Bejtlich.
Pearson Prentice Hall,, Madrid : (2005)
8420546003

[4 Básico] SNMP, SNMPv2, SNMPv3, and RMON 1 and 2 /

William Stallings.

Addison-Wesley,, Reading, Massachussetts : (1999) - (3rd. ed.)

0201485346

[5 Recomendado] A practical guide to SNMPv3 and network management /

David Zeltserman.

Prentice Hall,, Upper Saddle River, NJ : (1999)

0130214531

Equipo Docente

JOSÉ ANTONIO MUÑOZ BLANCO *(RESPONSABLE DE PRACTICAS)*

Categoría: CATEDRATICO DE UNIVERSIDAD

Departamento: INFORMÁTICA Y SISTEMAS

Teléfono: 928458754 **Correo Electrónico:** joseantonio.munoz@ulpgc.es

JUAN CARLOS QUEVEDO LOSADA *(COORDINADOR)*

Categoría: TITULAR DE UNIVERSIDAD

Departamento: INFORMÁTICA Y SISTEMAS

Teléfono: 928458757 **Correo Electrónico:** juancarlos.quevedo@ulpgc.es

Resumen en Inglés

In this