GUIA DOCENTE DE LA ASIGNATURA

SERVIDORES SEGUROS

Curso 2013- 2014

MÓDULO MATERIA	**CURSO**	**SEMESTRE**	**CRÉDITOS**	**TIPO**
Módulo 3: Computación de altas prestaciones	1º	2º	3	Optativa

PROFESOR(ES)	**DIRECCIÓN COMPLETA DE CONTACTO PARA TUTORÍAS (Dirección postal, teléfono, correo electrónico, etc.)**
• Antonio F. Díaz García	Departamento de Arquitectura y Tecnología de Computadores. Escuela Técnica Superior de Ingenierías Informática y de Telecomunicación. 2ª planta. C/ Periodista Daniel Saucedo Aranda s/n. 18071- Granada. Despacho: 29 Correo electrónico: afdiaz@ugr.es
	HORARIO DE TUTORÍAS
	Se puede consultar en: http://atc.ugr.es/static/InformacionAcademicaDepartamentos/*/docentes/f810fc966007adf072ad91a1d1fe2e09

MÁSTER EN EL QUE SE IMPARTE	**OTROS MÁSTERES A LOS QUE SE PODRÍA OFERTAR**
Máster Universitario Oficial en Ingeniería de Computadores y Redes	Máster Oficial en Desarrollo de Software Máster en Soft Computing y Sistemas Inteligentes

PRERREQUISITOS Y/O RECOMENDACIONES (si procede)
Tener conocimientos adecuados sobre sistemas operativos y seguridad

BREVE DESCRIPCIÓN DE CONTENIDOS (SEGÚN MEMORIA DE VERIFICACIÓN DEL MÁSTER)

Es esta asignatura se estudian aspectos relacionados con la seguridad de sistemas informáticos, principalmente orientado a servidores y cluster de computadores. Desde la comunicación con dicho servidor mediante protocolos seguros, la seguridad en las aplicaciones así como el control de acceso a los recursos.

COMPETENCIAS GENERALES Y ESPECÍFICAS

Competencias básicas (CB) y generales (CG) que se refieren a proporcionar, en los ámbitos propios de la Ingeniería de Computadores y Redes, la capacidad de aplicar los conocimientos adquiridos para la resolución de problemas, de integrar conocimientos y formular juicios teniendo en cuenta las responsabilidades sociales y éticas derivadas de su actividad, de comunicar de forma clara y precisa sus conclusiones, y de aprender de forma continuada, autodirigida y autónoma.
Competencias específicas (CE):
- CE1: Los estudiantes deben ser capaces de diseñar y configurar, implementar, y evaluar plataformas de cómputo y redes para que proporcionen los niveles de prestaciones y satisfagan los requisitos establecidos por las aplicaciones en cuanto a coste, velocidad, fiabilidad, disponibilidad y seguridad.
- CE2: Los estudiantes deben ser capaces de utilizar herramientas avanzadas en actividades propias de la ingeniería de computadores y redes: herramientas para la descripción, análisis, simulación, diseño e implementación de plataformas de cómputo, control y comunicación.
- CE3: Los estudiantes deben ser capaces de aplicar técnicas y metodologías que permiten abordar desde nuevas perspectivas los problemas de interés, gracias a la disponibilidad de las plataformas de computación y comunicación con niveles de prestaciones cada vez más elevados.

OBJETIVOS (EXPRESADOS COMO RESULTADOS ESPERABLES DE LA ENSEÑANZA)

Capacidad para evaluar los riesgos de seguridad en un sistema informático, principalmente orientado a servidores y cluster de computadores donde las posibilidades de un ataque pueden ser mayores debido a los servicios que deben ofrecer al exterior. Proteger a un computador de posibles ataques externos basándose tanto en cortafuegos como en mecanismos de seguridad propios.

- (AP0) Resultados relacionados con las competencias generales (CG): habilidades de resolución de problemas, de discusión, de comunicación oral y escrita, etc.
- (AP1) Establecer canales seguros de comunicación entre cliente y servidor a través de Internet de forma cifrada y evitando posibilidad de ataques “Man in theMiddle“
- (AP2) Distinguir entre túneles y VPN (redes privadas virtuales), así como saber cuál es más adecuado utilizar en función de los requerimientos exigidos.
- (AP3) Conocimiento de los modelos de seguridad basados en PKI (Public Key Infrastructure)
- (AP4) Configuración de cortafuegos y subredes intranet.
- (AP5) Conocimento de mecanismos de seguridad utilizados por aplicaciones informáticas.
- (AP6) Estudio de las redes inalámbricas utilizadas en la actualidad como sistemas de comunicación entre ordenadores, análisis de vulnerabilidades y establecimiento de modelos seguros.

TEMARIO DETALLADO DE LA ASIGNATURA

TEMARIO TEÓRICO:
Tema 1: Seguridad en protocolos de transporte

- 1.1 Túneles SSH. Túneles SSL: Seguridad en protocolos de transporte (SSL / TLS). Túneles HTTP
- 1.2 Redes Privadas Virtuales (VPN Virtual Private Network). Descripción, tipos VPN Microsoft, OpenVPN
- 1.3 Seguridad en redes inalámbricas. WPA-PSK, WPA utilizando servidores Radius. Herramientas de análisis wireless. Análisis de tráfico. Vulnerabilidades WEP

Tema 2. Seguridad en aplicaciones

- 2.1 Análisis de vulnerabilidades y Detección de ataques.
- 2.2 PKI (Public Key Infrastructure). Certificados. OpenSSL.
- 2.3 Seguridad en aplicaciones: apache, imap,….
- 2.4 Seguridad en sistemas de objetos distribuidos

Tema 3: Control de acceso al servidor.

- 3.1 IDS: Detección de intrusos. Ataques
- 3.2 Seguridad perimetral: Tcpwrapper, Iptables
- 3.3 Aplicaciones relacionadas con autentificación: Kerberos, LDAP, PAM,…
- 3.4 Seguridad: SE-Linux,
- 3.5 Seguridad en sistemas de ficheros

BIBLIOGRAFÍA

- Adams, Carlisle; Lloyd, Steve: ”Understanding PKI : concepts, standards, and deployment considerations” Boston [etc.] : Addison-Wesley, 2003
- Barrett, Daniel; Silverman, Richard E.: ”SSH, the secure shell : the definitive guide” Beijing [etc.] : O'Reilly , 2005
- Caballé, Santi; Xhafa, Fatos:”Aplicaciones distribuidas en Java con tecnología RMI” Madrid : Delta, 2008
- Iptables: http://www.linuxsecurity.com/resource_files/firewalls/IPTables-Tutorial/iptables-tutorial.html, 2011
- Lee, ByeongGi; Sunghyun Choi: “Broadband wireless access and local networks : mobile WiMax and WiFi”. Boston : ArtechHouse, 2011
- Mason, Andrew.:”Cisco firewall technology” Indianapolis, Ind. : Cisco Press, 2007
- OlegKolesnilov; Brian Hatch: “Guía avanzada : redes privadas virtuales con Linux” Madrid [etc.] : Prentice Hall, 2003
- OpenVPN: http://openvpn.source-forge.net, 2011
- Rescorla, Eric: “SSL and TLS : designing and building secure systems” Boston : Addison-Wesley, 2001
- TrueCrypt: http://www.truecrypt.org/, 2011
- VPNC: http://www.vpnc.org, 2011

ENLACES RECOMENDADOS

- http://www.stunnel.org
- http://www.vpnc.org

- http://openvpn.net/
- http://cve.mitre.org
- http://www.uscert.gov/
- http://web.nvd.nist.gov/view/vuln/search
- http://cert.inteco.es
- https://www.owasp.org
- http://www.openssl.org
- http://www.snort.org/
- http://www.sleuthkit.org

METODOLOGÍA DOCENTE

- Lección magistral
  - Descripción: Presentación en el aula de los conceptos propios de la materia haciendo uso de metodología expositiva con lecciones magistrales participativas y medios audiovisuales.
- Actividades prácticas
  - Descripción: Actividades a través de las cuales se pretende mostrar al alumnado cómo debe actuar a partir de la aplicación de los conocimientos adquiridos.
- Otras actividades presenciales
  - Descripción: Actividades individuales o en grupo, como tests de revisión.
- Actividades no presenciales individuales
  - Descripción: Actividades (guiadas y no guiadas) propuestas por el profesor a través de las cuales y de forma individual se profundiza en aspectos concretos de la materia posibilitando al estudiante avanzar en la adquisición de determinados conocimientos y procedimientos de la materia.
- Tutorías académicas
  - Descripción: interacción directa entre el estudiante y el profesor para la organización del proceso de enseñanza y aprendizaje.

EVALUACIÓN (INSTRUMENTOS DE EVALUACIÓN, CRITERIOS DE EVALUACIÓN Y PORCENTAJE SOBRE LA CALIFICACIÓN FINAL, ETC.)

La calificación final que aparecerá en el Acta será un número comprendido entre 0 y 10 con una precisión de un dígito decimal. En función de la convocatoria (ordinaria o extraordinaria), y del tipo de evaluación escogida, la calificación se obtendrá como se detalla a continuación:

Convocatoria ordinaria:
La metodología de evaluación por defecto según la normativa de la Universidad de Granada es la evaluación continua, que en el caso de esta asignatura se compone de las siguientes actividades:

- Asistencia y participación activa del estudiante en las actividades presenciales (20%).
- Aplicaciones prácticas y presentación de las mismas realizadas por el estudiante (40%).
- Investigación, obtención de información y desarrollo de ideas partiendo de las fuentes documentales accesibles para el estudiante (40%).

Alternativamente a la evaluación continua, para la convocatoria ordinaria el estudiante puede optar por la evaluación única final. Para acogerse a la evaluación única final, el estudiante, en las dos primeras semanas de impartición de la asignatura, lo solicitará al Coordinador del Máster, quien dará traslado al profesorado correspondiente, alegando y acreditando las razones que le asisten para no poder seguir el sistema de

evaluación continua. La evaluación única final consistirá en la evaluación de las siguientes actividades formativas:

- Aplicaciones prácticas realizadas por el estudiante (50%).
- Investigación, obtención de información y desarrollo de ideas partiendo de las fuen tes documentales accesibles para el estudiante (50%).

Convocatoria extraordinaria:
En las convocatorias extraordinarias se utilizará el sistema de evaluación única final, tal y como se ha descrito más arriba.
Todo lo relativo a la evaluación se regirá por la normativa sobre evaluación y calificación de los estudiantes de la Universidad de Granada (Boletín Oficial de la Universidad de Granada nº 71. 27 de mayo de 2013). El sistema de calificaciones se expresará mediante calificación numérica de acuerdo con lo establecido en el art. 5 del R. D 1125/2003, de 5 de septiembre, por el que se establece el sistema europeo de créditos y el sistema de calificaciones en las titulaciones universitarias de carácter oficial y validez en el territorio nacional.

INFORMACIÓN ADICIONAL

Página web oficial del Máster: http://masteres.ugr.es/master-icr/
Página web de la asignatura: https://swad.ugr.es/?CrsCod=1795