Guía docente de la asignatura

Servidores Seguros (M51/56/3/4)

Fecha de aprobación por la Comisión Académica: 26/07/2023

Máster	Máster Universitario en Ciencia de Datos e Ingeniería de Computadores
MÓDULO	Módulo de Nivelación de Conocimientos
RAMA	Ingeniería y Arquitectura
CENTRO RESPONSABLE DEL TÍTULO	Escuela Internacional de Posgrado

Semestre	Primero	**Créditos**	4	**Tipo**	Optativa	**Tipo de enseñanza**	Presencial

PRERREQUISITOS Y/O RECOMENDACIONES

Se recomienda haber cursado Introducción a la programación en Ingeniería de Computadores aunque no es imprescindible.

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

COMPETENCIAS BÁSICAS

- CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación.
- CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más

amplios (o multidisciplinares) relacionados con su área de estudio.
- CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios.
- CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades.
- CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.

COMPETENCIAS GENERALES

- CG01 - Capacidad de acceso y gestión de la información
- CG02 - Capacidad de análisis y síntesis
- CG03 - Capacidad de organización y planificación
- CG04 - Capacidad emprendedora
- CG05 - Capacidad para tomar decisiones de forma autónoma
- CG06 - Capacidad de uso de una lengua extranjera
- CG07 - Motivación por la calidad
- CG08 - Capacidad para trabajar en equipo

COMPETENCIAS ESPECÍFICAS

- CE01 - Capacidad para el diseño, configuración, implementación y evaluación de 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.
- CE02 - Capacidad de utilización de 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

COMPETENCIAS TRANSVERSALES

- CT01 - Ser consciente de la importancia del desarrollo sostenible y demostrar sensibilidad medioambiental.
- CT02 - Ser consciente del derecho a la no discriminación y al acceso universal al conocimiento de las personas con discapacidad.

RESULTADOS DE APRENDIZAJE (Objetivos)

Capacidad para evaluar los riesgos de seguridad en un sistema informático, principalmente orientado a servidores y clusters 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: habilidades de resolución

de problemas, de discusión, de comunicación oral y escrita.
- (AP1) Configuración de cortafuegos y subredes, intranet.
- (AP2) Evaluación de riesgos en la seguridad y respuesta.
- (AP3) Conocimiento de mecanismos de seguridad utilizados por aplicaciones informáticas.
- (AP4) Estudio de los modelos de seguridad basados en llave pública.
- (AP5) Establecer canales seguros de comunicación.
- (AP6) Distinguir entre túneles y redes privadas virtuales, así como saber cuál es más adecuado utilizar en función de los requerimientos exigidos.
- (AP7) Estudio de las redes inalámbricas utilizadas en la actualidad como sistemas de comunicación entre ordenadores, análisis de vulnerabilidades y establecimiento de modelos seguros.
- (AP8) Capacidad de establecimiento de auditorías de seguridad y análisis forense.

PROGRAMA DE CONTENIDOS TEÓRICOS Y PRÁCTICOS

TEÓRICO

1. Introducción a la seguridad informática.
    1. Contexto y Peligros reales.
    2. Elementos básicos de criptografía.
    3. Almacenamiento en nube y protección de datos.
2. Seguridad en sistemas operativos.
    1. Autenticación.
    2. Seguridad local y perimetral.
    3. Detección de intrusos. Ataques.
3. Seguridad en aplicaciones.
    1. Análisis de vulnerabilidades y detección de ataques.
    2. Infraestructura de llave pública (PKI).
    3. Seguridad en aplicaciones y servicios.
    4. Seguridad en aplicaciones distribuidas.
4. Seguridad en comunicaciones.
    1. Túneles. Seguridad en protocolos de transporte y recursos en la nube.
    2. Redes Privadas Virtuales.
    3. Seguridad en redes inalámbricas.

PRÁCTICO

1. Ejercicio de análisis de LOPD.
2. Actividades de implementación de buffer overflow.
3. Ejercicios en plataforma hackthebox y ataque con metasploit de una máquina virtual.
4. Crear VPN entre máquinas usando OpenVPN y ofrecer servicio oculto a través de TOR.

BIBLIOGRAFÍA

BIBLIOGRAFÍA FUNDAMENTAL

- Modern Operating Systems. 4th Edition. Andrew S. Tanenbaum and Herbert Bos. Pearson. 2014.

- Andrew Tanembaum Computer Networks 5a Edición Cáp 8.

- Informe anual del CNI: https://www.ccn-cert.cni.es/informes.html
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673
- https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673.
- https://www.owasp.org.
- Red Hat Certificate of Expertise in Server Hardening - Exam EX413 Training. William Rothwell, Oreilly.
- Linux Hardening in Hostile Networks: Server Security from TLS to Tor by Kyle Rankin Published by Addison-Wesley Professional, 2017.
- Documentación oficial del S.O. Red Hat, Fedora y CentOS: https://access.redhat.com/products
- ENISA Securing Machine Learning Algorithms, 2021: https://www.enisa.europa.eu/publications/securing-machine-learning-algorithms
- Plataforma de recursos: Try Hack Me https://tryhackme.com/
- Plataforma de recursos: Hack the box https://www.hackthebox.com/

BIBLIOGRAFÍA COMPLEMENTARIA

- 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

Enlaces proporcionados en el material de clase:

- 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.
- Tratado 108: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1.
- Tratado 185: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa41c.
- RGPD: https://www.boe.es/doue/2016/119/L00001-00088.pdf.
- Agencia Española de Protección de Datos: https://www.aepd.es/normativa/index.html.

METODOLOGÍA DOCENTE

- MD01 Lección magistral/expositiva
- MD02 Resolución de problemas y estudio de casos prácticos
- MD03 Prácticas de laboratorio
- MD04 Seminarios
- MD05 Análisis de fuentes y documentos
- MD06 Realización de trabajos en grupo

EVALUACIÓN (instrumentos de evaluación, criterios de evaluación y porcentaje sobre la calificación final)

EVALUACIÓN ORDINARIA

El artículo 17 de la Normativa de Evaluación y Calificación de los Estudiantes de la Universidad de Granada establece que la convocatoria ordinaria estará basada preferentemente en la evaluación continua del estudiante, excepto para quienes se les haya reconocido el derecho a la evaluación única final.

- El 50% de la nota procederá de la realización de pruebas diarias acerca de lo aprendido en las clases anteriores tanto de teoría como de prácticas. Todas las pruebas tienen el mismo valor.
- El otro 50% se basará en dos exámenes y en dos entregables (P1 y P2) donde se desarrollará trabajo de tipo práctico sobre temas relacionados con la materia de la asignatura (exploits, uso de frameworks, segurización de serividores y de sus comunicaciones,...).

EVALUACIÓN EXTRAORDINARIA

El artículo 19 de la Normativa de Evaluación y Calificación de los Estudiantes de la Universidad de Granada establece que los estudiantes que no hayan superado la asignatura en la convocatoria ordinaria dispondrán de una convocatoria extraordinaria. A ella podrán concurrir todos los estudiantes, con independencia de haber seguido o no un proceso de evaluación continua. De esta forma, el estudiante que no haya realizado la evaluación continua tendrá la posibilidad de obtener el 100% de la calificación mediante la realización de una prueba.

- Realización de una única prueba de evaluación de la asignatura completa.

EVALUACIÓN ÚNICA FINAL

El artículo 8 de la Normativa de Evaluación y Calificación de los Estudiantes de la Universidad de Granada establece que podrán acogerse a la evaluación única final, el estudiante que no pueda cumplir con el método de evaluación continua por causas justificadas. Para acogerse a la evaluación única final, el estudiante, en las dos primeras semanas de impartición de la asignatura o en las dos semanas siguientes a su matriculación si ésta se ha producido con posterioridad al inicio de las clases o por causa sobrevenidas. Lo solicitará, a través del procedimiento electrónico, a la Coordinación 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 en tal caso consistirá en:

- Realización de una única prueba de evaluación de la asignatura completa.

INFORMACIÓN ADICIONAL

Información de interés para estudiantado con discapacidad y/o Necesidades Específicas de Apoyo Educativo (NEAE): Gestión de servicios y apoyos (https://ve.ugr.es/servicios/atencion-social/estudiantes-con-discapacidad).