Guía docente de la asignatura

Seguridad en Sistemas Operativos (Especialidad Ingeniería de Software) (29611BF)

Fecha de aprobación: **26/06/2023**

Grado	Grado en Ingeniería Informática	**Rama**	Ingeniería y Arquitectura
Módulo	Complementos de Ingeniería del Software	**Materia**	Complementos de Programación Paralela y Sistemas Operativos

Curso	4º	**Semestre**	1º	**Créditos**	6	**Tipo**	Optativa

PRERREQUISITOS Y/O RECOMENDACIONES

No es necesario que los alumnos tengan aprobadas asignaturas, materias o módulos previos como requisito indispensable para cursar este módulo. No obstante se recomienda la superación de los contenidos y adquisición de competencias de las materias de formación básica y de rama.

BREVE DESCRIPCIÓN DE CONTENIDOS (Según memoria de verificación del Grado)

- Modelos de seguridad.
- Especificación e implementación de políticas de seguridad.
- Auditoría del sistema operativo.
- Análisis forense.
- Ingeniería inversa aplicada a la seguridad.

COMPETENCIAS ASOCIADAS A MATERIA/ASIGNATURA

COMPETENCIAS GENERALES

- CG08 - Conocimiento de las materias básicas y tecnologías, que capaciten para el aprendizaje y desarrollo de nuevos métodos y tecnologías, así como las que les doten de una gran versatilidad para adaptarse a nuevas situaciones.

COMPETENCIAS TRANSVERSALES

- CT02 - Capacidad para tomar decisiones basadas en criterios objetivos (datos experimentales, científicos o de simulación disponibles) así como capacidad de argumentar y justificar lógicamente dichas decisiones, sabiendo aceptar otros puntos de

vista.

RESULTADOS DE APRENDIZAJE (Objetivos)

1. Caracterizar diferentes modelos de seguridad relacionados con el control de acceso en sistemas operativos.
2. Identificar diferentes arquitecturas de seguridad de los sistemas operativos actuales.
3. Identificar cómo el sistema operativo controla la seguridad los objetos que gestiona.
4. Entender la importancia de definir una política de seguridad dentro del sistema y expresarla en un lenguaje de seguridad.
5. Conocer los mecanismos del lenguaje de política de seguridad que permiten seguridad multinivel y seguridad condicional.
6. Poder escribir módulos de política de seguridad para un sistema.
7. Conocer los procesos y herramientas necesarias para identificar los problemas de seguridad que puede provocar un programa.
8. Identificar la importancia del análisis forense en el contexto actual.
9. Identificar las técnicas utilizadas para recolectar, analizar y presentar evidencias.
10. Identificar los pasos necesarios para la construcción de software seguro.
11. Identificar los usos de la ingeniería inversa desde el punto de vista de la seguridad del sistema con objeto de poder detener posible ataques.

PROGRAMA DE CONTENIDOS TEÓRICOS Y PRÁCTICOS

TEÓRICO

- Tema 1. Introducción a la Ciberseguridad: Principios de Ciberseguridad y protección.Vulnerabilidades, ataques y contramedidas. Aspectos legales y éticos.
- Tema 2. Sistemas operativos seguros: Propiedades. Autenticación, autorización y control de acceso. Sistemas operativos confiables. Fortalecimiento del sistema (system hardening). Garantía de la seguridad.
- Tema 3. Programas maliciosos y programas seguros: Programas inseguros y programas maliciosos (malware). Análisis de malware. Construcción de programas y sistemas seguros.
- Tema 4. Hacking ético: Fundamentos hacking ético. Tipos y fases del hacking ético. Herramientas.
- Tema 5. Forense digital de sistemas: Conceptos básicos de Informática Forense. La evidencia digital. Métodos y herramientas.Técnicas anti-forenses.

PRÁCTICO

- Práctica 1: Administración de la seguridad del sistema: Privilegios y permisos. Fortalecimiento del sistema. Análisis de vulnerabilidades. Anti-rootkits. Mecanismos de control de acceso obligatorios. Cifrado de archivos, mensajes, y sistemas de archivos. Esteganografía.
- Práctica 2: Ingeniería inversa y vulnerabilidades: Formato de un ejecutable. Posibles ataques a ejecutables y mecanismos de protección.
- Práctica 3: Hacking ético: Metodología y herramientas de hacking ético.
- Práctica 3: Análisis digital forense: adquisición de evidencias de discos y memoria RAM. Análisis forense de las imágenes forenses.

BIBLIOGRAFÍA

BIBLIOGRAFÍA FUNDAMENTAL

1. Easttom, C. (2020). Computer security fundamentals (Fourth edition.). Pearson.
2. Kutuh Thakur, Al-Sakib Khan Pathan, Cybersecurity Fundamentals: A Real-World Perspective, CRC Press, 2020.
3. Hayes, D. (2021). A practical guide to digital forensics investigations (Second edition.). Pearson.
4. Sirapat Boonkrong. (2021). Authentication and access control : practical cryptography methods and tools (1st ed. 2021.). Apress. https://doi.org/10.1007/978-1-4842-6570-3
5. Tarandach, I., & Coles, M. (2021). Threat modeling : a practical guide for developing teams (1st edition). O'Reilly.
6. Maíllo Fernández, J. (2020). Ciberseguridad : hacking ético . Ra-Ma.
7. Hickey, M., & Arcuri, J. (2020). Hands on hacking . John Wiley and Sons.
8. Easttom, C. (2018). Penetration testing fundamentals (1st edition). Pearson.
9. Hayes, D. (2021). A practical guide to digital forensics investigations (Second edition.). Pearson.
10. Kävrestad, J. (2020). Fundamentals of Digital Forensics Theory, Methods, and Real-Life Applications (2nd ed. 2020.). Springer International Publishing.
11. Johansen, G. (2020). Digital forensics and incident response : incident response techniques and procedures to respond to modern cyber threats (Second edition.). Packt.
12. Mohanta, A., & Saldanha, A. (2020). Malware analysis and detection engineering : a comprehensive approach to detect and analyze modern malware (1st ed.). Apress.
13. Andriesse, D., & Bos, H. (2019). Practical binary analysis : build your own Linux tools for binary instrumentation, analysis, and disassembly (1st edition). No Starch Press.

BIBLIOGRAFÍA COMPLEMENTARIA

1. Edgar, T., & Manz, D. (2017). Research methods for cyber security (1st edition). Syngress.
2. Oakley, J. (2019). Professional Red Teaming Conducting Successful Cybersecurity Engagements (1st ed. 2019.). Apress. https://doi.org/10.1007/978-1-4842-4309-1.
3. Roussev, V. (2017). Digital forensic science : issues, methods, and challenges . Morgan & Claypool Publishers. https://doi.org/10.2200/S00738ED1V01Y201610SPT019.
4. Oettinger, W. (2020). Learn Computer Forensics (1st edition). Packt Publishing.
5. Chess, B., & West, J. (2007). Secure programming with static analysis (1st edition). Addison Wesley.
6. Viega, J., & Messier, M. (2003). Secure programming cookbook for C and C++ / . O'Reilly.
7. Eagle, C., & Nance, K. (2020). The Ghidra Book (1st edition). No Starch Press.
8. Troncone, P., & Albing, C. (2019). Cybersecurity Ops with bash : attack, defend, and analyze from the command line (First edition.). O'Reilly.
9. Reddy, N. (2019). Practical Cyber Forensics An Incident-Based Approach to Forensic Investigations (1st ed. 2019.). Apress. https://doi.org/10.1007.978-1-4842-4460-9.

ENLACES RECOMENDADOS

- Material docente, tanto de teoría como de prácticas, en PRADO (https://prado.ugr.es/).
- Web del Departamento (https://lsi.ugr.es/docencia/grados/grado-ingenieria-informatica/seguridad-sistemas-operativos-eingsoft/guia-docente).
- Enlaces de recurso docentes/didácticos: se indicarán tanto en la documentación de teoría como en las Guías de prácticas en los puntos correspondientes, disponibles en Prado.

METODOLOGÍA DOCENTE

- MD01 - Lección Magistral (Clases Teóricas-Expositivas)
- MD02 - Actividades Prácticas (Resolución de Problemas, Resolución de Casos Prácticos, Desarrollo de Proyectos, Prácticas en Laboratorio, Taller de Programación, Aula de Informática, Prácticas de Campo).
- MD03 - Seminarios (Debates, Demos, Exposición de Trabajos Tutelados, Conferencias, Visitas Guiadas, Monografías).
- MD04 - Actividades no presenciales Individuales.
- MD05 - Actividades no presenciales Grupales.
- MD06 - Tutorías Académicas.

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

EVALUACIÓN ORDINARIA

Consideraciones generales:

1. La asistencia tanto a clases teóricas (salvo la presentación de trabajos grupales) como de prácticas no será obligatoria, si bien se considera que el alumno se beneficiará de la misma para alcanzar las competencias propuestas. No obstante, se considera que se sigue el método de evaluación continua si realizan al menos un 80% de las actividades totales propuestas en la Asignatura.
2. Para superar la asignatura es necesario una calificación numérica igual o superior a 5 (sobre 10). Además, se establece el requisito adicional de que tanto las calificaciones de teoría como las de prácticas deben de ser mayores o iguales a 4 (sobre 10).
3. La calificación global corresponderá a la suma de los diferentes elementos/actividades citados en los puntos anteriores y que integran el sistema de evaluación. Por tanto, el resultado de la evaluación será una calificación numérica obtenida mediante la suma de las calificaciones correspondientes a una parte: teoría, práctica, trabajo y presentación grupal, cada una con la ponderación indicada.

En la convocatoria ordinaria la evaluación será continua. Para la misma se utilizarán las técnicas, todas ellas obligatorias, de evaluación y ponderaciones respecto a la calificación final que se indican a continuación:

1. Teoría - tiene un ponderación total será del 20%, y consta de 2 pruebas objetivas individuales, cada una de las cuales supondrá el 10% de la calificación de este bloque. Se realizará una prueba cada dos temas y constará de varias preguntas cortas y/o ejercicios sobre los contenidos de temas en estudio. Es necesario obtener al menos un 40% de la calificación del bloque para que sea considerada en la suma final.
2. Prácticas - se realizarán en el laboratorio utilizando los Guiones de Prácticas (un guion por semana y sesión) elaborados a tal fin y que incluyen los contenidos a abordar y las actividades a realizar por el alumno. Para mejor programación del trabajo del estudiante, las soluciones de las actividades propuestas en cada sesión deben ser entregadas con formato de informe/memoria individual de prácticas (conteniendo las evidencias de haber entendido y realizado los supuestos prácticos) en el plazo establecido al inicio de la misma (si bien el plazo puede modificarse). Estas actividades serán evaluadas globalmente al final del cuatrimestre mediante dado que el estudiante puede conocer por sí mismo si están correctamente resueltas. Los elementos que se valora para la calificación final de prácticas son:

1. La defensa de prácticas – se realiza bien mediante entrevista personal con estudiantes, bien con cuestionario escrito, que se realiza la última semana lectiva, donde se preguntará sobre el trabajo realizado en una actividad de una sesión de cada una de las tres prácticas que previamente ha debido resolver. Se realiza en el laboratorio con ordenador por lo que es posible probar o completar la respuesta a las actividades previamente resueltas en los informes de cada sesión. Se valorará la calidad, claridad y completitud de las soluciones dadas. Esta defensa se pondera con un 30% de la calificación global, y es necesario obtener al menos un 50% de la calificación para sumar las otras partes.
2. Los informes/memorias de prácticas se entregaran tras cada sesión de prácticas en la fecha establecida al publicar la sesión. Se evalúan globalmente y se valoran con un 10% la calificación. En los mismos se valorará la calidad, claridad y completitud de las soluciones dadas así como los detalles de cómo se ha resuelto. Para superar las prácticas es necesario entregar la memorias de al menos un 80% de las sesiones. Se considera superada si al menos se obtiene un 50% de la calificación del bloque.

3. Trabajos grupales - Consta de los siguientes elementos:
    1. Un trabajo escrito en grupo (20% de la calificación global) de carácter técnico y contenidos teórico-prácticos sobre un tema relacionad con la Ciberseguridad y cuyo formato estará disponible en la plataforma docente al inicio de curso. Se evaluará mediante una rúbrica, también publicada en la plataforma docente junto con el formato de trabajo). La calificación del trabajo grupal se reparte en la forma: 50% proviene de la calificación del profesor (hetero-evaluación) y el otro 50% es la media de la calificación dada por varios compañeros (co-evaluación) – el número de compañeros evaluadores y de los grupos dependerá de los alumnos matriculados en el curso. El trabajo deberá entregarse dos semanas antes de la finalización de las clases presenciales. Este trabajo podría ser individual si las circunstancias así lo exigen, si bien la evaluación se realizará sobre el trabajo, no sobre el número de participantes del grupo. Para su elaboración queda terminantemente prohibido el uso de plataformas de Inteligencia Artificial Generativa, de lo contrario la calificación del mismo no se tendrá en consideración.
    2. Presentación oral del trabajo grupal - En la última semana, todos los estudiantes que ha realizado trabajo grupal deberán exponer en clase el trabajo realizado. La valoración de la presentación grupal se realizará mediante rúbrica por parte del profesor (la rúbrica estará disponible en la plataforma docente con la antelación suficiente). La ponderación de la misma será del 20% del global.

EVALUACIÓN EXTRAORDINARIA

Constará de los siguientes elementos:

- Teoría – examen final escrito que constará de preguntas cortas y/o ejercicios sobre los temas teóricos de la Asignatura. Su ponderación a la calificación final será del 50%.
- Prácticas - Se hará una defensa de prácticas que consistirá en tres preguntas, una por cada práctica, varias preguntas sobre las actividades prácticas propuestas en la Guía de prácticas de la Asignatura (similares a las realizadas en la defensa de prácticas de la evaluación continua) y que se realizará en el laboratorio o con su ordenador personal. Para su realización, el estudiante deberá entregar previamente una memoria de prácticas, al igual que en la convocatoria ordinaria. La defensa de las prácticas supondrá un 40% de la calificación y la memoria, un 10%.

La calificación global corresponderá a la suma de las calificaciones obtenidas en teoría y prácticas. Por tanto, el resultado de la evaluación será una calificación numérica obtenida mediante la suma de las calificaciones correspondientes a teoría y práctica.

Para superar la Asignatura es necesario una calificación numérica igual o superior a 5 (sobre 10). Además, se establece el requisito adicional de que tanto las calificaciones de teoría como las de prácticas deben de ser mayores o iguales a 4 (sobre 10). En el caso de que el estudiante hubiese superado una de las partes (teoría o prácticas) en la convocatoria ordinaria, la calificación de la parte superada se mantendrá en esta convocatoria, si así lo desea.

EVALUACIÓN ÚNICA FINAL

La Evaluación Final Única constará de los siguientes elementos:

1. Examen final de Teoría – dicho examen será escrito y constará de preguntas cortas y/o ejercicios sobre los temas teóricos de la Asignatura. Su ponderación a la calificación final será del 50%.
2. Prácticas - Se hará una defensa de prácticas que consistirá en tres preguntas, una por cada práctica, varias preguntas sobre las actividades prácticas propuestas en la Guía de prácticas de la Asignatura (similares a las realizadas en la defensa de prácticas de la evaluación continua) y que se realizará en el laboratorio o con su ordenador personal. Para su realización, el estudiante deberá entregar previamente una memoria de prácticas, al igual que en la convocatoria ordinaria. La defensa de las prácticas supondrá un 40% de la calificación y la memoria, un 10%.

Para superar la asignatura es necesario una calificación numérica igual o superior a 5 (sobre 10). Además, se establece el requisito adicional de que tanto las calificaciones de teoría como las de prácticas deben de ser mayores o iguales a 4 (sobre 10).

INFORMACIÓN ADICIONAL

En todas las actividades se tendrá especial cuidado en adjuntar, en virtud del Art. 15 de la Normativa, una declaración explícita de autoría.