Explotación de Sistemas Software

Curso Académico: (2022 / 2023) **Fecha de revisión: 19-01-2023**

Departamento asignado a la asignatura: Departamento de Informática

Coordinador/a: GONZALEZ MANZANO, LORENA

Tipo: Obligatoria Créditos ECTS : 3.0

Curso : 1 Cuatrimestre : 1

REQUISITOS (ASIGNATURAS O MATERIAS CUYO CONOCIMIENTO SE PRESUPONE)

Ninguna

OBJETIVOS

Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación.

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.

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.

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.

Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando.

Comprender y aplicar métodos y técnicas de investigación de ciberataques a una instalación específica.

Elaborar concisa, clara y razonadamente documentos, planes y proyectos de trabajo en el ámbito de la Ciberseguridad.

Conocer las tendencias actuales en técnicas de ciberataque y las experiencias aprendidas en casos reales.

Conocer y aplicar los mecanismos de cifrado y esteganografiado pertinentes para proteger los datos residentes en un sistema o en tránsito por una red.

RESULTADOS DE APRENDIZAJE
Esta asignatura contribuye a los siguientes resultados de aprendizaje:

Explicar al menos una manera de introducirse en un sistema cuyas vulnerabilidades han sido detectadas.

Justificar mediante informes razonados las vulnerabilidades encontradas y el procedimiento detallado que se seguiría para la intrusión.

Explicar otras técnicas de ataque a un sistema que no sea susceptible de intrusión directa.

Proponer distintos ataques que se puedan realizar desde dentro de un sistema en un entorno controlado y explicar sus consecuencias.

Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación.

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.

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.

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.

Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando.

Comprender y aplicar métodos y técnicas de investigación de ciberataques a una instalación específica.

Elaborar concisa, clara y razonadamente documentos, planes y proyectos de trabajo en el ámbito de la Ciberseguridad.

Conocer las tendencias actuales en técnicas de ciberataque y las experiencias aprendidas en casos reales.

Conocer y aplicar los mecanismos de cifrado y esteganografiado pertinentes para proteger los datos residentes en un sistema o en tránsito por una red.

RESULTADOS DE APRENDIZAJE
Esta asignatura contribuye a los siguientes resultados de aprendizaje:

Explicar al menos una manera de introducirse en un sistema cuyas vulnerabilidades han sido detectadas.

Justificar mediante informes razonados las vulnerabilidades encontradas y el procedimiento detallado que se seguiría para la intrusión.

Explicar otras técnicas de ataque a un sistema que no sea susceptible de intrusión directa.

Proponer distintos ataques que se puedan realizar desde dentro de un sistema en un entorno controlado y explicar sus consecuencias.

DESCRIPCIÓN DE CONTENIDOS: PROGRAMA

Explotación de Sistemas Software:

1. Introducción
1.1. Vulnerabilidades en Componentes Software
1.2. Mecanismos de Explotación
1.3. Herramientas y Laboratorio de Análisis y Síntesis

2. Explotación de Vulnerabilidades en el Software
2.1. Violaciones de Memoria
2.2. Validación de Entrada de Datos e Inyección de Código
2.3. Condiciones de Carrera
2.4. Confusión de Privilegios
2.5. Explotación de la Interfaz de Usuario
2.6. Abuso de Funcionalidad y Configuraciones
2.7. Explotación de Cachés

3. Explotación de Sistemas Web
3.1. Vulnerabilidades en el Canal
3.2. Vulnerabilidades en el Servidor
3.3. Vulnerabilidades en el Navegador

4. Información sobre Vulnerabilidades y Formas de Explotación
4.1. Repositorios
4.2. Lenguajes y Estándares de Representación e Intercambio

ACTIVIDADES FORMATIVAS, METODOLOGÍA A UTILIZAR Y RÉGIMEN DE TUTORÍAS

ACTIVIDADES FORMATIVAS
Clase teórica
Prácticas de laboratorio
Tutorías
Trabajo individual del estudiante

METODOLOGÍAS DOCENTES
Exposiciones en clase del profesor con soporte de medios informáticos y audiovisuales, en las que se desarrollan los conceptos principales de la materia y se proporciona la bibliografía para complementar el aprendizaje de los alumnos.
Lectura de textos recomendados por el profesor: artículos de prensa, informes, manuales y/o artículos académicos, bien para su posterior discusión en clase o bien para ampliar y consolidar los conocimientos de la asignatura.
Elaboración de trabajos e informes de manera individual o en grupo.

SISTEMA DE EVALUACIÓN

Peso porcentual del Examen Final:	40
Peso porcentual del resto de la evaluación:	60

Evaluación continua:
- Prácticas de laboratorio (60%)
- Examen final (40%).
La suma de ambas parte se realizará siempre que se supere del examen final

En la convocatoria extraordinaria se plantean los siguientes casos:
-El alumno mantiene la nota de prácticas de laboratorio: se sigue los mismos criterios que en la convocatoria ordinaria.
-El alumno decide no mantener las notas de prácticas: se evaluarán las prácticas (40%) y la teoría (60%). Ambas partes se deben aprobar individualmente.

BIBLIOGRAFÍA BÁSICA

- Eagle, C The IDA pro book: the unofficial guide to the world's most popular disassembler, No Starch Press, 2008

- Klein, T A Bug Hunter's Diary, No Starch Press, 2011

- Ross Anderson Security engineering, John Wiley & Sons, 2008

- Stuttard, D., & Pinto, M. The web application hacker's handbook: discovering and exploiting security flaws, John Wiley & Sons, 2008

BIBLIOGRAFÍA COMPLEMENTARIA

- Anley, C., Heasman, J., Lindner, F., & Richarte, G. The Shellcoder's Handbook: Discovering and Exploiting Security Holes, John Wiley & Sons., 2011

- Dhanjani, N., Rios, B., & Hardin, B. Hacking: The next generation, O'Reilly Media, Inc., 2009

- Drake, J. J., Lanier, Z., Mulliner, C., Fora, P. O., Ridley, S. A., & Wicherski, G. Android Hacker's Handbook, John Wiley & Sons, 2014

- Gilberto Najera-Gutierrez Kali Linux Web Penetration Testing Cookbook: Identify, Exploit, and Prevent Web Application Vulnerabilities with Kali Linux 2018. x, Packt Publishing Ltd., 2018

- Hope, P., & Walther, B. Web Security Testing Cookbook: Systematic Techniques to Find Problems Fast, O'Reilly Media, Inc, 2008

- Miller, C., Blazakis, D., DaiZovi, D., Esser, S., Iozzo, V., & Weinmann, R. P IOS Hacker's Handbook, John Wiley & Sons, 2012

RECURSOS ELECTRÓNICOS BÁSICOS

- OWASP . OWASP: https://www.owasp.org/

- Safari Books . Safari Books: http://proquest.safaribooksonline.com