Análisis e Ingeniería de Malware

Curso Académico: (2019 / 2020) **Fecha de revisión: 26-04-2020**

Departamento asignado a la asignatura: Departamento de Informática

Coordinador/a: ESTEVEZ TAPIADOR, JUAN MANUEL

Tipo: Optativa Créditos ECTS : 3.0

Curso : 1 Cuatrimestre : 2

REQUISITOS (ASIGNATURAS O MATERIAS CUYO CONOCIMIENTO SE PRESUPONE)

- Explotación de Sistemas Software
- Comunicaciones Seguras
- Protección de Datos
- Sistemas de Ciberdefensa
- Técnicas de Ciberataque
- Ciberdelitos, Ciberterrorismo y Ciberguerra

OBJETIVOS

COMPETENCIAS
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 la normativa técnica y las disposiciones legales de aplicación en la materia de ciberseguridad, sus implicaciones en el diseño de sistemas y en la aplicación de herramientas de seguridad.

Analizar y detectar anomalías y firmas de ataques en los sistemas y redes.

Analizar y detectar técnicas de ocultación de ataques a sistemas y redes.

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.

DESCRIPCIÓN DE CONTENIDOS: PROGRAMA

1 Introducción
1.1 Conceptos Básicos y Evolución
1.2 Técnicas de Análisis de Malware
1.3 El Laboratorio

2 Técnicas Básicas de Análisis
2.1 La Vida de un Ejecutable
2.2 Análisis Estático Básico
2.3 Análisis Dinámico Básico

3 Técnicas Avanzadas de Análisis
3.1 Desensamblado x86
3.2 Construcciones C en Ensamblador
3.3 IDA Pro
3.4 La API de Windows
3.5 Depuración de binarios

4 Comportamientos
4.1 Cargadores
4.2 Puertas traseras
4.3 Espías
4.4 Persistencia
4.5 Ejecución encubierta
4.6 Codificación
4.7 Anti-desensamblado
4.8 Anti-depurado
4.9 Anti-virtualización
4.10 Packers

ACTIVIDADES FORMATIVAS, METODOLOGÍA A UTILIZAR Y RÉGIMEN DE TUTORÍAS

ACTIVIDADES FORMATIVAS

- Clases teórico prácticas
- Prácticas de laboratorio
- Tutorías
- Trabajo en grupo
- 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 crítica de textos recomendados por el profesor de la asignatura: Artículos de prensa, informes, manuales y/o artículos académicos, bien para su posterior discusión en clase, bien para ampliar y consolidar los conocimientos de la asignatura.

- Resolución de casos prácticos, problemas, etc. planteados por el profesor de manera individual o en grupo.

- Exposición y discusión en clase, bajo la moderación del profesor de temas relacionados con el contenido de la materia, así como de casos prácticos .

- Elaboración de trabajos e informes de manera individual o en grupo.

SISTEMA DE EVALUACIÓN

Evaluación continua (60% de la nota final). Desglosada como sigue:
- Práctica de análisis (40%)
- Tests (20%)

Examen final (40% de la nota final)

La evaluación en la convocatoria extraordinaria se realizará de la siguiente manera:
- Un único examen con peso del 40% si la evaluación continua está aprobada (es decir, mayor o igual al 25% de la nota máxima posible).
- Un único examen con peso del 100% si la evaluación continua está suspensa. Este examen incluirá preguntas prácticas.

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

BIBLIOGRAFÍA BÁSICA

- Michael Ligh, Steven Adair, Blake Harstein, Matthew Richard Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code, Wiley, 2010
- Michael Sikorski, Andrew Honig Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software, No Starch Press, 2012