## DESCRIPCIÓN DE LA ASIGNATURA

| | |
|---|---|
| **Grado/Máster en:** | Master Universitario en INGENIERÍA INFORMÁTICA por la Universidad de Málaga |
| **Centro:** | Escuela Técnica Superior de Ingeniería Informática |
| **Asignatura:** | ANÁLISIS DE MALWARE |
| **Código:** | 202 |
| **Tipo:** | Optativa |
| **Materia:** | ESPECIALIDAD EN CIBERSEGURIDAD |
| **Módulo:** | COMPLEMENTOS EN TECNOLOGÍAS INFORMÁTICAS |
| **Experimentalidad:** | |
| **Idioma en el que se imparte:** | Español |
| **Curso:** | 2 |
| **Semestre:** | 1 |
| **Nº Créditos** | 4,5 |
| **Nº Horas de dedicación del estudiante:** | 112,5 |
| **Nº Horas presenciales:** | 33,8 |
| **Tamaño del Grupo Grande:** | |
| **Tamaño del Grupo Reducido:** | |
| **Página web de la asignatura:** | |

## EQUIPO DOCENTE

**Departamento:** LENGUAJES Y CIENCIAS DE LA COMPUTACIÓN

**Área:** LENGUAJES Y SISTEMAS INFORMÁTICOS

| Nombre y Apellidos | Mail | Teléfono Laboral | Despacho | Horario Tutorías |
|---|---|---|---|---|
| Coordinador/a: JOSE ANTONIO ONIEVA GONZALEZ | onieva@uma.es | 952132898 | 3.2.40 - E.T.S.I. INFORMÁTICA | |

## RECOMENDACIONES Y ORIENTACIONES

Students are expected to have basic skills with the Windows architecture, programming and assembler code.

## CONTEXTO

Technology is undoubtedly a vital part of modern everyday life in any of its forms (mobile phones, tablets, computers, etc.). Unfortunately, the increasingly interconnected nature of the modern world has also allowed the spread of malicious software, or "malware", ranging from annoying adware to malware used as a technological weapon by different states (eg Stuxnet). As a result, the ability to detect, analyse, understand, control, and eradicate malware is an increasingly important issue at all levels of business and Defense. This course will introduce students to malware analysis techniques through readings and interactive analysis of real samples.
This course is divided into four main blocks. The first block provides the basis for the students to understand the existing types of malware, techniques and environments in which the analysis of malware can take place. The second block introduces static analysis, while the third block focuses on active running malware analysis. The four block introduces the student to anti-analysis techniques used by some of the existing malware.

## COMPETENCIAS

**1 Competencias generales y básicas.**

**Competencias básicas**

**1.1** CB6 - 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

**1.2** 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

**1.3** 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

**1.4** 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

**1.5** 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**

**1.8** CG8 - Capacidad para la aplicación de los conocimientos adquiridos y de resolver problemas en entornos nuevos o poco conocidos dentro de contextos más amplios y mulitidisciplinares, siendo capaces de integrar estos conocimientos.

**2 Competencias específicas.**

**2 Competencias específicas.**

**2.3** ETI3 - Capacidad para asegurar, gestionar, auditar y certificar la calidad de los desarrollos, procesos, sistemas, servicios, aplicaciones y productos informáticos.

**2.4** ETI4 - Capacidad para diseñar, desarrollar, gestionar y evaluar mecanismos de certificación y garantía de seguridad en el tratamiento y acceso a la información en un sistema de procesamiento local o distribuido.

**3 Competencias transversales.**

**3.2** CT2 - Capacidad para identificar estrategias, herramientas y métodos que responden a situaciones de éxito que pueden ser abordadas con los recursos disponibles.

## CONTENIDOS DE LA ASIGNATURA

**Malware Analysis Introduction**

- Malware Analysis Techniques
- Types of Malware
- Malware Analysis in controlled environments (Sandboxes, Virtual Machines, network configuration and tools for malware analysis)

**File Static Analysis**

- Hashing: a fingerprint for malware.
- Strings
- Packed and Obfuscated Malware
- PEF, DLLs and functions

**Dynamic Analysis**

- Monitoring and Registry Snapshots
- Reverse Engineering
- Using a disassembler and debugger

**Anti-analysis techniques**

- Anti-reversing
- Anti-VM
- Anti-debugging

## ACTIVIDADES FORMATIVAS

**Actividades presenciales**

**Actividades expositivas**
Lección magistral

**Actividades prácticas en instalaciones específicas**
Prácticas en aula informática

**Actividades no presenciales**

**Actividades de documentación**
Otras actividades de documentación

**Actividades de elaboración de documentos**
Elaboración de informes

**Actividades prácticas**
Estudios de casos
Desarrollo y evaluación de proyectos
Resolución de ejercicios en ordenador

**Estudio personal**
Estudio personal

## ACTIVIDADES DE EVALUACIÓN

**Actividades de evaluación no presenciales**

**Actividades de evaluación no presenciales**

**Actividades de evaluación de la asignatura con participación alumnos**

Cuestionario/encuesta
Informe del estudiante

**Actividades de evaluación presenciales**

**Actividades de evaluación del estudiante**

Realización de trabajos y/o proyectos
Participación en clase

## RESULTADOS DE APRENDIZAJE / CRITERIOS DE EVALUACIÓN

It is expected that, upon completion of the course, the students will have acquired the following skills:
- RA1. Perform an independent malware analysis using static analysis techniques. This skill allows for the acquisition of CG08, CT2.
- RA2. Perform an independent malware analysis using dynamic techniques. This skill allows for the acquisition of CG08, CT2.
- RA3. Knowledge about the executable, DLLs and Windows APIs, as well as the different techniques of analysis and malware. This skill allows for the acquisition of CG08, CT2.
- RA4. Extract malware's indicators associated with the host and the network. This skill allows for the acquisition of ETI3 and ET4.
- RA5. Apply techniques and concepts to unpack, extract, decrypt or deal with anti-analysis techniques in future malware samples. This skill allows for the acquisition of CB6, CB7.
- RA6. Master standard malware analysis tools. This skill allows for the acquisition of CG08, CT2.
- RA7. Have a critical view about contemporary Malware, state of the art and current (malicious or not) applications. This skill allows for the acquisition of CB8.

All skills contribute partially to the greater competences identified as ETI3 and ET4.

## PROCEDIMIENTO DE EVALUACIÓN

Evaluation of the contents of the course will be mainly based on projects and practical assignments developed by the student along the semester. Each chapter will have at least one assignment such that each of these assignments will evaluate the skills identified for this subject. Therefore:
- Assignments for chapter 1 will evaluate RA3, RA7
- Assignments for chapter 2 will evaluate RA1, RA3, RA4, RA5.
- Assignments for chapter 3 will evaluate RA2, RA3, RA4, RA6.
- Assignments for chapter 4 will evaluate RA5.

The contribution of each evaluation activity to the final score will be:
- 90 pts Assignments.
- 10 pts Test
- 10 pts Class participation and involvement.

A student is assumed to pass if his/her final score is equal or greater than 50 pts.

The assignments will be evaluated by the student's reports that follow a pre-established rubric template as well as on-site presentation of his/her results. This type of evaluation activities allow for the certification of competences CB09 and CB10 apart from those competences previously identified within each proposed skill (RAs).

Should the student need to pass the course in September or further, he/she will have to obtain 50 out of 100 points in a practical exercise.

## BIBLIOGRAFÍA Y OTROS RECURSOS

**Básica**

- Michael Hale Ligh, Steven Adair, Blake Hartstein and Matthew Richard (2011). Malware Analyst¿s. Cookbook and DVD. Tools and techniques for fighting malicious code.
- Michael Sikorski and Andrew Honig (2012). Practical Malware Analysis. No starch press

## DISTRIBUCIÓN DEL TRABAJO DEL ESTUDIANTE

### ACTIVIDAD FORMATIVA PRESENCIAL

| Descripción | Horas | Grupo grande | Grupos reducidos |
|---|---|---|---|
| Lección magistral | 11 | ☑ | ☐ |
| Prácticas en aula informática | 22,8 | ☑ | ☐ |
| TOTAL HORAS ACTIVIDAD FORMATIVA PRESENCIAL | 33,8 | | |

### ACTIVIDAD FORMATIVA NO PRESENCIAL

| Descripción | Horas | Grupo grande | Grupos reducidos |
|---|---|---|---|
| Desarrollo y evaluación de proyectos | 18 | | |
| Elaboración de informes | 20 | | |
| Otras actividades de documentación | 6 | | |
| Estudios de casos | 6 | | |
| Estudio personal | 6,4 | | |
| Resolución de ejercicios en ordenador | 11 | | |
| **TOTAL HORAS ACTIVIDAD FORMATIVA NO PRESENCIAL** | **67,45** | | |
| **TOTAL HORAS ACTIVIDAD EVALUACIÓN** | **11,25** | | |
| **TOTAL HORAS DE TRABAJO DEL ESTUDIANTE** | **112,5** | | |