



## DATOS IDENTIFICATIVOS

### Análisis de malware

Asignatura	Análisis de malware			
Código	V05M175V01204			
Titulación	Máster Universitario en Ciberseguridad			
Descriptores	Creditos ECTS	Seleccione	Curso	Cuatrimestre
	5	OB	1	2c
Lengua Impartición	Inglés			
Departamento	Ingeniería telemática			
Coordinador/a	Burguillo Rial, Juan Carlos			
Profesorado	Burguillo Rial, Juan Carlos			
Correo-e	jrial@uvigo.es			
Web				
Descripción general	El malware utiliza los sistemas y las redes de comunicaciones para propagar virus, secuestrar dispositivos o robar datos confidenciales. El objetivo de esta asignatura es dotar al alumno de la capacidad para analizar, detectar y eliminar malware. Para ello se explorarán y ejemplificarán, de forma práctica y con casos reales, las técnicas actuales de ocultación y persistencia de malware, así como las tendencias más novedosas para su detección y eliminación.			

## Competencias

Código	
A1	Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y aplicación de ideas, a menudo en un contexto de investigación.
B1	Tener capacidad de análisis y síntesis. Tener capacidad para proyectar, modelar, calcular y diseñar soluciones de seguridad de la información, las redes y/o los sistemas de comunicaciones en todos los ámbitos de aplicación
C8	Tener capacidad para concebir, diseñar, poner en práctica y mantener sistemas de ciberseguridad
C11	Reunir e interpretar datos relevantes dentro del área de la seguridad informática y de las comunicaciones.
C13	Tener capacidad de análisis, detección y eliminación de vulnerabilidades, y del malware susceptible de utilizarlas, en sistemas y redes
D4	Valorar la importancia de la seguridad de la información en el avance socioeconómico de la sociedad
D5	Tener capacidad para comunicarse oralmente y por escrito en inglés.

## Resultados de aprendizaje

Resultados previstos en la materia	Resultados de Formación y Aprendizaje
Analizar, detectar y eliminar malware en sistemas y redes.	B1 C11 C13 D5
Conocer, detectar y luchar contra las técnicas de ocultación y persistencia de malware en sistemas y redes.	A1 B1 C8 C11 C13 D5
Estudiar sistemas y redes para detectar y eliminar las vulnerabilidades susceptibles de ser utilizadas por el malware.	B1 C8 C11 C13 D5

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

A1  
B1  
D4  
D5

## Contenidos

Tema	
Introducción al análisis e ingeniería de malware.	a) ¿Qué es el malware? b) ¿Cómo detectarlo y eliminarlo? c) ¿En qué consiste la ingeniería de malware?
Tipos de malware.	a) Estructura. b) Componentes. c) Vectores de infección.
Ingeniería de malware.	a) Técnicas de propagación. b) Procesos de infección. c) Persistencia del malware. d) Técnicas de ocultación.
Ingeniería inversa de malware.	a) ¿Cómo analizar e inferir el funcionamiento del malware? b) Comprensión del funcionamiento de nuevos tipos de malware.
Herramientas de análisis de malware.	a) Herramientas para la detección de malware. b) Herramientas para la eliminación de malware.

## Planificación

	Horas en clase	Horas fuera de clase	Horas totales
Actividades introductorias	1	0	1
Lección magistral	13	36	49
Prácticas de laboratorio	15	45	60
Foros de discusión	0	1	1
Estudio de casos	4	4	8
Examen de preguntas objetivas	1	4	5
Pruebas de respuesta corta	1	0	1

\*Los datos que aparecen en la tabla de planificación son de carácter orientativo, considerando la heterogeneidad de alumnado

## Metodologías

	Descripción
Actividades introductorias	Hacer una introducción genérica a los objetivos, contenidos globales generales de la asignatura y resultados esperados. Esta actividad será realizada individualmente.
Lección magistral	Se introducen los distintos temas de la asignatura proporcionando el material docente necesario para su seguimiento.  Con esta metodología se trabajan las competencias CB1, CG1, CE8, CE11, CE13, CT4 y CT5. Esta actividad será realizada individualmente.
Prácticas de laboratorio	Se realizan prácticas de laboratorio para comprender mejor los contenidos vistos en las clases magistrales.  Con esta metodología se trabajan las competencias CG1, CE8, CE11, CE13 y CT5. Algunas prácticas se realizarán de forma individual y otras en grupos (dependiendo del número de estudiantes).
Foros de discusión	Los estudiantes deben participar en el foro dentro de la plataforma TEMA en FAITIC.  Con esta metodología se trabajan las competencias CE8, CE11, CE13 y CT5. Esta actividad será realizada individualmente.
Estudio de casos	Durante las clases magistrales y/o las prácticas de laboratorio se estudiarán casos típicos de problemas de seguridad conocidos.  Con esta metodología se trabajan las competencias CG1, CE11, CE13 y CT5. Esta actividad se realizará en grupo.

## Atención personalizada

Metodologías	Descripción
--------------	-------------

Actividades introductorias	En las actividades formativas prácticas y tutorías, los profesores de la asignatura ofrecerán guías de atención personalizada a cada alumno sobre las tareas a realizar, con el fin de orientar el planteamiento y la metodología de elaboración. También se ofrecerá información de coordinación con otros contenidos y asignaturas del programa de estudios. Se recomienda consultar las dudas al profesorado a lo largo de todo el desarrollo de la materia, tanto para la comprensión de los fundamentos como para la realización de los proyectos y actividades de evaluación.
Lección magistral	En las actividades formativas prácticas y tutorías, los profesores de la asignatura ofrecerán guías de atención personalizada a cada alumno sobre las tareas a realizar, con el fin de orientar el planteamiento y la metodología de elaboración. También se ofrecerá información de coordinación con otros contenidos y asignaturas del programa de estudios. Se recomienda consultar las dudas al profesorado a lo largo de todo el desarrollo de la materia, tanto para la comprensión de los fundamentos como para la realización de los proyectos y actividades de evaluación.
Estudio de casos	En las actividades formativas prácticas y tutorías, los profesores de la asignatura ofrecerán guías de atención personalizada a cada alumno sobre las tareas a realizar, con el fin de orientar el planteamiento y la metodología de elaboración. También se ofrecerá información de coordinación con otros contenidos y asignaturas del programa de estudios. Se recomienda consultar las dudas al profesorado a lo largo de todo el desarrollo de la materia, tanto para la comprensión de los fundamentos como para la realización de los proyectos y actividades de evaluación.
Prácticas de laboratorio	En las actividades formativas prácticas y tutorías, los profesores de la asignatura ofrecerán guías de atención personalizada a cada alumno sobre las tareas a realizar, con el fin de orientar el planteamiento y la metodología de elaboración. También se ofrecerá información de coordinación con otros contenidos y asignaturas del programa de estudios. Se recomienda consultar las dudas al profesorado a lo largo de todo el desarrollo de la materia, tanto para la comprensión de los fundamentos como para la realización de los proyectos y actividades de evaluación.
Foros de discusión	En las actividades formativas prácticas y tutorías, los profesores de la asignatura ofrecerán guías de atención personalizada a cada alumno sobre las tareas a realizar, con el fin de orientar el planteamiento y la metodología de elaboración. También se ofrecerá información de coordinación con otros contenidos y asignaturas del programa de estudios. Se recomienda consultar las dudas al profesorado a lo largo de todo el desarrollo de la materia, tanto para la comprensión de los fundamentos como para la realización de los proyectos y actividades de evaluación.

## Evaluación

	Descripción	Calificación	Resultados de Formación y Aprendizaje			
Prácticas de laboratorio	Los alumnos realizarán prácticas de laboratorio, donde se trabajará con los conceptos estudiados en las clases teóricas.	45	A1	B1	C8 C11 C13	D5
Foros de discusión	Los estudiantes deben participar en el foro de la plataforma TEMA.	5	A1	B1	C11 C13	D4 D5
Examen de preguntas objetivas	Tres test de evaluación sucesivos para el contenido parcial de la materia impartida hasta ese momento. Los tests serán individuales y de tiempo limitado.	45	A1	B1	C11 C13	D5
Pruebas de respuesta corta	Durante las clases magistrales se realizarán preguntas a los estudiantes para conocer su comprensión del tema bajo estudio.	5	A1		C11 C13	D5

## Otros comentarios sobre la Evaluación

Los elementos que forman parte de la evaluación de la asignatura son los siguientes:

- **Cuestionarios:** a lo largo del curso se realizarán 3 cuestionarios que aportarán un 15% de la nota final (cada uno).
- **Prácticas de laboratorio:** cada alumno deberá realizar individualmente y/o en grupo un conjunto de prácticas propuestas en el laboratorio que aportará un 45% de la nota final.
- **Participación en clase:** los estudiantes participarán y discutirán sobre las exposiciones realizadas por el profesor y esto contribuirá hasta un 5% a la nota final.
- **Participación en el foro:** los estudiantes deben participar en el foro de la asignatura, de forma individual, y esto contribuirá hasta un 5% a la nota final. Para conseguir dicho porcentaje se deben proporcionar, como mínimo, dos contribuciones relevantes.

Así tenemos:

**Nota Final** = Cuestionarios (3x15 = 45%) + Prácticas de lab. (45%) + Participación en clase (5%) + Foro (5%) = 100%.

Los estudiantes deben obtener al menos 4 puntos sobre 10 en la nota de los cuestionarios y la práctica para poder calcular la nota media final. Si cualquiera de estas notas estuviese por debajo de 4, entonces la nota final obtenida nunca será superior a un 4 sobre 10.

La planificación de las diferentes pruebas de evaluación intermedia se aprobará en una Comisión Académica de Grado (CAG) y estará disponible al principio del cuatrimestre.

En caso de detección de plagio en cualquiera de las pruebas (pruebas cortas, exámenes parciales o examen final), la

calificación final será de SUSPENSO (0) y el hecho será comunicado a la dirección del Centro para los efectos oportunos. Siguiendo las directrices propias de la titulación se ofrecerá a los alumnos que cursen esta materia dos sistemas de evaluación: evaluación continua y evaluación única (fin del cuatrimestre).

**Evaluación continua (EC):** el estudiante sigue la evaluación continua desde el momento en que se presenta a dos cuestionarios de la asignatura. Un alumno que opta por la evaluación continua se considera que se ha presentado a la asignatura, independientemente de que se presente o no a la evaluación única.

**Primera oportunidad:** el alumno deberá realizar un examen teórico que sustituye a los cuestionarios realizados a lo largo del curso, además de entregar las prácticas y los trabajos equivalentes a los que se han realizado como parte de la EC.

**Segunda oportunidad:** el alumno deberá realizar la parte que no haya superado. En el caso de no haber superado los cuestionarios deberá realizar un examen equivalente.

Los trabajos y tareas prácticas propuestas y realizadas en este curso no son recuperables y sólo son válidas para el curso actual.

---

## **Fuentes de información**

### **Bibliografía Básica**

Michael Hale Ligh, Andrew Case, Jamie Levy, Aaron Walters, **The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory**, 1, John Wiley & Sons Inc, 2014

### **Bibliografía Complementaria**

Michael Sikorski / Andrew Honig, **Practical Malware Analysis**, 1, William Pollock, 2012

---

## **Recomendaciones**

### **Asignaturas que se recomienda cursar simultáneamente**

Análisis forense de equipos/V05M175V01207

Fortificación de sistemas operativos/V05M175V01202

Seguridad en dispositivos móviles/V05M175V01206

### **Asignaturas que se recomienda haber cursado previamente**

Seguridad de aplicaciones/V05M175V01104