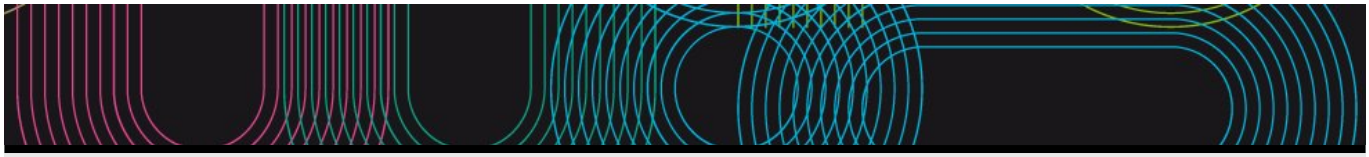

DATOS IDENTIFICATIVOS				
Análisis de malware				
Asignatura	Análisis de malware			
Código	V05M175V11109			
Titulacion	Máster Universitario en Ciberseguridad			
Descriptores	Creditos ECTS	Seleccione	Curso	Cuatrimestre
	5	OB	1	1c
Lengua Impartición	Inglés			
Departamento	Dpto. Externo Ingeniería telemática			
Coordinador/a	Burguillo Rial, Juan Carlos			
Profesorado	Burguillo Rial, Juan Carlos Hernández Pereira, Elena María Rivas López, Jose Luis			
Correo-e	jrial@uvigo.es			
Web	http://https://moovi.uvigo.gal			
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. Esta asignatura se impartirá en inglés.			

Resultados de Formación y Aprendizaje	
Código	
B2	Conocer las técnicas de ocultación y persistencia de malware; así como las tendencias actuales en malware mediante el estudio de casos reales.
C2	Detectar y eliminar las vulnerabilidades susceptibles a malware, así como malware, en sistemas y redes de comunicaciones, así como evadir técnicas de ocultación y persistencia de malware.
D3	Trabajar como analista de malware, para proteger aplicaciones, así como analizar su seguridad en cualquier área de aplicación.
D6	Identificar vulnerabilidades en un sistema real, así como variar sus parámetros y configurarlo para su protección frente a ellas; limitando así la exposición a amenazas conocidas.

Resultados previstos en la materia	Resultados de Formación y Aprendizaje
Proporcionar al estudiante la capacidad para analizar, detectar y eliminar malware.	B2 C2
Explorar y evaluar, de forma práctica y con estudios de caso, las técnicas utilizadas hoy en día para esconder malware.	D3
Aprender a encontrar vulnerabilidades en sistemas reales, así como proteger y limitar la exposición a amenazas conocidas.	D6

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	2	2	4
Lección magistral	10	30	40
Prácticas de laboratorio	15	40	55
Foros de discusión	0	2	2
Estudio de casos	5	4	9
Examen de preguntas objetivas	2	4	6
Resolución de problemas y/o ejercicios	3	6	9

*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 el conocimiento B2, la destreza C2 y la competencia D6. 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 trabaja el conocimiento B2, la destreza C2 y las competencias D3 y D6. 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 MOOVI. Con esta metodología se trabaja el conocimiento B2 y la competencia D6. Esta actividad será realizada individualmente.
Estudio de casos	Durante las clases magistrales se realizarán presentaciones de casos de estudio típicos de amenazas, problemas de seguridad conocidos o tecnologías actuales. Con esta metodología se trabaja el conocimiento B2, y las competencias D3 y D6. 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. El alumnado podrá consultar y solicitar tutorías a través de la plataforma Moovi (https://moovi.uvigo.gal).
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. El alumnado podrá consultar y solicitar tutorías a través de la plataforma Moovi (https://moovi.uvigo.gal).

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. El alumnado podrá consultar y solicitar tutorías a través de la plataforma Moovi (https://moovi.uvigo.gal).
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. El alumnado podrá consultar y solicitar tutorías a través de la plataforma Moovi (https://moovi.uvigo.gal).
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. El alumnado podrá consultar y solicitar tutorías a través de la plataforma Moovi (https://moovi.uvigo.gal).

Evaluación

	Descripción	Calificación	Resultados de Formación y Aprendizaje
Prácticas de laboratorio	Los alumnos realizarán prácticas de laboratorio (3 x 15% = 45%), donde se trabajará con los conceptos estudiados en las clases teóricas.	45	
Foros de discusión	Los estudiantes deben participar en el foro de la plataforma MOOVI.	5	
Estudio de casos	El alumnado realizará presentaciones de casos de estudio, seleccionados por ellos, para analizar amenazas actuales.	15	
Examen de preguntas objetivas	Dos test de evaluación sucesivos para el contenido parcial de la materia impartida hasta ese momento. Los tests serán individuales y de tiempo limitado.	30	
Resolución de problemas y/o ejercicios	Durante las clases magistrales se realizarán preguntas a los estudiantes para conocer su comprensión del tema bajo estudio.	5	

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 dos cuestionarios que aportarán un 15% de la nota final (cada uno).
- **Presentación de casos de estudio**: cada alumno (de forma individual o en grupo) deberá realizar una presentación original que aportará un 15% de la nota final.
- **Prácticas de laboratorio**: cada alumno deberá realizar individualmente y/o en grupo un conjunto de prácticas propuestas en el laboratorio (por defecto 3 prácticas con un peso de 15% cada una) 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 (2x15 = 30%) + Presentación de caso de estudio (15%) + 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, los casos de estudio y las prácticas 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 4.9 sobre 10.

La planificación de las diferentes pruebas de evaluación intermedia se aprobaraa en una Comisión Académica de Máster (CAM) y estará disponible al principio del cuatrimestre.

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: 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.

Evaluación global: 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 evaluación continua.

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

Convocatoria de fin de carrera: el alumno deberá realizar la parte que no haya superado. En el caso de no haber superado los cuestionarios deberá realizar un examen equivalente.

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.

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

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

Bibliografía Complementaria

Recomendaciones

Asignaturas que se recomienda cursar simultáneamente

Análisis forense/V05M175V11216