CENTRO UNIVERSITARIO DE TECNOLOGÍA Y ARTE DIGITAL

PLANIFICACIÓN DE LA DOCENCIA UNIVERSITARIA

GUÍA DOCENTE

Análisis de Malware

1. DATOS DE IDENTIFICACIÓN DE LA ASIGNATURA.

Título:	Grado en Ingeniería del Software
Facultad:	Centro Universitario de Tecnología y Arte Digital (U-TAD)
Materia:	Ciberseguridad
Denominación de la asignatura:	Análisis de Malware
Curso:	4
Cuatrimestre:	2
Carácter:	Obligatoria de mención
Créditos ECTS:	6
Modalidad/es de enseñanza:	Híbrido Presencial
Idioma:	Español
Profesor/a:	Rafael Vida Delgado
E-mail:	Rafael.Vida@u-tad.com
Teléfono:	

2. DESCRIPCIÓN DE LA ASIGNATURA

2.1 Descripción de la materia

Esta materia incluye los conocimientos y las competencias de la seguridad informática que requeriría un profesional de nivel de graduado. Se dedica al estudio de la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida en una computadora o circulante a través de las redes de computadoras. Para ello, los alumnos adquirirán los conocimientos relacionados con las técnicas de ataque y defensa de sistemas informáticos, así como las actividades relacionadas con el análisis forense de sistemas y el análisis del malware.

2.2 Descripción de la asignatura

Esta materia se dedica al estudio de las técnicas de análisis de malware, tanto de los procesos de infección como de propagación, además de revisar la estructura típica de los binarios para Unix y Windows, ademas de estudiar los procesos típicos de ocultación del malware. Se estudian procesos herramientas, tecnologías para realizar ese análisis y se estudiarán laboratorios de malware en varios escenarios.

3. COMPETENCIAS Y RESULTADOS DE APRENDIZAJE

3.1. COMPETENCIAS (Genéricas, específicas y transversales)

Competencias Básicas y Generales
CB1: Que los estudiantes hayan demostrado poseer y comprender conocimientos en un área de estudio que parte de la base de la educación secundaria general, y se suele encontrar a un nivel que, si bien se apoya en libros de texto avanzados, incluye también algunos aspectos que implican conocimientos procedentes de la vanguardia de su campo de estudio. CB2: Que los estudiantes sepan aplicar sus conocimientos a su trabajo o vocación de una forma profesional y posean las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro de su área de estudio. CB3: Que los estudiantes tengan la capacidad de reunir e interpretar datos relevantes (normalmente dentro de su área de estudio) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética. CB4: Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado. CB5: Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía CG1 - Capacidad para entender, planificar y resolver problemas a través del desarrollo de soluciones informáticas. CG2 - Desarrollo de soluciones informáticas respetuosas con el medio ambiente, los deberes sociales y los recursos naturales, además de cumplir con la legislación y la ética CG3 - Conocimiento de los fundamentos científicos aplicables a la resolución de problemas informáticos CG4 - Capacidad para simplificar y optimizar los sistemas informáticos atendiendo a la comprensión de su complejidad CG9 - Capacidad para aprender, modificar y producir nuevas tecnologías informáticas CG10 - Uso de técnicas creativas para la realización de proyectos informáticos CG11 - Capacidad de buscar, analizar y gestionar la información para poder extraer conocimiento de la misma
Competencias Específicas
CE10 - Capacidad para manejar un gestor de versiones de código y generar la documentación de una aplicación de forma automática.
Competencias Transversales
CT1 - Conocimiento de la definición, el alcance y la puesta en práctica de los fundamentos de las metodologías de gestión de proyectos de desarrollo tecnológico CT2 - Conocimiento de los principales agentes del sector y del ciclo de vida completo de un proyecto de desarrollo y comercialización de contenidos digitales CT4 - Capacidad de actualización del conocimiento adquirido en el manejo de herramientas y tecnologías digitales en función del estado actual del sector y de las tecnologías empleadas CT5 - Desarrollo de las habilidades necesarias para el emprendimiento digital.

4. CONTENIDOS

4.1. Temario de la asignatura

I. Anatomía de un binario
   1. Formato ELF
   2. Formato PE

II. Análisis básico de binarios
   1. Análisis estático
   2. Análisis dinámico

III. Análisis avanzado de binarios:
   1. Desensamblador
   2. Depurador
   3. Análisis de dependencias windows

IV. Técnicas de inyección para ELF
   1. Control de desvordamientos
   2. inyección de código

V. Herramientas avanzadas
   1. Introducción a la aplicación de ML a análisis de malware
   2. repaso de Python
   3. Introducción a redes complejas

VI. Identificación de campañas de ataque

VII. Detección de malware mediante técnicas de Machine Learning

VIII. Evaluación de sistemas de detección de malware

IX. Construcción de detectores con Machine Learning
   1. Laboratorio evaluable

X. Visualización de dinámica de malware
   1. Técnicas de visualización
   2. Herramientas

XI. Construcción de detector de malware con redes neuronales
   1. Redes neuronales
   2. Entrenamiento del sistema
   3. Pruebas de detección de malware real.

4.2. Desarrollo temporal

UNIDADES DIDÁCTICAS / TEMAS	PERÍODO TEMPORAL
1 Anatomía de un binario	Semana 1
2 Análisis básico de binarios	Semanas 2
3 Análisis avanzado de binarios:	Semanas 3
4 Técnicas de inyección para ELF	Semana 4
5 Herramientas avanzadas	Semanas 5, 6
6 Identificación de campañas de ataque	Semanas 7

7 Detección de malware mediante técnicas de Machine Learning	Semanas 8
8 Evaluación de sistemas de detección de malware	Semanas 9
9 Construcción de detectores con Machine Learning	Semanas 10,11
10 Visualización de dinámica de malware	Semanas 12
11 Construcción de detector de malware con redes neuronales	Semanas 13,14

5. ACTIVIDADES FORMATIVAS Y MODALIDADES DE ENSEÑANZAS

5.1. Modalidades de enseñanza

La asignatura se desarrollará a través de los siguientes métodos y técnicas generales, que se aplicarán diferencialmente según las características propias de la asignatura:

- **Método expositivo/Lección magistral:** el profesor desarrollará, mediante clases magistrales y dinámicas los contenidos recogidos en el temario.
- **Estudio de casos:** análisis de casos reales relacionados con la asignatura.
- **Resolución de ejercicios y problemas:** los estudiantes desarrollarán las soluciones adecuadas aplicando procedimientos de transformación de la información disponible y la interpretación de los resultados.
- **Aprendizaje basado en problemas:** utilización de problemas como punto de partida para la adquisición de conocimientos nuevos.
- **Aprendizaje orientado a proyectos:** se pide a los alumnos que, en pequeños grupos, planifiquen, creen y evalúen un proyecto que responda a las necesidades planteadas en una determinada situación.
- **Aprendizaje cooperativo:** Los estudiantes trabajan en grupo para realizar las tareas de manera colectiva.

5.2. Actividades formativas

Actividad Formativa	Horas	Presencialidad
AF1 Clases teóricas / Expositivas	30	100%
AF2 Clases Prácticas	24	100%
AF3 Tutorías	6	50%
AF4 Estudio independiente y trabajo autónomo del alumno	57,5	0%
AF5 Elaboración de trabajos (en grupo o individuales)	28,5	0%
AF6: Actividades de Evaluación	4	100%

6. SISTEMA DE EVALUACIÓN

ACTIVIDAD DE EVALUACIÓN	VALORACIÓN MÍNIMA RESPECTO A LA CALIFICACIÓN FINAL (%)	VALORACIÓN MÁXIMA RESPECTO A LA CALIFICACIÓN FINAL (%)
SE1 Evaluación de la participación en clase, en prácticas o en proyectos de la asignatura	10%	30%
SE2 Evaluación de trabajos, proyectos, informes, memorias	40%	80%
SE3 Exámenes intermedios o final (no continua)	10%	60%

6.1. Criterios de calificación

ACTIVIDAD DE EVALUACIÓN	VALORACIÓN RESPECTO A LA CALIFICACIÓN FINAL (%)
SE1 Evaluación del laboratorio, trabajo central.	20%
SE2 Evaluación de trabajos, proyectos, informes, memorias	20%
SE3 Exámenes intermedios o final (no continua)	60%

Consideraciones generales acerca de la evaluación:

- La evaluación de la participación en clase, en prácticas o en proyectos de la asignatura se realizará a partir de la asistencia y la participación activa en clase y en el resto de las actividades desarrolladas durante el curso. Este aspecto modulará el 10% de la calificación final de la asignatura en la convocatoria ordinaria.

- A lo largo del curso se plantearán actividades, ejercicios y problemas que deberán ser entregadas antes de la fecha indicada a través de la plataforma virtual. Este trabajo se evaluará a través de la propia plataforma virtual y supondrá un 20% de la calificación final de la asignatura en la convocatoria ordinaria.

- Para aprobar la asignatura en la convocatoria ordinaria, es imprescindible que la nota final (incluyendo el traajo y las prácticas) sea al menos 5.0 (sobre 10). Además de ese requisito, es necesario que la media de los exámenes parciales y la práctica sea al menos 5.0 (sobre 10). **En caso de no cumplirse alguno de estos requisitos, la asignatura se considerará automáticamente suspensa independientemente del resto de calificaciones.**
- En los exámenes no se permite el uso de apuntes a menos que se especifique lo contrario, para lo que el alumno debe remitirse a las instrucciones específicas del profesor sobre este tema.
- No se conservarán calificaciones de ningún tipo entre distintos cursos académicos, aunque si entre la convocatoria de Enero y Julio. Pudiendo el alumno presentarse a los exámenes, prácticas o ambas.

Consideraciones generales acerca del desarrollo de las clases:

- No está permitido el uso de teléfonos móviles en el aula durante el período de evaluación continua, excepto indicación expresa en sentido contrario del profesor. Los ordenadores portátiles podrán utilizarse únicamente para actividades relacionadas con la asignatura. El profesor podrá retirar el derecho al uso del ordenador a aquellos alumnos que lo utilicen para actividades que no estén relacionadas con la asignatura (consulta de correos, noticias o redes sociales, consulta o elaboración de actividades de otras asignaturas, etc.).

- No está permitido consumir bebidas ni comidas en el aula. Tampoco está permitida la presencia de cualquier tipo de bebida en las mesas, incluso en envases cerrados.

- Se demandará del alumno una participación activa, necesaria para el desarrollo de las clases.

- Se exigirá al alumno un buen comportamiento en todo momento durante el desarrollo de las clases. El mal comportamiento que impida el normal desarrollo de la clase puede conllevar la expulsión del aula por un tiempo a determinar por el profesor.

7. BIBLIOGRAFÍA / WEBGRAFÍA

Bibliografía Básica:

- Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software (English Edition)
- Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigate Windows malware
- Mastering Windows Security and Hardening: Secure and protect your Windows environment from intruders, malware attacks, and other

8. MATERIAL, SOFTWARE Y HERRAMIENTAS NECESARIAS

VirtualBox

Espacio para el almacenamiento de máquinas virtuales

Ordenador con Linux intalado.