GUÍA DOCENTE

ANÁLISIS DE MALWARE

GRADO EN **INGENIERÍA DEL SOFTWARE**

MODALIDAD: PRESENCIAL

CURSO ACADÉMICO: 2023-2024

Denominación de la asignatura:	Análisis de Malware
Titulación:	Ingeniería del Software
Facultad o Centro:	Centro Universitario de Tecnología y Arte Digital
Materia:	Ciberseguridad
Curso:	4º
Cuatrimestre:	2
Carácter:	OBM
Créditos ECTS:	6
Modalidad/es de enseñanza:	Presencial
Idioma:	Castellano
Profesor/a - email	Alejandro Ulises González Zugasti / alejandro.zugasti@live.u-tad.com
Página Web:	http://www.u-tad.com/

DESCRIPCIÓN DE LA ASIGNATURA

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, especialm

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

COMPETENCIAS Y RESULTADOS DE APRENDIZAJE

Competencias (genéricas, específicas y transversales)

COMPETENCIAS BÁSICAS Y GENERALRES

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

COMPETIENCIAS ESPECIFICAS

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.

Resultados de aprendizaje

Al acabar la titulación, el graduado o graduada será capaz de:

- Entender qué son las ciber amenazas, cuál es su origen, qué buscan y cómo podemos identificarlas.

- Ser capaz de identificar las amenazas y vulnerabilidades de ciberseguridad de un sistema informático concreto, compuesto por elementos diversos de

- hardware y software.

- Entender y aplicar los principios de la criptografía aplicada a la ciberseguridad.

- Conocer las herramientas y técnicas de auditoría forense.

- Conocer el entorno legal y de protección de datos en las aplicaciones de ciberseguridad

- Conocer experiencias documentadas de ciberataques y las contramedidas recomendadas-

- Entender los conceptos red team, blue team y estudiar su aplicación en escenarios concretos.

- Conocer los elementos y las buenas prácticas descritos en la familia de normas ISA/IEC -62443 e ISO/IEC-27000.

- Conocer y aplicar las técnicas para bastionar los sistemas ante ciberataques, usando detectores de intrusión y monitores.

- Aplicar conceptos de ciberseguridad para diseñar el hardware, la red de comunicaciones y el software de los sistemas en producción.

- Conocer las técnicas de análisis del malware.

- Ser capaz de desensamblar un código malicioso e identificar su origen

- Concebir, desarrollar y desplegar un proyecto de ciberseguridad integral para un sistema distribuid- o

CONTENIDO

Ingeniería inversa y ensamblador

Análisis estático y dinámico de malware

TEMARIO

Tema 1: Anatomía de un binario

1. Formato ELF
2. Formato PE

Tema 2: Análisis básico de binarios

1. Análisis estático
2. Análisis dinámico

Tema 3: Análisis avanzado de binarios

1. Desensamblador
2. Depurador
3. Análisis de dependencias Windows

Tema 4: Análisis de código ofuscado

1. Técnicas de ofuscación
2. Des-ofuscación

Tema 5: Técnicas de inyección

1. Inyección de código en ELF
2. Inyección de código en PE
3. Hooks

Tema 6: Herramientas avanzadas y Machine Learning

1. Introducción a la aplicación de ML a análisis de malware
2. Repaso de Python
3. Detección de malware mediante técnicas de ML

Tema 7: Construcción de detectores con Machine Learning

1. Laboratorio en Windows

ACTIVIDADES FORMATIVAS Y METODOLOGÍAS DOCENTES

Actividades formativas

Actividad Formativa	Horas totales	Horas presenciales
Clases teóricas / Expositivas	29,38	29,38
Clases Prácticas	23,25	23,25
Tutorías	4,00	0,00
Estudio independiente y trabajo autónomo del alumno	50,00	0,00
Elaboración de trabajos (en grupo o individuales)	31,88	0,00

Actividades de Evaluación	5,25	5,25
Seguimiento de Proyectos	6,25	6,25
TOTAL	150	64,13

Metodologías docentes

Método expositivo o lección magistral

Aprendizaje de casos

Aprendizaje basado en la resolución de problemas

Aprendizaje basado en proyectos

Aprendizaje cooperativo o colaborativo

Aprendizaje por indagación

Metodología Flipped classroom o aula invertida

Gamificación

Just in time Teaching (JITT) o aula a tiempo

Método expositivo o lección magistral

Método del caso

Aprendizaje basado en la resolución de problemas

Aprendizaje basado en proyectos

Aprendizaje cooperativo o colaborativo

Aprendizaje por indagación

Metodología flipped classroom o aula invertida

Gamificación

DESARROLLO TEMPORAL

UNIDADES DIDÁCTICAS / TEMAS	PERÍODO TEMPORAL
Presentación y creación del laboratorio	Semana 1
Tema 1. Anatomía de un binario	Semanas 2 y 3

Tema 2. Análisis básico de binarios Semanas 4 y 5

Tema 3. Análisis avanzado de binarios Semanas 6 y 7

Parcial 1 Semana 8

Tema 4. Análisis de código ofuscado Semanas 9 y 10

Tema 5. Técnicas de inyección Semana 11

Tema 6. Herramientas avanzadas y ML Semanas 12 y 13

Tema 7. Construcción de detectores con ML Semana 14

Parcial 2 Semana 15

SISTEMA DE EVALUACIÓN

ACTIVIDAD DE EVALUACIÓN	VALORACIÓN MÍNIMA RESPECTO A LA CALIFICACIÓN FINAL (%)	VALORACIÓN MÁXIMA RESPECTO A LA CALIFICACIÓN FINAL (%)
Evaluación de la participación en clase, en prácticas o en proyectos de la asignatura	10	30
Evaluación de trabajos, proyectos, informes, memorias	40	80
Prueba Objetiva	10	60

CRITERIOS ESPECÍFICOS DE EVALUACIÓN

ACTIVIDAD DE EVALUACIÓN	CONVOCATORIA ORDINARIA	CONVOCATORIA EXTRAORDINARIA
Evaluación de la participación en clase, en prácticas o en proyectos de la asignatura	10	10
Evaluación de trabajos, proyectos, informes, memorias	50	50
Prueba Objetiva	40	40

Consideraciones generales acerca de la evaluación

- La anterior tabla hace referencia tanto a la convocatoria ordinaria como a la extraordinaria.
- 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 representará 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 50% de la calificación final de la asignatura en la convocatoria ordinaria. Serán desarrolladas un total de 5 prácticas durante el desarrollo de la asignatura.
- Durante el desarrollo de la asignatura serán realizados un total de 2 exámenes parciales, que serán liberatorios si así lo desea el alumno con la condición de obtener al menos una calificación de 5.0 en dicho examen. Aquellos alumnos que no superen esa nota o que decidan descartarla voluntariamente, deberán realizar los exámenes correspondientes en la fecha asignada para la convocatoria ordinaria.
- Para aprobar la asignatura en la convocatoria ordinaria, es imprescindible que la nota final (incluyendo los exámenes parciales 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 caso de no conseguir el aprobado, el alumno podrá presentarse a la convocatoria extraordinaria de julio, donde realizará un examen final que representará el 40% de su calificación en dicha convocatoria, junto con una serie de ejercicios y prácticas que representarán el 50% restante.
- El restante 10% de la evaluación de la participación en clase en convocatoria extraordinaria coincidirá con la calificación obtenida en la convocatoria ordinaria en este criterio.
- 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.

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

MATERIALES, SOFTWARE Y HERRAMIENTAS NECESARIAS

Tipología del aula
Aula teórica

Equipo de proyección y pizarra

Materiales:
- Ordenador personal con Windows, Linux o OSX

Software:
VirtualBox

Espacio para máquinas virtuales