GUÍA DOCENTE

ANÁLISIS FORENSE

GRADO EN **INGENIERÍA DEL SOFTWARE**

MODALIDAD: A DISTANCIA

CURSO ACADÉMICO: 2023-2024

Denominación de la asignatura:	Análisis Forense
Titulación:	Ingeniería del Software
Facultad o Centro:	Centro Universitario de Tecnología y Arte Digital
Materia:	Ciberseguridad
Curso:	3º
Cuatrimestre:	2
Carácter:	OBM
Créditos ECTS:	6
Modalidad de enseñanza:	A distancia
Idioma:	Castellano
Profesor / Email:	Marcos González Sanz / marcos.sanz@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 asignatura pretender dar unos conocimientos y capacidades de análisis forense con un enfoque post-mortem. Para ello se va a ver la forma en la que se realiza la adquisición de evidencia y clonado de discos. A continuación, se verá la forma en la que analizar los sistemas operativos Windows y Linux. También se ahondará en los rastros forense en las redes, además del análisis de malware. También se conocerán los procedimientos de análisis de correos electrónicos.

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

Fundamentos del Análisis Forense

Análisis Forense en sistemas Windows

Análisis Forense en sistemas Unix

Análisis Forense de redes

Introducción a la Ingeniería Inversa

Introducción al análisis de Malware

TEMARIO

Tema 1: Introducción al forense digital

1. Introducción

2. Tipos de almacenamiento y sistema de ficheros
3. Metadatos
4. Adquisición de evidencias
5. Técnicas anti-forenses

Tema 2: Windows I

1. Introducción
2. Identificación de información volátil
3. Adquisición de memoria
4. Análisis de memoria

Tema 3: Windows II

1. Introducción
2. Identificación de información no volátil
3. Registro de Windows
4. Caché, Cookies e Historial
5. Análisis de ficheros Windows
6. Eventos de Windows
7. Frameworks

Tema 4: Linux

1. Introducción
2. Técnicas de ocultación
3. Información sobre el sistema
4. Información sobre las cuentas
5. Comandos básicos
6. Logs
7. Información Volátil
8. Backdoors
9. Herramientas automáticas
10. Dump de memoria

Tema 5: Redes

1. Introducción

2. Herramientas
3. Logs

Tema 6: Malware

1. Introducción
2. Ciclo de vida
3. IOCs
4. Análisis estático
5. Análisis Dinámico

Tema 7: Correos Electrónicos

1. Introducción
2. SMTP, POP3 e IMAP
3. Cabeceras

ACTIVIDADES FORMATIVAS Y METODOLOGÍAS DE APRENDIZAJE

Actividades formativas

Actividad Formativa	Horas totales	Horas síncronas
Sesiones teóricas virtuales síncronas	4,25	4
Sesiones teóricas virtuales asíncronas	22,50	0
Sesiones prácticas virtuales síncronas	2,25	2
Sesiones prácticas virtuales asíncronas	10,75	0
Debate y discusión oral y/o escrita.	8,50	0
Tutorías	4,00	4
Estudio independiente y trabajo autónomo del alumno	50,00	0
Elaboración de trabajos (en grupo o individuales	33,25	0
Actividades de Evaluación	3,75	4
Test de autoevaluación	5,00	0
Seguimiento de proyectos	5,75	6

TOTAL	150	20

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

Presentación - semana 1

Unidad 1 - semana 2-3

Unidad 2 - semana 4-5

Unidad 3 - semana 6-7

Unidad 4 - semana 7-8

Unidad 5 - semana 9-10

Unidad 6 - semana 11-12

Repaso - semana 13-14

Evaluación - 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	20
Evaluación de trabajos, proyectos, informes, memorias	10	20
Prueba Objetiva	60	70

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	20	10
Evaluación de trabajos, proyectos, informes, memorias	20	20
Prueba Objetiva	60	70

Consideraciones específicas acerca de la evaluación

Será necesario que obtener una nota mínima de 4 puntos (sobre 10) en la prueba final presencial para que se realice la media con las actividades formativas.

BIBLIOGRAFÍA / WEBGRAFÍA

Bibliografía Básica:

- Hacking Exposed 7: Network Security Secrets Solutions, Editorial: McGraw-Hill
- The Web Application Hacker's Handbook (Second Edition), Editorial: Wiley

Bibliografía Recomendada:

- Metasploit, Penetration Testers Guide, Editorial: No Starch Press
- Violent Python A Cookbook for Hackers Forensic, Editorial: Syngress
- Mastering Kali Linux for Advanced Penetration Testing, Editorial: Wiley

MATERIALES, SOFTWARE Y HERRAMIENTAS NECESARIAS

Materiales:
Ordenador personal con Windows, Linux o OSX

Software:
VirtualBox

Espacio para el almacenamiento de máquinas virtuales