ANX-PR/CL/001-01

GUÍA DE APRENDIZAJE

ASIGNATURA

93001010 - Ingeniería Inversa Y Análisis De Malware

PLAN DE ESTUDIOS

09AW - Master Universitario En Ciberseguridad

CURSO ACADÉMICO Y SEMESTRE

2021/22 - Primer semestre

Índice

Guía de Aprendizaje

1. Datos descriptivos

1.1. Datos de la asignatura

Nombre de la asignatura	93001010 - Ingeniería Inversa y Análisis de Malware
No de créditos	6 ECTS
Carácter	Obligatoria
Curso	Primer curso
Semestre	Primer semestre
Período de impartición	Septiembre-Enero
Idioma de impartición	Castellano
Titulación	09AW - Master Universitario en Ciberseguridad
Centro responsable de la titulación	09 - Escuela Tecnica Superior De Ingenieros De Telecomunicacion
Curso académico	2021-22

2. Profesorado

2.1. Profesorado implicado en la docencia

Nombre	Despacho	Correo electrónico	Horario de tutorías *
Alejandro Martin Garcia (Coordinador/a)	1220	alejandro.martin@upm.es	Sin horario.

* Las horas de tutoría son orientativas y pueden sufrir modificaciones. Se deberá confirmar los horarios de tutorías con el profesorado.

3. Competencias y resultados de aprendizaje

3.1. Competencias

CB06 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación

CB07 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio

CB08 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios

CB09 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades

CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo

CE06 - Capacidad de aplicar las principales metodologías y técnicas de seguridad en el desarrollo del software y sistemas informáticos

CE08 - Capacidad para abordar técnicamente la gestión de un incidente de ciberseguridad, incluyendo análisis de malware, análisis forense e ingeniería inversa

CG02 - Dotar al alumno del conocimiento de los distintos tipos de amenazas que pueden afectar a una organización y sus consecuencias en diferentes escenarios sociales, económicos e industriales y dotarle de la capacidad de aplicar las técnicas de análisis y gestión de todo tipo de riesgos para definir e implantar las salvaguardas necesarias para mitigar o eliminar sus impactos hacer resiliente a la organización

CG04 - Dotar al alumno de la capacidad de contribuir con su conocimiento e ideas a la solución o análisis de ataques y métodos de fraude desconocidos que tengan que ver con la ciberseguridad

CT01 - Uso de la Lengua Inglesa

CT03 - Creatividad

CT09 - Capacidad de análisis y síntesis

CT11 - Razonamiento crítico

CT12 - Aprendizaje autónomo, adaptación a nuevas situaciones y motivación por el desarrollo profesional permanente

3.2. Resultados del aprendizaje

RA15 - Reconocer, analizar y saber neutralizar los diferentes tipos de malware

RA16 - Aplicar ingeniería inversa sobre malware

4. Descripción de la asignatura y temario

4.1. Descripción de la asignatura

En esta asignatura se abordan los conceptos y el análisis básico y avanzado del malware, y el uso de la ingeniería inversa para realizar análisis avanzado de software malicioso. Algunos temas abordados incluyen: tipos de Malware, análisis estático y dinámico, packers y demás módulos del malware, análisis de comportamiento de ejecutables maliciosos, sistemas de intercepción y registro de actividades a nivel de red, parcheado de ejecutables maliciosos, y conceptos esenciales de la Ingeniería Inversa de código. Por último, se aborda el malware diseñado específicamente para la plataforma Android.

4.2. Temario de la asignatura

1. Introducción al análisis de malware
    1.1. Conceptos generales
    1.2. Historia y estado actual
    1.3. Entornos seguros
    1.4. Herramientas y utilidades
2. Análisis estático básico
    2.1. Antivirus
    2.2. Empaquetado y ofuscación
    2.3. Archivos PE
    2.4. Casos prácticos
3. Análisis dinámico básico

- 3.1. Introducción al análisis dinámico
- 3.2. Windows sysinternals
- 3.3. Máquinas virtuales
- 3.4. Técnicas de evasión
- 3.5. Entornos de sandboxing y virtualización

4. Ingeniería inversa
   - 4.1. Introducción a la ingeniería inversa
   - 4.2. Arquitectura x86
   - 4.3. Herramientas
5. Análisis estático avanzado
   - 5.1. Herramientas
   - 5.2. Estructura de C en ensamblador
   - 5.3. Uso de funcionalidades de Windows
   - 5.4. Ejecución del malware
6. Análisis dinámico avanzado
   - 6.1. Introducción
   - 6.2. Debuggers
   - 6.3. Debugging en el kernel
   - 6.4. Comportamientos típicos del malware
7. Análisis de Malware para Android
   - 7.1. La arquitectura Android
   - 7.2. Malware para Android
   - 7.3. Herramientas

5. Cronograma

5.1. Cronograma de la asignatura *

Sem	Actividad presencial en aula	Actividad presencial en laboratorio	Tele-enseñanza	Actividades de evaluación
1		**Tema 1** Duración: 04:00 LM: Actividad del tipo Lección Magistral **Tema 2** Duración: 04:00 LM: Actividad del tipo Lección Magistral		**Práctica** TI: Técnica del tipo Trabajo Individual Evaluación continua Presencial Duración: 00:00
2		**Tema 2** Duración: 04:00 PL: Actividad del tipo Prácticas de Laboratorio **Tema 3** Duración: 04:00 LM: Actividad del tipo Lección Magistral		
3		**Tema 3** Duración: 04:00 PL: Actividad del tipo Prácticas de Laboratorio **Tema 4** Duración: 02:00 LM: Actividad del tipo Lección Magistral		**Prueba Temas 1, 2 y 3** EP: Técnica del tipo Examen de Prácticas Evaluación continua Presencial Duración: 02:00
4		**Tema 4** Duración: 04:00 PL: Actividad del tipo Prácticas de Laboratorio **Tema 5** Duración: 04:00 LM: Actividad del tipo Lección Magistral		
5		**Tema 5** Duración: 04:00 PL: Actividad del tipo Prácticas de Laboratorio **Tema 5** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		
6		**Tema 6** Duración: 04:00 LM: Actividad del tipo Lección Magistral **Tema 6** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		**Prueba Temas 4 y 5** EP: Técnica del tipo Examen de Prácticas Evaluación continua Presencial Duración: 02:00

7		**Tema 6** Duración: 04:00 PL: Actividad del tipo Prácticas de Laboratorio **Tema 7** Duración: 02:00 LM: Actividad del tipo Lección Magistral		
8				
9				
10				
11				
12				
13				
14				
15				**Prueba final** EX: Técnica del tipo Examen Escrito Evaluación continua Presencial Duración: 04:00
16				
17				**Evaluación solo prueba final** EX: Técnica del tipo Examen Escrito Evaluación sólo prueba final Presencial Duración: 04:00

Para el cálculo de los valores totales, se estima que por cada crédito ECTS el alumno dedicará dependiendo del plan de estudios, entre 26 y 27 horas de trabajo presencial y no presencial.

* El cronograma sigue una planificación teórica de la asignatura y puede sufrir modificaciones durante el curso derivadas de la situación creada por la COVID-19.

6. Actividades y criterios de evaluación

6.1. Actividades de evaluación de la asignatura

6.1.1. Evaluación continua

Sem.	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
1	Práctica	TI: Técnica del tipo Trabajo Individual	Presencial	00:00	45%	4 / 10	CE06 CE08 CB07 CB09 CB10 CT03 CT09 CT11 CT12 CB08 CG02 CG04
3	Prueba Temas 1, 2 y 3	EP: Técnica del tipo Examen de Prácticas	Presencial	02:00	15%	4 / 10	CE08 CB07 CB09 CT01 CT09 CT11 CT12 CB08 CG02
6	Prueba Temas 4 y 5	EP: Técnica del tipo Examen de Prácticas	Presencial	02:00	15%	4 / 10	CE08 CB07 CB09 CT01 CT03 CT09 CT11 CB08 CB06 CG04
15	Prueba final	EX: Técnica del tipo Examen Escrito	Presencial	04:00	25%	4 / 10	CE06 CE08 CB09 CB10 CT01 CT09 CT11 CT12 CB08

							CG02 CG04

6.1.2. Evaluación sólo prueba final

Sem	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
17	Evaluación solo prueba final	EX: Técnica del tipo Examen Escrito	Presencial	04:00	100%	5 / 10	CE06 CE08 CB07 CB09 CB10 CT01 CT03 CT09 CT11 CT12 CB08 CB06 CG02 CG04

6.1.3. Evaluación convocatoria extraordinaria

Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
Evaluación convocatoria extraordinaria	EX: Técnica del tipo Examen Escrito	Presencial	02:30	100%	5 / 10	CE08 CB07 CB09 CB10 CT01 CT03 CE06 CT09 CT11 CT12 CB08 CB06 CG02 CG04

6.2. Criterios de evaluación

La evaluación continua se realizará mediante tres exámenes de prácticas, y un examen teórico escrito individual. Los pesos de cada prueba son:

- Práctica: 45%
- Examen Temas 1, 2 y 3: 15%
- Examen Temas 4 y 5: 15%
- Examen final: 25%

La evaluación mediante solo prueba final y la evaluación de la convocatoria extraordinaria consistirán en un examen que incluirá una parte teórica, escrita, y una parte práctica para realizar análisis estático y dinámico sobre una o varias muestras de malware, de manera individual.

En caso de escoger la evaluación mediante únicamente prueba final, se deberá notificar durante la primera semana del curso al coordinador de la asignatura.

7. Recursos didácticos

7.1. Recursos didácticos de la asignatura

Nombre	Tipo	Observaciones
moodle	Recursos web	Plataforma de educación de la UPM
Libro de referencia	Bibliografía	Sikorski, M., & Honig, A. (2012). Practical malware analysis: the hands-on guide to dissecting malicious software. no starch press.
Libro adicional	Bibliografía	Ligh, M., Adair, S., Hartstein, B., & Richard, M. (2010). Malware analyst's cookbook and DVD: tools and techniques for fighting malicious code. Wiley Publishing.

8. Otra información

8.1. Otra información sobre la asignatura

La docencia se impartirá de forma presencial. No obstante, se podrá cambiar de modalidad en función de las circunstancias.

En previsión de posibles recidivas de la epidemia de COVID, la presente guía contempla la impartición de la asignatura en formato bimodal: todas las actividades formativas planificadas inicialmente como actividades presenciales, en caso de ser necesario pasarán a desarrollarse a través de plataformas online.