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

2018/19 - 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	2018-19

2. Profesorado

2.1. Profesorado implicado en la docencia

Nombre	Despacho	Correo electrónico	Horario de tutorías *
Jesus Garcia Lopez De Lacalle (Coordinador/a)	2109	jesus.glopezdelacalle@upm.es	Sin horario.
Luis Miguel Pozo Coronado	2003	lm.pozo@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

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

RA16 - Aplicar ingeniería inversa sobre malware

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

4. Descripción de la asignatura y temario

4.1. Descripción de la asignatura

Conceptos esenciales de la Ingeniería Inversa de código. Patrones característicos del malware. Reconocimiento de malware empaquetado. Desempaquetado de malware. Herramientas de volcado de procesos y utilidades de reconstrucción de los imports. Interceptando conexiones de red en presencia de malware. Interacción con sitios web maliciosos para examinar su naturaleza. De-ofuscación de scripts de navegador. Identificar y neutralizar los métodos que utiliza el malware para detectar la presencia de herramientas de análisis (antisandboxing). Ingeniería inversa de programas Flash maliciosos. Análisis de memoria para evaluar las características del malware y reconstruir los procesos de infección.

Análisis de Malware. Análisis dinámico de Malware. Análisis estático esencial. Packers y demás módulos del malware. Análisis de comportamiento de ejecutables maliciosos. Sistema de intercepción y registro de actividades a nivel de red. Parcheado de ejecutables maliciosos. Aceleración del análisis de malware. Tipos de Malware. Diferentes tipos de ataques. Ingeniería social.

4.2. Temario de la asignatura

1. Introducción al análisis de malware
    1.1. Técnicas de análisis de malware
    1.2. Tipos de malware
    1.3. Reglas generales del análisis de malware
    1.4. Comportamiento del malware
2. Análisis estático básico
3. Análisis dinámico básico
4. Ingeniería inversa
    4.1. Niveles de abstracción: desde hardware a lenguajes de alto nivel
    4.2. Arquitectura x86
    4.3. Utilización de desemsambladores: IDA Pro
5. Análisis estático avanzado
    5.1. Estructura del código generado por distintos compiladores de C
    5.2. Funcionalidades de Windows utilizados por el malware
6. Análisis dinámico avanzado
    6.1. Debuggers
    6.2. OllyDbg y WinDbg
7. Tecnicas avanzadas de desarrollo de malware
    7.1. Malware encubierto
    7.2. Malware encriptado
    7.3. Técnicas para dificultar el desensamblado, el debugging y el análisis en máquinas virtuales
    7.4. Malware desarrollado en C++
    7.5. Malware para 64-bits

5. Cronograma

5.1. Cronograma de la asignatura *

Sem	Actividad presencial en aula	Actividad presencial en laboratorio	Otra actividad presencial	Actividades de evaluación
1		**Tema 1** Duración: 04:00 LM: Actividad del tipo Lección Magistral		
2		**Tema 2** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Tema 2** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		**Prueba Tema 2** TG: Técnica del tipo Trabajo en Grupo Evaluación continua Duración: 00:00
3		**Tema 3** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Tema 3** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		
4		**Tema 3** Duración: 04:00 PL: Actividad del tipo Prácticas de Laboratorio		**Prueba Tema 3** TG: Técnica del tipo Trabajo en Grupo Evaluación continua Duración: 00:00
5		**Tema 4** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Tema 4** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		
6		**Tema 4** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Tema 4** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		**Prueba Tema 4 - I** TG: Técnica del tipo Trabajo en Grupo Evaluación continua Duración: 00:00
7		**Tema 4** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Tema 4** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		**Prueba Tema 4 - II** TG: Técnica del tipo Trabajo en Grupo Evaluación continua Duración: 00:00

8		**Tema 5** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Tema 5** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		
9		**Tema 5** Duración: 04:00 PL: Actividad del tipo Prácticas de Laboratorio		**Prueba Tema 5** TG: Técnica del tipo Trabajo en Grupo Evaluación continua Duración: 00:00
10		**Tema 6** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Tema 6** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		
11		**tema 6** Duración: 04:00 PL: Actividad del tipo Prácticas de Laboratorio		**Prueba Tema 6 - I** TG: Técnica del tipo Trabajo en Grupo Evaluación continua Duración: 00:00
12		**Tema 6** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Tema 6** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		**Prueba Tema 6 - II** TG: Técnica del tipo Trabajo en Grupo Evaluación continua Duración: 00:00
13		**Tema 7** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Tema 7** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		
14		**Tema 7** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Tema 7** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		
15				**Prueba final** EX: Técnica del tipo Examen Escrito Evaluación continua Duración: 00:00
16				**Evaluación solo prueba final** EX: Técnica del tipo Examen Escrito Evaluación sólo prueba final Duración: 00:00 **Trabajos prácticos (Temas 2, 3, 4-I, 4-II, 5, 6-I y 6-II)** TI: Técnica del tipo Trabajo Individual Evaluación sólo prueba final

				Duración: 00:00
17				

Las horas de actividades formativas no presenciales son aquellas que el estudiante debe dedicar al estudio o al trabajo personal.

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.

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
2	Prueba Tema 2	TG: Técnica del tipo Trabajo en Grupo	No Presencial	00:00	10%	/ 10	CE08 CT12 CG04 CB06
4	Prueba Tema 3	TG: Técnica del tipo Trabajo en Grupo	Presencial	00:00	10%	/ 10	CE08 CB07 CT01 CG02
6	Prueba Tema 4 - I	TG: Técnica del tipo Trabajo en Grupo	No Presencial	00:00	10%	/ 10	CE08 CT03 CB08 CG04
7	Prueba Tema 4 - II	TG: Técnica del tipo Trabajo en Grupo	No Presencial	00:00	10%	/ 10	CE08 CB09 CT09 CG02
9	Prueba Tema 5	TG: Técnica del tipo Trabajo en Grupo	No Presencial	00:00	10%	/ 10	CE08 CB10 CT11 CG04
11	Prueba Tema 6 - I	TG: Técnica del tipo Trabajo en Grupo	Presencial	00:00	10%	/ 10	CE08 CT12 CG02 CB06
12	Prueba Tema 6 - II	TG: Técnica del tipo Trabajo en Grupo	No Presencial	00:00	10%	/ 10	CE08 CB07 CT01 CG04
15	Prueba final	EX: Técnica del tipo Examen Escrito	Presencial	00:00	30%	/ 10	CE08 CB09 CB10 CT03 CT09 CT11 CB08

6.1.2. Evaluación sólo prueba final

Sem	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
16	Evaluación solo prueba final	EX: Técnica del tipo Examen Escrito	Presencial	00:00	30%	/ 10	CE08 CB09 CB10 CT03 CT09 CT11 CB08
16	Trabajos prácticos (Temas 2, 3, 4-I, 4-II, 5, 6-I y 6-II)	TI: Técnica del tipo Trabajo Individual	No Presencial	00:00	70%	/ 10	CE08 CB07 CT01 CT12 CG02 CG04 CB06

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	00:00	30%	/ 10	CE08 CB09 CB10 CT03 CT09 CT11 CB08
Trabajos prácticos (Temas 2, 3, 4-I, 4-II, 5, 6-I y 6-II)	TI: Técnica del tipo Trabajo Individual	Presencial	00:00	70%	/ 10	CE08 CB07 CT01 CT12 CG02 CG04 CB06

6.2. Criterios de evaluación

La evaluación continua se realizará mediante la entrega de 7 trabajos prácticos en grupo y un examen escrito. Los pesos de cada prueba son:

- Trabajo práctico Tema 2: 10%
- Trabajo práctico Tema 3: 10%
- Trabajo práctico Tema 4-I: 10%
- Trabajo práctico Tema 4-II: 10%
- Trabajo práctico Tema 5: 10%
- Trabajo práctico Tema 6-I; 10%
- Trabajo práctico Tema 6-II: 10%
- Examen escrito: 30%

La evaluación mediante solo prueba final y la evaluación de la convocatoria extraordinaria es igual que la correspondiente a evaluación continua, salvo que los trabajos son individuales en lugar de en grupo.

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, Michael and Honig, Andrew, Practical Malware Analysis. The Hands-On Guide to Dissecting Malicious Software, No Starch Press, 2012.