ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA

GUIA DOCENTE

CURSO 2020/2021

Máster en Ingeniería Informática (Plan 2018)

DATOS DE LA ASIGNATURA				
Nombre:				
Análisis e Ingeniería de Malware				
Denominación en inglés:				
Malware Analysis				
Código:		**Carácter:**		
1180425		Optativo		
Horas:				
	Totales	**Presenciales**	**No presenciales**	
Trabajo estimado:	75	30	45	
Créditos:				
	Grupos reducidos			
Grupos grandes	**Aula estándar**	**Laboratorio**	**Prácticas de campo**	**Aula de informática**
1.5	0	0	0	1.5
Departamentos:		**Áreas de Conocimiento:**		
Tecnologías de la Información		Lenguajes y Sistemas Informáticos		
Curso:		**Cuatrimestre:**		
1º - Primero		Segundo cuatrimestre		

DATOS DE LOS PROFESORES			
Nombre:	**E-Mail:**	**Teléfono:**	**Despacho:**
*Abad Herrera, Pedro José	pedro.abad@dti.uhu.es	87678	ETP138
Suárez Fábrega, Antonio José	asuarez@uhu.es	959217677	ETP136

*Profesor coordinador de la asignatura

Consultar los horarios de la asignatura

DATOS ESPECÍFICOS DE LA ASIGNATURA

1. Descripción de contenidos

1.1. Breve descripción (en castellano):

- Tipos de Malware.
- Ingeniería e Ingeniería Inversa de Malware
- Análisis de Malware
- Herramientas de Análisis y Síntesis de Malware

1.2. Breve descripción (en inglés):

Types of known threats
Malware Analysis fundamentals
Reverse-Engineering Malware
Malware Analysis Tools and Techniques

2. Situación de la asignatura

2.1. Contexto dentro de la titulación:

La asignatura forma parte de las materias optativas dentro de la especialidad de "Ciberseguridad". Se imparte durante el segundo cuatrimestre del primer curso.

2.2. Recomendaciones:

No se necesita ninguna recomendación especial, más allá de haber cursado las materias obligatorias de la especialidad del primer cuatrimestre.

3. Objetivos (Expresados como resultados del aprendizaje):

Analizar y detectar anomalías y firmas de ataques en los sistemas.
Analizar y detectar técnicas de ocultación de ataques a sistemas.
Conocer las tendencias actuales en técnicas de ciberataque.
Conocer y aplicar los mecanismos de cifrado y esteganografiado pertinentes para proteger los datos residentes en un sistema o en tránsito por una red.

4. Competencias a adquirir por los estudiantes

4.1. Competencias específicas:

4.2. Competencias básicas, generales o transversales:

- **CB6:** 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
- **CB8:** 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
- **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
- **CG9:** Capacidad para comprender y aplicar la responsabilidad ética, la legislación y la deontología profesional de la actividad de la profesión de Ingeniero en Informática
- **CT2:** Dominar el proyecto académico y profesional, habiendo desarrollado la autonomía suficiente para participar en proyectos de investigación y colaboraciones científicas o tecnológicas dentro su ámbito temático, en contextos interdisciplinares y, en su caso, con un alto componente de transferencia del conocimiento.
- **CT4:** Comprometerse con la ética y la responsabilidad social como ciudadano y como profesional, con objeto de saber actuar conforme a los principios de respeto a los derechos fundamentales y de igualdad entre hombres y mujeres y respeto y promoción de los Derechos Humanos, así como los de accesibilidad universal de las personas discapacitadas, de acuerdo con los principios de una cultura de paz, valores democráticos y sensibilización medioambiental.
- **CT5:** Utilizar de manera avanzada las tecnologías de la información y la comunicación, desarrollando, al nivel requerido, las Competencias Informáticas e Informacionales ('CI2).

5. Actividades Formativas y Metodologías Docentes

5.1. Actividades formativas:

- Sesiones de Teoría sobre los contenidos del Programa.
- Sesiones Prácticas en Laboratorios Especializados o en Aulas de Informática.
- Actividades Académicamente Dirigidas por el Profesorado: seminarios, conferencias, desarrollo de trabajos, debates, tutorías colectivas, actividades de evaluación y autoevaluación.

5.2. Metologías docentes:

- Clase Magistral Participativa.
- Desarrollo de Prácticas en Laboratorios Especializados o Aulas de Informática en grupos reducidos.
- Resolución de Problemas y Ejercicios Prácticos.
- Tutorías Individuales o Colectivas. Interacción directa profesorado-estudiantes.
- Planteamiento, Realización, Tutorización y Presentación de Trabajos.
- Evaluaciones y Exámenes.

5.3. Desarrollo y justificación:

Las actividades formativas presenciales consistirán en:

- Sesiones de teoría: consistirán en la explicación de los conceptos y fundamentos de la asignatura mediante clases magistrales participativas.Durante dichas sesiones se presentarán ejemplos que ayuden a comprender los conceptos y su aplicación, tanto por parte del profesor, como de forma colectiva.
- Sesiones de prácticas, en el aula de informática, se propondrá la resolución de varias prácticas durante el curso,que podrá realizarse durante una o más sesiones, y que permita al estudiante aplicar a un problema concreto los conceptos y técnicas estudiados durante las sesiones teóricas.
- Actividades académicamente dirigidas: Durante todo el curso, el profesor estará a disposición de los estudiantes, en el horario de tutorías establecido, para atenderles en cualquier duda o aclaración que necesiten, tanto de los conceptos teóricos como de la resolución de las prácticas.A través del curso, se podrán realizar Conferencias y/o Seminarios que ahonden en algunos temás específicos.

Las actividades formativas no presenciales consistirán en:

- Lectura de los contenidos de los temas
- Entrega de ejercicios/prácticas/trabajos evaluables
- Actividades de autoevaluación
- Tutorías colectivas a través de plataformas de enseñanza virtual (foros, wikis, chats)
- Actividades no presenciales con evaluación por pares.
- Desarrollo cooperativo de trabajos utilizando herramientas de discusión asíncrona. (foros, wikis…)

Las metodologías docentes empleadas para las actividades no presenciales consistirán en:

- Visualización y escuchas de sesiones grabadas de seminarios ad hoc con entrevistas a expertos en algunos temas claves de la materia, o vídeos seleccionados que incentiven algunas competencias
- Tutorías en línea. Utilización de foros y otros medios de comunicación e interacción con el profesorado
- Trabajos colaborativos. Llevar a cabo una actividad basada en un objetivo común en el que el estudiante debe colaborar activamente para realizarla.

6. Temario desarrollado:

- Capítulo 0: Fundamentos del Análisis del Malware
- • 1 Objetivos del Análisis del Malware
  • 2 Técnicas de Análisis de Malware
  • 3 Tipos de Malware
  • 4. Reglas Generales para el Análisis de Malware
- Capítulo 1: Análisis de Malware en Máquinas Virtuales
- • 1 La estructura de una máquina virtual
  • 2 Configurando VirtualBox
- Capítulo 2: Técnicas Estáticas Básicas
- • 1 Escaneo antivirus: un primer paso útil
  • 2 Hashing: Una Huella Dactilar para el Malware
  • 3 Encontrar cadenas4 Malware empaquetado y ofuscado
  • 5 Formato de Archivo Portable Ejecutable (PE)
  • 6 Bibliotecas Vinculadas y Funciones
  • 7 Análisis Estático en la Práctica
  • 8 Los encabezados y Secciones del Archivo PE
- Capítulo 3: Análisis Dinámico Básico
- • 1 Introducción
  • 2 Sandboxes: El Enfoque Rápido y Sucio
  • 3 Ejecutando Malware
  • 4 Monitorizar con Process Monitor
  • 5 Visualización de Procesos con Process Explorer
  • 6 Comparando Instantáneas de Registro con Regshot
  • 7 Falsificando una Red
  • 8 Paquete Sniffing con Wireshark
  • 9 Using InetSim
  • 10 Herramientas Dinámicas Básicas en la Práctica
- Capitulo 4: Curso sobre desensamblado X86
- • 1 Niveles de abstracción.
  • 2 Ingeniería Inversa
  • 3 La arquitectura x86
- Capítulo 5: IDA PRO
- • 1 Introducción
  • 2 Carga de un Ejecutable
  • 3 La Interfaz de IDA Pro
  • 4 Uso de Referencias Cruzadas
  • 5 Análisis de Funciones
  • 6 Uso de las Opciones de Gráficos
  • 7 Mejoras para el Desmontaje
  • 8 Ampliación de IDA con Complementos
- Capítulo 6: Reconocer Construcciones de Código C en Ensamblador
- • 1 Introducción
  • 2 Variables Globales y Locales
  • 3 Desmontaje de Operaciones Aritméticas
  • 4 Reconocer las Instrucciones if
  • 5 Reconocimiento de Bucles
  • 6 Descripción de las Convenciones de las Llamadas de Función
  • 7 Análisis de las Instrucciones Switch
  • 8 Desmontaje de Arrays
  • 9 Identificación de Estructuras
  • 10 Análisis de una Lista Enlazada
- Capítulo 7: Analisis Malware de Windows
- • 1 Introducción
  • 2 La API de Windows
  • 3 El Registro de Windows
  • 4 API de Redes
  • 5 Siguiendo la Ejecución del Malware.
  • 6 Modo Kernel vs. Modo Usuario
  • 7 La API Nativa
- Capítulo 8: Debugging
- • 1 Depuradores de nivel fuente frente a nivel de ensamblado
  • 2 Depuración Kernel vs. Modo usuario
  • 3 Usando un depurador
  • 4 Excepciones
  • 5 Modificación de la ejecución con un depurador
  • 6 Modificación de la ejecución del programa en la práctica
- Capítulo 9. OLLYDBG
- • 1 Cargando Malware
  • 2 La interfaz de OllyDbg
  • 3 Mapa de memoria
  • 4 Viendo Hilos y Pilas

- 5 Ejecución de Código
- 6 Puntos de interrupción
- 7 Carga de DLL
- 8 Rastreo (Tracing)
- 9 Manejo de excepciones
- 10 Parches
- 11 Analizar Shellcode
- 12 Características de asistencia
- 13 Plug-ins

- Capítulo 10: Comportamiento del Malware
- • 1 Downloaders and Launchers
  - 2 Puertas traseras (Backdoors)
  - 3 Stealers de credenciales
  - 4 Mecanismos de Persistencia
  - 5 Escalamiento de privilegios
  - 6 Cubriendo sus pistas: rootkits en modo de usuario
- Capítulo 11: Lanzamiento de malware encubierto
- • 1 Launchers
  - 2 Process inyection
  - 3 Reemplazo de proceso
  - 4 Inyección de hook
  - 5 Detours
  - 6 Inyección de APC

7. Bibliografía

7.1. Bibliografía básica:

- Learning Malware Analysis. Monnappa K A. Packt Publishing. 2018
- Seguridad informática y Malwares Análisis de amenazas e implementación de contramedidas. Paul RASCAGNERES. Ediciones ENI. 2016
- Windows Malware Analysis Essentials. Victor Marak. Packt Publishing. 2015
- Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software. Michael Sikorski y Andrew Honig. No Starch Press; 2012

7.2. Bibliografía complementaria:

- Internal Hacking. Contramedidas En Entorno Windows (2º Edición). Philippe Kapfer. ENI. 2018.
- Seguridad informática - Hacking Ético. *Conocer el ataque para una mejor defensa (4a edición).* ACISSI - Damien BANCAL - David DUMAS - David PUCHE - Franck EBEL - Frédéric VICOGNE - Guillaume FORTUNATO - Jérôme HENNECART - Laurent SCHALKWIJK - Marion AGÉ - Raphaël RAULT - Robert CROCFER - Sébastien LASSON. ENI. 2018
- Cuckoo Sandbox Book. https://cuckoo.sh/docs/#cuckoo-sandbox-book

8. Sistemas y criterios de evaluación.

8.1. Sistemas de evaluación:

- Examen de teoría/problemas
- Defensa de Prácticas
- Seguimiento Individual del Estudiante
- Examen de prácticas

8.2. Criterios de evaluación y calificación:

Los principios de evaluación de la asignatura siguen unos criterios de evaluación preferentemente continua, entendiendo por tal la evaluación diversificada que se lleva a cabo en distintos momentos del curso académico en curso. Esta evaluación se realiza, para todas las convocatorias ordinarias, mediante los siguientes sistemas de evaluación y ponderaciones:

- Examen teórico que constará de preguntas teóricas y problemas: 10% de la nota final. (Competencias: CG9, CT2, CT4)
- Defensa de prácticas, a realizar en el aula de informática, y donde se deberán explicar con solvencia las prácticas realizadas : 50% de la nota final. (Competencias: CB6, CB8, CB10, CT5)
- Pruebas de evaluación mediante plataformas de enseñanza virtual: 20% de la nota final. (Competencias: CG9, CT2, CT4, CB6, CB8, CB10, CT5)
- Participación en las actividades propuestas: 20% de la nota final. (Competencias: CB6, CB8, CB10, CT5)

Aquellos estudiantes que así lo consideren pueden optar por la realización de una evaluación única final. En este caso deberá presentar una solicitud en el REGISTRO GENERAL de la Universidad, en cualquiera de sus REGISTROS AUXILIARES o en el REGISTRO TELEMÁTICO, dirigida a la dirección del departamento y al coordinador de la asignatura.
La evaluación única final consistirá, para todas las convocatorias oficiales, en un solo acto académico a celebrar en las fechas indicadas por el centro y que, para todas las convocatorias, estará formado por las siguientes pruebas:

- Examen teórico que constará de preguntas teóricas y problemas: 50% de la nota final. (Competencias: CG9, CT2, CT4)
- Examen de prácticas, a realizar en el aula de informática, y donde se deberán resolver con solvencia la práctica propuesta : 50% de la nota final. (Competencias: CB6, CB8, CB10, CT5). En dicho examen se incluye la pruebas de evaluación mediante plataformas de enseñanza virtual (10%) y la participación en las actividades propuestas (10%).

Ambas pruebas tendrán caracter presencial e individual, y versarán sobre la totalidad de la materia descrita en esta guía. No se podrá usar material adicional alguno, y la duración máxima de cada una de ellas será de 4 h.
La mención de Matrícula de Honor podrá ser otorgada a alumnos que hayan obtenido una calificación igual o superior a 9.5. Como norma general, estas menciones se irán otorgando en orden descendente a la nota final obtenida. En ningún caso el número de Matrículas de Honor concedidas será superior al máximo establecido para la asignatura en el curso académicoen curso. En caso de empate, primará la regularidad obtenida a lo largo de todos los sistemas de evaluación propuestos.

9. Organización docente semanal orientativa:

Semanas	Grupos Grandes	Grupos Reducidos Aula Estándar	Grupos Reducidos Aula de Informática	Grupos Reducidos Laboratorio	Grupos Reducidos prácticas de campo	Pruebas y/o actividades evaluables	Contenido desarrollado
#1	1	0	1	0	0		Tema 0
#2	1	0	1	0	0		Tema 1
#3	1	0	1	0	0		Tema 2
#4	1	0	1	0	0		Tema 2
#5	1	0	1	0	0	Entregas prácticas Tema 2	Tema 3
#6	1	0	1	0	0		Tema 3
#7	1	0	1	0	0	Entregas prácticas Tema 3	Tema 4
#8	1	0	1	0	0		Tema 5
#9	1	0	1	0	0		Tema 6
#10	1	0	1	0	0	Entrega prácticas Tema 6	Tema 7
#11	1	0	1	0	0	Entrega prácticas Tema 7	Tema 8
#12	1	0	1	0	0		Tema 9
#13	1	0	1	0	0	Entrega prácticas Tema 9	Tema 10
#14	1	0	1	0	0	Entrega prácticas Tema 10	Tema 11
#15	1	0	1	0	0	Prueba evaluable	
	15	0	15	0	0		