20-21

MÁSTER UNIVERSITARIO EN
CIBERSEGURIDAD

# GUÍA DE ESTUDIO PÚBLICA

# ANÁLISIS DE MALWARE

**CÓDIGO 31109078**

20-21

**ANÁLISIS DE MALWARE**

**CÓDIGO 31109078**

# ÍNDICE


PRESENTACIÓN Y CONTEXTUALIZACIÓN

REQUISITOS Y/O RECOMENDACIONES PARA CURSAR ESTA ASIGNATURA

EQUIPO DOCENTE

HORARIO DE ATENCIÓN AL ESTUDIANTE

COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE

RESULTADOS DE APRENDIZAJE

CONTENIDOS

METODOLOGÍA

SISTEMA DE EVALUACIÓN

BIBLIOGRAFÍA BÁSICA

BIBLIOGRAFÍA COMPLEMENTARIA

RECURSOS DE APOYO Y WEBGRAFÍA

| | |
|---|---|
| Nombre de la asignatura | ANÁLISIS DE MALWARE |
| Código | 31109078 |
| Curso académico | 2020/2021 |
| Título en que se imparte | MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD |
| Tipo | CONTENIDOS |
| Nº ETCS | 6 |
| Horas | 150.0 |
| Periodo | SEMESTRE 2 |
| Idiomas en que se imparte | CASTELLANO |

## PRESENTACIÓN Y CONTEXTUALIZACIÓN

Esta guía presenta las orientaciones básicas que requiere el estudiante para el estudio de la asignatura de Análisis de Malware, asignatura optativa del segundo semestre del Máster Universitario en Ciberseguridad. Por esta razón es muy recomendable leer con atención esta guía antes de iniciar el estudio, para adquirir una idea general de la asignatura y de los trabajos, actividades y prácticas que se van a desarrollar a lo largo del curso.

El malware representa un porcentaje muy elevado de las amenazas de los sistemas informáticos actuales. Esta asignatura se centra en ser capaz de identificar las principales características del malware y tenerlas en cuenta para poder realizar una detección temprana, así como aplicar técnicas de buenas prácticas para evitar la inyección de código malicioso en las aplicaciones desarrolladas en una organización. Por tanto, los conocimientos y habilidades prácticas el estudiante adquiera al cursar esta asignatura le servirán de cara a mejorar su perfil profesional dentro del contexto del análisis del malware, desde un punto de vista estático y otro dinámico, además de comprender y protegerse ante las técnicas de persistencia del malware dentro de los sistemas.

La asignatura de Análisis de Malware es una asignatura de 6 créditos ECTS, optativa, impartida en el segundo semestre del Máster Universitario en Ciberseguridad. Guarda relación con las siguientes asignaturas también disponibles en el mismo Máster:

- Análisis forense, asignatura de 6 créditos ECTS y obligatoria del primer semestre. El análisis forense es el proceso de identificar, preservar, analizar y presentar las evidencias de que un sistema informático ha sido comprometido de forma legal y aceptable. Mientras que la respuesta ante incidentes tiene como objetivo el volver el sistema a un estado operativo con un mínimo de garantías, el análisis forense por su parte tiene el objetivo de lograr analizar cómo se ha producido un ataque y localizar a sus responsables, sin tener en cuenta el tiempo que lleve esta búsqueda.
- Hacking Ético, asignatura de 6 créditos ECTS y obligatoria del primer semestre. En esta asignatura se presentan los contenidos y habilidades necesarios para analizar la seguridad de sistemas y aplicaciones. La asignatura cubrirá los conceptos de escaneo, pruebas, hacking y aseguración de sistemas. Se analizarán los diferentes problemas, amenazas y vulnerabilidades de los sistemas de información como detección, creación de políticas, análisis, control de acceso.

## REQUISITOS Y/O RECOMENDACIONES PARA CURSAR ESTA ASIGNATURA

Para cursar adecuadamente esta asignatura es recomendable tener los siguientes conocimientos previos:

•Conocer los fundamentos de seguridad en sistemas locales y distribuidos.

•Saber analizar y monitorizar elementos hardware y software de una infraestructura de red.

•Estar familiarizado con los sistemas operativos.

•Tener cierta experiencia en el manejo de software de virtualización.

•Saber programar scripts de gestión y configuración.

•Conocer (leer y escribir) el inglés técnico.

## EQUIPO DOCENTE


| | |
|---|---|
| Nombre y Apellidos | ANTONIO ROBLES GOMEZ (Coordinador de asignatura) |
| Correo Electrónico | arobles@scc.uned.es |
| Teléfono | 91398-8480 |
| Facultad | ESCUELA TÉCN.SUP INGENIERÍA INFORMÁTICA |
| Departamento | SISTEMAS DE COMUNICACIÓN Y CONTROL |

| | |
|---|---|
| Nombre y Apellidos | JUAN CARLOS LAZARO OBENSA |
| Correo Electrónico | jclo@scc.uned.es |
| Teléfono | 91398-7163 |
| Facultad | ESCUELA TÉCN.SUP INGENIERÍA INFORMÁTICA |
| Departamento | SISTEMAS DE COMUNICACIÓN Y CONTROL |

| | |
|---|---|
| Nombre y Apellidos | MIGUEL ROMERO HORTELANO |
| Correo Electrónico | mromero@scc.uned.es |
| Teléfono | 91398-7943 |
| Facultad | ESCUELA TÉCN.SUP INGENIERÍA INFORMÁTICA |
| Departamento | SISTEMAS DE COMUNICACIÓN Y CONTROL |


## HORARIO DE ATENCIÓN AL ESTUDIANTE

Las consultas sobre los contenidos y funcionamiento de la asignatura se plantearán principalmente en los foros del curso virtual, que serán atendidas por el Equipo Docente de la asignatura.

Para contactar directamente con el Equipo Docente se utilizará preferentemente el correo electrónico, pudiéndose también realizar consultas telefónicas y entrevista personal en los horarios establecidos.

**Datos del equipo docente:**

Antonio Robles Gómez

Horario: Lunes lectivos de 10:00 a 14:00

Email: arobles@scc.uned.es

Tfno: 91 398 8480

Andrés Duque Fernández
Horario: Lunes lectivos de 12:00 a 13:00 y de 15:00 a 18:00 horas
Email: aduque@scc.uned.es
Tfno: 91 398 7162

Juan Carlos Lázaro Obensa
Horario: Lunes lectivos de 16:00 a 20:00 horas
Email: jclo@scc.uned.es
Tfno: 91 398 7163

**Dirección postal:**
Escuela Técnica Superior de Ingeniería Informática
Dpto. de Sistemas de Comunicación y Control
C/ Juan del Rosal, 16
28040 - Madrid

## COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE

**COMPETENCIAS BÁSICAS**

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

CB7 - 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

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

CB9 - 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.

**COMPETENCIAS GENERALES**

CG1 - Analizar métodos y técnicas de ciberataques.

CG4 - Identificar, gestionar y desarrollar medidas y protocolos de seguridad en la operación y gestión de sistemas informáticos.

**COMPETENCIAS TRANSVERSALES**

CT1 - Ser capaz de abordar y desarrollar proyectos innovadores en entornos científicos, tecnológicos y multidisciplinares.

CT2 - Ser capar de tomar decisiones y formular juicios basados en criterios objetivos (datos

experimentales, científicos o de simulación disponibles).

**COMPETENCIAS ESPECÍFICAS**

CE5 - Analizar e identificar técnicas de ocultación de ataques a sistemas de comunicaciones y aplicaciones.

## RESULTADOS DE APRENDIZAJE

Los resultados más relevantes que se pretenden alcanzar con el estudio de esta asignatura son los siguientes:

•Comprender y aplicar métodos y técnicas de investigación de ciberataques a un sistema informático.

•Analizar y detectar anomalías y firmas de ataques en los sistemas informáticos.

•Analizar y detectar técnicas de ocultación de ataques a sistemas informáticos.

•Conocer las tendencias actuales en técnicas malware y las experiencias aprendidas en casos reales.

•Conocer y aplicar los mecanismos pertinentes para proteger los datos residentes en un sistema o en tránsito por una red.

## CONTENIDOS

### 1. Introducción al análisis de malware

•¿Qué es el malware?

•¿Por qué analizar malware?

•Tipos de análisis

### 2. Herramientas y métodos de análisis de malware

•El lenguaje ensamblador

•Herramientas básicas

•Métodos de depuración de malware

### 3. Metodología de análisis y sistemas de obtención de análisis de malware

•Análisis estático

•Análisis dinámico

### 4. Técnicas de ofuscación de malware

•Codificación simple

•Cifrado de malware

•Desempaquetado de malware

5. Amenazas Avanzadas Persistentes (Advanced Persistent Threats, APTs)

•Concepto de APT
•Técnicas de persistencia

6. Detección, Confinamiento y Erradicación

•Introducción
•Respuesta ante incidentes

## METODOLOGÍA

Esta asignatura ha sido diseñada para la enseñanza a distancia. Por tanto, el sistema de enseñanza-aprendizaje estará basado en gran parte en el estudio independiente o autónomo del estudiante. Para ello, el estudiante contará con diversos materiales que permitirán su trabajo autónomo y la Guía de Estudio de la asignatura, que incluye orientaciones para la realización de las actividades prácticas. Asimismo, mediante la plataforma virtual de la UNED existirá un contacto continuo entre el equipo docente y los/as estudiantes, así como una interrelación entre los propios estudiantes a través de los foros, importantísimo en la enseñanza no presencial.
El estudio de esta asignatura se realizará a través de los materiales que el Equipo Docente publicará en el curso virtual.
Esta asignatura de 6 créditos ECTS está planificada en 150 horas. El tiempo de las actividades formativas, siguiendo la anterior metodología, se han distribuido de forma orientativa de la siguiente manera:

•Estudio de los contenidos teóricos-prácticos utilizando la bibliografía y los materiales complementarios: 60 horas.
•Tutorías: 15 horas.
•Actividades en la plataforma virtual, incluyendo la participación en los debates propuestos en los foros de debate: 15 horas.
•Prácticas informáticas: 30 horas.
•Trabajos, de carácter individual y/o colectivo: 30 horas.

Tanto los trabajos individuales como los colectivos, además de las prácticas se podrán basar en el uso de software libre, así como de máquinas virtuales o simuladores disponibles que permitan emular diversos casos de estudio asociados con los objetivos propuestos en la asignatura.
Por otra parte, los medios necesarios para el aprendizaje son los siguientes:

1. **Materiales teórico-prácticos** preparados por el Equipo Docente para cubrir los conceptos básicos del temario.

1. **Bibliografía complementaria**. El estudiante puede encontrar en ella información adicional para completar su formación.
1. **Curso Virtual** de la asignatura, donde el estudiante encontrará:

•Una **guía de la asignatura** en la que se hace una descripción detallada del plan de trabajo propuesto.

•Un **calendario** con la distribución temporal de los temas propuesta por el Equipo Docente y con las fechas de entrega de las actividades teórico-prácticas que el estudiante tiene que realizar para su evaluación.

•Enunciado de las **actividades teórico-prácticas** propuestas y zona donde depositar los entregables asociados a dichas actividades.

•Los **foros de debate** por medio de los cuales el Equipo Docente aclarará las dudas de carácter general y que se usarán también para comunicar todas aquellas novedades que surjan a lo largo del curso. Éste será el principal medio de comunicación entre los distintos participantes en la asignatura.

## SISTEMA DE EVALUACIÓN

**TIPO DE PRUEBA PRESENCIAL**

| | |
|---|---|
| Tipo de examen | Examen mixto |
| Preguntas test | 10 |
| Preguntas desarrollo | 1 |
| Duración del examen | 120 (minutos) |

Material permitido en el examen

Ninguno.

Criterios de evaluación

El examen presencial constará de dos partes. La primera de ellas será un cuestionario de 10 preguntas de respuesta múltiple (4 opciones, de las cuales sólo una será correcta) que valdrá 7.5 puntos. Una respuesta bien contestada se valorará con 0.75 puntos, y cada fallo penalizará 0.25 puntos. Por su parte, la segunda parte será un ejercicio escrito de 2.5 puntos. Para que el equipo docente evalúe la segunda parte, será necesario que el estudiante haya obtenido al menos 3.5 puntos en el cuestionario.

| | |
|---|---|
| % del examen sobre la nota final | 40 |
| Nota del examen para aprobar sin PEC | |
| Nota máxima que aporta el examen a la calificación final sin PEC | 4 |
| Nota mínima en el examen para sumar la PEC | 4 |

Comentarios y observaciones

Las preguntas del cuestionario versarán sobre los contenidos teóricos y prácticos, tanto del material multimedia alojado en el curso virtual como del libro recomendado. El ejercicio escrito estará relacionado con dicho material desde una vertiente más práctica.
**La fecha de realización de la prueba presencial puede encontrarse en la web de Pruebas Presenciales: http://www.uned.es/pruebas-presenciales (apartado *Calendarios de exámenes*).**
**Para aprobar la asignatura se exigirá una nota mínima de 5 puntos y haber obtenido al menos 4 puntos en el examen presencial antes de ponderarla. La calificación final de la asignatura se calculará de la siguiente forma:**
En caso de que la nota del examen presencial antes de ponderarla sea inferior a 4, entonces la nota final será la nota de la prueba presencial sin ponderación.
En otro caso, se calculará la nota final sumando las diferentes pruebas de evaluación ponderadas con los porcentajes descritos arriba.

**CARACTERÍSTICAS DE LA PRUEBA PRESENCIAL Y/O LOS TRABAJOS**

Requiere Presencialidad: No

Descripción

Las prácticas informáticas son OBLIGATORIAS de realizar y superar. Consistirán en dos actividades prácticas que el estudiante deberá elaborar a lo largo del curso. Versarán sobre el análisis de malware estático/dinámico, ofuscación del malware, persistencia e inyección de código, etc. Los enunciados concretos de las mismas se publicarán en el curso virtual con la suficiente antelación. El seguimiento de las prácticas informáticas se realizará en la plataforma de aprendizaje del curso.
**Las prácticas son las siguientes:**
Práctica 1. Análisis estático/dinámico de malware en un entorno controlado y virtual. El plazo estimado de entrega es finales de abril.
Práctica 2. Estudiar técnicas de ofuscación de malware y técnicas de persistencia e inyección de código. El plazo estimado de entrega es mediados/finales de mayo.
**No será necesario que el estudiante acuda al Centro Asociado para realizar las prácticas informáticas y los trabajos, ya que podrán realizarse de forma online en su totalidad y se presentarán a través del curso virtual.**

Criterios de evaluación

El equipo docente publicará una guía para su realización, especificando los criterios de evaluación. Se debe obtener al menos un 5 en estas prácticas para que se haga media para la nota final.

Ponderación de la prueba presencial y/o los trabajos en la nota final: 50%

Fecha aproximada de entrega

Comentarios y observaciones

Las prácticas informáticas se podrán entregar tanto en el semestre en que se imparte la asignatura como en la convocatoria extraordinaria. El plazo previsto de entrega ordinaria será a principios de junio y el de entrega extraordinaria será a mediados/finales de julio.

**PRUEBAS DE EVALUACIÓN CONTINUA (PEC)**

¿Hay PEC? No

Descripción

Criterios de evaluación

Ponderación de la PEC en la nota final

Fecha aproximada de entrega

Comentarios y observaciones

**OTRAS ACTIVIDADES EVALUABLES**

¿Hay otra/s actividad/es evaluable/s? Si,no presencial

Descripción

Una de las actividades propuestas es la creación de un entorno virtual y controlado para llevar a cabo el análisis de malware y otras acciones en las Prácticas informáticas. Esta actividad es VOLUNTARIA, siendo el plazo de entrega la segunda/tercera semana de marzo.

**Otros aspectos a tener en cuenta serán la participación activa en los foros, la realización de los tests de autoevaluación y la participación en los debates propuestos por el equipo docente a lo largo del curso.**

Criterios de evaluación

Ponderación en la nota final 10%

Fecha aproximada de entrega

Comentarios y observaciones

**¿CÓMO SE OBTIENE LA NOTA FINAL?**

Para calcular la nota final de la asignatura se sumarán las notas obtenidas en la prueba presencial, prácticas informáticas y trabajos con los siguientes pesos:
Examen presencial —40%
Prácticas informáticas —50%
Trabajos —10%
**Para aprobar la asignatura se exigirá una nota mínima de 5 puntos y haber obtenido al menos 4 puntos en el Examen presencial antes de ponderarla. La calificación final de la asignatura se calculará de la siguiente forma:**
En caso de que la nota del Examen presencial antes de ponderarla sea inferior a 4, entonces la nota final será la nota de la prueba presencial sin ponderación.
Las Prácticas informáticas son OBLIGATORIAS y es necesario haber obtenido al menos 5 puntos en cada una de ellas.
En otro caso, se calculará la nota final sumando las diferentes pruebas de evaluación ponderadas con los porcentajes descritos arriba.
**Nota final = (Examen presencial x 0.4) + (Prácticas informáticas x 0.5) + (Trabajos x 0.1)**
**Las Prácticas informáticas se podrán entregar tanto en el semestre en que se imparte la asignatura como en la convocatoria extraordinaria. El plazo previsto de entrega ordinaria será a principios de junio y el de entrega extraordinaria será a mediados/finales de julio. En cambio, los Trabajos son voluntarios y sólo podrían realizarse durante el periodo ordinario de la asignatura de febrero a mayo.**

## BIBLIOGRAFÍA BÁSICA

ISBN(13):9781788397520
Título:LEARNING MALWARE ANALYSIS
Autor/es:Monnappa, K. A. ;
Editorial:Packt Publishing

El libro de Monnappa es accesible a través del siguiente enlace (una vez logado en Campus UNED): https://learning.oreilly.com/library/view/learning-malware-analysis/9781788392501/
Además, la bibliografía básica adicional será proporcionada al estudiante dentro del curso virtual, estará compuesta por materiales teórico-prácticos propuestos por el equipo docente.
Gran parte de la bibliografía, así como los recursos proporcionados al estudiante en el curso virtual pueden estar únicamente en inglés, debido a la novedad de algunos de los contenidos propuestos para la asignatura.
Se fomentará el uso de software libre siempre y cuando sea posible para la realización de las actividades y las practicas propuestas.

## BIBLIOGRAFÍA COMPLEMENTARIA

ISBN(13):9781593272906
Título:PRACTICAL MALWARE ANALYSIS
Autor/es:Andrew Honig ; Michael Sikorski ;
Editorial:No starch Press

ISBN(13):9781593278595
Título:MALWARE DATA SCIENCE
Autor/es:Hillary Sanders ; Joshua Saxe ;
Editorial:No starch Press

ISBN(13):9781788993111
Título:MASTERING MACHINE LEARNING FOR PENETRATION TESTING
Autor/es:Chiheh Chebbi ;
Editorial:Packt Publishing

El libro de Sikorski y Honig (Practical Malware Analysis) es accesible a través del siguiente enlace (una vez logado en Campus UNED): https://learning.oreilly.com/library/view/practical-malware-analysis/9781593272906/
El libro de Chebbi (Mastering Machine Learning for Penetration Testing) es accesible a través del siguiente enlace (una vez logado en Campus UNED): https://learning.oreilly.com/library/view/mastering-machine-learning/9781788997409/
El libro de Saxe y Sanders (Malware Data Science) es accesible a través del siguiente enlace (una vez logado en Campus UNED): https://learning.oreilly.com/library/view/malware-data-science/9781492067672/

## RECURSOS DE APOYO Y WEBGRAFÍA

Los/as estudiantes dispondrán de los siguientes recursos de apoyo al estudio:

- **Guía de la asignatura.** Incluye el plan de trabajo y orientaciones para su desarrollo. Esta guía será accesible desde el curso virtual.
- **Curso virtual.** A través de esta plataforma los/as estudiantes tienen la posibilidad de consultar información de la asignatura, realizar consultas al Equipo Docente a través de los foros correspondientes, consultar e intercambiar información con el resto de los compañeros/as.
- **Documentación de la asignatura.** El equipo docente publicará recursos adicionales que faciliten o profundicen los contenidos desarrollados en la asignatura, además de los contenidos ya ofrecidos.
- **Biblioteca.** El estudiante tendrá acceso tanto a las bibliotecas de los Centros Asociados como a la biblioteca de la Sede Central, en ellas podrá encontrar un entorno adecuado para el estudio, así como de distinta bibliografía que podrá serle de utilidad durante el proceso de

aprendizaje.

## IGUALDAD DE GÉNERO

En coherencia con el valor asumido de la igualdad de género, todas las denominaciones que en esta Guía hacen referencia a órganos de gobierno unipersonales, de representación, o miembros de la comunidad universitaria y se efectúan en género masculino, cuando no se hayan sustituido por términos genéricos, se entenderán hechas indistintamente en género femenino o masculino, según el sexo del titular que los desempeñe.