Guías docentes UJA

Horarios de tutorías

Llamamientos PEvAU

Guía docente 2024-25 - 77212010 - Ingeniería inversa y análisis de malware

Volver

TITULACIÓN: Máster Univ. en Seguridad informática (77212010)
CENTRO: ESCUELA POLITÉCNICA SUPERIOR (JAÉN)
TITULACIÓN: Doble Máster en Ingeniería informática y Seguridad informática (77612010)
CENTRO: ESCUELA POLITÉCNICA SUPERIOR (JAÉN)
CURSO: 2024-25
ASIGNATURA: Ingeniería inversa y análisis de malware

GUÍA DOCENTE

1. DATOS BÁSICOS DE LA ASIGNATURA

NOMBRE: Ingeniería inversa y análisis de malware
CÓDIGO: 77212010 (*) CURSO ACADÉMICO: 2024-25
TIPO: Obligatoria
Créditos ECTS: 3.0 CURSO: 1 CUATRIMESTRE: SC
WEB: https://platea.ujaen.es

2. DATOS BÁSICOS DEL PROFESORADO

NOMBRE: GÓMEZ ESPINOLA, JOSÉ IGNACIO
IMPARTE: Teoría [Profesor responsable]
DEPARTAMENTO: U118 - INFORMÁTICA
ÁREA: 570 - LENGUAJES Y SISTEMAS INFORMÁTICOS
N. DESPACHO: A3 - 122 E-MAIL: nacho@ujaen.es TLF: 953212382
TUTORÍAS: https://uvirtual.ujaen.es/pub/es/informacionacademica/tutorias/p/58125
URL WEB: http://www4.ujaen.es/~nacho
ORCID: https://orcid.org/0000-0003-0230-3307

NOMBRE: SÁNCHEZ PEREA, ANTONIO
IMPARTE: Teoría
DEPARTAMENTO: -
ÁREA: -
N. DESPACHO: - E-MAIL: - TLF: -
TUTORÍAS: https://uvirtual.ujaen.es/pub/es/informacionacademica/tutorias/p/79716
URL WEB: -
ORCID: -

NOMBRE: Sánchez Perea, Antonio
E-MAIL: asanchez@plutec.net TLF: -
URL WEB: https://hispasec.com/es/
INSTITUCIÓN: Hispasec Sistemas

3. PRERREQUISITOS, CONTEXTO Y RECOMENDACIONES

PRERREQUISITOS:

-

CONTEXTO DENTRO DE LA TITULACIÓN:

.

RECOMENDACIONES Y ADAPTACIONES CURRICULARES:

Se recomienda asistir regularmente a clase y participar activamente en las distintas actividades que se vayan proponiendo a lo largo del curso

El alumnado que presente necesidades específicas de apoyo educativo, lo ha de notificar personalmente al Servicio de Atención y Ayudas al Estudiante para proceder a realizar, en su caso, la adaptación curricular correspondiente.

4. COMPETENCIAS Y RESULTADOS DE APRENDIZAJE

código	Denominación de la competencia
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
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
CG1MSEGI	Conocer y utilizar las Tecnologías de la Información y la Comunicación aplicadas a la Seguridad Informática
CG3MSEGI	Comprender y ser capaz de aplicar las herramientas básicas de investigación en el ámbito de la Seguridad Informática.
CTI2	Conocer y aplicar las políticas y prácticas de atención a colectivos sociales especialmente desfavorecidos e incorporar los principios de igualdad entre hombres y mujeres y de accesibilidad universal y diseño para todos a su ámbito de estudio
CTI3	Conocer y aplicar las herramientas para la búsqueda activa de empleo y el desarrollo de proyectos de emprendimiento.
E10MSEGI	Saber aplicar técnicas y algoritmos de ingeniería inversa al código fuente de aplicaciones que afecten a la Seguridad Informática.

Resultados de aprendizaje

Resultado RB7	Saber aplicar e integrar sus conocimientos, la comprensión de estos, su fundamentación científica y sus capacidades de resolución de problemas en entornos nuevos y definidos de forma imprecisa, incluyendo contextos de carácter multidisciplinar tanto investigadores como profesionales altamente especializados.
Resultado RB9	Saber transmitir de un modo claro y sin ambigüedades a un público especializado o no, resultados procedentes de la investigación científica y tecnológica o del ámbito de la innovación más avanzada, así como los fundamentos más relevantes sobre los que se sustentan.
Resultado RE10MSE	Aplica las técnicas y algoritmos de ingeniería inversa al código fuente de aplicaciones que afecten a la Seguridad Informática.
Resultado RG1mSEGI	Demuestra que conoce y utiliza las Tecnologías de la Información y la Comunicación aplicadas a la Seguridad Informática.
Resultado RG3mSE	Demuestra que comprende y utiliza las herramientas básicas de investigación en el ámbito de la Seguridad Informática.
Resultado RT2	Demuestra conocimiento y es capaz de aplicar las políticas y prácticas de atención a colectivos sociales especialmente desfavorecidos incorporando los principios de igualdad entre hombres y mujeres y de accesibilidad universal y diseño para todos a su ámbito de estudio.
Resultado RT3	Conoce y aplica las herramientas para la búsqueda activa de empleo y el desarrollo de proyectos de emprendimiento.

5. CONTENIDOS

· Código máquina y archivos binarios.
· Desensamblado y descompilado de código.
· Lenguajes compilados.
· Lenguajes interpretados.
· Lenguajes basados en códigos intermedios.
· Sandboxes.

Bloque

I. Análisis básico de binarios

- Máquinas virtuales
- Análisis básico estático
- Análisis básico dinámico

Bloque

II. Análisis estático avanzado

- Arquitectura x86
- Código C visto en ensamblador
- Analizando binarios maliciosos en Windows
- IDA Pro

Bloque

III. Funcionalidades del malware

- Tipos
  de malware y sus funcionalidades
- Cómo
  se lanza el malware
- Codificación de datos
- Detección
  basada en conexiones de red

Bloque
IV. Análisis dinámico avanzado

- Depuración
- Ollydbg

Bloque V. Android

- Análisis
  de Malware en Android

Prácticas

El alumnado tendrá la posibilidad de desarrollar diferentes prácticas relacionadas con el contenido desarrollado en las sesiones presenciales

6. METODOLOGÍA Y ACTIVIDADES

ACTIVIDADES	HORAS PRESEN-CIALES	HORAS TRABAJO AUTÓ-NOMO	TOTAL HORAS	CRÉDITOS ECTS	COMPETENCIAS (códigos)
A1 - Clases expositivas en gran grupo ▪ M 32 - Conferencia plenaria, sesión magistral	6.0	9.0	15.0	0.6	▪ CG3MSEGI ▪ CTI2 ▪ CTI3 ▪ E10MSEGI
A2a - Actividades en pequeño grupo ▪ M2a - Docencia en pequeño grupo: seminarios, debates, actividades prácticas y aclaración de dudas	6.0	9.0	15.0	0.6	▪ CB7 ▪ CB9 ▪ E10MSEGI
A3a - Actividades dirigidas en plataforma de docencia virtual ▪ M3A - -	0.0	45.0	45.0	1.8	▪ CG1MSEGI ▪ CTI2
TOTALES:	12.0	63.0	75.0	3.0	

INFORMACIÓN DETALLADA:

Sesiones presenciales

- Clases magistrales
- Exposición de teoría y práctica
- Aplicación práctica de los conceptos expuestos
- Resolución de dudas

Sesiones no presenciales

- Seguimiento de ejercicios
- Seguimiento de prácticas
- Resolución de dudas

7. SISTEMA DE EVALUACIÓN

ASPECTO	CRITERIOS	INSTRUMENTO	PESO
Asistencia y/o participación en actividades presenciales y/o virtuales	Asistencia en actividades presenciales	-	10.0%
Conceptos teóricos de la materia	Examen sobre los conceptos teóricos y prácticos de la materia	-	30.0%
Realización de trabajos, casos o ejercicios	Realización de trabajos, casos o ejercicios prácticos	-	50.0%
Prácticas de laboratorio/campo/uso de	Participación en actividades presenciales	-	10.0%

ASPECTO	CRITERIOS	INSTRUMENTO	PESO
herramientas TIC			

El sistema de calificación se regirá por lo establecido en el RD 1125/2003 de 5 de septiembre por el que se establece el sistema europeo de créditos y el sistema de calificaciones en la titulaciones universitarias de carácter oficial

INFORMACIÓN DETALLADA:

Competencias por **Sistema de Evaluación**:

- S1 (asistencia): CB7, CG1MSEGI, CTI2, CTI3
- S2 (examen): CB7, CB9, CG1MSEGI, CG3MSEGI, E10MSEGI
- S3 (ejercicios y trabajos): CB7, CB9, CG1MSEGI, CG3MSEGI, E10MSEGI
- S4 (participación): CB7, CB9, CG1MSEGI, CG3MSEGI

Resultados por **Sistema de Evaluación**:

-
  - S1 (asistencia): RB7, RT2, RT3
  - S2 (examen): RB7, RB9, RE10MSE, RG1mSEGI, RG3mSE
  - S3 (ejercicios y trabajos): RB7, RB9, RE10MSE, RG1mSEGI, RG3mSE
  - S4 (participación): RB7, RB9, RE10MSE, RG1mSEGI, RG3mSE

Descripción detallada:

CTI2. Se evaluarán cuestiones relacionadas con la igualdad de oportunidades en el ámbito de la seguridad informática y a colectivos sociales especialmente desfavorecidos, aplicado a nuestro contexto socio-económico.

CTI3. Se debatirá, con el alumnado, y dentro del ámbito de la disciplina que desarrolla la asignatura, las diferentes oportunidades de trabajo existentes dentro de su futura especialización.

Se llevará a cabo una **evaluación global** de la asignatura, recogida en el artículo 13 del Reglamento de Régimen Académico y de Evaluación del Alumnado de la Universidad de Jaén, para lo cual se tendrán en cuenta los siguientes apartados:

-Teoría (hasta 3 puntos): examen escrito. Es necesario presentarse al examen para poder sumar el resto de puntuaciones obtenidas en la asignatura

-Prácticas (hasta 5 puntos): desarrollo de prácticas en sesiones no presenciales. Es necesario obtener al menos 2.5 puntos para poder sumar el resto de puntuaciones obtenidas en la asignatura

- Asistencia a sesiones presenciales: hasta 1 punto

- Participación en sesiones presenciales: hasta 1 punto

Para poder superar la asignatura es necesario haberse presentado al examen de teoría y obtener al menos 2.5 puntos en la evaluación del trabajo práctico aplicado. Además, será necesario sumar al menos 5 puntos entre todos los apartados puntuables.

Para poder aprobar la convocatoria extraordinaria es obligatorio haber superado la parte práctica durante la última convocatoria ordinaria.

En la convocatoria extraordinaria se evaluará el apartado de Teoría (examen escrito), dando opción a obtener hasta 3 puntos. Para garantizar la opción a obtener la máxima nota posible en dicha convocatoria (de acuerdo con el Reglamento de Régimen Académico y de Evaluación del Alumnado de la Universidad de Jaén, aprobado en Consejo de Gobierno nº33, de 21/11/2013), a dicha puntuación se le sumará la puntuación obtenida en los restantes apartados evaluables (asistencia, prácticas y participación) durante la última convocatoria ordinaria

8. DOCUMENTACIÓN / BIBLIOGRAFÍA

ESPECÍFICA O BÁSICA:

- Intelligent Mobile Malware Detection. Edición: -. Autor: -. Editorial: CRC Press.
  - **Observaciones**: Recurso electrónico
  (C. Biblioteca)
- Practical malware analysis [Recurso electrónico] : the hands-on guide to dissecting malicious softwa. Edición: -. Autor: Sikorski, Michael. Editorial: San Francisco : No Starch Press, 2012 (C. Biblioteca)

GENERAL Y COMPLEMENTARIA:

- Mastering malware analysis : a malware analyst's practical guide to combating malicious software, APT, cybercrime, and IoT attacks . Edición: Second edition.. Autor: Kleymenov, Alexey, author.. Editorial: Packt Publishing Ltd. (C. Biblioteca)

9. CRONOGRAMA

Semana	A1	A2	A3	Trabajo autónomo	Observaciones

Nº 1: 24 feb 2025 - 1 mar 2025	1	1	7.5	3	Bloque I
Nº 2: 3 - 8 mar 2025	1	1	7.5	3	Bloque II
Nº 3: 10 - 15 mar 2025	1	1	7.5	3	Bloque II
Nº 4: 17 - 22 mar 2025	1	1	7.5	3	Bloque III
Nº 5: 24 - 29 mar 2025	1	1	7.5	3	Bloque IV
Nº 6: 31 mar - 5 abr 2025	1	1	7.5	3	Bloque V
Total	6	6	45	18	

10. OBJETIVOS DE DESARROLLO SOSTENIBLE

Igualdad de género

Industria, innovación e infraestructura

Paz, justicia e instituciones sólidas

Alianzas para lograr objetivos

INFORMACIÓN DETALLADA:

La asignatura "Ingeniería Inversa y Análisis de Malware" del Máster de Seguridad Informática juega un papel crucial en la lucha contra las ciberamenazas y la protección de la sociedad digital. Al abordar el análisis y la comprensión del malware, esta asignatura contribuye directamente al logro de varios Objetivos de Desarrollo Sostenible (ODS) de las Naciones Unidas. A continuación, se detallan los ODS más relevantes para la asignatura, junto con una breve explicación de su aplicabilidad:

ODS 5: Igualdad de género

Principal utilidad para la asignatura:

- Fomentar la participación de las mujeres en el campo de la ciberseguridad, un área predominantemente masculina

ODS 9: Industria, innovación e infraestructura

Principal utilidad para la asignatura:

- Incentivar la investigación y el desarrollo de herramientas y técnicas avanzadas de ingeniería inversa y análisis de malware.
- Promover la colaboración entre el ámbito académico, la industria y el sector público para combatir las nuevas amenazas cibernéticas.
- Fomentar la adopción de prácticas de seguridad robustas en el desarrollo de software y sistemas informáticos.

ODS 16: Paz, justicia e instituciones sólidas

Principal utilidad para la asignatura:

- Capacitar a los profesionales para investigar delitos cibernéticos.
- Desarrollar mecanismos para la cooperación internacional en la lucha contra el cibercrimen.
- Promover la protección de los derechos humanos en el ámbito digital, incluyendo la privacidad y la libertad de expresión.

ODS 17: Alianzas para lograr los objetivos

Principal utilidad para la asignatura:

- Fomentar el intercambio de información y mejores prácticas entre expertos en seguridad informática de todo el mundo.
- Promover la creación de plataformas de colaboración para el desarrollo de herramientas y técnicas de análisis de malware.
- Apoyar a los países en vías de desarrollo en la construcción de capacidades para combatir el cibercrimen.

En resumen, la asignatura "Ingeniería Inversa y Análisis de Malware" del Máster de Seguridad Informática contribuye al logro de diversos ODS al empoderar a las mujeres en la lucha contra el cibercrimen, impulsar la innovación tecnológica, fortalecer la ciberseguridad para la paz y la justicia, y fomentar

alianzas globales para combatir el malware. Al abordar estos desafíos, la asignatura contribuye a crear un mundo digital más seguro y equitativo para todos.

11. ESCENARIO MIXTO

1) METODOLOGÍA DOCENTE Y ACTIVIDADES FORMATIVAS.

Actividades formativas	Formato (presencial/online)*	Metodología Docente Descripción
A1 - Clases expositivas en gran grupo	Presencial 100% (*)	Clase a todos los estudiantes del grupo en el horario y aula asignados.
A2 - Clases en pequeño grupo	Presencial 100% (*)	Clase a todos los estudiantes del grupo en el horario y aula asignados.

(*) El Centro podrá variar el porcentaje de presencialidad dependiendo del número de estudiantes y el aforo del aula/laboratorio. En caso de presencialidad inferior al 100%, se realizará rotación periódica de estudiantes según determine el Centro.

2) SISTEMA DE EVALUACIÓN.

El sistema e instrumentos de evaluación serán los mismos que para la modalidad presencial, sustituyendo las pruebas presenciales por pruebas similares desarrolladas mediante el uso de la plataforma de docencia online u otras que la Universidad permita o habilite, siempre que se garantice la identidad del estudiante.

3) RECURSOS.

Se utilizarán los sistemas de videoconferencia que estén disponibles en los espacios que se habiliten para la docencia, así como la plataforma de docencia de la Universidad. Las actividades que no puedan realizarse de forma presencial se realizarán mediante actividades síncronas y/o asíncronas realizadas mediante la plataforma de docencia virtual.

Queda expresamente prohibida la grabación por ningún medio de las actividades presenciales o no presenciales síncronas sin permiso explícito del docente.

12. ESCENARIO NO PRESENCIAL

1) METODOLOGÍA DOCENTE Y ACTIVIDADES FORMATIVAS.

Las actividades que no puedan realizarse de forma presencial se realizarán mediante actividades síncronas y/o asíncronas realizadas mediante la plataforma de docencia virtual y los mecanismos que la Universidad permita o habilite.

2) SISTEMA DE EVALUACIÓN.

El sistema e instrumentos de evaluación serán los mismos que para la modalidad presencial, sustituyendo las pruebas presenciales por pruebas similares desarrolladas mediante el uso de la plataforma de docencia online u otras que la Universidad permita o habilite, siempre que se garantice la identidad del estudiante.

3) RECURSOS.

Las actividades que no puedan realizarse de forma presencial se realizarán mediante actividades síncronas y/o asíncronas realizadas mediante la plataforma de docencia virtual.

En todo caso, queda expresamente prohibida la grabación por ningún medio de las actividades presenciales o no presenciales síncronas sin permiso explícito del docente.

CLÁUSULA DE PROTECCIÓN DE DATOS (evaluación on-line)

Responsable del tratamiento: Universidad de Jaén, Campus Las Lagunillas, s/n, 23071 Jaén

Delegado de Protección de Datos:dpo@ujaen.es

Finalidad: Conforme a la Ley de Universidades y demás legislación estatal y autonómica vigente, realizar los exámenes correspondientes a las asignaturas en las que el alumno o alumna se encuentre matriculado. Con el fin de evitar fraudes en la realización del mismo, el examen se realizará en la

modalidad de video llamada, pudiendo el personal de la Universidad de Jaén contrastar la imagen de la persona que está realizando la prueba de evaluación con los archivos fotográficos del alumno en el momento de la matrícula. Igualmente, con la finalidad de dotar a la prueba de evaluación de contenido probatorio de cara a revisiones o impugnaciones de la misma, de acuerdo con la normativa vigente, la prueba de evaluación será grabada.

Legitimación: cumplimiento de obligaciones legales (Ley de Universidades) y demás normativa estatal y autonómica vigente.

Destinatarios: prestadores de servicios titulares de las plataformas en las que se realicen las pruebas con los que la Universidad de Jaén tiene suscritos los correspondientes contratos de acceso a datos.

Plazos de conservación: los establecidos en la normativa aplicable. En el supuesto en concreto de las grabaciones de los exámenes, mientras no estén cerradas las actas definitivas y la prueba de evaluación pueda ser revisada o impugnada.

Derechos: puede ejercitar sus derechos de acceso, rectificación, cancelación, oposición, supresión, limitación y portabilidad remitiendo un escrito a la dirección postal o electrónica indicada anteriormente. En el supuesto que considere que sus derechos han sido vulnerados, puede presentar una reclamación ante el Consejo de Transparencia y Protección de Datos de Andalucía www.ctpdandalucia.es

Cláusula grabación de clases PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

Responsable del tratamiento: Universidad de Jaén, Paraje Las Lagunillas, s/n; Tel.953 212121; www.ujaen.es

Delegado de Protección de Datos (DPO): TELEFÓNICA, S.A.U. ; Email: dpo@ujaen.es

Finalidad del tratamiento: Gestionar la adecuada grabación de las sesiones docentes con el objetivo de hacer posible la enseñanza en un escenario de docencia multimodal y/o no presencial.

Plazo de conservación: Las imágenes serán conservadas durante los plazos legalmente previstos en la normativa vigente.

Legitimación: Los datos son tratados en base al cumplimiento de obligaciones legales (Ley Orgánica 6/2001, de 21 de diciembre, de Universidades) y el consentimiento otorgado mediante la marcación de la casilla habilitada a tal efecto.

Destinatarios de los datos (cesiones o transferencias): Toda aquella persona que vaya a acceder a las diferentes modalidades de enseñanza.

Derechos: Ud. podrá ejercitar los derechos de Acceso, Rectificación, Cancelación, Portabilidad, Limitación del tratamiento, Supresión o, en su caso, Oposición. Para ejercitar los derechos deberá presentar un escrito en la dirección arriba señalada dirigido al Servicio de Información, Registro y Administración Electrónica de la Universidad de Jaén, o bien, mediante correo electrónico a la dirección de correo electrónico. Deberá especificar cuál de estos derechos solicita sea satisfecho y, a su vez, deberá acompañarse de la fotocopia del DNI o documento identificativo equivalente. En caso de que actuara mediante representante, legal o voluntario, deberá aportar también documento que acredite la representación y documento identificativo del mismo. Asimismo, en caso de considerar vulnerado su derecho a la protección de datos personales, podrá interponer una reclamación ante el Consejo de Transparencia y Protección de Datos de Andalucía www.ctpdandalucia.es