DATOS GENERALES DE LA ASIGNATURA

ASIGNATURA: Ataques a Sistemas Informáticos
PLAN DE ESTUDIOS: Grado en Ingeniería Informática (PGR-INFORM)
GRUPO: 2526-T1
CENTRO: Escuela Politécnica Superior
CARÁCTER DE LA ASIGNATURA: Optativo
ECTS: 6,0
CURSO: 4º
SEMESTRE: 1º Semestre
IDIOMA EN QUE SE IMPARTE:
Castellano, excepto las asignaturas de idiomas que se impartirán en el idioma correspondiente

DATOS DEL PROFESOR

NOMBRE Y APELLIDOS: BLAS TORREGROSA GARCÍA
EMAIL: btorregrosa@uemc.es
TELÉFONO: 983 00 10 00
HORARIO DE TUTORÍAS: Lunes a las 20:00 horas
CV DOCENTE:
Desde el año 2022 a la actualidad he impartido docencia en la UEMC en el Máster en Gestión y Análisis de Grandes Volúmenes de Datos: Big Data :

- Técnicas de Desarrollo Avanzado de Aplicaciones Big Data
- Plataformas Avanzadas de Desarrollo

CV PROFESIONAL:

- Ingeniero en Informática y Máster en Segureidad Informática
- Más de 20 años de experiencia profesional en AA.PP. y en la empresa privada en el ámbito del desarrollo software, administración de sistemas así como en ciberseguridad y en computación en la nube
- Certificaciones: HTB CPTS, CRTA, AWS DevOps, AWS Developer, AWS Architect

DATOS ESPECÍFICOS DE LA ASIGNATURA

DESCRIPTOR DE LA ASIGNATURA:
En un entorno digital cada vez más complejo y expuesto a amenazas constantes, entender cómo se produce un ataque y cómo defenderse eficazmente se ha vuelto esencial tanto en el ámbito personal como profesional. Administradores, defensores y atacantes éticos deben conocer las técnicas utilizadas por actores maliciosos para comprometer sistemas, así como las estrategias de defensa para detectar, contener y responder a incidentes.

Esta asignatura se centra en los roles del *Red Team* (equipo ofensivo) y del *Blue Team* (equipo defensivo), ofreciendo una visión práctica y aplicada del ciclo completo de un ataque y su detección. A lo largo del curso se abordarán los siguientes ejes:

- Fundamentos de ciberseguridad (pensamiento ofensivo y defensivo)
- Técnicas de reconocimiento y obtención de información
- Principales vectores de ataque utilizados por los atacantes
- Métodos de explotación de vulnerabilidades y respuesta defensiva

Se recomienda haber cursado previamente asignaturas como **Redes de Comunicaciones** y **Fundamentos de Seguridad Informática y Criptografía**, ya que proporcionan la base teórica necesaria. Además, es conveniente tener conocimientos de sistemas operativos, de programación en algún lenguaje (Python, Java, ...) así como herramientas de virtualización para realizar prácticas.

CONTENIDOS DE LA ASIGNATURA:

1. **Fundamentos de ciberseguridad**
    1. Introducción y conceptos básicos
    2. Ingeniería social
2. **Recopilación de información**
    1. Fuentes abiertas OSINT
    2. Reconocimiento de infraestructura
    3. Enumeración de servicios
3. **Ataques a redes y sistemas informáticos**
    1. Ataques a redes TCP/IP. Metasploit
    2. Ataques a aplicaciones web
    3. Persistencia, escalado de privilegios y pivotaje

RECURSOS DE APRENDIZAJE:

- **Hacking ético.** J.L. BERENGUEL GÓMEZ y P. ESTEBAN SÁNCHEZ. Ed. Paraninfo. 2024
- **The Hacker Playbook 3**: Practical Guide To Penetration Testing. Peter KIM. Ed. Secure Planet. 2018
- **Criptografía Ofensiva** 1 y 2. A. Muñoz Muñoz. 2020/2024

Webs

- Libro online de hacktricks. https://book.hacktricks.wiki/en/index.html
- Sitio web de Hacking Articles: https://www.hackingarticles.in/
- Academia hacker de INCIBE: https://www.incibe.es/ed2026/talento-hacker/academia-hacker
- HackTheBox: https://app.hackthebox.com/
- HackTheBox Academy: https://academy.hackthebox.com/
- TryHackMe: https://tryhackme.com/

COMPETENCIAS Y RESULTADOS DE APRENDIZAJE A ADQUIRIR POR EL ALUMNO

COMPETENCIAS BÁSICAS:

- CB1. Que los estudiantes hayan demostrado poseer y comprender conocimientos en un área de estudio que parte de la base de la educación secundaria general, y se suele encontrar a un nivel que, si bien se apoya en libros de texto avanzados, incluye también algunos aspectos que implican conocimientos procedentes de la vanguardia de su campo de estudio
- CB2. Que los estudiantes sepan aplicar sus conocimientos a su trabajo o vocación de una forma profesional y posean las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro de su área de estudio
- CB5. Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía

COMPETENCIAS GENERALES:

- CG01. Capacidad de organización y planificación en el ámbito tecnológico
- CG02. Capacidad y habilidad para la toma de decisiones en el ámbito tecnológico

COMPETENCIAS ESPECÍFICAS:

- TI7. Capacidad para comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos
- SI5. Capacidad para comprender y aplicar los principios de la evaluación de riesgos y aplicarlos

correctamente en la elaboración y ejecución de planes de actuación
- CEN4. Capacidad para identificar y comprender los distintos vectores de ataque que pueden ser utilizados para vulnerar la seguridad de un sistema.
- CEN5. Capacidad para la realización y comprensión de un informe de una auditoria de seguridad.

RESULTADOS DE APRENDIZAJE:

El alumno será capaz de:

- Conocer los principios y técnicas de la realización de auditorías de seguridad
- Identificar posibles vectores de ataques
- Buscar y explotar vulnerabilidades.

BIBLIOGRAFÍA Y RECURSOS DE REFERENCIA GENERALES

BIBLIOGRAFÍA BÁSICA:

- J.L. BERENGUEL GÓMEZ y P. ESTEBAN SÁNCHEZ. (2024): Hacking ético.. Paraninfo. ISBN: 9788428362672

WEBS DE REFERENCIA:

Web / Descripcion
Libro online de Hacktricks(https://book.hacktricks.wiki/en/index.html) HackTricks es un libro online colaborativo que recopila técnicas, trucos y recursos utilizados en hacking ético, pentesting y CTFs. Es una referencia muy completa para red teamers, con ejemplos prácticos sobre explotación, escalada de privilegios, evasión de defensas y más.

PLANIFICACIÓN DEL PROCESO DE ENSEÑANZA-APRENDIZAJE DE LA ASIGNATURA

METODOLOGÍAS:

MÉTODO DIDÁCTICO:

Esta asignatura cuenta con suficiente carga teórica como para utilizar el método didáctico o expositivo. Se basa en el concepto de clase magistral, en el que también se incluye la resolución en clase de ejercicios y problemas.

MÉTODO DIALÉCTICO:

En algunos componentes de la asignatura, como la presentación y la corrección de los trabajos, se utiliza el método dialéctico, que habilita una participación más activa de los alumnos.

MÉTODO HEURÍSTICO:

La realización de los trabajos propuestos, relacionados con diversos campos de la seguridad informática, requiere un trabajo autónomo a desarrollar por parte del alumno.

CONSIDERACIONES DE LA PLANIFICACIÓN:

La asignatura se planifica teniendo en cuenta las siguientes actividades formativas:

- Clase presencial. Se sucederán a lo largo de todo el curso. Se utilizará, principalmente, el método didáctico o expositivo.
- Presentación de trabajos. Los alumnos deberán realizar (y entregar para su evaluación) una serie de trabajos sobre temáticas relacionadas con la asignatura. Algunos de dichos trabajos se presentarán en clase.
- Tutorías individuales. Las tutorías individuales se desarrollaran en modalidad online en el horario especificado en la guía docente.
- Evaluación. La asignatura se evalúa –en su modo de evaluación continua– mediante una combinación de pruebas de evaluación parciales asociadas al Programa de Teoría de la misma y una serie de trabajos prácticos realizados y entregados por el alumno.

Estructura temporal de la asignatura:

- Bloque 1 de contenidos teóricos y prácticos. Se desarrolla entre el comienzo de curso y la 3ª semana, aproximadamente.
- Bloque 2 de contenidos teóricos y prácticos. Se desarrolla entre la 4ª y la 8ª aproximadamente
- Bloque 3 de contenidos teóricos y prácticos. Se desarrolla entre la 9ª y la 15ª semana de curso, aproximadamente.
- Ejercicios prácticos. Se desarrollarán a lo largo de todo el curso, en paralelo a la teoría.

Esta planificación estimada podrá verse modificada por causas ajenas a la organización académica primeramente presentada. El profesor informará convenientemente a los alumnos de las nuevas modificaciones puntuales

PROGRAMACIÓN DE ACTIVIDADES Y EVALUACIONES:

PROGRAMACIÓN DE ACTIVIDADES:

Actividad	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	¿Se evalúa?	CO	CE
1ª actividad de evaluación continua y entrega de trabajos				X												X	X	X
2ª actividad de evaluación continua								X								X	X	X
3ª actividad de evaluación continua															X	X	X	X

CONSIDERACIONES DE LA EVALUACIÓN EN LA CONVOCATORIA ORDINARIA:

El conocimiento de los contenidos y la adquisición de las competencias relativas a esta asignatura se evalúan de forma continua, utilizando los sistemas que a continuación se detallan:

Tanto las pruebas de evaluación parciales como las finales (en el caso de que fueran necesarias) constarán siempre de un conjunto de preguntas de tipo respuesta corta, desarrollo y/o tipo ejercicio. La información concreta sobre cada prueba se publica en el e-Campus de la asignatura con la debida antelación.

- 1ª actividad de evaluación continua. Corresponde al bloque 1 (20% de la nota final).
  Pruebas escritas (50%) - Ejecución de prácticas (50%)
- 2ª actividad de evaluación continua. Corresponde al bloque 2 (20% de la nota final).
  Pruebas escritas (50%) - Ejecución de prácticas (50%)
- 3ª actividad de evaluación continua. Corresponde al bloque 3 (30% de la nota final).
  Pruebas escritas (50%) - Ejecución de prácticas (50%)

Los alumnos deberán realizar una serie de ejercicios prácticos que deberán ser entregados junto con un trabajo final. Estas actividades (los ejercicios prácticos y el trabajo final), suponen un 25% de la nota final, ya que junto con los ejercicios, se deberá presentar una memoria sobre la realización de la actividad. Tanto la herramienta de entrega como las instrucciones concretas con respecto a esta actividad se publican en el e-Campus de la asignatura con la debida antelación.
Las competencias de tipo genérico (capacidad de análisis y síntesis; organización; planificación; toma de decisiones; trabajo en equipo; creatividad; razonamiento crítico; etc.) serán evaluadas mediante Técnicas de observación en cada una de las actividades realizadas a lo largo del curso. En global, estas competencias suponen un 5% de la nota final.

Para superar la asignatura es necesario que el alumno obtenga una calificación global (media) mínima de 5 puntos sobre 10.

Sólo se habilita un plazo para la entrega de trabajos y prácticas, por lo que la calificación de esta primera entrega (llevada a cabo dentro del proceso de evaluación continua) es la definitiva para la convocatoria ordinaria.
Para superar la asignatura aplicando la evaluación continua sólo se permitirá un suspenso en cualquiera de las actividades propuestas (bien sea en las actividades de evaluación o en los ejercicios), siempre que ese suspenso no tenga una nota inferior a 4 puntos sobre 10 y que, evidentemente, la media global supere el 5.
Si la nota media no supera el 5, en el expediente aparecerá la nota media.
En caso de tener mas de una actividad suspensa y la media es superior a 5, en el expediente aparecerá una nota media de 4.

En caso de tener una actividad suspensa con una nota inferior a 4 y la media es superior a 5, en el expediente aparecerá una nota media de 4.
Los alumnos que no logren el aprobado mediante el sistema de evaluación continua deben superar de nuevo una prueba de evaluación correspondiente a la prueba de evaluación que tenían suspensa. Es decir, existirán 3 pruebas de evaluación que servirán para recuperar la nota de cada una de las pruebas suspensas. Cada una de estas pruebas tendrá el peso establecido anteriormente.

En cuanto al 25% correspondiente a la parte de actividades, será recuperable mediante un trabajo/proyecto que costará de varios tipos de ejercicios o problemáticas tratadas durante el desarrollo de la asignatura. Se deberá obtener un mínimo de 5 puntos (teniendo en cuenta los porcentajes de puntuación antes citados para cada prueba de recuperación) para superar la asignatura. Siendo necesario aprobar ambas partes.
Esta planificación tiene un carácter meramente orientativo y podrá ser modificada a criterio del profesor, en función de circunstancias externas y de la evolución del grupo. El profesor informará convenientemente a los alumnos de dichas modificaciones. Los sistemas de evaluación descritos en esta guía docente son sensibles tanto a la evaluación de las competencias como de los contenidos de la asignatura. La realización fraudulenta de cualquiera de las pruebas de evaluación, así como la extracción de información de las pruebas de evaluación, será sancionada según lo descrito en el Reglamento 7/2015, de 20 de noviembre, de Régimen Disciplinario de los estudiantes, Arts. 4, 5 y 7 y derivarán en la pérdida de la convocatoria correspondiente, así como en el reflejo de la falta y de su motivo en el expediente académico del alumno.

CONSIDERACIONES DE LA EVALUACIÓN EN LA CONVOCATORIA EXTRAORDINARIA:

El Programa de Teoría de la asignatura se evaluará mediante una prueba única y global sobre el contenido teórico.
En la convocatoria extraordinaria se habilitará una nueva opción para la entrega de los ejercicios y de la memoria de los mismos. Los alumnos que hubieran realizado la correspondiente entrega en la opción habilitada en convocatoria ordinaria pueden mantener su nota.

En la convocatoria extraordinaria no se aplicará el sistema de calificación Técnicas de observación ya que el carácter extraordinario (no presencial para ciertas actividades) de dicha convocatoria no lo permite.
La nota final, por lo tanto, tiene en cuenta el resultado de la prueba única sobre el Programa de Teoría (70%) y la calificación de Trabajos/proyectos (30%).

SISTEMAS DE EVALUACIÓN:

SISTEMA DE EVALUACIÓN	PORCENTAJE (%)
Ejecución de prácticas	40%
Pruebas escritas	55%
Técnicas de observación	5%