GUÍA DOCENTE

HACKING ÉTICO

GRADO EN **INGENIERÍA DEL SOFTWARE**

MODALIDAD: PRESENCIAL

CURSO ACADÉMICO: 2023-2024

Denominación de la asignatura:	Hacking Ético
Titulación:	Ingeniería del Software
Facultad o Centro:	Centro Universitario de Tecnología y Arte Digital
Materia:	Ciberseguridad
Curso:	3º
Cuatrimestre:	2
Carácter:	OBM
Créditos ECTS:	6
Modalidad/es de enseñanza:	Presencial
Idioma:	Castellano
Profesor/a - email	Eduardo Arriols Nuñez / eduardo.arriols@u-tad.com
Página Web:	http://www.u-tad.com/

DESCRIPCIÓN DE LA ASIGNATURA

Descripción de la materia

Esta materia incluye los conocimientos y las competencias de la seguridad informática que requeriría un profesional de nivel de graduado. Se dedica al estudio de la protección de la infraestructura computacional y todo lo relacionado con esta y, especialm

Descripción de la asignatura

Esta asignatura pretender dar unos conocimientos y capacidades de Hacking ético. Esto es una forma de referirse al acto de una persona, o mejor conocido como hacker, que utiliza sus conocimientos de informática y seguridad para encontrar vulnerabilidades o fallas de seguridad en el sistema, con el objetivo de reportarlas en la organización para que se tomen todas las medidas necesarias que posibilite prevenir una catástrofe cibernética, como el robo de información.

Se estudiarán una serie de pruebas o test denominados “Test de penetración” cuyo objetivo es poder burlar las diferentes vallas de seguridad que tiene la red para diferentes organizaciones, con la única intención de probar su efectividad, o por el contrario, demostrar la vulnerabilidad de aquel sistema

COMPETENCIAS Y RESULTADOS DE APRENDIZAJE

Competencias (genéricas, específicas y transversales)

COMPETENCIAS BÁSICAS Y GENERALRES

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.

CB3: Que los estudiantes tengan la capacidad de reunir e interpretar datos relevantes (normalmente dentro de su área de estudio) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética.

CB4: Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado.

CB5: Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía

CG1 - Capacidad para entender, planificar y resolver problemas a través del desarrollo de soluciones informáticas.

CG2 - Desarrollo de soluciones informáticas respetuosas con el medio ambiente, los deberes sociales y los recursos naturales, además de cumplir con la legislación y la ética

CG3 - Conocimiento de los fundamentos científicos aplicables a la resolución de problemas informáticos

CG4 - Capacidad para simplificar y optimizar los sistemas informáticos atendiendo a la comprensión de su complejidad

CG9 - Capacidad para aprender, modificar y producir nuevas tecnologías informáticas

CG10 - Uso de técnicas creativas para la realización de proyectos informáticos

CG11 - Capacidad de buscar, analizar y gestionar la información para poder extraer conocimiento de la misma

COMPETIENCIAS ESPECIFICAS

CE10 - Capacidad para manejar un gestor de versiones de código y generar la documentación de una aplicación de forma automática.

COMPETENCIAS TRANSVERSALES

CT1 - Conocimiento de la definición, el alcance y la puesta en práctica de los fundamentos de las metodologías de gestión de proyectos de desarrollo tecnológico

CT2 - Conocimiento de los principales agentes del sector y del ciclo de vida completo de un proyecto de desarrollo y comercialización de contenidos digitales

CT4 - Capacidad de actualización del conocimiento adquirido en el manejo de herramientas y tecnologías digitales en función del estado actual del sector y de las tecnologías empleadas

CT5 - Desarrollo de las habilidades necesarias para el emprendimiento digital.

Resultados de aprendizaje

Al acabar la titulación, el graduado o graduada será capaz de:

- Entender qué son las ciber amenazas, cuál es su origen, qué buscan y cómo podemos identificarlas.

- Ser capaz de identificar las amenazas y vulnerabilidades de ciberseguridad de un sistema informático concreto, compuesto por elementos diversos de

- hardware y software.

- Entender y aplicar los principios de la criptografía aplicada a la ciberseguridad.

- Conocer las herramientas y técnicas de auditoría forense.

- Conocer el entorno legal y de protección de datos en las aplicaciones de ciberseguridad

- Conocer experiencias documentadas de ciberataques y las contramedidas recomendadas-

- Entender los conceptos red team, blue team y estudiar su aplicación en escenarios concretos.

- Conocer los elementos y las buenas prácticas descritos en la familia de normas ISA/IEC -62443 e ISO/IEC-27000.

- Conocer y aplicar las técnicas para bastionar los sistemas ante ciberataques, usando detectores de intrusión y monitores.

- Aplicar conceptos de ciberseguridad para diseñar el hardware, la red de comunicaciones y el software de los sistemas en producción.

- Conocer las técnicas de análisis del malware.

- Ser capaz de desensamblar un código malicioso e identificar su origen

- Concebir, desarrollar y desplegar un proyecto de ciberseguridad integral para un sistema distribuid- o

CONTENIDO

Fundamentos de Hacking Ético

Intrusión en sistemas informáticos

Intrusión en webs y aplicaciones móviles

Intrusión en redes

TEMARIO

Tema 1: Hacking de aplicaciones web

1. Data encoding y evasión de filtros
2. Análisis completo de aplicaciones web
3. Uso de herramientas automáticas para la identificación de vulnerabilidades
4. Explotación avanzada de vulnerabilidades

a. XSS
b. SQL Injection
c. File Upload
d. Ataques XML y SSRF
e. Otras vulnerabilidades

Tema 2: Técnicas de Red Teaming

1. Introducción
2. Reconocimiento de activos
3. Vectores de acceso
4. Descubrimiento interno
5. Acceso a credenciales
6. Movimiento lateral
7. Despliegue de persistencia

Tema 3: Desarrollo de exploits

1. Repaso de conceptos básicos
2. Desarrollo de exploit para Buffer Overflow
3. Evasión de medidas de seguridad (DEP, ASLR, …)

ACTIVIDADES FORMATIVAS Y METODOLOGÍAS DOCENTES

Actividades formativas

Actividad Formativa	Horas totales	Horas presenciales
Clases teóricas / Expositivas	29,38	29,38

Clases Prácticas	23,25	23,25
Tutorías	4,00	0,00
Estudio independiente y trabajo autónomo del alumno	50,00	0,00
Elaboración de trabajos (en grupo o individuales)	31,88	0,00
Actividades de Evaluación	5,25	5,25
Seguimiento de Proyectos	6,25	6,25
TOTAL	150	64,13

Metodologías docentes

Método expositivo o lección magistral

Aprendizaje de casos

Aprendizaje basado en la resolución de problemas

Aprendizaje basado en proyectos

Aprendizaje cooperativo o colaborativo

Aprendizaje por indagación

Metodología Flipped classroom o aula invertida

Gamificación

Just in time Teaching (JITT) o aula a tiempo

Método expositivo o lección magistral

Método del caso

Aprendizaje basado en la resolución de problemas

Aprendizaje basado en proyectos

Aprendizaje cooperativo o colaborativo

Aprendizaje por indagación

Metodología flipped classroom o aula invertida

Gamificación

DESARROLLO TEMPORAL

UNIDADES DIDÁCTICAS / TEMAS PERÍODO TEMPORAL

Presentación de la asignatura 01/02/2024

Tema 1. Hacking en aplicaciones web 08/02/2024

15/02/2024

22/02/2024

Examen temas 1 29/02/2024

Tema 2. Técnicas de Red Teaming 07/03/2024

14/03/2024

21/03/2024

30/03/2024

Examen tema 2 04/04/2024

Tema 3. Desarrollo de exploits 11/04/2024

18/04/2024

Examen tema 3 09/05/2024

Retos final 16/05/2024

SISTEMA DE EVALUACIÓN

ACTIVIDAD DE EVALUACIÓN	VALORACIÓN MÍNIMA RESPECTO A LA CALIFICACIÓN FINAL (%)	VALORACIÓN MÁXIMA RESPECTO A LA CALIFICACIÓN FINAL (%)
Evaluación de la participación en clase, en prácticas o en proyectos de la asignatura	10	30
Evaluación de trabajos, proyectos, informes, memorias	40	80
Prueba Objetiva	10	60

CRITERIOS ESPECÍFICOS DE EVALUACIÓN

ACTIVIDAD DE EVALUACIÓN	CONVOCATORIA ORDINARIA	CONVOCATORIA EXTRAORDINARIA
Evaluación de la participación en clase, en prácticas o en proyectos de la asignatura	10	10
Evaluación de trabajos, proyectos, informes, memorias	50	50
Prueba Objetiva	40	40

Consideraciones generales acerca de la evaluación

Práctica 1: Hacking de aplicaciones web Evaluación de 0 a 10. Entrega por blackboard y evaluación por parte del profesor sin necesidad de defensa presencial. 20%

Práctica 2: Red Teaming Evaluación de 0 a 10. Entrega por blackboard y evaluación por parte del profesor sin necesidad de defensa presencial. 20%

Práctica 3: Exploiting Evaluación de 0 a 10. Entrega por blackboard y evaluación por parte del profesor sin necesidad de defensa presencial. 10%

Examen 1: Hacking de aplicaciones webEvaluación de 0 a 10. Es necesario obtener al menos un 6 en el examen para liberar materia. Hay un total de 3 exámenes intermedios. 15%

Examen 2: Red Teaming Evaluación de 0 a 10. Es necesario obtener al menos un 6 en el examen para liberar materia. Hay un total de 3 exámenes intermedios. 15%

Examen 3: Exploiting Evaluación de 0 a 10. Es necesario obtener al menos un 6 en el examen para liberar materia. Hay un total de 3 exámenes intermedios. 10%

Examen final de la asignatura Evaluación de 0 a 10. Es necesario obtener al menos un 5 en el examen para aprobar la teoría de la asignatura. 40% (en caso de no haber sido liberadas las partes)

Participación en clase Evaluación de 0 a 10. Entrega por blackboard y posible defensa presencial. 10%

A medida que se avance en el temario habrá problemas o ejercicios cortos planteados por el profesor. Los problemas y ejercicios están pensados para que el alumno los resuelva en el tiempo de clase, pero, si no le da tiempo a acabarlos del todo, deberá finalizarlos fuera de clase.

En clase se explicarán los problemas y ejercicios propuestos. Durante el periodo de ejercicios de cada clase, el profesor irá pasando por cada alumno para corregir y valorar, delante de él, sus ejercicios de la clase anterior. El alumno deberá responder adecuadamente a las preguntas que el profesor le haga sobre sus ejercicios.

A todos los efectos, una nota inferior a un 5 se considera suspensa. Es necesario obtener al menos un 5 en la nota final tanto de teoría como de práctica para poder aprobar la asignatura. Existen dos oportunidades para ello: la convocatoria ordinaria y la extraordinaria.

En la convocatoria ordinaria:

1. Si la nota final del conjunto de prácticas es igual o superior a un 5 pero el examen final ordinario está suspenso, la asignatura estará suspensa con una calificación máxima de 4.

2. Si la nota de los exámenes intermedios es superior a 6, esta parte quedara liberada, eximiendo al alumno de realizarla en el examen final de la asignatura. Si un alumno hubiera liberado los 3 exámenes no tendrá que presentarse al examen, a menos que quiera subir nota.

3. Si la nota del examen final ordinario es igual o superior a un cinco, la nota final de la asignatura se calculará obteniendo la media ponderada de esta con las prácticas.

En la convocatoria extraordinaria:

1. Aquellos alumnos que hayan suspendido la asignatura en la convocatoria ordinaria, deberán realizar la parte que tengan suspensa (teoría y/o practica) en la convocatoria extraordinaria.

El porcentaje de presencialidad es del 80%. Las notas del examen final y de las prácticas no se guardan entre cursos académicos sucesivos.

Las prácticas o cualquier examen estarán suspensos si se descubre que un alumno (o varios) ha copiado a otro (o a varios, todos los alumnos involucrados estarán suspensos) o bien ha copiado de un libro o de Internet. Además, la Universidad abrirá expedientes disciplinarios a todos los alumnos involucrados, pudiendo desembocar incluso en su expulsión.

Los exámenes y los ejercicios constarán de uno o varios de los siguientes tipos de preguntas:

- Cuestiones teóricas cortas.
- Preguntas de tipo test sobre teoría o elegir el resultado final de un ejercicio.
- Problemas y casos prácticos.
- Preguntas sobre las prácticas.

BIBLIOGRAFÍA / WEBGRAFÍA

Bibliografía Básica:

- Hacking Exposed 7: Network Security Secrets Solutions, Editorial: McGraw-Hill
- The Web Application Hacker's Handbook (Second Edition), Editorial: Wiley

Bibliografía Recomendada:

- Metasploit, Penetration Testers Guide, Editorial: No Starch Press
- Violent Python A Cookbook for Hackers Forensic, Editorial: Syngress
- Mastering Kali Linux for Advanced Penetration Testing, Editorial: Wiley

MATERIALES, SOFTWARE Y HERRAMIENTAS NECESARIAS

Tipología del aula
Aula teórica

Equipo de proyección y pizarra

Materiales:
Ordenador personal con Windows, Linux o OSX

Software:
VirtualBox y VirtualBox Extension Pack