CENTRO UNIVERSITARIO DE TECNOLOGÍA Y ARTE DIGITAL

PLANIFICACIÓN DE LA DOCENCIA UNIVERSITARIA

GUÍA DOCENTE

Hacking Ético

1. DATOS DE IDENTIFICACIÓN DE LA ASIGNATURA.

Título:	Grado en Ingeniería del Software
Facultad:	Centro Universitario de Tecnología y Arte Digital (U-TAD)
Materia:	Ciberseguridad
Denominación de la asignatura:	Hacking Ético
Curso:	3
Cuatrimestre:	2
Carácter:	Obligatoria de mención
Créditos ECTS:	6
Modalidad/es de enseñanza:	Híbrido Presencial
Idioma:	Castellano
Profesor/a:	Eduardo Arriols Nuñez
E-mail:	eduardo.arriols@u-tad.com
Teléfono:	

2. DESCRIPCIÓN DE LA ASIGNATURA

2.1 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, especialmente, la información contenida en una computadora o circulante a través de las redes de computadoras. Para ello, los alumnos adquirirán los conocimientos relacionados con las técnicas de ataque y defensa de sistemas informáticos, así como las actividades relacionadas con el análisis forense de sistemas y el análisis del malware.

2.2 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 estudiaran 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

3. COMPETENCIAS Y RESULTADOS DE APRENDIZAJE

3.1. COMPETENCIAS (Genéricas, específicas y transversales)

Competencias Básicas y Generales
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
Competencias Específicas
CE10 - Capacidad para entnder un incident de seguridad y ser capaces de trazar un plan de acción para analizar y remediar
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.

4. CONTENIDOS

4.1. Temario de la asignatura

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: Hacking de aplicaciones móviles

1. Introducción
2. Fundamentos
3. Entornos de pruebas
4. Reversing de apps
5. Captura de tráfico de red
6. Análisis dinámico y estático

Tema 3: 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 4: Desarrollo de exploits

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

4.2. Desarrollo temporal

UNIDADES DIDÁCTICAS / TEMAS	PERÍODO TEMPORAL
Presentación de la asignatura	08/02/2021
Tema 1. Hacking en aplicaciones web	09/02/2021 15/02/2021 16/02/2021 22/02/2021 23/02/2021 01/03/2021 02/03/2021 08/03/2021
Tema 2. Hacking en aplicaciones móviles	09/03/2021 15/03/2021 16/03/2021
Examen temas 1 y 2	22/03/2021
Tema 3. Técnicas de Red Teaming	23/03/2021 06/04/2021 12/04/2021 13/04/2021 19/04/2021 20/04/2021 26/04/2021 27/04/2021
Examen tema 3	10/05/2021
Tema 4. Desarrollo de exploits	11/05/2021 17/05/2021 18/05/2021
Examen tema 4	24/05/2021

5. ACTIVIDADES FORMATIVAS Y MODALIDADES DE ENSEÑANZAS

5.1. Modalidades de enseñanza

La asignatura se desarrollará a través de los siguientes métodos y técnicas generales, que se aplicarán diferencialmente según las características propias de la asignatura:

- **Método expositivo/Lección magistral:** el profesor desarrollará, mediante clases magistrales y dinámicas los contenidos recogidos en el temario.
- **Estudio de casos:** análisis de casos reales relacionados con la asignatura.
- **Resolución de ejercicios y problemas:** los estudiantes desarrollarán las soluciones adecuadas aplicando procedimientos de transformación de la información disponible y la interpretación de los resultados.
- **Aprendizaje basado en problemas:** utilización de problemas como punto de partida para la adquisición de conocimientos nuevos.
- **Aprendizaje orientado a proyectos:** se pide a los alumnos que, en pequeños grupos, planifiquen, creen y evalúen un proyecto que responda a las necesidades planteadas en una determinada situación.
- **Aprendizaje cooperativo:** Los estudiantes trabajan en grupo para realizar las tareas de manera colectiva.

5.2. Actividades formativas

Actividad Formativa	Horas	Presencialidad
AF1 Clases teóricas / Expositivas	30	100%
AF2 Clases Prácticas	24	100%
AF3 Tutorías	6	50%
AF4 Estudio independiente y trabajo autónomo del alumno	57,5	0%
AF5 Elaboración de trabajos (en grupo o individuales)	28,5	0%
AF6: Actividades de Evaluación	4	100%

6. SISTEMA DE EVALUACIÓN

ACTIVIDAD DE EVALUACIÓN	VALORACIÓN MÍNIMA RESPECTO A LA CALIFICACIÓN FINAL (%)	VALORACIÓN MÁXIMA RESPECTO A LA CALIFICACIÓN FINAL (%)
SE1 Evaluación de la participación en clase, en prácticas o en proyectos de la asignatura	10%	30%
SE2 Evaluación de trabajos, proyectos, informes, memorias	40%	80%
SE3 Exámenes intermedios o final (no continua)	10%	60%

6.1. Criterios de calificación

ACTIVIDAD DE EVALUACIÓN	CRITERIOS DE EVALUACIÓN	VALORACIÓN RESPECTO A LA CALIFICACIÓN FINAL (%)
Práctica 1: Hacking de aplicaciones web y móvil	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 web y movil	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 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%

Consideraciones generales acerca de la evaluación:

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.

7. BIBLIOGRAFÍA / WEBGRAFÍA

Bibliografía Básica:

- Incident Response & Computer Forensics. Jason T. Luttgens, Matthew Pepe and Kevin Mandia.
- Windows Forensic Analysis Toolkit. Harlan Carvey.
- Windows Registry Forensics. Windows Registry Forensics.
- The Art of Memory Forensics. Michael Hale Ligh, Jamie Levy, AAron Walters, Andrew Case.
- Practical Forensic Imaging: Securing Digital Evidence with Linux Tools. Bruce Nikkel.
- Linux Forensics. Philip Polstra.
- Hands-On Network Forensics. Nipun Jaswal.
    - Practica Malware Analysis. Michael Sikorski, Andrew Honig

Bibliografía Recomendada:

8. MATERIAL, SOFTWARE Y HERRAMIENTAS NECESARIAS

Materiales necesarios del alumno:

- Ordenador personal con Windows, Linux o OSX
- VirtualBox y VirtualBox Extension Pack