Guía Docente: Hacking Ético

DATOS GENERALES	
Facultad	Facultad de Ciencias y Tecnología
Titulación	Máster en Ciberseguridad
Plan de estudios	2018
Materia	Análisis de la ciberseguridad
Carácter	Obligatorio
Período de impartición	Tercer Trimestre
Curso	Primero
Nivel/Ciclo	Máster
Créditos ECTS	6
Lengua en la que se imparte	Castellano
Prerrequisitos	No se prevén requisitos previos, por tanto los requisitos serán los propios del título.

DATOS DEL PROFESORADO			
Profesor Responsable	Diego Ramírez Jiménez	**Correo electrónico**	diego.ramirez@ui1.es
Área		**Facultad**	Facultad de Ciencias y Tecnología
Perfil Profesional 2.0	Mi Linkedin		

CONTEXTUALIZACIÓN Y JUSTIFICACIÓN DE LA ASIGNATURA	
Asignaturas de la materia	• Hacking Ético
Contexto y sentido de la asignatura en la titulación y perfil profesional	El *hacking ético* dentro de la seguridad informática se podría definir como el proceso de evaluación del estado de la seguridad de los sistemas informáticos. Estas acciones, como su propio nombre indica son éticas, realizadas por profesionales cuyo único fin y objetivo es descubrir vulnerabilidades para corregirlas, comunicarlas e impedir que se exploten por cibercriminales. A estos profesionales se les conoce como *hackers* siendo esta asignatura, un medio para formar este tipo de perfiles. Aprenderemos las fases fundamentales del *hacking ético,* poniendola en práctica mediante ejercicios, utilizando herramientas para analizar redes, sistemas o aplicaciones con el fin de detectar vulnerabilidades en ellas. Expondremos las principales técnicas para vulnerar los sistemas, aplicando diferentes ataques cómo son los ataques de fuerza bruta, *man in the middle* o de denegación de servicio. Estudiaremos el malware o software malicioso, sus diferentes variantes, comportamiento, vectores de ataque y como combatirlos. También, aprenderemos las principales técnicas de análisis de malware para comprender su funcionamiento y aprender a montar un laboratorio de pruebas donde diseccionar diferentes muestras de malware y poder aprender cómo actúan los virus, troyanos o *ransomware*. Aprenderemos a realizar auditorías de seguridad en aplicaciones, páginas web y aplicaciones móviles, siguiendo las técnicas de las principales metodologías de referencia que aplicaremos en entornos de prueba donde poder testearlas. Esta asignatura está ubicada en el máster en Ciberseguridad dentro de la materia de Análisis de la ciberseguridad.

COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE Y RESULTADOS DE APRENDIZAJE	
Competencias de la asignatura	Generales y 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. • CB9: 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. • 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. • CG1: Ser capaz de analizar, sintetizar y organizar la información dentro del área de seguridad informática y de las comunicaciones • CG2: Ser capaz de permanecer eficaz dentro de un medio cambiante, así como a la hora de enfrentarse con nuevas tareas, retos y personas • CG5: Ser capaz de proponer soluciones imaginativas y originales así como ser capaz de promover la innovación e identificación de alternativas contrapuestas a los métodos y enfoques tradicionales en el ámbito de la ciberseguridad • CG6: Conocer y aplicar métodos de protección en sistemas tecnológicos industriales y sociales avanzados. Específicas • CE02: Conocer las tendencias actuales en técnicas de ciberataque • CE04: Comprender, aplicar y evaluar técnicas de hacking ético. • CE06: Comprender, aplicar y evaluar la gestión de la seguridad de sistemas altamente securizados por su naturaleza o criticidad. • CE09: Analizar e identificar las vulnerabilidades de un sistema informático, y ser capaz de desarrollar métodos de protección de la información.
Resultados de aprendizaje de la asignatura	• Adquirir las competencias básicas y generales detalladas anteriormente. • Conocer las diferentes técnicas de escaneo de vulnerabilidades para permitir su detección. • Analizar algunas vulnerabilidades de distintos tipos de sistemas y ver cómo estas pueden ser explotadas por software malicioso. • Desarrollar técnicas y métodos de protección ante vulnerabilidades de distintos tipos de sistemas.

PROGRAMACION DE CONTENIDOS	

Breve descripción de la asignatura	En esta asignatura se verá, entre otros:
	• Análisis de riesgos:
	  ◦ Evolución de las amenazas.
	  ◦ Casos de estudio reales.
	• Tipos de vulnerabilidades:
	  ◦ *Software* malicioso.
	  ◦ Vulnerabilidades en redes.

	◦ Vulnerabilidades en aplicaciones web. • Análisis y detección de vulnerabilidades: ◦ Ataques ◦ Herramientas de monitorización ◦ Explotación y gestión de vulnerabilidades ◦ Estimación de impactos • Análisis de malware: ◦ Estático y dinámico ◦ Tendencias de ataques ◦ Explotación y gestión de vulnerabilidades
Contenidos	**Unidad Didáctica 1. Introducción y fundamentos del hacking ético** • Historia, estado del arte y evolución • Conceptos éticos frente a ciberdelito • Conocimientos previos **Unidad Didáctica 2. Análisis pasivo y activo** • Fase footprinting • Fase fingerprinting • Ingeniería social • Principales herramientas de análisis **Unidad Didáctica 3. Enumeración, análisis y explotación de vulnerabilidades** • Enumeración en sistemas Windows • Enumeración en sistemas Linux • Explotación de vulnerabilidades • Informes técnicos y ejecutivos **Unidad Didáctica 4. Tipos de ataques** • Clasificación • Ataques contra la integridad • Ataques contra la disponibilidad • Ataques contra la privacidad • Amenazas persistentes avanzadas • Ataques en entornos industriales e infraestructuras críticas • Estudio de casos reales **Unidad Didáctica 5. Estudio del malware** • Tipos de malware • Análisis estático • Análisis dinámico • Herramientas y entorno de pruebas • Tendencias **Unidad Didáctica 6. Hacking ético en aplicaciones, páginas web y móviles** • Vulnerabilidades en código • Pentesting en aplicaciones y páginas web • Pentesting de aplicaciones móviles • Herramientas y entornos de análisis

METODOLOGÍA	
Actividades formativas	En cada una de las 6 Unidades didácticas, el alumnado deberá llevar a cabo actividades que le conduzcan a la asimilación de los conceptos y a su puesta en práctica. Entre otros, se propondrán las siguientes actividades: • **Estudio de Caso:** Se plantearán estudios de caso reales sobre algún tema de la unidad. Se trata de ejercicios introductorios sobre el que se deberá investigar en la web para resolverlos y donde el alumno deberá utilizar los recursos necesarios aplicando los conceptos y aspectos desarrollados en las unidades didácticas. Han de servir además como motivación y conducción del pensamiento reflexivo personal. • **Foros de Debate:** Los alumnos debatirán para aportar ideas sobre temas de la asignatura. • **Trabajo Colaborativo:** Se planteará un ejercicio práctico relacionado con los contenidos de la asignatura, y que deberá resolverse siguiendo alguna técnica de trabajo colaborativo grupal. • **Trabajo Individual:** Ejercicio práctico que el alumno tendrá que resolver individualmente, no solo indicando su propuesta o solución sino como la llevaría a cabo. • **Cuestionarios:** preguntas evaluables para poner a prueba los conocimientos adquiridos.

EVALUACIÓN	
Sistema evaluativo	*En caso de que la situación sanitaria impida la realización presencial de los exámenes con todas las garantías, la Universidad Isabel I celebrará dichas pruebas en modalidad online. Para la realización de dichos exámenes, la universidad incorporará la herramienta de proctoring a nuestra plataforma tecnopedagógica, con el objetivo de garantizar los procesos de autentificación del alumno, como el control del entorno durante el desarrollo de las pruebas de evaluación. A su vez, la Universidad Isabel I pondrá a disposición del alumnado una Unidad de Exámenes Online específica para ofrecer apoyo técnico durante todo el proceso y así solventar todas las incidencias que se puedan presentar.* El sistema de evaluación se basará en una selección de las pruebas de evaluación más adecuadas para el tipo de competencias que se trabajen. El sistema de calificaciones estará acorde con la legislación vigente *(Real Decreto 1125/2003, de 5 de septiembre, por el que se establece el sistema europeo de créditos y el sistema de calificaciones en las titulaciones universitarias de carácter oficial y de validez en todo el territorio nacional)*. El sistema de evaluación de la Universidad Isabel I queda configurado de la siguiente manera: **Sistema de evaluación convocatoria ordinaria** **Opción 1. Evaluación continua** Los estudiantes que opten por esta vía de evaluación deberán realizar el **seguimiento de la evaluación continua (EC)** y podrán obtener hasta un **60 %** de la calificación final a través de las actividades que se plantean en la evaluación continua. Además, deberán realizar un **examen final presencial (EX)** que supondrá el **40 %** restante. Esta prueba tiene una parte dedicada al control de la identidad de los estudiantes que consiste en la verificación del trabajo realizado durante la evaluación

continua y otra parte en la que realizan diferentes pruebas teórico-prácticas para evaluar las competencias previstas en cada asignatura.

Para la aplicación de los porcentajes correspondientes, el estudiante debe haber obtenido una nota mínima de un 4 en cada una de las partes de las que consta el sistema de evaluación continua.

Se considerará que el estudiante supera la asignatura en la convocatoria ordinaria por el sistema de evaluación continua, siempre y cuando al aplicar los porcentajes correspondientes se alcance una calificación mínima de un 5.

Opción 2. Prueba de evaluación de competencias

Los estudiantes que opten por esta vía de evaluación deberán realizar una **prueba de evaluación de competencias (PEC)** y un **examen final presencial (EX)**.

La **PEC** se propone como una prueba que el docente plantea con el objetivo de evaluar en qué medida el estudiante adquiere las competencias definidas en su asignatura. Dicha prueba podrá ser de diversa tipología, ajustándose a las características de la asignatura y garantizando la evaluación de los resultados de aprendizaje definidos. Esta prueba supone el 50 % de la calificación final.

El **examen final presencial**, supondrá el **50 %** de la calificación final. Esta prueba tiene una parte dedicada al control de la identidad de los estudiantes que consiste en la verificación del seguimiento de las actividades formativas desarrolladas en el aula virtual y otra parte en la que realizan diferentes pruebas teórico-prácticas para evaluar las competencias previstas en cada asignatura.

Al igual que con el sistema de evaluación anterior, para la aplicación de los porcentajes correspondientes el estudiante debe haber obtenido una puntuación mínima de un 4 en cada una de las partes de las que consta la opción de prueba de evaluación de competencias.

Se considerará que el estudiante supera la asignatura en la convocatoria ordinaria por el sistema de la prueba de evaluación de competencias siempre y cuando al aplicar los porcentajes correspondientes se alcance una calificación mínima de un 5.

Sistema de evaluación convocatoria extraordinaria

Todos los estudiantes, independientemente de la opción seleccionada, que no superen las pruebas evaluativas en la convocatoria ordinaria tendrán derecho a una convocatoria extraordinaria.

La convocatoria extraordinaria completa consistirá en la realización de una **prueba de evaluación de competencias** que supondrá el **50 %** de la calificación final y un **examen final presencial** cuya calificación será el **50 %** de la calificación final.

Para la aplicación de los porcentajes correspondientes, el estudiante debe haber obtenido una nota mínima de un 4 en cada una de las partes de las que consta el sistema de evaluación de la convocatoria extraordinaria.

Los estudiantes que hayan suspendido todas las pruebas evaluativas en convocatoria ordinaria (evaluación continua o prueba de evaluación de competencias y examen final) o no se hayan presentado deberán realizar la convocatoria extraordinaria completa, como se recoge en el párrafo anterior.

En caso de que hayan alcanzado una puntuación mínima de un 4 en alguna de las pruebas evaluativas de la convocatoria ordinaria (evaluación continua o prueba de

	evaluación de competencias y examen final), se considerará su calificación para la convocatoria extraordinaria, debiendo el estudiante presentarse a la prueba que no haya alcanzado dicha puntuación o que no haya realizado. En el caso de que el alumno obtenga una puntuación que oscile entre el 4 y el 4,9 en las dos partes de que se compone la convocatoria ordinaria (EC o PEC y examen), solo se considerará para la convocatoria extraordinaria la nota obtenida en la evaluación continua o prueba de evaluación de competencias ordinaria (en función del sistema de evaluación elegido), debiendo el alumno realizar el examen extraordinario para poder superar la asignatura. Al igual que en la convocatoria ordinaria, se entenderá que el alumno ha superado la materia en convocatoria extraordinaria si, aplicando los porcentajes correspondientes, se alcanza una calificación mínima de un 5.

BIBLIOGRAFÍA Y OTROS RECURSOS	
Bibliografía básica	Messier Ric. "CEH v10 Certified Ethical Hacker Study Guide" (June 2019), ISBN: 978-1119533191 MCCLURE, S; SCAMBRAY, J; KURTZ, G. *Hacking Exposed. Network Security Secrets and Solutions*. Nueva York McGraw Hill, ISBN: 0072121270 El primer libro corresponde a la guía de referencia y de preparación para obtener el certificado en Hacking Ético o CEH del EC-Council. Recoge los conocimientos fundamentales del hacking ético y es una de las principales fuentes de información de esta asignatura. El segundo libro algo más técnico, profundiza en los distintos tipos de pruebas y fases del hacking ético con una gran cantidad de ejemplos para comprender las pruebas y ataques de forma más fácil.
BibliografÍa complementaria	Abu-Shaqra B, Luppicini R. (2018) *A Technoethical Study Of Ethical Hacking Communication And Management Within A Canadian University*. IGI Global. Leonhardt F. (2010) *Auditing, Penetration Testing And Ethical Hacking*. World Scientific Publishing Co.; 2010. Available from: Scopus®, Ipswich, MA. Himma K, Tavani H. (2008) Ethical Issues Involving Computer Security: Hacking, Hacktivism, and Counterhacking. *Handbook Of Information & Computer Ethics* [serial online]. January 2008;:191. Available from: Complementary Index, Ipswich, MA. Vignesh R, Rohini K. (2018) Analysis to determine the scope and Challenging responsibilities of Ethical Hacking employed in Cyber Security. *International Journal Of Engineering And Technology(UAE)* [serial online]. January 1, 2018;7(3.27 Special Issue 27):196-199. Berger H, Jones A. (2016) Cyber security & ethical hacking for SMEs. *ACM International Conference Proceeding Series* [serial online]. July 25, 2016;Part F130520(Proceedings of the 11th International Knowledge Management in Organizations Conference on the Changing Face of Knowledge Management Impacting Society, KMO 2016) Patil S, Jangra A, Bhale M, Raina A, Kulkarni P. (2018) Ethical hacking: The need for cyber security. *IEEE International Conference On Power, Control, Signals And Instrumentation Engineering, ICPCSI 2017* [serial online]. June 20, 2018;(IEEE International Conference on Power, Control, Signals and Instrumentation Engineering,

ICPCSI 2017):1602-1606.

Molina F. (2015) La evolución de las técnicas de 'hacking' ético. *Red Seguridad: Revista Especializada En Seguridad Informática, Protección De Datos Y Comunicaciones*[serial online]. 2015;(. 68):62.

Mitnick K.(2006) El arte de la intrusión : la verdadera historia de las hazañas de hackers, instrusos e impostores.

?tefan I, Ramona (2018) M. MALWARE FOR MOBILE DEVICES AND THEIR SECURITY. *Fiabilitate ?i Durabilitate, Vol 1, Iss 21, Pp 267-272 (2018)* [serial online]. 2018;(21):267.

Sikorski M, Honig's A. (2011) Practical Malware Analysis (No Starch). *Linux Journal*, (211), 49.

Stuttard D, Pinto M. (2011) *The Web Application Hacker's Handbook. [Recurso Electrónico]* [e-book]. Sussex John Wiley & Sons 2011; n.d.

Otros recursos

OWASP. Testing Guide. Recuperado de https://owasp.org/www-project-web-security-testing-guide/assets/archive/OWASP_Testing_Guide_v4.pdf. Consultado en mayo de 2020.

Perez D, Picó J. Ampliando el arsenal de ataque Wi-Fi. Recuperado de https://www.youtube.com/watch?v=Lpfdd0kOB5g. Consultado en mayo de 2020.

Sanchez E. Taller: Destripando Pokemon Go OWASP (auditoría para aplicaciones Android). Recuperado de https://www.youtube.com/watch?v=onD4acSorZU&t=3119s. Consultado en septiembre 2018.

Arroyo M. Taller: Pentesting de aplicaciones iOS. Recuperado de https://www.youtube.com/watch?v=1zk6aC3xxhU. Consultado en mayo de 2020.

Awesome Hacking. A collection of awesome lists for hackers, pentesters & security researchers. Recuperado de https://github.com/Hack-with-Github/Awesome-Hacking. Consultado en mayo de 2020.

Tori C. Hacking Ético. Recuperado de https://openlibra.com/es/book/hacking-etico. Consultado en mayo de 2020.

Kali Linux, distribución para hacking y test de penetración (web principal). Recuperado de https://www.kali.org/. Consultado en mayo de 2020.

VirusTotal, servicio de análisis de archivos y URLs sospechosas para la detección de malware. Recuperado de https://www.virustotal.com/es/. Consultado en mayo de 2020.

Bleeping Computer, Foro de informática con un destacado subforo en ciberseguridad centrado en las últimas novedades en malware. Recuperado de https://www.bleepingcomputer.com/forums/f/79/security/. Consultado en mayo de 2020.

Shodan, motor de búsqueda de dispositivos, utilizada para búsqueda de vulnerabilidades. Recuperado de https://www.shodan.io/ Consultado en mayo de 2020.