Guía de Asignatura

ASIGNATURA: HACKING ÉTICO

Título: *MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD*
Materia: *AUDITORÍA SE SISTEMAS DE INFORMACIÓN*
Créditos: *6 ECTS*
Código: *01MCYB*

Índice

1. Organización general

1.1. Datos de la asignatura

TITULACIÓN	*MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD*
ASIGNATURA	*HACKING ÉTICO*
CÓDIGO - NOMBRE ASIGNATURA	*01MCYB_HACKING_ÉTICO*
Carácter	Obligatorio
Cuatrimestre	Primero
Idioma en que se imparte	Castellano
Requisitos previos	No existen
Dedicación al estudio por ECTS	**25 horas**

1.2. Introducción a la asignatura

Una de las estrategias que a menudo se utilizan para evaluar la seguridad de los sistemas de información consiste en analizar la seguridad de los sistemas siguiendo los pasos que llevaría a cabo un posible atacante. Como “ethical hacking” se entiende el conjunto de técnicas y prácticas que se utilizan a nivel profesional para auditar la seguridad simulando ataques informáticos a partir de metodologías de trabajo debidamente definidas a tales efectos. El objetivo del curso consiste en el análisis y la revisión de las técnicas y metodologías más actuales que se utilizan para el análisis de vulnerabilidades y la realización de pruebas de penetración en sistemas informáticos.

El equipo docente que imparte el curso es uno de los mejores equipos en auditorías de hacking ético a nivel internacional y a nivel de formación dispone de una amplia experiencia en la realización de cursos de hacking.

1.3. Competencias y resultados de aprendizaje

COMPETENCIAS GENERALES

CG.1-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.

CG.2 -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.

CG.3-Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios.

CG.4-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.

CG.5-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.

COMPETENCIAS ESPECÍFICAS DE LA ASIGNATURA.

C.E.1 - Realizar auditorías de seguridad de acuerdo con la normativa y marco legal establecido.

C.E.4 - Identificar las vulnerabilidades, amenazas, y software malicioso a los que estén expuestos los diferentes activos de una organización.

C.E.7 - Conocer las tendencias actuales en ciberataques, técnicas de ocultación y principales vectores utilizados.

C.E.8 - Crear informes de carácter ejecutivo y de carácter científico-técnico que respondan a las necesidades de comunicación en términos de ciberseguridad dentro de una organización

2. Contenidos/temario

Bloques temáticos:

- Definiciones y planificación: etapas y metodologías del proceso de auditoría de seguridad.
- Information Gathering (herramientas y organización de la información). y vulnerabilidades comunes.
- Vulnerabilidades comunes: CVSS (Common Vulnerability Scoring System), reportes, vulnerabilidades "0-day".
- Herramientas para análisis manual y automatizado.
- Exploiting: romper la seguridad como parte del proceso de auditoría de seguridad, consideraciones éticas y sistemas críticos.
- Técnicas para elevación de privilegios.
- Límites legales: marco regulatorio y normativa en auditorías de seguridad.
- Elaboración de informes técnicos y ejecutivos

El docente desarrollará el temario en más detalle.

3. Metodología

La modalidad de enseñanza propuesta para el presente título guarda consonancia con la Metodología General de la Universidad Internacional de Valencia, aprobada por el Consejo de Gobierno Académico de la Universidad y de aplicación en todos sus títulos.

Este modelo, que vertebra el conjunto de procesos de enseñanza y aprendizaje de la institución, combina la naturaleza síncrona (mismo tiempo-diferente espacio) y asíncrona (diferente tiempo -diferente espacio) de los entornos virtuales de aprendizaje, siempre en el contexto de la modalidad virtual.

El elemento síncrono se materializa en sesiones de diferente tipo (clases expositivas y prácticas, tutorías, seminarios y actividades de diferente índole durante las clases online) donde el profesor y el estudiante comparten un espacio virtual y un tiempo determinado que el estudiante conoce con antelación.

Las actividades síncronas forman parte de las actividades formativas necesarias para el desarrollo de la asignatura y, además, quedan grabadas y alojadas para su posterior visualización.

Por otro lado, estas sesiones no solamente proporcionan espacios de encuentro entre estudiante y profesor, sino que permiten fomentar el aprendizaje colaborativo, al generarse grupos de trabajo entre los estudiantes en las propias sesiones.

Los elementos asíncronos del modelo se desarrollan a través del Campus Virtual, que contiene las aulas virtuales de cada asignatura, donde se encuentran los recursos y contenidos necesarios para el desarrollo de actividades asíncronas, así como para la interacción y comunicación con los profesores y con el resto de departamentos de la Universidad.

4. Actividades formativas

La metodología VIU, basada en la modalidad virtual, se concreta en una serie de actividades formativas y metodologías docentes que articulan el trabajo del estudiante y la docencia impartida por los profesores.

Durante el desarrollo de cada una de las asignaturas, se programan una serie de actividades de aprendizaje que ayudan a los estudiantes a consolidar los conocimientos trabajados en cada una de las asignaturas. A continuación, listamos las actividades genéricas que pueden formar parte de cada asignatura, dependiendo de las competencias a desarrollar en los estudiantes en cada asignatura.

1. Clases presenciales

2. Clases virtuales síncronas

Constituyen el conjunto de acciones formativas que ponen en contacto al estudiante con el profesor, con otros expertos y con compañeros de la misma asignatura en el mismo momento temporal a través de herramientas virtuales. Las actividades recurrentes (por ejemplo, las clases) se programan en el calendario académico y las que son ocasionales (por ejemplo, sesiones con expertos externos) se avisan mediante el tablón de anuncios del campus. Estas actividades se desglosan en las siguientes categorías:

a. Clases expositivas: El profesor expone a los estudiantes los fundamentos teóricos de la asignatura.

b. Clases prácticas: El profesor desarrolla junto con los estudiantes actividades prácticas que se basan en los fundamentos vistos en las clases expositivas. En términos generales, su desarrollo consta de las siguientes fases, pudiéndose adaptar en función de las necesidades docentes:

I. La primera fase se desarrolla en la sala principal de la videoconferencia, donde el profesor plantea la actividad.

II. A continuación, divide a los estudiantes en grupos de trabajo a través de las salas colaborativas y se comienza con la actividad. En esta fase el profesor va entrando en cada sala colaborativa rotando los grupos para resolver dudas, dirigir el trabajo o dar el feedback oportuno. Los estudiantes también tienen posibilidad de consultar al profesor en el momento que consideren necesario.

III. La tercera fase también se desarrolla en la sala principal y tiene como objetivo mostrar el ejercicio o explicar con ejemplos los resultados obtenidos. Por último, se ponen en común las conclusiones de la actividad realizada.

No obstante, el profesor puede utilizar otras metodologías activas y/o herramientas de trabajo colaborativo en estas clases.

c. Seminarios: En estas sesiones un experto externo a la Universidad acude a presentar algún contenido teórico-práctico directamente vinculado con el temario de la asignatura. Estas sesiones permiten acercar al estudiante a la realidad de la disciplina en términos no sólo profesionales, sino también académicos. Todas estas sesiones están vinculadas a contenidos de las asignaturas y del programa educativo.

3. Actividades asíncronas supervisadas

Se trata de un conjunto de actividades supervisadas por el profesor de la asignatura vinculadas con la adquisición por parte de los estudiantes de los resultados de aprendizaje y el desarrollo de sus competencias. Estas actividades, diseñadas con visión de conjunto, están relacionadas entre sí para ofrecer al estudiante una formación completa e integral. Esta categoría se desglosa en el siguiente conjunto de actividades:

a. Actividades y trabajos prácticos: se trata de un conjunto de actividades prácticas realizadas por el estudiante por indicación del profesor que permiten al estudiante adquirir las competencias del título, especialmente aquellas de carácter práctico. Estas actividades, entre otras, pueden ser de la siguiente naturaleza: actividades vinculadas a las clases prácticas (resúmenes, mapas conceptuales, one minute paper, resolución de problemas, análisis reflexivos, generación de contenido multimedia, exposiciones de trabajos, test de autoevaluación, participación en foros, entre otros). Estas actividades serán seleccionadas por el profesor en función de las necesidades docentes. Posteriormente, estas actividades son revisadas por el profesor, que traslada un feedback al estudiante sobre las mismas, pudiendo formar parte de la evaluación continua de la asignatura.

b. Actividades guiadas con recursos didácticos audiovisuales e interactivos: se trata de un conjunto de actividades en las que el estudiante revisa o emplea recursos didácticos (bibliografía, videos, recursos interactivos) bajo las indicaciones realizadas previamente por el profesor; con el objetivo de profundizar en los contenidos abordados en las sesiones teóricas y prácticas. Estas sesiones permiten la reflexión o práctica por parte del estudiante, y pueden complementarse a través de la puesta en común en clases síncronas o con la realización de actividades y trabajos prácticos. Posteriormente, estas actividades son revisadas por el profesor, que traslada un feedback al estudiante sobre las mismas, pudiendo formar parte de la evaluación continua de la asignatura.

4. Tutorías

En esta actividad se engloban las sesiones virtuales de carácter síncrono y las comunicaciones por correo electrónico o campus virtual destinadas a la tutorización de los estudiantes. En ellas, el profesor comparte información sobre el progreso del trabajo del estudiante a partir de las evidencias recogidas, se resuelven dudas y se dan orientaciones específicas ante dificultades concretas en el desarrollo de la asignatura. Pueden ser individuales o colectivas, según las necesidades de los estudiantes y el carácter de las dudas y orientaciones planteadas. Tal y como se ha indicado, se realizan a través de videoconferencia y e-mail.

Se computan una serie de horas estimadas, pues, aunque existen sesiones comunes para todos los estudiantes, éstos posteriormente pueden solicitar al docente tantas tutorías como estimen necesarias.

Dado el carácter mixto de esta actividad formativa, se computa un porcentaje de sincronía estimado del 30%.

5. Estudio autónomo

En esta actividad el estudiante consulta, analiza y estudia los manuales, bibliografía y recursos propios de la asignatura de forma autónoma a fin de lograr un aprendizaje significativo y superar la evaluación de la asignatura de la asignatura. Esta actividad es indispensable para adquirir las competencias del título, apoyándose en el aprendizaje autónomo como complemento a las clases y actividades supervisadas.

6. Examen final

Como parte de la evaluación de cada una de las asignaturas (a excepción de las prácticas y el Trabajo fin de título), se realiza una prueba o examen final. Esta prueba se realiza en tiempo real (con los medios de control antifraude especificados) y tiene como objetivo evidenciar el nivel de adquisición de conocimientos y desarrollo de competencias por parte de los estudiantes. Los exámenes o pruebas de evaluación final se realizan en las fechas y horas programadas con antelación y con los sistemas de vigilancia online (proctoring) de la universidad.

5. Evaluación

5.1. Sistema de evaluación

El Modelo de Evaluación de estudiantes en la Universidad se sustenta en los principios del Espacio Europeo de Educación Superior (EEES), y está adaptado a la estructura de formación virtual propia de esta Universidad. De este modo, se dirige a la evaluación de competencias.

Sistema de Evaluación	Ponderación
Portafolio*	60 %
Sistema de Evaluación	Ponderación
Prueba final*	40 %

***Es requisito indispensable para superar la asignatura aprobar cada apartado (portafolio y prueba final)** con un mínimo de 5 para ponderar las calificaciones.

Los enunciados y especificaciones propias de las distintas actividades serán aportados por el docente, a través del Campus Virtual, a lo largo de la impartición de la asignatura.

Atendiendo a la Normativa de Evaluación de la Universidad, se tendrá en cuenta que la utilización de **contenido de autoría ajena** al propio estudiante debe ser citada adecuadamente en los trabajos entregados. Los casos de plagio serán sancionados con suspenso (0) de la actividad en la que se detecte. Asimismo, el uso de **medios fraudulentos durante las pruebas de evaluación** implicará un suspenso (0) y podrá implicar la apertura de un expediente disciplinario.

5.2. Sistema de calificación

La calificación de la asignatura se establecerá en los siguientes cómputos y términos:

Nivel de aprendizaje	Calificación numérica	Calificación cualitativa
Muy competente	9,0 - 10	Sobresaliente
Competente	7,0 - 8,9	Notable
Aceptable	5,0 -6,9	Aprobado
Aún no competente	0,0 -4,9	Suspenso

Sin detrimento de lo anterior, el estudiante dispondrá de una **rúbrica simplificada** en el aula que mostrará los aspectos que valorará el docente, como así también los **niveles de desempeño que tendrá en cuenta para calificar las actividades vinculadas a cada resultado de aprendizaje.**

La mención de «**Matrícula de Honor**» podrá ser otorgada a estudiantes que hayan obtenido una calificación igual o superior a 9.0. Su número no podrá exceder del cinco por ciento de los estudiantes matriculados en una materia en el correspondiente curso académico, salvo que el número de estudiantes matriculados sea inferior a 20, en cuyo caso se podrá conceder una sola «Matrícula de Honor.

6. Bibliografía

I_n_t_r_o_d_u_c_c_i_ón_ _y_ _P_l_a_n_i_f_i_c_a_c_i_ón_ _

[_1_]_ _M_a_n_e_l_ _M_e_d_i_n_a_,_ _M_e_r_c_è _M_o_l_i_s_t_._ _(_2_0_1_5_)_._

_C_i_b_e_r_c_r_i_m_e_n_._ _B_a_r_c_e_l_o_n_a_:_ _T_i_b_i_d_a_b_o_._ _

[2] jon Erickson. (2008). Hacking, the art of exploitation. San Francisco:No starch press

[3] OWASP. (2016). OWASP Testing Guide. Septiembre 2016, Sitio web:

https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents

A_n_ál_i_s_i_s_ _

[1] OpenVas [2016]. Technical documentation. Noviembre 2016, Sitio Web:

http://docs.greenbone.net/index.html#user_documentation

[2] Wfuzz [2016]. Edge Security. Noviembre 2016, Sitio Web:

http://www.edge-security.com/wfuzz.php

[3] Kali Linux Downloads [2016]. Noviembre 2016, Sitio Web:

https://www.kali.org/downloads/

Information gathering:

[1] OWASP [2016]. Testing: Information Gathering. Octubre 2016, Sitio web:

https://www.owasp.org/index.php/Testing:_Information_Gathering V.04 9

G_u_ía_ _d_i_d_ác_t_i_c_a_ *_H_a_c_k_i_n_g_ _Ét_i_c_o_ _*

[_2_]_ _B_o_r_j_a_ _M_e_r_i_n_o_,_ _J_o_s_e_ _M_i_g_u_e_l_ _O_l_g_u_ín_._ _[_2_0_1_1_]_ _P_e_n_t_e_s_t_:_ _R_e_c_o_l_e_c_c_i_ón_ _d_e_ _i_n_f_o_r_m_a_c_i_ón_ _(Information Gathering). INCIBE https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_seguridad_information_gathering.pdf

[3] FOCA [2016]. Eleven paths. Octubre 2016, Sitio Web: https://www.elevenpaths.com/es/labstools/foca-2/index.html

E_x_p_l_o_t_a_c_i_ón_:_ _

[_1_]_ _H_D_ _M_o_o_r_e_ _&_ _V_a_l_s_m_i_t_h_._ _[_2_0_0_7_]_ _T_a_c_t_i_c_a_l_ _E_x_p_l_o_i_t_a_t_i_o_n_:_ _“t_h_e_ _o_t_h_e_r_ _w_a_y_ _t_o_ _p_e_n_t_e_s_t_”._ _Black Hat USA. https://www.blackhat.com/presentations/bh-usa-07/Moore_and_Valsmith/Presentation/bh-usa-07-moore_and_valsmith.pdf

[2] Anley, Chris, and Jack Koziol. [2007] The shellcoder's handbook: discovering and exploiting security holes. ISBN 978-0470080238.

[3] Erickson, Jon. [2008] Hacking: the art of exploitation.ISBN 978-1593271442

[4] Kennedy, David. Metasploit: the penetration tester's guide. ISBN 978-1593272883.

[5] Offensive Security. Metasploit Unleashed: The ultimate guide to the Metasploit Framework.https://www.offensive-security.com/metasploit-unleashed/

[6] Corelan Team. https://www.corelan.be/

P_o_s_t_ _E_x_p_l_o_t_a_c_i_ón_:_ _

[1] g0tmi1k. [2011] Basic Linux Privilege Escalation. https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/

[2] Jonathan Renard [2015] To Shell And Back: Adventures In Pentesting. http://toshellandback.com/2015/11/24/ms-priv-esc/

[3] FuzzySecurity Team. [2014] Windows Privilege Escalation Fundamentals. http://www.fuzzysecurity.com/tutorials/16.html

[4] Ignacio Sorribas. [2014] Post-E_x_p_l_o_i_t_a_t_i_o_n_ _w_i_t_h_ _“I_n_c_o_g_n_i_t_o_”._ _h_t_t_p_:_/_/_h_a_r_d_s_e_c_._n_e_t_/_p_o_s_t_-exploitation-with-incognito