23-24

MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD

GUÍA DE ESTUDIO PÚBLICA

HACKING ÉTICO

CÓDIGO 31109044

UNED

23-24

HACKING ÉTICO

CÓDIGO 31109044

ÍNDICE

Nombre de la asignatura	HACKING ÉTICO
Código	31109044
Curso académico	2023/2024
Título en que se imparte	MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD
Tipo	CONTENIDOS
Nº ETCS	6
Horas	150.0
Periodo	SEMESTRE 1
Idiomas en que se imparte	CASTELLANO

PRESENTACIÓN Y CONTEXTUALIZACIÓN

Presentación

Esta guía presenta las orientaciones básicas que requiere el estudiante para el estudio de la asignatura de Hacking Ético, asignatura obligatoria del primer semestre del Máster Universitario en Ciberseguridad. Por esta razón es muy recomendable leer con atención esta guía antes de iniciar el estudio, para adquirir una idea general de la asignatura y de los trabajos, actividades y prácticas que se van a desarrollar a lo largo del curso.

El objetivo del curso es presentar a los estudiantes los contenidos y habilidades necesarios para analizar la seguridad de sistemas y aplicaciones. La asignatura cubrirá los conceptos de escaneo, pruebas, hacking y aseguración de sistemas. Se analizarán los diferentes problemas y vulnerabilidades de los sistemas de información para poner en marcha mecanismos prevención de amenazas, mediante la detección, creación de políticas, análisis, control de acceso, test de penetración, etc. Estos conocimientos adquiridos al cursar la asignatura, sentarán las bases para poder desarrollar trabajos de consultores de seguridad y miembros de equipos rojos en el mercado laboral actual.

Contextualización

La asignatura de Hacking Ético se trata de una asignatura de 6 créditos ECTS, obligatoria, impartida en el primer semestre del Máster Universitario en Ciberseguridad. Guarda relación con las siguientes asignaturas también disponibles en el mismo Máster:

- *Análisis del Malware.* El Malware es una de las principales herramientas asociadas a los incidentes. Comprender mejor el funcionamiento de estos programas facilita la realización de test donde intervengan este tipo de elementos.
- *Auditoria y Monitorización de la Seguridad*. Un atacante podrá ser descubierto en base a los mecanismos de monitorización disponibles en un sistema. Por lo tanto, esquivar los mecanismos que registren la actividad es un elemento clave en los tests de penetración.
- *Gestión de Incidentes de Seguridad.* Como ya hemos comentado la respuesta ante incidentes tiene como objetivo volver a un sistema a un estado operativo tras la detección de incidente. Saber cómo un incidente es detectado es fundamental para evitar ser detectado y como cubrir nuestros pasos durante un test de seguridad.
- *Ciberilícitos.* En esta asignatura se profundiza sobre los límites de los análisis de seguridad de infraestructuras, así como la legalidad vigente sobre crimen digital.

REQUISITOS Y/O RECOMENDACIONES PARA CURSAR ESTA ASIGNATURA

Para cursar adecuadamente esta asignatura es recomendable tener los siguientes conocimientos previos:

•Estar familiarizado con las redes computadores, los servicios de redes y los protocolos de red.

•Estar familiarizado con los sistemas operativos y su funcionamiento.

•Saber programar scripts de configuración.

•Conocer (leer y escribir) el inglés técnico.

EQUIPO DOCENTE

Nombre y Apellidos	ELIO SAN CRISTOBAL RUIZ (Coordinador de asignatura)
Correo Electrónico	elio@ieec.uned.es
Teléfono	91398-9381
Facultad	ESCUELA TÉCN.SUP INGENIEROS INDUSTRIALES
Departamento	INGENIERÍA ELÉCTRICA, ELECTRÓNICA, CONTROL, TELEMÁTICA Y QUÍMICA APLICADA A LA INGENIERÍA

Nombre y Apellidos	ANTONIO ROBLES GOMEZ
Correo Electrónico	arobles@scc.uned.es
Teléfono	91398-8480
Facultad	ESCUELA TÉCN.SUP INGENIERÍA INFORMÁTICA
Departamento	SISTEMAS DE COMUNICACIÓN Y CONTROL

Nombre y Apellidos	GABRIEL DIAZ ORUETA
Correo Electrónico	gdiaz@ieec.uned.es
Teléfono	91398-8255
Facultad	ESCUELA TÉCN.SUP INGENIEROS INDUSTRIALES
Departamento	INGENIERÍA ELÉCTRICA, ELECTRÓNICA, CONTROL, TELEMÁTICA Y QUÍMICA APLICADA A LA INGENIERÍA

HORARIO DE ATENCIÓN AL ESTUDIANTE

La comunicación entre estudiantes y el equipo docente se realizará preferiblemente a través de la plataforma virtual aLF o por correo electrónico con los profesores. También se facilitan los teléfonos, horarios de guardia y correo postal.

Elio San Cristobal Ruiz

Horario: Martes Lectivos de 10:00 a 14:00 horas

Correo electrónico: elio@ieec.uned.es

Teléfono: 91 398 93 81

Dirección Postal:

ETSI Industriales. UNED

C/Juan del Rosal 12.

28040. Madrid

Antonio Robles Gómez
Horario: Lunes lectivos de 10:00 a 14:00
Email: arobles@scc.uned.es
Tfno: 91 398 84 80
Dirección Postal:
ETSI Informática. UNED
C/Juan del Rosal 16.
28040. Madrid

COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE

COMPETENCIAS 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

CB8 - 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

CB9 - 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

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

COMPETENCIAS GENERALES

CG1 - Analizar métodos y técnicas de ciberataques.

CG3 - Conocer la normativa y la legislación en materia de ciberseguridad, sus implicaciones en el diseño y puesta en marcha de sistemas informáticos.

COMPETENCIAS ESPECÍFICAS

CE2 - Diseñar mecanismos de prevención de amenazas a la seguridad, así como de reconocer y resolver incidentes de seguridad en los sistemas críticos.

CE4 - Analizar e identificar vulnerabilidades ante posibles ataques en los sistemas de comunicaciones y los servicios asociados.

CE6 - Conocer las tendencias actuales en técnicas de ciberataque, los mecanismos de defensa mediante aprendizaje automático y especialmente dirigido a casos reales

RESULTADOS DE APRENDIZAJE

Los resultados de aprendizaje más relevantes que se pretenden alcanzar con el estudio de esta asignatura son los siguientes:

•Estudio y análisis de los sistemas de información para el aseguramiento de los mismos.

•Comprender y aplicar métodos y técnicas de hacking ético en sistemas y aplicaciones.

•Análisis de problemas y vulnerabilidades de los sistemas de información para el establecimiento de mecanismos de prevención de amenazas.

•Diseño de técnicas y uso de herramientas de seguridad en los sistemas de información.

CONTENIDOS

1. Introducción al hacking ético

En este tema se van a repasar algunos de los conceptos básicos de seguridad. Estos conceptos de vulnerabilidad, riesgo, políticas de seguridad, etc. son esenciales para cualquier persona que quiera dedicarse a la seguridad. Posteriormente, veremos cómo los hackers pueden ser clasificados según sus propósitos y nos centraremos en los denominados hackers éticos. Estos hackers suelen realizar pruebas de penetración y deben cumplir con las leyes establecidas en el país o países donde van a desarrollar su actividad.

2. Footprinting, reconocimiento

La recolección de información o fase de reconocimientos es donde el hacker, tanto ético como no, recopila toda la información posible de un sistema. En este tema se pretende dar respuesta a dos preguntas muy importantes ¿Qué clase de información se busca? Y ¿Cómo obtener esa información?

Para ello, se mostrarán diferentes tipos de técnicas de reconocimiento y footprinting, como:

•Motores de búsqueda (Google hacking)

•Herramientas para hacer copías de sitios Web, por ejemplo, HTTrack

•Herramientas Web que permiten ver historico de instantaneas Web o información de DNS, Servidores Web, etc.

•Comandos como whois, nslookup, dig o nmap

Esta etapa es fundamental, para posteriormente revisar posibles vulnerabilidades, amenazas y riesgos del sistema a auditar.

3. Hacking de servidores y aplicaciones Web

Este tema describirá algunos de los servidores más utilizados actualmente. Posteriormente, se centrará en las etapas definidas por EC-Council para atacar un servidor. Por último, se describirán algunos de los ataque más frecuentes en servidores y aplicaciones Web.
Entre los ataques que, tanto de servidores como de aplicaciones Web, podemos encontrar están:

- Denegación de servicio por amplificación de DNS.
- Ataque de directorio trasversal.
- Envenenamiento de la Web cache
- Ataque de secuencias de comandos en sitios cruzados o Cross-site scripting (XSS)
- Ataque por desbordamiento de buffer o buffer overflow
- Inyección SQL

El alumno deberá conocer su funcionamiento y algunas plataformas libres que facilitan la práctica de dichos ataques.

4. Ingeniería social

La ingeniería social es utilizada en nuestra vida cotidiana. Este capítulo definirá que es la ingeniería social y sus principios básicos. Así como los métodos y técnicas, tanto a nivel personal como tecnológico, que se utilizan para explotar aspectos humanos como la confianza, el deseo, etc. Por último, se describirá el uso de la herramienta Social Engineering Toolkit que proporciona realizar ataques sociales de una manera rápida y sencilla.
La ingeniería social es uno de los métodos más utilizados a la hora de realizar un ataque. Conceptos como spear phising, whaling o smishing empiezan a formar parte de nuestra vida y debemos ser conscientes de su peligrosidad y de su uso. Además, es importante remarcar que algunos de estos ataques se basan en la información recopilada con técnicas del tema 2 del curso "Footprinting, reconocimiento" como correos electrónicos, teléfonos, etc.

5. Mecanismos de prevención de amenazas: Firewalls

Los cortafuegos o firewalls son herramientas muy utilizadas en redes de comunicaciones. Este capítulo introduce conceptos como tipos de firewalls, funcionamiento y uso de listas de control de acceso a ACLs
Las listas de control de acceso permiten filtrar paquetes de información y por tanto minimizar el riesgo de algunos ataques. Veremos algunos ejemplos de aplicación y también se remarcará que, aunque un firewall minimiza riesgos, existen mecanismo de evasión de firewalls, tema 6 del curso "Evadirse de IDS, Firewalls y Honeypots"

6. Evadirse de IDS, Firewalls y Honeypots

En este tema se estudia algunas de las técnicas utilizadas para la evasión de firewalls y de sistema de detección de intrusiones (IDS). También el uso de Honeypots que permite dirigir al atacante a un sistema controlado y monitoreado, y que permite a la organización aprender como un atacante trabaja.
El tema presenta al estudiante los conceptos de IDSs y Honeypots. El concepto de firewall ya se estudió en el tema 5 "Mecanismos de prevención de amenazas: Firewalls". Por último, se introducen algunos de los mecanismos de evasión más conocidos como: IP Spoofing o suplantación de direcciones IP, fragmentación de paquetes o uso servidores proxy.

7. Hacking de plataformas móviles

El número de dispositivos móviles ha aumentado enormemente. También, su capacidad de procesamiento, almacenamiento y comunicación a aumentando de forma importante. Esto hace que sea un objetivo de posibles ataques.
En este tema se estudiaránn algunos de los ataques más utilizados en dispositivos móviles. Entre los más destacados están:
•El uso incorrecto de las opciones de seguridad de la plataforma móvil.
•Almacenamiento inseguro de los datos.
•Comunicaciones inseguras.
•Calidad del código de aplicaciones de terceros.
Estas características pueden ser explotadas por atacantes. El hacker ético debe conocer los métodos de ataque y comprobar las posibles vulnerabilidades de la organización que lo contrata.

METODOLOGÍA

Esta asignatura ha sido diseñada para la enseñanza a distancia. Por tanto, el sistema de enseñanza-aprendizaje estará basado en gran parte en el estudio independiente o autónomo del estudiante. Para ello, el estudiante contará con diversos materiales que permitirán su trabajo autónomo y la Guía de Estudio de la asignatura, que incluye orientaciones para la realización de las actividades prácticas. Asimismo, mediante la plataforma virtual de la UNED existirá un contacto continuo entre el equipo docente y los/as estudiantes, así como una interrelación entre los propios estudiantes a través de los foros, importantísimo en la enseñanza no presencial.
Esta asignatura de 6 créditos ECTS está planificada en 150 horas. El tiempo de las actividades formativas, siguiendo la anterior metodología, se han distribuido de forma orientativa de la siguiente manera:

•Estudio de los contenidos teóricos-prácticos utilizando la bibliografía y los materiales complementarios: 60 horas.
•Tutorías: 15 horas.
•Actividades en la plataforma virtual, incluyendo la participación en los debates propuestos en los foros de debate: 13 horas.
•Prácticas informáticas: 30 horas.
•Trabajos, de carácter individual y/o colectivo: 30 horas.
•Examen final: 2 horas.

SISTEMA DE EVALUACIÓN

TIPO DE PRUEBA PRESENCIAL

Tipo de examen	Examen tipo test
Preguntas test	10
Duración del examen	90 (minutos)

Material permitido en el examen

Ninguno

Criterios de evaluación

La prueba presencial se tratará de un cuestionario de 10 preguntas teórico-prácticas que versarán sobre los contenidos de la asignatura. Cada cuestión tendrá un máximo de cuatro respuestas posibles, siendo sólo correcta una. Cada cuestión tendrá un valor de un punto en caso de contestar de forma correcta. Y restaran 0.45 puntos en caso de contestarse de forma errónea. El estudiante dispondrá de 90 minutos para la realización de este examen. Además de que no se permite ningún material durante su realización.

El examen contará un 60% para la nota final de la asignatura.

Se exige un 4 para que haga media con los trabajos.

% del examen sobre la nota final	60
Nota del examen para aprobar sin PEC	
Nota máxima que aporta el examen a la calificación final sin PEC	
Nota mínima en el examen para sumar la PEC	

Comentarios y observaciones

El examen contará un 60% para la nota final de la asignatura.

CARACTERÍSTICAS DE LA PRUEBA PRESENCIAL Y/O LOS TRABAJOS

Requiere Presencialidad	No

Descripción

Las prácticas informáticas **OBLIGATORIAS** consistirán en varias actividades prácticas que el estudiante deberá elaborar a lo largo del curso de manera incremental. Estás práctica estarán relacionadas con uno o varios modulos de la asignatura y se dividirán en dos categorías:

Práctica 1 Reconocimiento y ataques sobre aplicaciones Web (Temas 1, 2 y 3).

Práctica 2 Ingeniería social, comunicaciones y dispositivos móviles (Temas 4, 5, 6 y 7)

El seguimiento de las prácticas informáticas se realizará en la plataforma de aprendizaje del curso. No será necesario que el estudiante acuda al Centro Asociado para realizar las prácticas informáticas y los trabajos, ya que podrán realizarse de forma online en su totalidad y se presentarán a través del curso virtual.

Criterios de evaluación

El equipo docente publicará una guía para cada práctica. Donde se especificará el desarrollo de la práctica y los criterios de evaluación. Se debe obtener al menos un 5 en estas prácticas para que se haga media para la nota final.

Las prácticas informáticas cuentan un 20% de la nota final de la asignatura.

Las prácticas informáticas se podrán entregar tanto en el semestre en que se imparte la asignatura como en la convocatoria extraordinaria. En el caso que el alumno se vaya a presentar en septiembre, se abrirá un plazo de entrega de las prácticas que se indicará en el curso virtual.

Ponderación de la prueba presencial y/o los trabajos en la nota final	El 20% de la nota final de la asignatura.
Fecha aproximada de entrega	
Comentarios y observaciones	

PRUEBAS DE EVALUACIÓN CONTINUA (PEC)

¿Hay PEC?	No
Descripción	
Criterios de evaluación	
Ponderación de la PEC en la nota final	
Fecha aproximada de entrega	
Comentarios y observaciones	

OTRAS ACTIVIDADES EVALUABLES

¿Hay otra/s actividad/es evaluable/s?	Si,no presencial
Descripción	

Otro tipo de actividades evaluable es el trabajo de la asignatura. Este trabajo será de tipo teórico o teórico-práctico y se centrará en uno o varios temas de la asignatura. Es de carácter **OBLIGATORIO** y su entrega se hará desde la plataforma de Aprendizaje.

Los trabajos pueden incluir temas tan variados como:

Investigación de nuevas herremientas para ataques a nivel de Web.

Evolución e impacto de los ataques de ingeniería social en el mundo de la información y en la industria.

Diseño de IDS y aplicación de seguridad fronteriza.

Etc.

También debemos remarcar que el seguimiento del trabajo se realizará en la plataforma de aprendizaje del curso. No será necesario que el estudiante acuda al Centro Asociado para realizar las prácticas informáticas y los trabajos, ya que podrán realizarse de forma online en su totalidad y se presentarán a través del curso virtual.

El trabajo se podrá entregar tanto en el semestre en que se imparte la asignatura como en la convocatoria extraordinaria. En el caso que el alumno se vaya a presentar en septiembre, se abrirá un plazo de entrega de las prácticas que se indicará en el curso virtual.

Criterios de evaluación

El equipo docente publicará una guía del trabajo a realizar. Donde se especificará el desarrollo de la práctica y los criterios de evaluación. Se debe obtener al menos un 5 en dicho trabajo para que se haga media para la nota final.

El trabajo cuenta con un 20% de la nota final de la asignatura.

Ponderación en la nota final — El 20% de la nota final

Fecha aproximada de entrega

Comentarios y observaciones

¿CÓMO SE OBTIENE LA NOTA FINAL?

Nota final = (Examen Final x 0,6) + (Prácticas infórmaticas x 0,2) + (Trabajo x 0,2)

El examen final (EF) contará un 60% para la nota final de la asignatura.

Las prácticas informáticas (PI) cuentan un 20% de la nota final de la asignatura.

Trabajo (T) cuenta un 20% de la nota final de la asignatura.

IMPORTANTE: Para aprobar la asignatura, el alumno deberá presentar y aprobar las dos prácticas informáticas, el trabajo, y el examen.

BIBLIOGRAFÍA BÁSICA

La bibliografía básica será proporcionada al estudiante dentro del curso virtual, estará compuesta por materiales teórico-prácticos propuestos por el equipo docente.
Gran parte de la bibliografía, así como los recursos proporcionados al estudiante en el curso virtual pueden estar únicamente en inglés, debido a la novedad de algunos de los contenidos propuestos para la asignatura.

BIBLIOGRAFÍA COMPLEMENTARIA

- Advanced Infrastructure Penetration Testing. Autor: Chiheb Chebbi. Publisher: Packt Publishing. Release Date: February 2018. ISBN: 9781788624480. URL: https://learning.oreilly.com/library/view/advanced-infrastructure-penetration/9781788624480/
- Learn Ethical Hacking from Scratch. Autor: Zaid Sabih. Publisher: Packt Publishing. Release Date: July 2018. ISBN: 9781788622059. URL: https://learning.oreilly.com/library/view/learn-ethical-hacking/9781788622059/

RECURSOS DE APOYO Y WEBGRAFÍA

Los/as estudiantes dispondrán de los siguientes recursos de apoyo al estudio:

- **Guía de la asignatura.** Incluye el plan de trabajo y orientaciones para su desarrollo. Esta guía será accesible desde el curso virtual.
- **Curso virtual.** A través de esta plataforma los/as estudiantes tienen la posibilidad de consultar información de la asignatura, realizar consultas al Equipo Docente a través de los foros correspondientes, consultar e intercambiar información con el resto de los compañeros/as.
- **Documentación de la asignatura.** El equipo docente publicará recursos adicionales que faciliten o profundicen los contenidos desarrollados en la asignatura, además de los contenidos ya ofrecidos.
- **Biblioteca.** El estudiante tendrá acceso tanto a las bibliotecas de los Centros Asociados como a la biblioteca de la Sede Central, en ellas podrá encontrar un entorno adecuado para el estudio, así como de distinta bibliografía que podrá serle de utilidad durante el proceso de aprendizaje.

IGUALDAD DE GÉNERO

En coherencia con el valor asumido de la igualdad de género, todas las denominaciones que en esta Guía hacen referencia a órganos de gobierno unipersonales, de representación, o miembros de la comunidad universitaria y se efectúan en género masculino, cuando no se hayan sustituido por términos genéricos, se entenderán hechas indistintamente en género femenino o masculino, según el sexo del titular que los desempeñe.