Guía Docente

DATOS DE IDENTIFICACIÓN

Titulación:	Diploma en Ciberseguridad y Hacking Ético (Título Propio asociado a Ingeniería Informática)
Rama de Conocimiento:	Ingeniería y Arquitectura
Facultad/Escuela:	Escuela Politécnica Superior
Asignatura:	Hacking Ético y Pentesting I
Tipo:	Propia Obligatoria
Créditos ECTS:	2
Curso:	2
Código:	56413
Periodo docente:	Tercer semestre
Tipo de enseñanza:	Presencial
Idioma:	Castellano
Total de horas de dedicación del alumno:	50

Equipo Docente	Correo Electrónico
Constantino Malagón Luque	constantino.malagon@ufv.es

DESCRIPCIÓN DE LA ASIGNATURA

El objetivo de esta asignatura es enseñar los conceptos básicos en torno al Hacking ético y a una de sus herramientas principales, el test de penetración o pentesting.
En concreto, los grandes bloques del curso serán:
1. Instalación y configuración del entorno de pruebas
2. Introducción al Hacking ético
3. Técnicas de obtención de información

OBJETIVO

El objetivo final es que cada alumno tenga un conocimiento básico de las principales herramientas que se pueden usar a la hora de realizar un test de penetración en un entorno Linux.

CONOCIMIENTOS PREVIOS

Se necesitan conocimientos previos de administración de sistemas Linux

CONTENIDOS

Tema 1 – Instalación y configuración de Kali Linux - Creación y configuración de máquinas virtuales - Configuración de un entorno de pruebas
Tema 2 - Introducción al Hacking ético - ¿Qué es el hacking ético? - Conceptos fundamentales - Ethical hacking report
Tema 3 - Técnicas de obtención de información. escaneo de puertos y detección de vulnerabilidades - Conceptos básicos de TCP/IP, servicios y comunicaciones. - Métodos no intrusivos para la obtención de información. - Métodos intrusivos para la obtención de información. - Descubrimiento de equipos en la red. Uso de Netdiscover. - Técnicas de rastreo o sniffing. Uso de Wireshark. - Escaneo de puertos. Uso de Nmap.
Tema 4 - Técnicas de intrusión y ataque - Técnicas de ataque en redes locales usando ataque MItM (Man in the Midle). Uso de Bettercap. - El servicio DNS. Ataques de DNS spoofing.

ACTIVIDADES FORMATIVAS

Se combinan lecciones expositivas con clases prácticas de manera que se favorezca la participación y la interacción alumno/profesor y alumno/alumno como vía para fomentar el aprendizaje colaborativo y la capacidad de autoaprendizaje, todo ello mediante estrategias de resolución de situaciones y metodologías de intervención. Las actividades no presenciales, que pueden ser tanto de tipo individual como colectivo, serán supervisadas por el profesor en clases y tutorías estando encaminadas a favorecer el aprendizaje autónomo y colaborativo. Se complementa la lección expositiva, por una parte, con las clases prácticas para la asimilación y aplicación de los conocimientos adquiridos y, por otra, con laboratorios que permitan realizar prácticas para la resolución de problemas y casos, con la supervisión directa del profesor y el enriquecimiento del trabajo en grupo.
Finalmente, con el fin de facilitar al alumno el acceso a los materiales y la planificación de su trabajo, así como la comunicación con el profesor y el resto de alumnos, se empleará el Aula Virtual de la Universidad.

DISTRIBUCIÓN DE LOS TIEMPOS DE TRABAJO

ACTIVIDAD PRESENCIAL	TRABAJO AUTÓNOMO/ACTIVIDAD NO PRESENCIAL
25 horas	25 horas

COMPETENCIAS

Instalación y configuración de un entorno de pruebas para la realización de tests de penetración

Obtención de información mediante técnicas pasivas y activas

RESULTADOS DE APRENDIZAJE

Capacidad para instalar y configurar una máquina basada en Kali Linux

Capacidad para configurar un entorno en red para la realización de tests de penetración

Realización y comprensión de diferentes ataques en redes de área local

SISTEMA DE EVALUACIÓN DEL APRENDIZAJE

El sistema de evaluación contempla dos tipos de pruebas:
•Prueba de carácter teórico-práctico: tiene un peso del 45% en la nota final.
•Prueba de carácter teórico-práctico final: tiene un peso del 45% en la nota final.
•Prácticas de clase y participación: tiene un peso del 10% en la nota final.

Es necesario obtener un mínimo de 5 puntos sobre 10 en todas las pruebas para poder aprobar la asignatura.
Aquellos alumnos que estén exentos de la obligación de asistir a clase, bien por segunda matrícula en la asignatura o sucesivas, bien por contar con autorización expresa de la Dirección del Grado, serán evaluados por el mismo tipo de pruebas.
Recuperación en convocatoria extraordinaria
Los alumnos que no hayan alcanzado la nota mínima en las pruebas teórico prácticas y en la presentación y defensa de trabajos, habiendo suspendido por tanto en la convocatoria ordinaria, podrán optar a una recuperación en la convocatoria extraordinaria.
En la recuperación extraordinaria el alumno se presentará sólo a las partes que tenga evaluadas por debajo de 5.
A efecto de cómputo de convocatorias en una asignatura, solamente se contabilizarán como consumidas aquellas en las que el alumno se haya presentado a todas las pruebas de evaluación, o a una parte de las mismas, siempre que su peso en la nota final supere el 50%. Se entenderá que un alumno se ha presentado a una prueba aunque la abandone una vez comenzada la misma. La condición de No Presentado en la convocatoria extraordinaria estará ligada a la no asistencia o entrega de ninguna prueba, práctica o trabajo que esté pendiente. El alumno dispone de 6 convocatorias para superar esta asignatura. La Normativa de Evaluación de la UFV recoge todo lo relativo a los procesos de evaluación y consumo de convocatorias.
Cualquier tipo de fraude o plagio por parte del alumno en una actividad evaluable, será sancionado según se recoge en la Normativa de Convivencia de la UFV. A estos efectos, se considerará "plagio" cualquier intento de defraudar el sistema de evaluación, como copia en ejercicios, exámenes, prácticas, trabajos o cualquier otro tipo de entrega, bien de otro compañero, bien de materiales o dispositivos no autorizados, con el fin de hacer creer al profesor que son propios.

BIBLIOGRAFÍA Y OTROS RECURSOS

Básica

Gregg, Michael CEH Certified Ethical Hacker Cert Guide Pearson IT Certification; 4ª edición

Complementaria

Vijay Kumar Velu Mastering Kali Linux for Advanced Penetration Testing Packt Publishing; 4ª ed