Guía docente
230711 - UCASES - Casos de Uso en Ciberseguridad

Última modificación: 26/05/2023

Unidad responsable: Escuela Técnica Superior de Ingeniería de Telecomunicación de Barcelona
Unidad que imparte: 744 - ENTEL - Departamento de Ingeniería Telemática.

Titulación: MÁSTER UNIVERSITARIO EN INGENIERÍA DE TELECOMUNICACIÓN (Plan 2013). (Asignatura optativa).
MÁSTER UNIVERSITARIO EN TECNOLOGÍAS AVANZADAS DE TELECOMUNICACIÓN (Plan 2019). (Asignatura optativa).
MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD (Plan 2020). (Asignatura optativa).

Curso: 2023 **Créditos ECTS:** 5.0 **Idiomas:** Inglés

PROFESORADO

Profesorado responsable: Consultar aquí / See here: https://telecos.upc.edu/ca/estudis/curs-actual/professorat-responsables-coordinadors/responsables-assignatura

Otros: Consultar aquí / See here: https://telecos.upc.edu/ca/estudis/curs-actual/professorat-responsables-coordinadors/professorat-assignat-idioma

METODOLOGÍAS DOCENTES

OBJETIVOS DE APRENDIZAJE DE LA ASIGNATURA

El curso tiene como objetivo poner en práctica conceptos de penetration testing, utilizando herramientas open source, y mediante diferentes enfoques (red team, blue team, forensics), también se incluyen aspectos de ethical hacking.

HORAS TOTALES DE DEDICACIÓN DEL ESTUDIANTADO

Tipo	Horas	Porcentaje
Horas grupo pequeño	39,0	31.20
Horas aprendizaje autónomo	86,0	68.80

Dedicación total: 125 h

CONTENIDOS

Preparar un entorno de máquinas visrtuales

Descripción:
Preparar un entorno virtual con sistemas operativos vulnerables (Windows y Linux) para que actúe como una caja de arena para técnicas de pentesting

Objetivos específicos:
Comprender lo peligroso que puede ser un pentest y preparar un entorno seguro.

Actividades vinculadas:
Sesión de laboratorio

Dedicación: 3h
Grupo mediano/Prácticas: 3h

Comportamiento ético de los profesionales de la ciberseguridad

Descripción:
Diferencia entre ética Hacker y Hacking ético. Guías de buenas prácticas ante dilemas éticos. Documentación a tener en cuenta antes de iniciar un hacking ético. Aspectos administrativos y legales

Actividades vinculadas:
Sesión de laboratorio

Dedicación: 3h
Grupo mediano/Prácticas: 3h

Fase de reconocimiento

Descripción:
contenido castellano

Dedicación: 3h
Grupo mediano/Prácticas: 3h

Armamento hacker (1)

Descripción:
scapy

Dedicación: 3h
Grupo mediano/Prácticas: 3h

Análisis Automático de Vulnerabilidades

Descripción:
Nessus

Dedicación: 3h
Grupo mediano/Prácticas: 3h

Shells

Descripción:
Netcat & Nikto

Dedicación: 3h
Grupo grande/Teoría: 3h

fase de exploit (1)

Descripción:
Metasploit

Dedicación: 3h
Grupo mediano/Prácticas: 3h

Fase de exploit (2)

Descripción:
Meterpreter

Dedicación: 3h
Grupo mediano/Prácticas: 3h

Fase de exploit (3)

Descripción:
Empire

Dedicación: 3h
Grupo mediano/Prácticas: 3h

Actuar como Equipo Azul

Descripción:
EDR, SIEM

Dedicación: 3h
Grupo mediano/Prácticas: 3h

Incident Response

Descripción:
GRR como herramienta rápida de incident response

Dedicación: 3h
Grupo mediano/Prácticas: 3h

Análisis Forense Digital

Descripción:
Autopsy & SleuthKit

Dedicación: 3h
Grupo mediano/Prácticas: 3h

Evaluación

Descripción:
Examen práctico

Dedicación: 3h
Grupo grande/Teoría: 3h

SISTEMA DE CALIFICACIÓN

BIBLIOGRAFÍA

Básica:
- Hertzog, R.; O'Gorman, J.; Aharoni, M. Kali Linux revealed: mastering the penetration testing distribution. Cornelius: Offsec Press, 2017. ISBN 9780997615609.

Complementaria:
- Ramos Fraile, A.; Yepes Alía, R. Hacker épico. 2a ed. Móstoles, Madrid: Zeroxword Computing, [2014]. ISBN 9788461621934.