Guia docent
230711 - UCASES - Casos d'Ús en Ciberseguretat

Última modificació: 24/05/2024

Unitat responsable: Escola Tècnica Superior d'Enginyeria de Telecomunicació de Barcelona
Unitat que imparteix: 744 - ENTEL - Departament d'Enginyeria Telemàtica.

Titulació: MÀSTER UNIVERSITARI EN ENGINYERIA DE TELECOMUNICACIÓ (Pla 2013). (Assignatura optativa).
MÀSTER UNIVERSITARI EN TECNOLOGIES AVANÇADES DE TELECOMUNICACIÓ (Pla 2019). (Assignatura optativa).
MÀSTER UNIVERSITARI EN CIBERSEGURETAT (Pla 2020). (Assignatura optativa).

Curs: 2024 **Crèdits ECTS:** 5.0 **Idiomes:** Anglès

PROFESSORAT

Professorat responsable: JOSEP RAFEL PEGUEROLES VALLES

Altres: Segon quadrimestre:
RUBÉN BARCELÓ ARMADA - 31, 33
JOSEP RAFEL PEGUEROLES VALLES - 31, 33

METODOLOGIES DOCENTS

OBJECTIUS D'APRENENTATGE DE L'ASSIGNATURA

El curs té com objectiu posar en pràctica conceptes de testos d'intrusió, mitjançant eines de codi obert, i a partir dels enfocaments d'equip atacant, equip defensor o enginyer forense, també es tracten temes de hacking ètic.

HORES TOTALS DE DEDICACIÓ DE L'ESTUDIANTAT

Tipus	Hores	Percentatge
Hores grup petit	39,0	31.20
Hores aprenentatge autònom	86,0	68.80

Dedicació total: 125 h

CONTINGUTS

Preparar un entorn de màquines virtuals

Descripció:
Preparar un entorn virtual amb sistemes operatius vulnerables (Windows i Linux) per actuar com a sandbox per a les tècniques de pentesting

Objectius específics:
Comprendre el perillós que pot ser un pentest i preparar un entorn segur

Activitats vinculades:
Sessió de laboratori

Dedicació: 3h
Grup mitjà/Pràctiques: 3h

Comportament ètic dels professionals de la ciberseguretat

Descripció:
Diferència entre ètica Hacker i Hacking ètic. Guies de bones pràctiques davant dilemes ètics. Documentació a tenir en compte abans d'iniciar un hacking ètic. Aspectes administratius i legals

Activitats vinculades:
Sessió de laboratori

Dedicació: 3h
Grup mitjà/Pràctiques: 3h

Fase de reconeixement

Descripció:
contingut català

Dedicació: 3h
Grup mitjà/Pràctiques: 3h

Armes hacker (1)

Descripció:
scapy

Dedicació: 3h
Grup mitjà/Pràctiques: 3h

Anàlisis Automàtic de Vulnerabilitats

Descripció:
Nessus

Dedicació: 3h
Grup mitjà/Pràctiques: 3h

Shells

Descripció:
Netcat & Nikto

Dedicació: 3h
Grup gran/Teoria: 3h

Fase d'exploit (1)

Descripció:
Metasploit

Dedicació: 3h
Grup mitjà/Pràctiques: 3h

Fase d'exploit (2)

Descripció:
Meterpreter

Dedicació: 3h
Grup mitjà/Pràctiques: 3h

Fase d'exploit (3)

Descripció:
Empire

Dedicació: 3h
Grup mitjà/Pràctiques: 3h

Actuar com Equip Blau

Descripció:
EDR, SIEM

Dedicació: 3h
Grup mitjà/Pràctiques: 3h

Incident Response

Descripció:
GRR com a eina ràpida per incident response

Dedicació: 3h
Grup mitjà/Pràctiques: 3h

Anàlisi Forense Digital

Descripció:
Autopsy & SleuthKit

Dedicació: 3h
Grup mitjà/Pràctiques: 3h

Avaluació

Descripció:
Examen Pràctic

Dedicació: 3h
Grup gran/Teoria: 3h

SISTEMA DE QUALIFICACIÓ

BIBLIOGRAFIA

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

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