Course guide
230711 - UCASES - Cybersecurity Use Cases

Last modified: 11/04/2025

Unit in charge: Barcelona School of Telecommunications Engineering
Teaching unit: 744 - ENTEL - Department of Network Engineering.

Degree: MASTER'S DEGREE IN TELECOMMUNICATIONS ENGINEERING (Syllabus 2013). (Optional subject).
MASTER'S DEGREE IN ADVANCED TELECOMMUNICATION TECHNOLOGIES (Syllabus 2019). (Optional subject).
MASTER'S DEGREE IN CYBERSECURITY (Syllabus 2020). (Optional subject).

Academic year: 2025 **ECTS Credits:** 5.0 **Languages:** English

LECTURER

Coordinating lecturer: JOSEP RAFEL PEGUEROLES VALLES

Others:

PRIOR SKILLS

Students have to proof basic knowledge of Linux and Network Security concepts

TEACHING METHODOLOGY

The course is structured in 12 sessions (3 hours long) in which after a short introduction of a Use Case, students have to solve by themselves, with the help of the professors, and working in groups (2-3 people) the goals and questions posed in the statement.

LEARNING OBJECTIVES OF THE SUBJECT

The course aims to put into practice penetration testing concepts, using open source tools, and through different approaches (red team, blue team, forensics), also including aspects of ethical hacking

STUDY LOAD

Type	Hours	Percentage
Self study	86,0	68.80
Hours small group	39,0	31.20

Total learning time: 125 h

CONTENTS

Setting up a VM to perform Penetration Testing

Description:
Preparing a virtual environment with vulnerable operating systems (Windows and Linux) to act as a sandbox for testing pentesting techniques

Specific objectives:
To understand how dangerous can be a pentest and preparing a safe environment

Related activities:
Lab Session

Full-or-part-time: 3h
Practical classes: 3h

Ethical behaviour of a cybersecurity professional

Description:
Difference between Hacker's ethics and Ethical Hacking. Good practice guides for ethical dilemmas. Documentation to take into account before starting an ethical hacking. Administrative and legal aspects

Related activities:
Lab session

Full-or-part-time: 3h
Practical classes: 3h

Recon phase

Description:
content english

Full-or-part-time: 3h
Practical classes: 3h

Weaponizationi (1)

Description:
scapy

Full-or-part-time: 3h
Practical classes: 3h

Automatic Vulnerability Analysis

Description:
Nessus

Full-or-part-time: 3h
Practical classes: 3h

Shells

Description:
Netcat & Nikto

Full-or-part-time: 3h
Theory classes: 3h

Exploit phase (1)

Description:
Metasploit

Full-or-part-time: 3h
Practical classes: 3h

Exploit phase (2)

Description:
Meterpreter

Full-or-part-time: 3h
Practical classes: 3h

Exploit phase (3)

Description:
Empire

Full-or-part-time: 3h
Practical classes: 3h

Acting as Blue Team

Description:
EDR, SIEM

Full-or-part-time: 3h
Practical classes: 3h

Incident Response

Description:
GRR as a Rapid Response tool

Full-or-part-time: 3h
Practical classes: 3h

Digital Forensics Analysis

Description:
Autopsy & SleuthKit

Full-or-part-time: 3h
Practical classes: 3h

Assessment session

Description:
Practical exam

Full-or-part-time: 3h
Theory classes: 3h

GRADING SYSTEM

Assessment is based on the reports submitted for every session/usecase. In case that professors have doubts on the authority of the reports, or in order to determine which student provided the main contribution, individual interviews to defend the reports can be required.

EXAMINATION RULES.

All reports have the same weight. Final qualification will be the arithmetic mean of the different grades.

BIBLIOGRAPHY

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

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