ESIROI
ÉCOLE D'INGÉNIEURS
UNIVERSITÉ DE LA RÉUNION

DEPARTMENT : *IT*
SEMESTER : *S7*

IDENTIFICATION

Course code :	ESI-SPI-CI-IN4-UE4-EC2
ECTS :	1

DURATION

Lectures :	0
Tutorial classes :	14
Labs :	10
Total :	24

Project :
Personnal work :

ASSESSMENT

Continuous assessments and evaluated practical work.

TEACHING MATERIALS

Slides, guided work sheets, and practical work sheets.

LANGUAGE

English

CONTACT

Train students in offensive security methodologies and tools so they can conduct penetration tests in a structured and documented manner. Through an ethical hacking approach, they will learn to identify, exploit, and report vulnerabilities in an information system, while respecting the applicable legal and regulatory framework (GDPR, NIS2).

Modified : 9 juillet 2026

UE : UE7-CYBER

COURSE : Cybersecurity : Offensive Security Methodologies

SCOPE OF THE COURSE

OBJECTIVES

COMPETENCE AND SKILLS

- Apply an audit and penetration testing methodology (PTES, OWASP, MITRE ATT&CK) on a real or simulated information system
- Conduct a risk analysis based on documentation, an offensive cybersecurity campaign, and the regulatory framework
- Identify and exploit network, system, and application vulnerabilities using appropriate tools
- Carry out an ethical hacking process in compliance with national and international legal frameworks (GDPR, NIS2)
- Write a structured intrusion report, including an executive summary, CVSS-scored findings, and associated recommendations

PROGRAM

- **Introduction to offensive security and ethical hacking :** legal framework (GDPR, NIS2, criminal law), pentester responsibilities, Red Team / Blue Team / Purple Team distinctions, engagement types (black box, gray box, white box).
- **Methodologies and standards for penetration testing :** PTES, OWASP Testing Guide, OSSTMM, MITRE ATT&CK — tactics, techniques, and procedures (TTP), phases of a pentest.
- **Reconnaissance and OSINT :** passive information gathering (WHOIS, DNS, Shodan, FOCA), social engineering, attack surface mapping.
- **Scanning and enumeration :** host and port discovery (Nmap), service and OS detection, service enumeration (SMB, SNMP, LDAP, HTTP).
- **Vulnerability analysis and exploitation :** CVE research (Exploit-DB, NVD), network and system exploitation with Metasploit, attacks on unpatched services.
- **Identity and web service attacks :** brute force, password spraying, SQL injection, XSS, IDOR, buffer overflow.
- **Network attacks :** denial-of-service attacks (DoS/DDoS), man-in-the-middle, ARP poisoning.
- **Post-exploitation :** privilege escalation, pivoting, persistence, log cleaning.
- **Detection and countermeasures :** honeypots, intrusion detection systems (IDS/IPS), event correlation.
- **Writing the intrusion report :** professional structure, executive summary, CVSS-scored findings, recommendations, and remediation plan.

BIBLIOGRAPHY

- Georgia Weidman - *Penetration Testing : A Hands-On Introduction to Hacking* - No Starch Press, 2014
- Kim Crawley - *The Pentester Blueprint* - Wiley, 2020

— Chris McNab - *Network Security Assessment* - O'Reilly, 3rd ed., 2016
— Dafydd Stuttard & Marcus Pinto - *The Web Application Hacker's Handbook* - Wiley, 2nd ed., 2011
— Jon Erickson - *Hacking : The Art of Exploitation* - No Starch Press, 2nd ed., 2008
— PTES - *Penetration Testing Execution Standard* : `http://www.pentest-standard.org`
— OWASP Testing Guide v4.2 : `https://owasp.org/www-project-web-security-tes`
— MITRE ATT&CK Framework : `https://attack.mitre.org`
— NIST SP 800-115 - *Technical Guide to Information Security Testing and Assessment* : `https://csrc.nist.gov/publications/detail/sp/800-115/final`
— OSSTMM v3 - ISECOM : `https://www.isecom.org/OSSTMM.3.pdf`
— ANSSI - Guides and recommendations : `https://www.ssi.gouv.fr/guide/`
— PortSwigger Web Security Academy : `https://portswigger.net/web-security`
— HackTheBox Academy : `https://academy.hackthebox.com`
— TryHackMe : `https://tryhackme.com`

REQUIREMENTS

— **SEC502 - Cybersecurity : Principles, Practices, and Threats :** CIA model, threat typology (malware, phishing, DoS), introduction to attacks and defenses.
— **SEC602 - Cryptography and Applications :** symmetric/asymmetric encryption, hash functions, PKI, TLS/SSL protocols — essential for understanding protocol vulnerabilities.
— **SEC701 - Cybersecurity : Secure Architecture and Infrastructure (parallel) :** networks, firewalls, DMZ, segmentation, security policies — deployment context for offensive techniques.
— **SYSRES 501 - Principles of Networks and IoT :** OSI model, TCP/IP protocols, IP addressing, routing, DNS, HTTP, SMTP — essential foundation for network scanning and exploitation.
— **SYSRES 502 - Operating Systems and Command Language :** Linux/Windows administration, process management, permissions, Bash scripting — proficiency with Kali Linux environment.
— **Expected cross-disciplinary skills :**

  — Linux terminal practice (shell, permissions, networking)
  — Scripting basics (Bash, Python)
  — Understanding of client-server architectures and web services
  — Ability to read technical documentation in English