OFFENSIVE CYBERSECURITY (EMaCS-03-05)				
DEGREE PROGRAM:	Master in Computer Science for the Human-Centric and Sustainable Industry			
SEMESTER: Third	**TYPE:** Basic	**CREDITS:** 5 ECTS	**WORKLOAD:** 125 hours	**MENTORING:** 0,5 hours/week
LANGUAGE: English				

OBJECTIVES	
General	Students learn the skills necessary to perform software penetration testing and report the results effectively for all stakeholders.
Specific	• Assess the effectiveness of security controls, reveals and utilise cybersecurity vulnerabilities, assessing their criticality if exploited by threat actors.

SUSTAINABILITY

The course makes a meaningful contribution to sustainability by instilling a strong awareness of Ethical and Legal Considerations within the domain of offensive cybersecurity. By emphasizing ethical hacking principles and considering the legal implications of penetration testing, the curriculum ensures that cybersecurity practices align with principles of responsibility and sustainability. This approach promotes the ethical treatment of information systems, fostering a sustainable cybersecurity mindset that considers the broader societal and environmental impact.

RESILIENCE AND HUMAN-CENTRIC DEVELOPMENT

In terms of resilience and human-centric development, the program equips students with essential skills in Identifying and Solving Cybersecurity-Related Issues. By fostering a problem-solving mindset, the curriculum enables students to contribute to the resilience of digital ecosystems. Moreover, the emphasis on Communication, Presentation, and Reporting to Relevant Stakeholders highlights the human-centric aspect, emphasizing the importance of effective communication in the realm of offensive cybersecurity. The course also encourages a Creative and Out-of-the-Box Thinking approach, promoting adaptability and innovation in addressing evolving cybersecurity challenges. Through ethical hacking principles and a focus on people and companies' protection, the curriculum ensures a resilient and human-centric development in offensive cybersecurity practices.

SUBJECT MATTER

- Penetration testing methods and processes.
- Ethical and legal considerations.
- Testing tools and techniques.
- Reporting.

COMPETENCES

C1. AQUIRING DATA, INFORMATION AND DIGITAL CONTENT
C5. PROGRAMMING
C7. PROTECTING PERSONAL DATA AND PRIVACY
C8. PROTECTING HEALTH AND WELL-BEING
C9. REFLECTING ON ETHICAL OUTCOMES
C10. EXPLORATORY AND CRITICAL THINKING
C11. PROBLEM FRAMING
C12. IDENTIFYING NEEDS AND TECHNOLOGICAL RESPONSES
C14. SOLVING TECHNICAL PROBLEMS
C18. COLLABORATING THROUGH DIGITAL TECHNOLOGIES

LEARNING OUTCOMES	
Knowledge	• Know about: ○ Ethical and legal considerations of penetration testing. ○ Cybersecurity attack procedures. ○ Operating systems security.

	○ Computer networks security. ○ Penetration testing procedures. ○ Penetration testing standards, methodologies, and frameworks. ○ Penetration testing tools. ○ Computer systems vulnerabilities. ○ Cybersecurity recommendations and best practices.
Skills	• Acquire the ability to: ○ Identify and exploit vulnerabilities. ○ Conduct ethical hacking. ○ Identify and solve cybersecurity-related issues. ○ Use penetration testing tools effectively. ○ Conduct technical analysis and reporting. ○ Decompose and analyse systems to identify weaknesses and ineffective controls.
Attitudes/values	• Be willing of the ethical hacking considering basic principles for protection of people and companies. • Develop and use a creatively thinking and outside the box. • Be aware of the need to communicate, present and report to relevant stakeholders.

TEACHING METHODS

Method	Class Workload	Individual Workload	Total
Theoretical Sessions	4	12	16
Laboratory Sessions	8	24	32
Assessment Report	4	69	73
Practical Examination	4	0	4
TOTAL	**20 hours**	**105 hours**	**125 hours**

EVALUATION

Evaluation Procedure	Percentage on the subject grade
Laboratory Assignments	20%
Assessment Report	60%
Written Examinations	20%
TOTAL	**100%**

PRECONDITIONS	
Basics of programming (Python), Linux operating system, Virtualization	
DEPARTMENT	School of ICT
LECTURERS	Jani Ekqvist
LITERATURE	To be defined later