






5.00 credits	30.0 h + 15.0 h	Q2
--------------	-----------------	----

Teacher(s)	Sadre Ramin ;
Language :	English > French-friendly
Place of the course	Louvain-la-Neuve
Main themes	<ul style="list-style-type: none"> • Forged E-Mail, Spam and Malwares, • Basics in cryptography, • Network and Application Vulnerabilities: IT spoofing, session hijacking, exploits, sniffing, • Firewalls, • Proxies, IDS, Hacking methods, • Secure communications, • Security at the User Level.
Learning outcomes	<p>At the end of this learning unit, the student is able to :</p> <p>Given the learning outcomes of the "Master in Computer Science and Engineering" program, this course contributes to the development, acquisition and evaluation of the following learning outcomes:</p> <ul style="list-style-type: none"> • INFO1.1-3 • INFO2.1-5 • INFO5.2, INFO4-5 • INFO6.1, INFO6.3, INFO6.4 <p>Given the learning outcomes of the "Master [120] in Computer Science" program, this course contributes to the development, acquisition and evaluation of the following learning outcomes:</p> ¹ <ul style="list-style-type: none"> • SINF1.M1 • SINF2.1-5 • SINF5.2, SINF4-5 • SINF6.1, SINF6.3, SINF6.4 <p>The course provides a broad view of computer system security that provides a general knowledge of the field for non - specialists and a base for future specialists.</p> <p>Students completing successfully this course will be able to</p> <ul style="list-style-type: none"> • defend the need for protection and security, and the role of ethical considerations in computer use, • identify security strengths and weaknesses in computer systems, • explain the problems addressed by digital forensics and outline the basic principles involved in its practice, • compare and contrast current methods for implementing security.
Evaluation methods	<p>Mode of evaluation for the June session:</p> <ul style="list-style-type: none"> • Exam (50% of the final mark) • Project activities in groups (35% of the final mark) • Individual project activity (15% of the final mark) <p>August session: The project activities (in groups and individual) cannot be done or redone for the August session and the student will keep the grades obtained for them in the June session with the weights for the final mark as indicated above. Not participating to the project activities at the dates indicated by the teacher will result in a zero mark for the respective part.</p> <p>The teacher may request a student to go through an additional oral exam as a complement of the exam and/or of the project activities, in cases including, but not limited to, technical issues, or suspicion of irregularities.</p>
Teaching methods	<ul style="list-style-type: none"> • Lectures • Scientific readings • Practical lab sessions • Project activities
Content	<p>The course provides an introduction to a wide range of security problems linked to computer networks and devices connected to such networks.</p> <p>We will see the major attack mechanisms (Denial of Service, cache poisoning, XSS, code injection, etc.), as well as defense mechanisms such as encryption, firewalls, and intrusion detection. The latter includes state of the</p>

	<p>art signature based detection and machine-learning based anomaly detection. In the exercises, you will learn to perform such attacks, how to identify them, and how to secure a system against them.</p> <p>Some topics addressed in previous years:</p> <ul style="list-style-type: none"> • Code injection (including SQL injection and XSS) • DDoS attacks and reflection • Network monitoring with netflow and protection with firewalls • Intrusion detection systems • Introduction to cryptography and how it is used to secure network communication and DNS
<p>Inline resources</p>	<p>Teams and/or Moodle</p>
<p>Other infos</p>	<p>You will need basic knowledge in network protocols, computer systems, and C programming, for example from the following courses:</p> <ul style="list-style-type: none"> • Networks: LINFO1341 or LELEC2920 • Computer systems and C: LINFO1252 or LINFO2241
<p>Faculty or entity in charge</p>	<p>INFO</p>

Programmes containing this learning unit (UE)				
Program title	Acronym	Credits	Prerequisite	Learning outcomes
Master [120] in Electrical Engineering	ELEC2M	5		
Master [120] in Computer Science and Engineering	INFO2M	5		
Master [120] in Computer Science	SINF2M	5		
Master [120] in Mathematical Engineering	MAP2M	5		
Master [120] in Data Science Engineering	DATE2M	5		
Master [120] in Data Science: Information Technology	DATI2M	5		