Ecole Supérieure d'Informatique et du Numérique COLLEGE OF ENGINEERING & ARCHITECTURE	**Syllabus**	**School:** ESIN **level**: ING4	**Year**: 2024-2025 **Semester**: S05

Course general information		
	Contact hours distribution	
Course number: **Course name**: Introduction to Cybersecurity **Coordinator: Anass Sebbar** **Credit hours**: 56 **Contact hours:** **Categorization of credits:** (math and basic science, engineering topic, and/or other).	**Course (C)**	02 h
	Tutorial (T)	00 h
	Laboratory (lab)	02 h
	IT-Tutorial	00 h
	Project	00 h
	Percentage in E-learning	00 %

		C	**T**	**Lab**
Instructors	**Name: Anass Sebbar** **E-mail Address: Anass.sebbar@uir.ac.ma** **Tel:** **Office**: B314 **Office hours:**	x	x	-
Required textbook	COMPUTER SECURITY PRINCIPLES AND PRACTICE Fourth Edition William Stallings, Lawrie Brown UNSW Canberra at the Australian Defence Force Academy			

Specific course information	
catalog description	The course provides an overview of cyber-security aspects confidentiality, integrity, availability and traceability in order to highlight cryptography, network security, software security and malware defenses. The course gives an understanding of each of these topics while discussing the main strengths and weaknesses of each technology. During the lab sessions, students will apply the class material to launch basic cyber-attacks and common defenses
Prerequisites	Routing and Switching
Type of course	required
Grading criteria	Continuous evaluation (30%) Labs(20%) Final exam(50%)____

Specific goals for the course			
Goals for the course	The course provides an overview cyber-security aspects confidentiality integrity availability and tracability in order to hilight cryptography, network security, software security and malware defenses. The course gives an understanding of each of these topics while discussing the main strengths and weaknesses of each technology. During the lab sessions, students will apply the class material to launch basic cyber attacks and common defenses		
Course Outcomes (CO)	**Course Learning outcomes:** students will be able to	**Student Outcomes**	**Assessment tools**
	CO 1 : Understand security information system		
	CO 2: Describe and analyze typical threats and outline techniques	SOi	CC/CF/HW/Lab
	CO 3: Use some cryptographic systems to protect information system		
	CO 4: Describe the popular network security mechanisms		

Course/student outcomes matrix

E= Emphasize (Strong), **R**= Reinforce (Intermediate), **I**= Introduce (Weak)

	SO1	SO2	SO3	SO4	SO5	SO6	SO7
CO1	R						
CO2		R		R			
CO3	R			E			
CO4		R		R	R		

Brief list of topics to be covered	
N°	**Content**
1	**Introduction To CyberSecurity** Computer Security Concepts Threats, Attacks, and Assets Security Functional Requirements Fundamental Security Design Principles Attack Surfaces and Attack Trees Computer Security Strategy
2	**Network Security**
3	**User Authentication** Digital User Authentication Principles Password-Based Authentication Token-Based Authentication Biometric Authentication Remote User Authentication

	Security Issues for User Authentication
4	**Types of Firewalls (staless, statful, application and next generation firewall)**
5	**Firewalls and packet filtering**
6	**Cryptographic Tools** Confidentiality with Symmetric & Asymmetric Encryption Message Authentication and Hash Functions Public-Key Encryption Digital Signatures and Key Management SSL/TLS protocol and CA management
	Labs
	Lab 01 : CIA network Analysis – wireshark – FTP, TELNET, SSH Lab 02 : Authentication cracking Unix passworg : Jhon the ripper Lab 03 : firewalling Iptables Lab 04 : NextGeneration firewall : fortinet VPN SITE to SITE Lab 05 : Crypto Symetric : Operatory mode ECB -CBC … Lab 06: Crypto Symetric 2 : shema fiestel and DES using python Lab 07: Crypto Asymetric and signature : GPG2 Lab 08: CA and TLS/SSL communication : Crypt and decrypt TLS/SSL communications

Classroom rules and Academic Ethics

- As a courtesy to both your professor and your fellow students, all cellular phones, electronic games, radios, CD players, or other devices that generate sound must be turned off during class.
- Please avoid any disruptive behaviors such as: coming late to class, leaving early, intoxication, inconsiderate behavior (e.g., sleeping, reading for pleasure, working on outside assignments, excessive talking, eating/drinking.) A warning may be given for the first offense; repeated violators will be penalized and may face expulsion from the class and/or other disciplinary proceedings. Please be considerate of your fellow classmates and your professor.
- The institution is committed to a policy of honesty in academics. Conduct compromising this policy may result in academic and/or disciplinary action. Cheating is a violation of student academic behavior standards. The honor Code is found on the student guide and applies to all activities and assignments in this course. Students must refrain from cheating, lying, plagiarizing, and stealing. This includes completing your own original work and giving credit to any other person whose ideas and printed materials (including those on the Internet) are paraphrased or directly quoted. Any student who violates, or helps another student violate academic behavior standards will be penalized according to the student guide rules.