UNIVERSITÀ DEGLI STUDI DI PALERMO

DEPARTMENT	Ingegneria
ACADEMIC YEAR	2022/2023
MASTER'S DEGREE (MSC)	COMPUTER ENGINEERING
SUBJECT	CYBERSECURITY
TYPE OF EDUCATIONAL ACTIVITY	B
AMBIT	50369-Ingegneria informatica
CODE	22213
SCIENTIFIC SECTOR(S)	ING-INF/05
HEAD PROFESSOR(S)	LO RE GIUSEPPE Professore Ordinario Univ. di PALERMO
OTHER PROFESSOR(S)	
CREDITS	12
INDIVIDUAL STUDY (Hrs)	192
COURSE ACTIVITY (Hrs)	108
PROPAEDEUTICAL SUBJECTS	
MUTUALIZATION	
YEAR	2
TERM (SEMESTER)	1° semester
ATTENDANCE	Not mandatory
EVALUATION	Out of 30
TEACHER OFFICE HOURS	**LO RE GIUSEPPE** Tuesday 15:00 17:00

DOCENTE: Prof. GIUSEPPE LO RE

PREREQUISITES	Computer Networks , Operating Systems
LEARNING OUTCOMES	Conoscenza e capacita' di comprensione (knowledge and understanding): Lo studente, al termine del corso, avra' acquisito conoscenze e metodologie per affrontare problematiche legate alla sicurezza dei sistemi di elaborazione delle informazioni. Lo studente sara' in grado di analizzare protocolli ed applicazioni di autenticazione, sicurezza della posta elettronica e del Web, e tutti gli aspetti legati alla sicurezza dei sistemi informatici. Conoscenza e capacita' di comprensione applicate (applying knowledge and understanding): Lo studente avra' acquisito conoscenze e metodologie per collaudare, progettare e realizzare sistemi informatici sicuri che facciano uso delle tecniche e degli strumenti analizzati durante il corso. Autonomia di giudizio (making judgements): Lo studente avra' acquisito una metodologia di analisi dei meccanismi che garantiscono la sicurezza di un sistema informatico e sara' in grado di giudicare la validita' di progetti di sistemi sicuri per l'elaborazione delle informazioni. Abilita' comunicative (communication skills): Lo studente sara' in grado di discutere con competenza e proprieta' di linguaggio problematiche complesse legate alla sicurezza dei sistemi informatici di elaborazione delle informazioni e delle reti. Capacita' di apprendere (learning skills): Lo studente sara' in grado di affrontare con autonomia qualsiasi problematica relativa alla sicurezza dei sistemi informatici e di networking. Sara' in grado di indagare sulle tecniche di crittografia dei dati, di firma digitale, di autenticazione, di integrita' e di non ripudiabilita.
ASSESSMENT METHODS	Written (and oral examination. Assessment procedure for the Written Exam During the course, according to the course timetable, students can do a mid-term test. Such exam has to be completed with the final test that will take place at the end of the course and before the regular exams. The written examination (mid-term + final, or unique written examination) will seek to determine the possession of skills, abilities and skills required. It includes at least three questions that aim to verify knowledge and understanding in the topics of the course, and the ability to apply knowledge and understanding to new problems. In the written exam the theoretical comments of the numerical findings are appreciated. The assessment is expressed in thirtieth and admission to oral test is determined by a minimum score (15), in case of lower score the exam fails. Evaluation criteria for the oral examination The oral test consists of an interview aimed to check that you have the skills and knowledge disciplinary provided by the course; the evaluation is expressed in thirtieths. The solutions proposed in the written examination will be discussed during the oral exam. Here, some questions will be asked to the students in order to test their achievement of educational goals and their communication skills. Moreover, in order to evaluate the ability to make independent judgements, the students will be asked to propose suitable solutions for a specific application scenario. The final evaluation will take into account both the score of the written exam (50%) and that of the oral exam. Excellent 30-30 and praise, outstanding knowledge of the topics, excellent properties of language, good analytical ability, the student is able to apply knowledge to solve complex problems. He should solve complex problems that require a deep understanding of all the topics of the course and the ability to jointly use them. He should also be able to know how to find the information needed to solve the problem. Very Good 27-29, Good command of the main topics, full of language, the student is able to apply knowledge to solve problems proposed. Good 24-26 good understanding of the main topics, discrete properties of language, with some abilities to independently solve the proposed problems. Satisfactory 21-23, the student has sufficiently mastered the main teaching subjects but he/she has the knowledge, satisfactory property language, limited ability to independently apply the knowledge acquired. Sufficient 18-20, Minimum basic understanding of the major teaching and technical language issues, very little or no ability to independently apply the knowledge acquired. Insufficient, it does not have an acceptable knowledge of the contents of the topics covered in the teaching.
EDUCATIONAL OBJECTIVES	

	The course aims to provide the students with a basic knowledge of computer and network security. The course analyses the security problems in the context of operating systems, DB and software applications. Furthermore the course deals with secure communication protocols, and focuses on the best practices for designing secure distributed systems.
TEACHING METHODS	Lectures and computer laboratories
SUGGESTED BIBLIOGRAPHY	William Stallings – Crittografia Pearson ISBN 978-8891924841 William Stallings - Sicurezza dei Computer e delle Reti, Pearson ISBN 978-8891915290

SYLLABUS

Hrs	Frontal teaching
6	Network Security
4	Computer Systems Security
4	Message authentication and SHA-1
4	Message Authentication Code
4	Digital Signatures
6	User authentication: Kerberos
4	Electronic mail security
4	IP security
4	Transport-level security
4	Firewall
4	Wireless network security
3	User Authentication
3	Access Control
3	Database and Data Center Security
3	Malicious Software
3	Intrusion Detection
3	Software Security
3	Operating System Security
2	Ligthweigth Cryptography
2	Post-Quantum Cryptografy
2	Buffer Overflow
3	Cryptographic Key Management and Distribution
2	Denial-of-Service Attacks

Hrs	Practice
5	Secure protocols
7	Computer laboratories
3	Digital Signatures
3	Message Authentication Code
3	Cryptographic hash functions
2	Buffer Overflow
3	user autentication
2	Malaware