UNIVERSITÀ DEGLI STUDI LINK

BACHELOR'S DEGREE

A.Y. 2023/2024

Teaching	Programming (Elective from Security in Computer Service)
CFU	6
Course year	
Semester	first
Lecturer(s)	Prof. Marco Angelini
email	m.angelini@unilink.it
reception	at the end of the lessons or by appointment to be arranged by e-mail.

LEARNING OUTCOMES

The course aims to achieve the following learning outcomes:

1. **KNOWLEDGE AND UNDERSTANDING**: the student must be able to learn and recognize the fundamental principles of computer security, the quantities that characterize it, the main characteristics of cyber attackers, attacks, computer vulnerabilities, malware. They will have to further learn the principles of a correct cyber defense and the main techniques and actors necessary to implement an adequate cybersecurity posture.
2. **APPLIED KNOWLEDGE AND UNDERSTANDING**: at the end of the course, the student must be able to assess the danger of a cyber threat, extract information from public vulnerability databases and be able to interpret, recognize and reason about actions to reduce the surface of exposure to threats in order to implement a correct cyber posture.
3. **MAKING JUDGEMENTS**: the student will have to acquire a critical and analytical vision on the fundamental aspects and principles of computer security and be able to correctly assess the threat surface and its exposure, identifying high-level corrective actions necessary to inform technical implementations.
4. **COMMUNICATION SKILLS**: the student will also have to acquire the mastery of the specialized language of the subject and develop the ability to argue both with technical staff and with personnel assigned to decision-making choices in the field of cyber posture.
5. **LEARNING SKILLS**: the student will have to demonstrate a correct assessment of the threat surface and its exposure, identifying high-level corrective actions necessary to inform technical implementations.

DETAILED PROGRAM

The course deals in detail with the following topics:

1. Introduction to Cybersecurity
2. Cybersecurity Fundamentals
3. The CIA Triad
4. The CIA Triad: Advanced Aspects
5. Authentication
6. Multi-Factor Authentication
7. Cyber vulnerabilities
8. Public vulnerability repositories and scoring systems
9. Examples of cyberattacks
10. Actors and attackers involved in cyberattacks
11. Malware
12. Advanced Malware and APTs

13. Authorization and access control
14. Hardening: Fundamentals
15. Hardening: Measures
16. Types of cyberattacks
17. Cyberattack modeling
18. Response to cyberattacks, SOCs and CERTs

RECOMMENDED PREREQUISITES

none

HOW TO CONDUCT THE EXAM

The final exam consists of the production of a written paper on a topic chosen from the topics of the course and an oral interview that presents the same and allows you to answer a series of questions on the paper and the topics of the course.

ASSESSMENT CRITERIA

In the oral exam, the student must demonstrate:

1. **KNOWLEDGE AND UNDERSTANDING**: to have acquired the fundamental notions of IT security on all the topics covered in the course.
2. **APPLIED KNOWLEDGE AND UNDERSTANDING**: one's ability to apply the fundamental notions of IT security on all the topics covered in the course.
3. **MAKING JUDGEMENTS**: to have developed an ability to evaluate and apply the fundamental notions of IT security on all the topics covered in the course.
4. **COMMUNICATION SKILLS**: to have mastery in communicating the aspects of computer security covered in the course and their technical jargon.
5. **LEARNING SKILLS**: their ability to use the conceptual and methodological tools acquired concerning the fundamental notions of IT security on all the topics covered in the course.

CRITERIA FOR AWARDING THE FINAL GRADE

The grade is awarded in thirtieths. The final grade will be taken into account:

1. for 50% of the written paper produced for the exam
2. for 25%, in the presentation of the written paper and the ability to answer questions.
3. for 25%, in the ability to answer oral questions related to the topics of the course.

TEACHING MATERIALS

For the preparation of the exam, it is essential to integrate the contents provided during the lessons with the following **mandatory texts**:

There are no mandatory texts. The following text is recommended:
Security in Computing, 6th Edition
by Charles Pfleeger, Shari Lawrence Pfleeger, Lizzie Coles-Kemp Released August 2023
Publisher(s): Addison-Wesley Professional

ISBN: 9780137891375

Non-attending students **will** also have to study the following compulsory textbook: ...

TEACHER'S ADVICE

Follow the lessons, study the teaching material provided and integrate with external sources or the recommended book.