University of Nicosia, Cyprus

Course Code	**Course Title**	**ECTS Credits**
COMP-432	Network Security	6
Department	**Semester**	**Prerequisites**
Computer Science	Fall/Spring	COMP-358
Type of Course	**Field**	**Language of Instruction**
Elective	Computer Science	English
Level of Course	**Year of Study**	**Lecturer(s)**
1st Cycle	4th	Dr Ioanna Dionysiou
Mode of Delivery	**Work Placement**	**Co-requisites**
Face-to-face	N/A	None

Objectives of the Course:

The main objectives of the course are to:

- appreciate the need for network security practices in organizational units
- provide students with deep knowledge on various concepts of classical computer and network security paradigms
- build foundations to assess contemporary security policies and security mechanisms within organizations and illustrate the balance of the managerial and technical aspects of network security
- examine and report current security practices that are deployed in Cypriot/International organizations

Learning Outcomes:

After completion of the course students are expected to be able to:

1. explain and use the fundamentals of cryptography such as symmetric/asymmetric encryption, digital signatures, and hash functions.
2. discuss and explain current network authentication applications, PKI, Web security and their vulnerabilities that are exploited by intentional and unintentional attacks
3. identify network attacks (denial of service, flooding, sniffing and traffic redirection, inside attacks, etc.) and basic network defense tools
4. differentiate between organizational security policies and security mechanisms
5. analyze the security needs of a small enterprise, design a strategic plan to address those security requirements, and select the appropriate tools to implement the organizational policies
6. appreciate the importance of ethics as a network security practitioner
7. use automated tools to generate and manage keys as well as be able to use cryptographic libraries to perform security operations such as key generation, encryption, decryption, etc.

Course Contents:

1. Motivation of network security
2. Overview of the discipline of cryptography - algorithms and protocols

underlying network security applications, encryption, hash functions, digital signatures, and key exchange
3. Authentication protocols, including Kerberos and PKI
4. Presentation of network security applications such as IP Security and Web Security
5. Overview of computer and network threats and attacks, including denial of service, flooding, sniffing and traffic redirection, exploit attacks, infrastructure attacks (DNS hijacking, route blackholing, etc.)
6. Contemporary network defense countermeasures such as intrusion detection tools and firewalls
7. Planning and implementing security policies for an organization with real-world case studies
8. Legal, ethical, and professional aspects of network security practices

Learning Activities and Teaching Methods:

Lectures, case studies, hands-on experience with tools, on-site visits to IT departments of Cypriot enterprises, guest lectures by Cypriot IT specialists

Assessment Methods:

Written and programming assignments, team project, midterm exam, final exam

Required Textbooks/Reading:

Authors	Title	Publisher	Year	ISBN
W. Stallings	*Network Security Essentials: Applications and Standards, Third edition*	Prentice Hall	2007	0132380331

Recommended Textbooks/Reading:

Authors	Title	Publisher	Year	ISBN
R. Anderson	*Security Engineering: A Guide to Building Dependable Distributed Systems, Second Edition*	John Willey and Sons	2008	0470068523
M. Merkow, J. Breithaupt	*Information Security: Principles and Practices*	Prentice Hall	2006	0131547291
C. Pfleeger, S.L. Pfleeger	*Security in Computing, fourth edition*	Prentice Hall	2006	0132390779