UNIVERSITY of NICOSIA

Course Syllabus

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

Course Objectives:

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 Content:

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, Practical Exercises, Project, and Assignments

Assessment Methods:

Final Exam, Midterm Exam, Assignments, and Team Project

Required Textbooks / Readings:

Title	Author(s)	Publisher	Year	ISBN
Network Security Essentials: Applications and Standards (6th Edition)	W. Stallings	Pearson	2016	978-0134527338

Recommended Textbooks / Readings:

Title	Author(s)	Publisher	Year	ISBN
Security Engineering: A Guide to Building Dependable Distributed Systems (2nd Edition)	R. J. Anderson	John Wiley & Sons	2008	978-0470068526
Information Security: Principles and Practices (2nd Edition)	M. Merkow and J. Breithaupt	Pearson IT Certification	2014	978-0789753250
Security in Computing (5th Edition)	C. Pfleeger, S.L. Pfleeger, and J. Margulies	Prentice Hall	2015	978-0134085043