UNIVERSITY of NICOSIA

Course Syllabus

Course Code	Course Title	ECTS Credits
COMP-432	Ethical Hacking	6
Prerequisites	**Department**	**Semester**
COMP-358	Computer Science	Spring
Type of Course	**Field**	**Language of Instruction**
Elective	Computer Science	English
Level of Course	**Lecturer(s)**	**Year of Study**
1st Cycle	Kyriakos Costa, MSc	3rd or 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 of 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 deployed in Cypriot/International organizations.

Learning Outcomes:

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

- explain and use the fundamentals of cryptography such as symmetric/asymmetric encryption, digital signatures, and hash functions
- discuss and explain current network authentication applications, PKI, Web security and their vulnerabilities that are exploited by intentional and unintentional attacks
- identify network attacks (denial of service, flooding, sniffing and traffic redirection, inside attacks, etc.) and basic network defense tools
- differentiate between organizational security policies and security mechanisms

- 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
- appreciate the importance of ethics as a network security practitioner
- 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. Introduction to Network Security
    a. CIA Triad
    b. Threat Landscape
    c. Basic Concepts and Terminologies
    d. Network Security Appliances
    e. Core Systems
    f. Traditional vs Modern Architectures
2. Cryptography Fundamentals
    a. Symmetric / Asymmetric Encryption
    b. X.509
    c. Digital Signatures
    d. Secure Storage, Distribution, and Use of Keys
3. Network Protocols and Security
    a. DNS Spoofing
    b. ARP Poisoning
    c. Packer Sniffing
    d. Golden Ticket Attack
    e. Denial of Service
4. Secure Network Designs and Architecture
    a. Securing Local Infrastructures
    b. Securing Cloud Environments
    c. Architecture Challenges
5. Wireless Network Security
    a. Wifi Vulnerabilities
    b. Authentication and Encryption mechanisms
    c. WiFi Modern Protections
6. Secure Emails and Messaging
    a. Domain Protections
    b. Email Gateways
    c. Modern Message Exchange
7. Virtualization and Cloud Security
    a. Managing Hypervisors
    b. Identity Service Providers
    c. Managed Services
8. Emerging Trends in Network Security

a. Internet of Things
b. Blockchain Security
c. Artificial Intelligence

Learning Activities and Teaching Methods:

Lectures, Practical Exercises, and Assignments.

Assessment Methods:

Final Exam, Midterm Exam, Assignments, and Projects

Required Textbooks / Readings:

Title	Author(s)	Publisher	Year	ISBN
Gray Hat Hacking The Ethical Hackers Handbook, 6th Edition	Allen Harper, Ryan Linn, Stephen Sims, Michael Baucom, Daniel Fernandez, Huascar Tejeda, Moses Frost	McGraw-Hill Osborne	2022	978-1264268948

Recommended Textbooks / Readings:

Title	Author(s)	Publisher	Year	ISBN
Network Security Assessment – Know Your Network (3rd Edition)	Chris McNab	O'Reily	2017	978-1491910955
The Hacker Playbook 3: Practical Guide to Penetration Testing	Peter Kim	Independentl y Published	2018	978-1980901754