



# UNIVERSITY OF NICOSIA

## ΠΑΝΕΠΙΣΤΗΜΙΟ ΛΕΥΚΩΣΙΑΣ

University of Nicosia, Cyprus

<b>Course Code</b>	<b>Course Title</b>	<b>ECTS Credits</b>
COMP-529	Network Defense and Countermeasures	10
<b>Department</b>	<b>Semester</b>	<b>Prerequisites</b>
Computer Science	Fall/Spring	COMP-514 Cryptography and Network Security
<b>Type of Course</b>	<b>Field</b>	<b>Language of Instruction</b>
Required for <i>CyberSecurity</i> concentration	Computer Science	English
<b>Level of Course</b>	<b>Year of Study</b>	<b>Lecturer(s)</b>
2nd Cycle	1st	Dr Ioanna Dionysiou
<b>Mode of Delivery</b>	<b>Work Placement</b>	<b>Co-requisites</b>
face-to-face	N/A	None

### Objectives of the Course:

The main objectives of the course are to:

- present the layered defense approach to securing systems.
- present risk assessment as a technique to protect assets and information.
- expose students to security policy design and implementation.
- expose students to practical techniques that aim in defending computer networks from network attacks and malicious software.
- provide a comprehensive view of contemporary network defending technologies.
- motivate the need to integrate security in the system development lifecycle to better protect the system.

## Learning Outcomes:

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

1. discuss a wide range of network attacks.
2. apply risk assessment techniques related to security threats.
3. identify network attacks (denial of service, flooding, sniffing and traffic redirection, inside attacks, etc.) and basic network defense tools.
4. identify various types of malicious software and use countermeasure defense/detection tools.
5. apply practical ways to harden Web and Internet Resources, as well as Operating Systems.
6. create a solid enterprise-wide information security infrastructure, including analyzing the security needs of the enterprise, designing a strategic plan to address the security requirements, selecting the appropriate tools to implement the security organizational policies, and establishing recovery techniques from disruptive and destructive information security events.

## Course Contents:

1. Network Security Threats, Attacks, and Vulnerabilities.
2. Using Layered Defense Strategy: defense in depth.
3. Attack Classification and Examples of Attacks.
4. Risk Analysis: threat and risk assessment, economic impacts, techniques for minimizing risk.
5. Security Policy Creation: security policy lifecycle, security policy development and best practices, handling security incidents (response team, responding procedures, etc.), business continuity.
6. Network Attacks Landscape: network reconnaissance, attack techniques, malicious code, countermeasures.
7. Analysis of Network Traffic: CVE identifiers, signature and traffic analysis, identification of suspicious events.
8. Web and Internet Resources: hardening DNS servers, Web Servers, Routers
9. Hardening Operating Systems: configuring properly Windows, Unix, Android, patching.
10. Network Defending Technology: Intrusion Detection and Prevention Systems, Firewalls, VPN, Proxy Servers, Honeypots, Antivirus, etc.
11. Security Management and Standards.
12. Security in the System Development Lifecycle: Initiation Phase (security categorization), Development and Acquisition Phase (risk assessment, security functional requirements analysis, security plan), Implementation Phase (technology best practices, security control testing plan), Maintenance Phase (continuous monitoring plan).

**Learning Activities and Teaching Methods:**

Lectures, case studies, lab activities, guest lectures

**Assessment Methods:**

Written and programming assignments, lab exercises, project, midterm exam, final exam

**Required Textbooks/Reading:**

<b>Authors</b>	<b>Title</b>	<b>Publisher</b>	<b>Year</b>	<b>ISBN</b>
Randy Weaver, Dawn Weaver, Dean Farwood	Guide to Network Defense and Countermeasures, Third edition	Cengage Learning	2013	1133727948
William (Chuck) Easttom, II	Network Defense and Countermeasures: Principles and Practices, Second Edition	Pearson IT Certification	2014	0789750945

**Recommended Textbooks/Reading:**

<b>Authors</b>	<b>Title</b>	<b>Publisher</b>	<b>Year</b>	<b>ISBN</b>
Charles P. Pfleeger and Shari Lawrence Pfleeger	Analyzing Computer Security: A Threat / Vulnerability / Countermeasure Approach	Prentice Hall	2012	0132789469