Detailed Course Description - Course Plan Development and Updating Procedures/ Computer Science/Computer Network Department	QFXX/0408-3.0E

Faculty	Faculty of Science and IT	Department	Computer Science/Computer Network
Course number	0122447	Course title	Network Security
Number of credit hours	3	Pre-requisite/co-requisite	Information Security

Brief course description

In this course, student will learn the fundamental principle of network and mobile security by studying attacks on mobile, network, and web site. Students will learn how those attacks work and how to prevent and detect them. This course will cover the design and analyze secure networked systems, develop secure programs with basic cryptography, perform vulnerability scanning, and secure networked systems with Firewall and IDS. The course emphasizes "learning by doing", and requires students to conduct a series of lab exercises. Through these labs, students can enhance their understanding of the principles, and be able to apply those principles to solve real problems.

	Course goals and learning outcomes
Goal 1	An ability to understand and explain network security and its attacks
Learning outcomes	1.1 Define network security and its related terminologies. 1.2 Understand of passive and active network attacks. 1.3 Describe and explain the basic principles of defenses to counter attacks. 1.4 Understand and discuss different types of networking-based attacks.
Goal 2	An ability to explain the most important concepts for securing both hardware and software, and understanding wireless & mobile security and their countermeasures
Learning outcomes	2.1 List and understand the steps for securing a host computer. 2.2 Understand and configure Firewall to secure host computer and network. 2.3 Describe and discuss the different types of wireless network attacks, and explain how to secure it. 2.4 List and explain the risks associated with mobile devices.
Goal 3	An ability to describe, detect and assess various security vulnerabilities in network and its countermeasures
Learning outcomes	3.1 Define vulnerability assessment and explain why it is important. 3.2 Explain the differences between vulnerability scanning and penetration testing. 3.3 Perform vulnerability scanning by using Kali Linux tools. 3.4 Understand IP security and cryptographic transport protocols, and explain how to implement them in order to secure network.
Goal 4	An ability to secure an enterprise computer network
Learning outcomes	4.1 Explain how network technologies can enhance security 4.2 Describe secure network design elements 4.3 Explain how network administration principles can be applied 4.4 Understand and implement access management in order to limit unauthorized users to access network resources.
Textbook	1.- Mark Ciampa, Security+ Guide to Network Security Fundamentals. Course Technology Incorporated, sixth edition, 2018, Cengage learning.

	2- William Stallings, Network Security Essentials: Applications and Standards, sixth edition, 2016, Pearson.
Supplementary references	1.- William Stalling, Cryptography and Network Security, 7th Ed., Pearson Education, 2017 2-Mark Rhodes-Ousley, The Complete Reference™ Information Security, Second Edition, 2013 3- Georgia Weidman, Penetration Testing: A Hands-On Introduction to Hacking, 2014 4- Daniel W. Dieterle, Basic Security Testing with Kali Linux 2, 2016 5- Gordon Fyodor Lyon, Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning, 2009

Course timeline				
Week	**Number of hours**	**Course topics**	**Pages (textbook)**	**Notes**
01	**1** **1** **1**	Introduction to network security Passive and active network attacks Defenses Against Attacks	**27-33, Supplementary ref(1)** **32-35, textbook(1)**	
02	**1** **1** **1**	Network based attacks: (Denial of Service (DoS), Interception, Poisoning) Securing the Host	**191-200, 375-378, textbook(1)**	
03	**1** **1** **1**	Securing the Operating System Software Firewalls	**379-387, textbook (1)** **410-427, textbook(2)**	
04	**1** **1** **1**	Windows firewall configuration Securing with Antimalware	**Internet resources**	
05	**1** **1** **1**	Network security devices, Design, and technology: Security Through Network Devices: Standard Network Devices Network Security Hardware	**235-259, textbook(1)**	
06	**1** **1** **1**	Security Through Network Technologies: Network Access Control (NAC)	**260-264, textbook(1)**	
07	**1**	Security Through Network Architecture:	**265-268,**	

	1 1	Security Zones **First exam**	**textbook(1)**	
08	1 1 1	Administering a secure network Secure Network Protocols: SNMP, DNS, FTP secure Email Protocols Using Secure Network Protocols	**281-291, textbook(1)**	
09	1 1 1	Monitoring and Analyzing Logs Port security Port Scanning tools	**Supplementary ref(3,4,5)**	
10	1 1 1	Wireless Attacks: (Bluetooth Attacks, NFC, WLAN)	**321-340, textbook(1)**	
11	1 1 1	Vulnerabilities of IEEE Wireless Security: (WEP, WPS, MAC Address Filtering, Disabling SSID Broadcasts) Wireless Security Solutions: (WPA, WPA2)	**341-351, textbook(1)**	
12	1 1 1	Type of mobile device Mobile Device Risks **Second exam**	**423-438, textbook(1)**	
13	1 1 1	IP security Cryptographic transport protocols	**174-178, textbook(1)** **302-334, textbook(2)**	
14	1 1 1	Assessing Vulnerabilities: What Is Vulnerability Assessment? Assessment Techniques Assessment Tools	**565-583, Textbook(1)**	
15	1 1 1	Vulnerability Scanning vs. Penetration Testing: Vulnerability Scanning Access management: Implementing access control	**584-587, 542-543, Textbook(1)**	
16	1 1 1	Access management: Identity and access services **Final exam**	**544-551, Textbook(1)**	

Theoretical course evaluation methods and weight	Participation = 10% First exam 20% Second exam 20% Final exam 50%	**Practical (clinical) course evaluation methods**	Semester students' work = 50% (Reports, research, quizzes, etc.) Final exam = 50%

Approved by head of		**Date of approval**	

department			

Extra information (to be updated every semester by corresponding faculty member)

Name of teacher	Dr. Zeyad Mohammad	Office Number	**314**
Phone number (extension)		Email	Z.Dosooq@zuj.edu.jo
Office hours			