Course Specification

(Bachelor)

Course Title:	Network Security
Course Code:	IT 461
Program:	Information Technology
Department:	Information Technology
College:	Computer and Information Sciences
Institution:	Majmaah University
Version:	2
Last Revision Date:	12 September 2023

Table of Contents

A. General information about the course:

1. Course Identification

1. Credit hours: 3(3,0,1)					
2. Course type					
A.	☐University	☒ College	☐Department	☐Track	☐Others
B.	☐Required		☒ Elective		
3. Level/year at which this course is offered: (Level 9)					
4. Course general Description:					
This course aims to introduce secure networking, security attacks, network security practice, email security, IP security, web security, intrusion detection and prevention systems. In this course students will also learn advanced concepts in network security and their implementation in network and how to analyze and assess security of network installations in different setups. Hand on experiments include the execution of attacks, the setup of intrusion detection and prevention, securing computers and wired and wireless networks.					
5. Pre-requirements for this course (if any)**:**					
70 Credits					
6. Co-requisites for this course (if any)**:**					
7. Course Main Objective(s):					
Aim of the course is to understand and Identify computer and network security threats, classify the threats and develop a security model to prevent, detect and recover from the attacks.					

2. Teaching mode (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	Traditional classroom	60	100
2	E-learning		
3	Hybrid • Traditional classroom • E-learning		

No	Mode of Instruction	Contact Hours	Percentage
4	Distance learning		

3. Contact Hours (based on the academic semester)

No	Activity	Contact Hours
1.	**Lectures**	45
2.	**Laboratory/Studio**	
3.	**Field**	
4.	**Tutorial**	15
5.	**Others (specify)**	
Total		60

B. Course Learning Outcomes (CLOs), Teaching Strategies and Assessment Methods

Code	Course Learning Outcomes	Code of CLOs aligned with program	Teaching Strategies	Assessment Methods
1.0	**Knowledge and understanding**			
1.1				
1.2				
...				
2.0	**Skills**			
2.1	Design secure network architectures by using the basic concepts of secure communication.	**S4**		
2.2	Understand the security issues involved with different Network.	**S4**		
...	Understanding the Wireless Security Architectures	**S4**		

Code	Course Learning Outcomes	Code of CLOs aligned with program	Teaching Strategies	Assessment Methods
3.0	**Values, autonomy, and responsibility**			
3.1	Evaluate and recognize a problem as being a possible network security threat.	**V1**		
3.2	Describe security assessment of networks and identify some of the factors driving the need for network security	**V2**		
...				

C. Course Content

No	List of Topics	Contact Hours
1.	**Introduction to Network Security**: The OSI Security Architecture, Security Attacks, Security Services, Security Mechanisms, Model for Network Security and Standards	**6**
2.	**Network Access Control**: Network Access Control overview, Authentication protocol, IEEE 802. IX Port Based Network Access Control	**7**
3.	**Network Security Threat Model:** Types of threats, Threats against the application (Cross-site scripting, Session hijacking, Information Disclosure), Threat modeling	**8**
4.	**Wireless Network Security:** Wireless & Mobile Device Security, IEEE 802.11 Wireless LAN,	**8**

	IEEE 802.11i Wireless LAN Security	
5.	**Transport-Level Security:** Secure Socket Layer, Transport Layer Security, HTTPS, Secure Shell (SSH)	**8**
6.	**Electronic Mail Security:** Internet mail Architecture, E-mail formats, E-mail threats and security, Pretty Good Privacy, S/MIME, Domain Keys Identified Mail, Domain-based message authentication	**7**
7.	**IP Security:** IP Security Policy Encapsulating security payload Internet Key Exchange Cryptographic Suites	**8**
8.	**Intrusion detection & Firewall:** Intrusion Detection Password Management Firewall Characteristics Types of Firewalls Firewall Basing Firewall Location and Configurations	**8**
Total		**60**

D. Students Assessment Activities

No	Assessment Activities *	Assessment timing (in week no)	Percentage of Total Assessment Score
1.	Quiz	Every 2 Weeks	20%
2.	Mid Term Exam	Week 8	20%
3.	Assignment	Every 2 Weeks	20%
4.	Final Exam	Week 16	40%

*Assessment Activities (i.e., Written test, oral test, oral presentation, group project, essay, etc.).

E. Learning Resources and Facilities

1. References and Learning Resources

Essential References	Network Security Essentials: Applications and Standards (6th Edition) by William Stallings ISBN-13: 978-0134527338 Pearson (Aug 7, 2016)
Supportive References	1. Introduction to Network Security by Douglas Jacobson Chapman & Hall/CRC Computer and Information Science Series, ISBN-13: 978-1584885436 2. Introduction to Network Security: Theory and Practice 2nd Edition, by JieWang , Zachary A. Kissel, Publisher: Wiley; 2 edition (October 5, 2015), ISBN-13: 978-1118939482
Electronic Materials	
Other Learning Materials	

2. Required Facilities and equipment

Items	Resources
facilities (Classrooms, laboratories, exhibition rooms, simulation rooms, etc.)	Classroom
Technology equipment (projector, smart board, software)	PC or Laptop with Windows/Linux, Smart Board, Projector
Other equipment (depending on the nature of the specialty)	Internet Connection

F. Assessment of Course Quality

Assessment Areas/Issues	Assessor	Assessment Methods
Effectiveness of teaching	Students	Indirect
Effectiveness of Students assessment	Instructor	Direct
Quality of learning resources	Instructor	Direct
The extent to which CLOs have been achieved		
Other		

Assessors (Students, Faculty, Program Leaders, Peer Reviewer, Others (specify)

Assessment Methods (Direct, Indirect)

G. Specification Approval

COUNCIL /COMMITTEE	Information Technology Dep.
REFERENCE NO.	
DATE	