



Course Specification

— (Bachelor)

Course Title: **Network Security**

Course Code: **APIS3215**

Program: **Diploma in Information Security**

Department: **Diplomas**

College: **Applied College**

Institution: **Umm Al Qura University**

Version: **1**

Last Revision Date: **14/12/2024**

Table of Contents

A. General information about the course:	3
B. Course Learning Outcomes (CLOs), Teaching Strategies and Assessment Methods	4
C. Course Content.....	5
D. Students Assessment Activities	6
E. Learning Resources and Facilities.....	6
F. Assessment of Course Quality	7
G. Specification Approval	8





A. General information about the course:

1. Course Identification

1. Credit hours: (3)

2. Course type

A. ☐ University ☐ College ☒ Department ☐ Track ☐ Others
B. ☒ Required ☐ Elective

3. Level/year at which this course is offered: (level 3, 2nd year)

4. Course general Description:

This course explores fundamental concepts of computer network security. Topics include security threats, vulnerabilities, and countermeasures such as firewalls, intrusion detection systems, cryptography, and authentication protocols. Students will gain knowledge of network security architectures, best practices, and the legal and ethical implications of cybersecurity.

5. Pre-requirements for this course (if any):

Computer Networks (APIS2208), Database Concepts (APIS2210)

6. Pre-requirements for this course (if any):

7. Course Main Objective(s):

To provide students with a comprehensive understanding of fundamental computer network security principles and practices, enabling them to identify, analyze, and mitigate security risks in network environments.

2. Teaching mode (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	Traditional classroom	60	100%
2	E-learning		
3	Hybrid <ul style="list-style-type: none"> Traditional classroom E-learning 		
4	Distance learning		



3. Contact Hours (based on the academic semester)

No	Activity	Contact Hours
1.	Lectures	30
2.	Laboratory/Studio	30
3.	Field	
4.	Tutorial	
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	Understand fundamental security principles, cryptographic techniques, and strategies for securing network infrastructures.	K1	Course lectures, HomeWorks, project	Quiz, Exam
2.0	Skills			
2.1	Configure secure network infrastructure by implementing appropriate network protocols, services, firewall rules, and access control lists to monitor and restrict unauthorized network access.	S4	Lab coursework Lab Project	Labs and Project
2.2	Apply cryptographic protocols such as VPNs	S4		

Code	Course Learning Outcomes	Code of CLOs aligned with program	Teaching Strategies	Assessment Methods
	and IPsec to ensure secure communication.			
2.3	Monitor network traffic, identify potential threats, and apply appropriate measures to mitigate network threats.	S3		
3.0	Values, autonomy, and responsibility			
3.1				
3.2				

C. Course Content

No	List of Topics	Contact Hours
1.	Introduction to Network Security (Book 1: Ch.1 – Introduction) <ul style="list-style-type: none"> Computer Security Concepts The OSI Security Architecture Security Attacks Security Services Security Mechanisms A Model for Network Security 	2
2.	Network Security Principles (Book 2: Ch 6) <ul style="list-style-type: none"> Security Through Network Devices Security Through Network Technology Security Through Network Design Elements 	2
3.	Cryptography (Book 1: Ch.2 & Ch.3) <ul style="list-style-type: none"> Conventional Encryption and Message Confidentiality Public-Key Cryptography and Message Authentication 	4
4.	Firewalls (Book 1: Ch 12) <ul style="list-style-type: none"> The Need for Firewalls Firewall Characteristics Types of Firewalls Firewall Basing Firewall Location and Configurations 	4
5.	Intrusion Detection (Book 1: Ch11.2, Book 3: Ch13)	4
6.	Network protocols security	5





	<ul style="list-style-type: none"> Transport-Level Security (Book 1: Ch5) IPSec (Book 1: Ch8) 	
6.	Authentication and Remote Access (Book 3: Ch.11) <ul style="list-style-type: none"> The Remote Access Process IEEE 802.1X RADIUS TACACS+ Authentication Protocols FTP/FTPS/SFTP VPNs Vulnerabilities of Remote Access Methods 	5
7.	Wireless Network Security (Book 3: Ch.12)	2
8.	Intruders and Malicious Software (Book 1: Ch. 10 & Ch. 11.1)	2
Total		30

D. Students Assessment Activities

No	Assessment Activities *	Assessment timing (in week no)	Percentage of Total Assessment Score
1.	Quizzes	1 - 15	10%
2.	Labs	1 - 15	15%
3.	Assignments or Project	1 - 15	15%
4.	Midterm	Midterm's Week	20%
5.	Final Exam	Final's Week	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	<ol style="list-style-type: none"> Network Security Essentials, by William Stallings, 6th edition, 2017, ISBN 978-0-134-52733-8. CompTIA Security+ Guide to Network Security Fundamentals, Mark Ciampa, 5th Edition, ISBN10: 1305093917 Principles of Computer Security: CompTIA Security+ and Beyond by Wm.A. Conklin et al., McGraw Hill, 3rd Edition, ISBN-10: 0071786198
-----------------------------	---





Supportive References	<ul style="list-style-type: none"> Principles of Computer Security: CompTIA Security+ and Beyond Lab Manual by Wm.A. Conklin et al., McGraw Hill, 2nd Edition, ISBN: 978-0-07-174857-5
Electronic Materials	Umm Al Qura e-learning system containing teaching resources (Slides, assignment papers, etc.)
Other Learning Materials	N/A

2. Required Facilities and equipment

Items	Resources
facilities (Classrooms, laboratories, exhibition rooms, simulation rooms, etc.)	Lecture room with: * at least 30 seats * A data show projector connected to a PC preferably with Internet connection * sliding board * PC Lab (at least 30 seats)
Technology equipment (projector, smart board, software)	30 Linux/Windows PCs
Other equipment (depending on the nature of the specialty)	A maintenance lab + A PC lab with various operating systems such as Linux windows etc.

F. Assessment of Course Quality

Assessment Areas/Issues	Assessor	Assessment Methods
Effectiveness of teaching	Students	Indirect
Effectiveness of Students' assessment	Peers	Direct
Quality of learning resources	Quality Assurance Committee/ Curriculum Committee	Direct





Assessment Areas/Issues	Assessor	Assessment Methods
The extent to which CLOs have been achieved	Instructor	Direct
Other		

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

Assessment Methods (Direct, Indirect)

G. Specification Approval

COUNCIL /COMMITTEE	Umm Al-Qura University Council
REFERENCE NO.	851141114462/190358
DATE	1446/11/22

