Course Specifications

Course Title:	Network security
Course Code:	CSEC 413
Program:	**Information and Computer Science**
Department:	**Computer Science and Information**
College:	**Science Az Al-Zulfi**
Institution:	**Majmaah University**

Table of Contents

A. Course Identification

1. Credit hours:3
2. Course type **a.** University ☐ College ☐ Department ☑ Others ☐ **b.** Required ☐ Elective ☑
3. Level/year at which this course is offered Selective subject
4. Pre-requisites for this course (if any)**: ICS 312 and CSEC 313**
5. Co-requisites for this course (if any)**:Nil**

6. Mode of Instruction (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	**Traditional classroom**	48	80%
2	**Blended**	6	10%
3	**E-learning**	6	10%
4	**Correspondence**	-	-
5	**Other**	-	-

7. Actual Learning Hours (based on academic semester)

No	Activity	Learning Hours
Contact Hours		
1	**Lecture**	30
2	**Laboratory/Studio**	30
3	**Tutorial**	
4	**Others** (specify)	
	Total	60
Other Learning Hours*		
1	**Study**	30
2	**Assignments**	30
3	**Library**	
4	**Projects/Research Essays/Theses**	10
5	**Others** (specify)	30
	Total	100

* The length of time that a learner takes to complete learning activities that lead to achievement of course learning outcomes, such as study time, homework assignments, projects, preparing presentations, library times

B. Course Objectives and Learning Outcomes

1. Course Description

This course provides an introduction to the field of network security. Specific topics to be examined include:

1. security attacks, mechanisms, and services.
2. network security
3. access security models
4. network security practice
5. Email security
6. IP security
7. web security
8. Intrusion detection
9. prevention systems
10. firewalls and virtual private networks
11. cellular and wireless network security.

2. Course Main Objective

1. Be familiar with the fundamental principles of **security attacks, mechanisms, and services** and network security
2. Be able to use **network security practice and IP security**
3. Have the ability to experiment with and use new **web security** methods
4. Be able to design, develop and test fully functioning and well-behaved **firewalls and virtual private networks**
5. Be able to describe, discuss and apply the main theories, models and methodologies of **Intrusion detection**
6. Have the ability to design and implement effective and usable **prevention systems**

3. Course Learning Outcomes

CLOs		Aligned PLOs
1	**Knowledge:**	
1.1	Describe the notion of an agent, how agents are distinct from other software paradigms (e.g. objects) and the characteristics of applications that lend themselves to agent-oriented software	K3-CS
1.2	Understand the key issues associated with constructing agents capable of intelligent autonomous action and the main approaches taken to developing such agents.	
2	**Skills :**	
2.1	Analyze the key issues in designing societies of agents that can effectively cooperate to solve problems, including an understanding of the key types of multi-agent interactions possible in such systems.	S3- CS
3	**Competence:**	
3.1	Be familiar with the main application areas of agent-based systems	C3-CS

C. Course Content

No	List of Topics	Contact Hours
1	Introduction to The importance of network security.	4
2	Key Distribution and User Authentication • Symmetric Key Distribution Using Symmetric Encryption • Kerberos • Key Distribution Using Asymmetric Encryption • X.509 Certificates • Public Key Infrastructure • Federated Identity Management	8
3	Transport-Level Security • Web Security Issues • Secure Sockets Layer (SSL) • Transport Layer Security (TLS) • HTTPS • Secure Shell (SSH)	8
4	Wireless Network Security • IEEE 802.11 Wireless LAN Overview • IEEE 802.11i Wireless LAN Security • Wireless Application Protocol Overview • Wireless Transport Layer Security • WAP End-to-End Security	8
5	IP Security • IP Security Overview • IP Security Policy • Encapsulating Security Payload • Combining Security Associations • Internet Key Exchange • Cryptographic Suites	8
6	Email Security • PGP • S/MIME • Domain Keys Identifications Mail	8

7	Multiple Forms and Hidden Controls	8
8	Handling files	4
9	GUI Design Issues	4
Total		60

D. Teaching and Assessment

1. Alignment of Course Learning Outcomes with Teaching Strategies and Assessment Methods

Code	Course Learning Outcomes	Teaching Strategies	Assessment Methods
1.0	**Knowledge**		
1.1	Describe the notion of an agent, how agents are distinct from other software paradigms (e.g. objects) and the characteristics of applications that lend themselves to agent-oriented software	Lectures Lab demonstrations Case studies Individual presentations	Written Exam Homework assignments Lab assignments Class Activities Quizzes
1.2	Understand the key issues associated with constructing agents capable of intelligent autonomous action and the main approaches taken to developing such agents		
2.0	**Skills**		
2.1	Analyze the key issues in designing societies of agents that can effectively cooperate to solve problems, including an understanding of the key types of multi-agent interactions possible in such systems	Lectures Lab demonstrations Case studies Individual presentations Brainstorming	Written Exam Homework assignments Lab assignments Class Activities Quizzes Observations
3.0	**Competence**		
3.1	Be familiar with the main application areas of agent-based systems	Small group discussion Whole group discussion Brainstorming Presentation	Written Exam Homework assignments Lab assignments Class Activities Quizzes

2. Assessment Tasks for Students

#	Assessment task*	Week Due	Percentage of Total Assessment Score
1	First written mid-term exam	6	15%
2	Second written mid-term exam	12	15%
3	Presentation, class activities, and group discussion	Every week	10%
4	Homework assignments	After each chapter	10%
5	Implementation of presented protocols	Every two	10%

#	Assessment task*	Week Due	Percentage of Total Assessment Score
		weeks	
6	Final written exam	16	40%
7	Total		100%

***Assessment task** (i.e., written test, oral test, oral presentation, group project, essay, etc.)

E. Student Academic Counseling and Support

Arrangements for availability of faculty and teaching staff for individual student consultations and academic advice :

Office hours: Sun: 10-12, Mon. 10-12, Wed. 10-12

Email: m.wagieh@mu.edu.sa

F. Learning Resources and Facilities

1.Learning Resources

Required Textbooks	Guide to Computer Network Security, J. Migga Kizza, Springer,2020
Essential References Materials	W. Stallings, Cryptography and Network Security, Principles and Practice, 2013, 9780134850757
Electronic Materials	-
Other Learning Materials	-

2. Facilities Required

Item	Resources
Accommodation (Classrooms, laboratories, demonstration rooms/labs, etc.)	Classroom and Labs as that available at college of science at AzZulfi are enough.
Technology Resources (AV, data show, Smart Board, software, etc.)	Smart Board
Other Resources (Specify, e.g. if specific laboratory equipment is required, list requirements or attach a list)	N/A

G. Course Quality Evaluation

Evaluation Areas/Issues	Evaluators	Evaluation Methods
Questionnaires (course evaluation) achieved by the students and it is electronically organized by the university.	Students	Indirect

Evaluation Areas/Issues	Evaluators	Evaluation Methods
Student-faculty management meetings.	Program Leaders	Direct
Discussion within the staff members teaching the course	Peer Reviewer	Direct
Departmental internal review of the course.	Peer Reviewer	Direct
Reviewing the final exam questions and a sample of the answers of the students by others.	Peer Reviewer	Direct
Visiting the other institutions that introduce the same course one time per semester.	Faculty	Indirect

Evaluation areas (e.g., Effectiveness of teaching and assessment, Extent of achievement of course learning outcomes, Quality of learning resources, etc.)
Evaluators (Students, Faculty, Program Leaders, Peer Reviewer, Others (specify)
Assessment Methods (Direct, Indirect)

H. Specification Approval Data

Council / Committee	
Reference No.	
Date	