هيئة تقويم التعليم والتدريب
Education & Training Evaluation Commission

T-104
2022

Course Specification

هيئة تقويم التعليم والتدريب
Education & Training Evaluation Commission

T-104
2022

Course Specification

Course Title:	NetworkSecurity
Course Code:	0216 شبك
Program:	Cybersecurity
Department:	Applied Sciences
College:	Applied College
Institution:	Imam Mohammad Bin Saud Islamic University
Version:	1st version
Last Revision Date:	2023/02/26

Table of Contents:

A. General information about the course:

Course Identification					
1. Credit hours:	3 (2 Theory, 2 lab)				
2. Course type:					
a.	University ☐	College ☐	Department☒	Track☐	Others☐
b.	Required ☒	Elective☐			
3. Level/year at which this course is offered: 3rd Level					
4. Course general Description: Students explore how information is exchanged on the Internet and the security issues that arise due to information exchange between different technologies. Students learn concepts of authentication, authorization, access control in network security. Students gain knowledge about Use of cryptography for data and network security. Students are introduced to the topics such as firewalls, public key infrastructure, security standards and protocols, virtual private networks, and wireless network security.					
5. Pre-requirements for this course (if any):					
6. Co- requirements for this course (if any): N/A					
7. Course Main Objective(s):					

1. Teaching mode (mark all that apply)

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

2. Contact Hours (based on the academic semester)

No	Activity	Contact Hours
1.	Lectures	12
2.	Laboratory/Studio	48
3.	Field	
4.	Tutorial	
5.	Others (specify)	150
	Total	210

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			

Code	Course Learning Outcomes	Code of CLOs aligned with program	Teaching Strategies	Assessment Methods
1.1	Understand basic concept of how to protect and design private network.	ع1، ع5	Class lectures. Class discussion. Questions/Answers session in class. Home work. Learning by discovery. Self-education. Brainstorming. Online search. KWL learning table. Mind maps. Concept maps.	Quizzes. Homework and Assignments. Written and online exams. Writing reports. Presentations. Discussion and debate. Achievement file. Performance
1.2	Understand how to protect security of information	ع1، ع5		
1.3	Use theoretical and practical knowledge in securing data transfer and authentication	ع1، ع5		
2.0	Skills			
2.1	Attacker goals, capabilities, and motivations (such as underground economy, digital espionage, cyberwarfare, insider threats, hacktivism, advanced persistent threats)	ع1، ع5	Class lectures. Class discussion. Questions/Answers session in class. Home work. Learning by discovery. Self-education. Brainstorming. Online search. Mind maps. Concept maps.	Quizzes. Homework and Assignments. Written and online exams. Writing reports. Presentations. Discussion and debate. Achievement file. Performance tests.
2.2	Architectures for secure networks (e.g., secure channels, secure routing protocols, secure DNS, VPNs, anonymous communication protocols, isolation)	ع1، ع5		
2.3	Use of cryptography for data and network securit	ع1، ع5		
3.0	Values, autonomy, and responsibility			
3.1	Collaboration, teamwork, and professional ethics.	ق1	Class lectures. Class discussion. Questions/Answers session in class. Home work. Learning by discovery. Self-education. Brainstorming. Online search. Mind maps. Concept maps.	Quizzes. Homework and Assignments. Written and online exams. Writing reports. Presentations. Discussion and debate. Achievement file. Performance.
3.2	Take the responsibility for continuous learning, and self-development.	ق2		
3.3	Effective and efficient time management when applying acquired knowledge and skills.	ق3		

C. Course Content

No	List of Topics	Contact Hours
1.	**Introduction:** ○ Computer Security Concepts ○ The OSI Security Architecture ○ Security Attacks ○ Security Services ○ Security Mechanisms ○ A Model for Network Security	4
2.	**Network Security:** ○ Security Through Network Devices ○ Security Through Network Technology ○ Security Through Network Design Elements	8
3	**Firewalls:** ○ The Need for Firewalls ○ Firewall Characteristics ○ Types of Firewalls ○ Firewall Basing ○ Firewall Location and Configurations	8
4	**Cryptography:** ○ Algorithms ○ Hashing Functions ○ Symmetric Encryption ○ Asymmetric Encryption	3
5	**Public Key Infrastructure:** ○ The Basics of Public Key Infrastructures ○ Certificate Authorities ○ Registration Authorities ○ Certificate Repositories ○ Trust and Certificate Verification ○ Digital Certificates	4
6	**Security Standards and Protocols:** ○ PKIX and PKCS ○ X.509 ○ SSL/TLS ○ ISAKMP ○ CMP ○ PGP ○ HTTPS ○ IPsec ○ Common Criteria for Information Technology Security (Common Criteria or CC) ○ ISO/IEC 27002	5
7	**Authentication and Remote Access:** ○ The Remote Access Process ○ SSH/Telnet	5

	○ IEEE 802.1X ○ RADIUS ○ TACACS+ ○ Authentication Protocols ○ FTP/FTPS/SFTP ○ VPNs ○ IPsec ○ Vulnerabilities of Remote Access Methods	
8	**IDS/IPS** ○ Explain the functions and operations of IDS and IPS systems. ○ Describe the characteristics of IPS signatures	4
9	**Virtual Private Networks:** ○ VPN Fundamentals ○ VPN Management ○ VPN Technologies	4
10	**Wireless Network Security:** ○ Introduction to Wireless Networking ○ 802.11Attacking, New Security Protocols, and Implementation	3
Total		48

D. Students Assessment Activities

No	Assessment Activities *	Assessment timing (in week no)	Percentage of Total Assessment Score
1.	Mid-term	Week 7	20%
2.	Quizzes (From 3-4 Quizzes)	Week 5, 10	10%
3.	1st Practical Evaluation	Week 2-11	20%
4	2nd Practical Evaluation	Week 11	15%
5	Participation	Week 1-11	5%
6	Final	Week 12	30%
7	Total Marks		100%

*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, Firewalls, and VPNS, by J. Michael Stewart, 2010, ISBN 10: 076379130X ○ Cryptography and Network Security: Principles and Practices by W.Stallings, Prentice Hall, 5 th Edition, ISBN-10: 0136097049 ○ Principles of Computer Security: CompTIA Security+ and Beyond by Wm.A. Conklin et al., McGraw Hill, 3 rd Edition, ISBN-10: 0071786198
Supportive References	N/A
Electronic Materials	Online resources will be provided during class lectures on LMS.
Other Learning Materials	N/A

2. Required Facilities and equipment

Items	Resources
Facilities (Classrooms, laboratories, exhibition rooms, simulation rooms, etc.)	Classroom – A computer lab equipped and connected to a shared printer and the internet.
Technology equipment (projector, smart board, software)	Smart board, data projector, Microsoft Visio or Edraw Max and Internet browser.
Other equipment (depending on the nature of the specialty)	N\A

F. Assessment of Course Quality

Assessment Areas/Issues	Assessor	Assessment Methods
Effectiveness of teaching	Peer references – students.	1.Questionnaires and referendums approved by the department. 2.Peer evaluation of faculty members. 3.Review the results of the students' evaluation.
Effectiveness of students assessment	Peer references - program leaders - faculty members – students.	1.Questionnaires and referendums approved by the department. 2.Review course descriptions and course reports periodically.

Assessment Areas/Issues	Assessor	Assessment Methods
		3.Peer evaluation and periodic exchange of correction and scrutiny among fellow faculty members. 4.Review samples of students' work.
Quality of learning resources	Program leaders - faculty members - students	1.Questionnaires and referendums approved by the department. 2.Write-offs and monitoring.
The extent to which CLOs have been achieved	Program leaders - faculty members.	1.Review the course report. 2. Analysis of exams forms, grades, students' work and records of achievement.
Other		

Assessor (Students, Faculty, Program Leaders, Peer Reviewer, Others (specify)
Assessment Methods (Direct, Indirect)

G. Specification Approval Data

COUNCIL /COMMITTEE	Department of Applied Sciences – Applied College
REFERENCE NO.	
DATE	