هيئة تقويم التعليم والتدريب
Education & Training Evaluation Commission

اعتماد
NCAAA

2024
TP-153

Course Specification
(Bachelor)

Course Title:	Network Security
Course Code:	CNET 411
Program:	Computer & Network Engineering
Department:	Electrical & Electronics Engineering
College:	College of Engineering & Computer Science
Institution:	Jazan University
Version:	15
Last Revision Date:	21 September 2024

Table of Contents

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: (9/5)					
4. Course General Description:					
This course introduces the fundamentals concepts of security goals, attacks, services, mechanisms. In addition, security mechanisms at the network, transport, and application layers are introduced. This includes IPSec, SSL. and TLS, email security, firewalls, and IDS. The lab portion of the course is interactive such that students are given various challenges and they are assessed based on their ability to solve these challenges					
5. Pre-requirements for this course (if any)**:**					
326 CNET-3 Cryptographic Techniques					
6. Co-requisites for this course (if any)**:**					
7. Course Main Objective(s):					
This course will develop the students' ability to learn: ●Understanding security goals, attacks, services, and mechanisms. ●Description of security mechanisms at the network, transport, and application layers. ●Ability to determine the appropriate security mechanism to protect the network. ●Analysis of firewalls and intrusion detection systems. ●Performing lab tasks on each theoretical topic using Linux and tools such as Nmap and Wireshark. ●Ability to self-study and self-assessment.					

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		
4	Distance learning		

3. Contact Hours (based on the academic semester)

No	Activity	Contact Hours
1.	**Lectures**	26
2.	**Laboratory/Studio**	26
3.	**Field**	--
4.	**Tutorial**	--
5.	**Others (specify)**	8
Total		60

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

Code	Course Learning Outcomes	Code of PLOs aligned with the program	Teaching Strategies	Assessment Methods
1.0	**Knowledge and understanding**			
1.1	**Explain** security goals, attacks, services, and mechanisms effectively.	K2	● Lectures ● Classroom discussions ● Lab exercises	● Mid-Term Exam ● Assignment 1 Final Exam
1.2	**Describe** security mechanisms at the network, transport, and application layers clearly.	K2	● Lectures ● Classroom discussions ● Lab exercises	● Mid-Term Exam ● Assignment 1 Final Exam

Code	Course Learning Outcomes	Code of PLOs aligned with the program	Teaching Strategies	Assessment Methods
2.0	**Skills**			
2.1	**Apply** the appropriate security mechanism to protect the network when given a scenario for application, transport, and network layers.	S2	• Lectures • Classroom discussions • Lab exercises	• Mid-Term Exam • Assignment 1 • Mini Project Final Exam
2.2	**Differentiate** between the types of firewalls and intrusion detection systems effectively.	S5	• Lectures • Classroom discussions • Lab exercises	• Mid-Term Exam • Lab Exam • Mini Project Final Exam
2.3	**Solve** problems using Linux, Nmap, Wireshark, TLS, IPsec, firewalls, IDS & trusted computing effectively.	S2	• Lectures • Classroom discussions • Lab exercises	• Mid-Term Exam • Lab Exam • Mini Project Final Exam
3.0	**Values, autonomy, and responsibility**			
3.1	**Perform** self-study and self-assessment through lab assignments.	V2	• Lectures • Classroom discussions • Lab exercises	• Lab Exam • Mini Project

C. Course Content

No	List of Topics	Contact Hours
1.	**Chapter 1: Introduction to Security Concepts** **Security Goals** • **Confidentiality** • **Integrity** • **Availability** **Attacks** • **Attacks threatening Confidentiality** • **Attacks threatening Integrity** • **Attacks threatening Availability** • **Passive Versus Active Attacks** **Services and Mechanism**	4T + 4P

	• Security Services • Security Mechanisms **Relations between Services and Mechanisms**	
2.	**Chapter – 2: Cryptography in Networks** **Network Encryption** • Symmetric • Asymmetric • SSH • SSL & TLS • Onion Routing • IPsec **VPN**	6T + 6P
3.	**Chapter - 3: Denial of Service** • DoS Definition • Types of Service Denial • Types of Flooding • DoS by Addressing Failures • Distributed DoS (DDOS) • DoS Prevention	6T + 6P

4.	**Chapter – 4: Firewalls**
	• What is a firewall?
	• Design of Firewalls
	• Chrematistics of firewall
	• Types of Firewalls
	  ○ Application-level gateways
	  ○ Circuit-level gateways
	  ○ Guards
	  ○ Packet filtering gateways
	  ○ Stateful inspection
	  ○ Personal firewalls
		4T + 4P

5.	**Chapter – 5: Intrusion Detections Systems (IDS) & Side Channel Attacks** • Types of IDS • Intrusion Prevention Systems • Intrusion Response • Goals for Intrusion Detection Systems • IDS Strengths and Limitations • Introudction to SNORT	

	• SNORT Design • SNORT Rules & Architecure	4T + 4P
6.	Chapter 6: Side channel attacks • Side Channel Attacks • Types of side channel attacks • Trusted Computing • Key Technology of trusted Computing • What Trusted Computing Provides?	2T+2P
7.	Revision all contents	2T+2P
8.	Final Exam	2T + 2P
Total		60

D. Students Assessment Activities

No	Assessment Activities *	Assessment timing (in week no)	Percentage of Total Assessment Score
1.	Assignments	4th Week	10%
2.	Midterm Exam	8th Week	20%
3.	Mini Project	12th Week	10%
4.	Lab Exam	13th Week	20%
5.	Final Exam	15th 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	Security in Computing, Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies, 5th Edition, Prentice Hall, Year-2015, ISBN 0134085051, 9780134085050
Supportive References	Cryptography And Network Security, By Behrouz A. Forouzan, 1st edition, McGraw-Hill Education, Year-2010, ISBN-13 : 978-0073327532
Electronic Materials	Recent topics on Network Security from SDL, https://sdl.edu.sa/SDLPortal/ar/Publishers.aspx
Other Learning Materials	**www.tryhackme.com**

2. Required Facilities and equipment

Items	Resources
facilities (Classrooms, laboratories, exhibition rooms, simulation rooms, etc.)	**Classroom equipped with projector and whiteboard and sufficient seating arrangements.** **Lab with software installed and individual computer terminal for each student.**
Technology equipment (projector, smart board, software)	**Computer Lab with Linux OS and a working network setup. A network monitoring tool such as Wireshark. A network scanning tool such as NMAP. The package OpenSSL for X.509 certificates management. The package OpenVPN for creating a VPN server and client. And the IDS Snort.** **GNS3**
Other equipment (depending on the nature of the specialty)	**None**

F. Assessment of Course Quality

Assessment Areas/Issues	Assessor	Assessment Methods
Effectiveness of teaching	**Students, HOD**	**Indirect, Direct**
Effectiveness of Students assessment	**CT / CC / HoD**	**Direct**
Quality of learning resources	**TL / CRC / PQC**	**Indirect, Direct**
The extent to which CLOs have been achieved	**CT / CC /TL / PQC**	**Indirect, Direct**
Other		

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

Assessment Methods (Direct, Indirect)

G. Specification Approval

COUNCIL /COMMITTEE	**DEPARTMENT COUNCIL**
REFERENCE NO.	**ENGCSEEE2411**
DATE	**10/10/24**