هيئة تقويم التعليم والتدريب
Education & Training Evaluation Commission

اعتماد
NCAAA

2024

TP-153

Course Specification

(Bachelor)

Course Title:	Network Security Management
Course Code:	CNET 463
Program:	Computer & Network Engineering
Department:	Electrical & Electronics Engineering
College:	College of Engineering & Computer Science
Institution:	Jazan University
Version:	2
Last Revision Date:	30 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: (7/4)

4. Course General Description:

The main purpose of the course is demonstrate security issues of all common networking devices such as hubs, switches, access points, and routers, as well as vulnerable network protocols such as ARP, SRP, ICMP and DHCP • Design and develop the latest technological solutions, practices, and principles on network and information security for management, administrative, and research purposes. The course is intended to bridge the gap in knowledge between research communities and security professionals.

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):

NA

6. Co-requisites for this course (if any):

NA

7. Course Main Objective(s):

This course will develop the students' ability to learn:

Describe security issues of all common networking devices as well as vulnerablenetwork protocols such as DoS, Information Leakage.

Discuss Organizational Policy and Security policy issues of the components that areresponsible for provisioning multidomain network services

Differentiate complexity of network systems warrants a need for a framework that canbe used to assess security in such systems.

Design the latest technological solutions, practices, and principles on network andinformation security for management, administrative, and research purposes.

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	Describe security issues of all common networking devices as well as vulnerable network protocols.	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
1.2	Discuss latest trends, current research in Network security management.	K3	● Lectures ● Classroom discussions ● Lab exercises	● Mid-Term Exam ● Assignment 1 Final Exam
2.0	**Skills**			
2.1	Differentiate Organizational and security policy issues of the components for provisioning multi-domain network services	S2	● Lectures ● Classroom discussions ● Lab exercises	● Mid-Term Exam ● Assignment 1 ● Mini Project Final Exam
2.2	Evaluate sheer complexity of network systems warrants a need for a framework that can be used to assess security in such systems.	S3	● Lectures ● Classroom discussions ● Lab exercises	● Mid-Term Exam ● Lab Exam ● Mini Project Final Exam
2.3	Identify the latest technological solutions, practices, and principles on network and information security	S1	● Lectures ● Classroom discussions ● Lab exercises	● Mid-Term Exam ● Lab Exam ● Mini Project Final Exam
3.0	**Values, autonomy, and responsibility**			
3.1	Recognize ethical and professional responsibilities in network security and provide appropriate solutions	V3	● Lectures ● Classroom discussions ● Lab exercises	● Lab Exam ● Mini Project

C. Course Content

No	List of Topics	Contact Hours
1.	**1. Introduction** **1.1 WHY Network Security is Needed**	4T + 4P

	1.2 Management Principles **1.3 Security Principles** **1.4 Network Management** **1.5 Security Attacks** **1.5.1 Denial-of-Service (DoS)** **1.5.2 Information Leakage** **1.5.3 Regular File Access** **1.5.4 Misinformation** **1.5.5 Special File/Database Access** **1.5.6 Remote Arbitrary Code Execution** **1.5.7 Elevation of Privileges**	
2.	**Chapter – 2: Organizational Policy and Security** **2.1 Security Policies, Standards and** **2.2 Guidelines Information Policy** **2.3 Security Policy** **2.4 Physical Security** **2.5 Social Engineering** **2.6 Security Procedures** **2.7 Building a Security Plan** **2.7.1 Elements of Security** **2.7.2 Plan Network Security** **2.8 Implementing Planninga Security Policy**	6T + 6P
3.	**Chapter - 3: Security Infrastructure** **3.1 Infrastructure Components** **3.1.1 Network Category** **3.1.2 Platform Category** **3.1.3 Physical Components** **3.1.4 Process Category** **3.2 Goals of Security Infrastructure** **3.2.1 Data Confidentiality** **3.2.2 Data Integrity** **3.2.3 Data Availability** **3.3 Design Guidelines**	6T + 6P

	3.3.1 Authentication 3.3.2 Authorization 3.3.3 Accounting 3.3.4 Physical Access Controls 3.3.5 Logical Access Controls 3.4 Security Models 3.4.1 Bell–La Padula Confidentiality Model	
4.	Chapter - 4: Hardware and Software Security 4.1 Hardware Security 4.2 Smart Card 4.3 Biometrics 4.4 Virtual Private Networks (VPNs) 4.4.1 Types of VPNs 4.4.2 Virtual Private Network Software 4.5 Operating Systems 4.5.1 A Bit of History 4.5.2 Trusted Operating Systems 4.5.3 Security Breaches 4.6 Kerberos 4.7 Public Key Infrastructure (PKI) 4.8 Pretty Good Privacy (PGP) 4.9 Security Protocols 4.9.1 Secure Socket Layer 4.9.2 Transport Layer Security 4.9.3 IPSec 4.9.4 S/MIME (Secure/Multipurpose Internet Mail Extension)	4T + 4P
5.	Chapter – 5: Information Systems Security 5.1 Distributed Systems Security 5.2 Distributed Computing Environment 5.3 System Vulnerability and Abuse 5.3.1 Internet Vulnerabilities	

	5.3.2 Malicious Software: Viruses, Worms, Trojan Horses, and Spyware 5.3.3 Hackers, Spoofing, and Sniffing 5.3.4 Denial of Service Attacks 5.3.5 Internal Threats: Employees 5.3.6 Software Vulnerability	4T + 4P
6.	Chapter 6: ● Qualities of a Good Network ● Biba Integrity Model ● Clark-Wilson Security Model ● Software Security ● Reliability, Safety, and Security ● Management Framework of Security and Control ● Role of Auditing in the Control Process ● Technology and Tools for Safeguarding Information Resources	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	1.A Practical Introduction to Enterprise Network and Security Management , Auerbach Publications; 2nd edition, Year -2021, ISBN-13: 978-1032048024 ISBN-10: 1032048026

	2. 1.Network Security and Management, PHI Publications; 3rd edition, Year -2012, ISBN-13: 978-8120344976, ISBN-10: 8120344979
Supportive References	1. Network Security, Administration and Management: Advancing Technology and Practice by Dulal Chandra Kar (Texas A&M University, USA) and Mahbubur Rahman Syed (Minnesota State University, USA),1st Edition, ,Year 2011, ISBN13: 9781609607777|ISBN10: 1609607775 2.ACFE. (2008). Managing the Business Risk of Fraud - A Practical Guide. Retrieved from http://www.acfe.com/ documents/managing-business-risk.pdf
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. Cisco Packet Tracer & 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**