QF01/0408-4.0E	Course Plan for Bachelor program - Study Plan Development and Updating Procedures/ Cyber Security Department

Study plan No.	**2024/2025**		**University Specialization**		**Cybersecurity**		
Course No.	**0133220**		**Course name**		**Network Security**		
Credit Hours	**3**		**Prerequisite Co-requisite**		**Network**		
Course type	☐ MANDATORY UNIVERSITY REQUIREMENT	☐ UNIVERSITY ELECTIVE REQUIREMENTS	☐ FACULTY MANDATORY REQUIREMENT	☐ Support course family requirements	☐ ✓ **Mandatory requirements**	☐ Elective requirements	
Teaching style	☐ **Full online learning**		☐ Blended learning		☐ ✓Traditional learning		
Teaching model	☐ 2Synchronous: 1asynchronous		☐ 2 face to face: 1synchronous		☐ ✓3 Traditional		

Faculty member and study divisions information (to be filled in each semester by the subject instructor)

Name	Academic rank	Office No.	Phone No.	E-mail	
Adnan Hnaif	**professor**	**323**		**Adnan_hnaif@zuj.edu.jo**	
Division number	**Time**	**Place**	**Number of students**	**Teaching style**	**Approved model**
0125	**2:00 – 3:30**	**9250**	**23**	**Traditional**	

Brief description

Network security is a critical component of information technology, ensuring the confidentiality, integrity, and availability of data in networked systems. This course provides an in-depth exploration of the principles, techniques, and best practices for securing computer networks against various threats and vulnerabilities. Students will gain a comprehensive understanding of the key concepts, tools, and methodologies used in network security and be prepared to design, implement, and manage secure network infrastructures.

Learning resources

Course book information (Title, author, date of issue, publisher ... etc)	"Network Security Essentials: Applications and Standards" by William Stallings, 2021			
Supportive learning resources (Books, databases, periodicals, software, applications, others)	Certified Network Defender" by the EC-Council, 2022 1. https://www.eccouncil.org/train-certify/certified-network-security-course/			
Supporting websites				
The physical environment for teaching	☐ **Class room**	☐ ✓labs	☐ **Virtual educational platform**	☐ Others
Necessary equipment and software	**Sophos Firewall**			
Supporting people with special needs				

QF01/0408-4.0E	Course Plan for Bachelor program - Study Plan Development and Updating Procedures/ Cyber Security Department

For technical support	E-learning and Open Educational Center. Computer Center

Course learning outcomes (S= *Skills, C= Competences K= Knowledge,)*

No.	Course learning outcomes	The associated program learning output code
	Knowledge	
K1	Remembering of various network protocols and their associated vulnerabilities, including the OSI model, TCP/IP, and common application layer protocols.	**3**
K2	Students will be able to identify different attack vectors, such as denial of service (DoS) attacks, malware propagation, and social engineering techniques.	**1**
K3		**3**
	Skills	
S1	Students should develop the ability to critically assess network security issues and vulnerabilities	**6**
S2	Students should develop skills in risk assessment and management, which includes the capacity to identify and evaluate security risks in a networked environment	
	Competences	
C1	Students should gain hands-on experience in configuring and administering network devices and services.	**11**
C2	Students often work on projects and assignments in groups or interact with other team members to build a complete project with documents.	**12**

Mechanisms for direct evaluation of learning outcomes

Type of assessment / learning style	Fully electronic learning	Blended learning	Traditional Learning (Theory Learning)	Traditional Learning (Practical Learning)
First exam	0	**0**	0	0
Second / midterm exam	%30	**%30**	%30	%30
Participation / practical applications	0	**0**	0	0
Asynchronous interactive activities	%30	**%30**	%30	%30
final exam	%40	**%40**	%40	%40

Note: Asynchronous interactive activities are activities, tasks, projects, assignments, research, studies, projects, work within student groups ... etc, which the student carries out on his own, through the virtual platform without a direct encounter with the subject teacher.

Schedule of simultaneous / face-to-face encounters and their topics

Week	Subject	learning style*	Reference **
1	Introduction to Network Security	**Lecture**	**content on the e-learning platform**

2	Introduction to Sophos Firewall	**Lecture**	**content on the e-learning platform**
3	Network Security Threats, Vulnerabilities, and Attacks	**Lecture**	**content on the e-learning platform**
4	Create Definitions on Sophos Firewall	**Lecture**	**content on the e-learning platform**
5	Configure Zones and Interfaces on Sophos Firewall	**Lecture**	**content on the e-learning platform**
6	Implementing IDS and IPS	**Lecture**	**content on the e-learning platform**
7			
8	**Midterm Exam**		
9	Authentication on Sophos	**Lecture**	**content on the e-learning platform**
10	Network Defender	**Lecture**	**content on the e-learning platform**
11	CND Labs Module 01 Computer Network and Defense Fundamentals	**Lecture**	**content on the e-learning platform**
12	CND_Labs_Module_03_Network_Security	**Lecture**	**content on the e-learning platform**
13	CND_Labs_Module_04_Network_Security	**Lecture**	**content on the e-learning platform**
14	CND Labs Module 12 Network Risk and Vulnerability Manage	**Lecture**	**content on the e-learning platform**
15			
16	Final Exam		

*** Learning styles: Lecture, flipped learning, learning through projects, learning through problem solving, participatory learning ... etc.**
**** Reference: Pages in a book, database, recorded lecture, content on the e-learning platform, video, website ... etc.**

Schedule of asynchronous interactive activities (in the case of e-learning and blended learning)

This activities was designed using the **Project-Based Learning (PBL)**
Project : Network Vulnerability Assessment

Task / Activity	Reference	Expected Results
Define project scope, objectives, and target network	Network Security textbooks, NIST Guidelines	Clear definition of assessment boundaries and goals
Identify tools (Nmap, Wireshark, OpenVAS, Nessus)	Official tool documentation, security labs	Selection of appropriate tools
Perform network scanning & mapping	Nmap documentation, lab tutorials	List of active hosts, services, and open ports
Conduct vulnerability scanning	OpenVAS/Nessus user guides	Identified vulnerabilities with details
Analyze vulnerabilities & classify severity (CVSS)	CVSS v3.1 documentation	Ranked vulnerabilities (Low–Critical)
Evaluate risks associated with vulnerabilities	NIST Risk Management Framework	Structured risk assessment table
Recommend mitigation & security controls	Best security practices, CIS Benchmarks	Practical and feasible mitigation plan
Document findings in professional report	IEEE / academic report format	Final vulnerability assessment report

Task / Activity	Reference	Expected Results
Reflection & learning summary	PBL methodology	Demonstration of learning outcomes and insights