جامعــة الـزيـتـونـــة الأردنيــة

Al–Zaytoonah University of Jordan

كلية العلوم وتكنولوجيا المعلومات

Faculty of Science and Information Technology

" عراقة وجودة"

"Tradition and Quality"

F01/0408-4.0E	Course Plan for Bachelor program - Study Plan Development and Updating Procedures/ Cyber Security Department

Study plan No.	**2024/2025**		**University Specialization**		**Cybersecurity**	
Course No.	**0133308**		**Course name**		**Cybersecurity Tools and Techniques**	
Credit Hours	**3**		**Prerequisite Co-requisite**		**Secure Communication Protocols**(0133333)	
Course type	☐ MANDATORY UNIVERSITY Requirement	☐ University elective Requirement	☐ FACULTY MANDATORY Requirement	☐ Support course family requirements	☐ Mandatory requirement	☐ √ **Elective requirements**
Teaching style	☐ **Full online learning**		☐ ✓Blended learning		☐ Traditional learning	
Teaching model	☐ Synchronous:1asynchronous		☐2 face to face: synchronous		☐ **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

Division number	Time	Place	Number of students	Teaching style	Approved model

Brief description

This course introduces tools and techniques for password cracking test password strength in your operating system, or for auditing one remotely. Students will be able to use different penetration testing tools to discover remote software vulnerabilities. They will also know how to conduct necessary penetration tests on small networks, run spot checks on the exploitability of vulnerabilities, or discover the network or import scan data.

Learning resources

Course book information (Title, author, date of issue, publisher ... etc)	Cybersecurity Blue Team Toolkit 1st edition . Nadean H. Tanner . WILEY.
Supportive learning resources (Books, databases, periodicals, software, applications, others)	1. Blue Team Handbook: SOC, SIEM, and Threat Hunting (V1.02). Don Murdoch. 2. Blue Team Handbook: Incident Response Edition. Don Murdoc 3. The Pentester BluePrint. Phillip L. Wylie

Supporting websites				
The physical environment for teaching	☐ **Class room**	☐ labs	☐ **Virtual educational platform**	☐ Others
Necessary equipment and software				
Supporting people with special needs				
For technical support	**E-learning and Open Educational Center. Computer Center**			

Security Department

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

No.	Course learning outcomes	The associated program learning output code
	Knowledge	
K1	Students will learn the underlying principles and techniques associated with the cybersecurity practice known as penetration testing or ethical hacking.	**MK1**
K2	Knowledge with the entire penetration testing process including planning, reconnaissance, scanning, exploitation, post-exploitation and result reporting.	**MK2**
K3	Describe web applications, their vulnerabilities and the tools used to attack them.	**MK4**
K4	Identify and describe network protection systems.	**MK1**
	Skills	
S1	Plan a vulnerability assessment and penetration test for a network.	**MS1**
S2	Execute a penetration test using standard hacking tools in an ethical manner.	**MS2**
S3	Report on the strengths and vulnerabilities of the tested network.	**MS3**
S4	Identify legal and ethical issues related to vulnerability and penetration testing.	**MS4**
	Competences	
C1	Gain a foundational understanding of a subject or tool	**MC1**
C2	Prepare students for industry-recognized certifications like CompTIA Security+, CISSP, and Certified Ethical Hacker (CEH).	**MC2**
C3	Familiarize students with various cybersecurity tools, such as antivirus software, IDS/IPS, SIEM (Security Information and Event Management), and vulnerability scanners	**MC3**

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	Fundamental Networking and Security Tools-1	Lecture	
2	Troubleshooting Microsoft Windows-1	Lecture	
3	Nmap—The Network Mapper-1	Lecture	
4	Vulnerability Management-1	Lecture	
5	Monitoring with OSSEC-1	Lecture	
6	Protecting Wireless Communication	Lecture	
7	Wireshark part 1	Lecture	
8	Midterm Exam (30%)	Lecture	
9	Access Management-1	Lecture	
10	Managing Logs-1	Lecture	
11	Metasploit-1	Lecture	
12	Web Application Security-1	Lecture	
13	Patch and Configuration Management-1	Lecture	
14	Securing OSI Layer 8-1	Lecture	
15	Projects Discussion	learning through projects	
16	Final Exam		

Security Department

*** 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.**

Project : System & Application Security (PBL)

This activities was designed using the **Project-Based Learning (PBL)**

Task / Activity	Reference	Expected Results
Identify and collect system logs	Managing Logs – 1	Structured log records collected
Analyze logs for security events	Managing Logs – 1	Detection of abnormal activities
Use Metasploit for vulnerability testing	Metasploit – 1	Identified system weaknesses
Perform basic exploitation in controlled lab	Metasploit – 1	Demonstrated penetration simulation
Apply security measures to reduce risks	Web Application Security – 1	Improved system protection
Prepare security assessment documentation	PBL Documentation	Professional security report

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

Week	Task / activity	Reference	Expected results
1			
2			
3			
4			
5			
6			
7			
8			