



University of Fallujah
College of Information Technology
Department of Cybersecurity

MODULE DESCRIPTION FORM

نموذج وصف المادة الدراسية

Module Information			
معلومات المادة الدراسية			
Module Title	Cybersecurity Fundamentals		Module Delivery
Module Type	Core		☒ Theory ☒ Lecture ☒ Lab ☐ Tutorial ☐ Practical ☐ Seminar
Module Code	CYS108		
ECTS Credits	7		
SWL (hr/sem)	175		
Module Level	1	Semester of Delivery	
Administering Department	Dept. of Cybersecurity	College	College of Information Technology
Module Leader	Dr. Ahmad A. AlSabhany	e-mail	Ahmad.alsabhany@uofallujah.edu.iq
Module Leader's Acad. Title	Asst. Prof.	Module Leader's Qualification	Ph.D.
Module Tutor	Dr. Ahmad A. AlSabhany	e-mail	Ahmad.alsabhany@uofallujah.edu.iq
Peer Reviewer Name	Dr. Omar Salah Farhan	e-mail	omar.alshareef@uofallujah.edu.iq
Scientific Committee Approval Date	25-5-2026	Version Number	1.0

Relation with other Modules			
العلاقة مع المواد الدراسية الأخرى			
Prerequisite module	None	Semester	
Co-requisites module	None	Semester	

Module Aims, Learning Outcomes and Indicative Contents أهداف المادة الدراسية ونتائج التعلم والمحتويات الإرشادية	
Module Objectives أهداف المادة الدراسية	1. Explain the fundamental concepts, principles, and terminology of cybersecurity. 2. Identify common cyber threats, vulnerabilities, and security controls used to protect systems and networks. 3. Demonstrate basic cybersecurity skills using virtual machines, Linux systems, and command-line security tools. 4. Apply network analysis and reconnaissance techniques to evaluate networked systems. 5. Perform introductory security testing and traffic analysis using industry-standard cybersecurity tools. 6. Apply ethical, legal, and professional responsibilities in cybersecurity practice.
Module Learning Outcomes مخرجات التعلم للمادة الدراسية	1. Describe the fundamental concepts, principles, and terminology of cybersecurity. 2. Recognize common cyber threats, vulnerabilities, and security controls used to protect systems and networks. 3. Use virtual machines, Linux systems, and basic command-line tools in a cybersecurity environment. 4. Perform basic network reconnaissance and analysis activities using appropriate cybersecurity tools. 5. Conduct introductory security testing and network traffic analysis using industry-standard cybersecurity tools. 6. Demonstrate ethical, legal, and professional behavior when performing cybersecurity-related activities.
Indicative Contents المحتويات الإرشادية	Total hrs = 175 = SSWL - (Exam hrs) = 78 - 3 = 75 hr (5 x 15 weeks)

Learning and Teaching Strategies استراتيجيات التعلم والتعليم	
Strategies	Type something like: The main strategy that will be adopted in delivering this module is to encourage students' participation in the exercises, while at the same time refining and expanding their critical thinking skills. This will be achieved through classes, interactive tutorials and by considering types of simple experiments involving some sampling activities that are interesting to the students.

Student Workload (SWL)			
الحمل الدراسي للطلاب محسوب لـ ١٥ اسبوعا			
Structured SWL (h/sem) الحمل الدراسي المنتظم للطلاب خلال الفصل	78	Structured SWL (h/w) الحمل الدراسي المنتظم للطلاب أسبوعيا	5
Unstructured SWL (h/sem) الحمل الدراسي غير المنتظم للطلاب خلال الفصل	97	Unstructured SWL (h/w) الحمل الدراسي غير المنتظم للطلاب أسبوعيا	6
Total SWL (h/sem) الحمل الدراسي الكلي للطلاب خلال الفصل	175		

Module Evaluation					
تقييم المادة الدراسية					
		Time/Number	Weight (Marks)	Week Due	Relevant Learning Outcome
Formative assessment	Quizzes	2	10% (10)	5 and 10	LO #1, #2 and #10, #11
	Assignments	2	10% (10)	2 and 12	LO #3, #4 and #6, #7
	Projects / Lab.	1	10% (10)	Continuous	All
	Report	1	10% (10)	13	LO #5, #8 and #10
Summative assessment	Midterm Exam	2hr	10% (10)	7	LO #1 - #7
	Final Exam	3hr	50% (50)	16	All
Total assessment			100% (100 Marks)		

Delivery Plan (Weekly Syllabus)	
المنهاج الاسبوعي النظري	
	Material Covered
Week 1	Introduction to Cybersecurity: Security Goals, Threats, Vulnerabilities, Attacks, Ethics and Legal Considerations
Week 2	Windows Security Basics: User Accounts, Authentication, Permissions, NTFS
Week 3	Windows Security Basics: Event Logs, Windows Defender, Windows Firewall
Week 4	Virtualization Fundamentals: Virtual Machines, Hypervisors, VMware Workstation
Week 5	Linux Fundamentals: File System, Commands, Users, Permissions, Processes
Week 6	Kali Linux Fundamentals: Security Tools, Networking Basics, Package Management
Week 7	Password Security: Authentication, Password Hashing, Password Cracking Concepts
Week 8	Midterm Examination

Week 9	Netcat Fundamentals: Client-Server Communication, TCP and UDP Concepts
Week 10	Netcat Advanced Usage: Shells, Redirection, and Remote Access Concepts
Week 11	Wireshark Fundamentals: Packets, Protocols, and Traffic Analysis
Week 12	Wireshark Analysis: TCP Streams, Credentials, and File Transfers
Week 13	Web Security Fundamentals: HTTP Requests, Responses, Methods, and Web Architecture
Week 14	Burp Suite Basics: Intercept, Repeater, Intruder, Decoder
Week 15	Capture-the-Flag Competition Team challenge combining: network analysis, password cracking, web exploitation, and log analysis.
Week 16	Preparatory week before the final Exam

Delivery Plan (Weekly Lab. Syllabus) المنهاج الاسبوعي للمختبر	
	Material Covered
Week 1	Introduction to the laboratory environment and course tools
Week 2	Managing users, groups, files, and folder permissions in Windows
Week 3	Reviewing security logs, malware scanning, and firewall configuration
Week 4	Creating and configuring virtual machines
Week 5	Linux command-line and system administration exercises
Week 6	Exploring the Kali Linux environment and security tools
Week 7	Hash generation and John the Ripper exercises
Week 8	Midterm Practical Assessment
Week 9	Netcat listeners, connections, and file transfer
Week 10	Bind shell, reverse shell, and manual HTTP request demonstrations
Week 11	Capturing traffic and applying protocol filters
Week 12	Session reconstruction and network investigation exercises
Week 13	Burp Suite installation and proxy configuration
Week 14	Web security testing using OWASP Juice Shop
Week 15	Integrated cybersecurity skills

Learning and Teaching Resources مصادر التعلم والتدريس		
	Text	Available in the Library?
Required Texts	The Web Application Hacker's Handbook by Dafydd Stuttard & Marcus Pinto	Yes

	- Penetration testing by Georgia Weidman - Cybersecurity Essentials by Charles J. Brooks et. al	
Recommended Texts	The Web Application Hacker's Handbook	Yes
Websites	https://www.tryhackme.com	

Grading Scheme مخطط الدرجات				
Group	Grade	التقدير	Marks %	Definition
Success Group (50 - 100)	A - Excellent	امتياز	90 - 100	Outstanding Performance
	B - Very Good	جيد جدا	80 - 89	Above average with some errors
	C - Good	جيد	70 - 79	Sound work with notable errors
	D - Satisfactory	متوسط	60 - 69	Fair but with major shortcomings
	E - Sufficient	مقبول	50 - 59	Work meets minimum criteria
Fail Group (0 – 49)	FX – Fail	راسب (قيد المعالجة)	(45-49)	More work required but credit awarded
	F – Fail	راسب	(0-44)	Considerable amount of work required
Note: Marks Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above.				