MODULE DESCRIPTION FORM

نموذج وصف المادة الدراسية

Module Information معلومات المادة الدراسية					
Module Title	**Network Security / أمنية الشبكات**			**Module Delivery**	
Module Type	**Core**			☒ **Theory** ☒ **Lecture** ☒ **Lab** ☐ **Tutorial** ☐ **Practical** ☐ **Seminar**	
Module Code	CYBT209				
ECTS Credits	**6**				
SWL (hr/sem)	**150**				
Module Level			**Semester of Delivery**	4	
Administering Department	Department of Cybersecurity Technical Engineering		**College**	Technical Engineering College of Computer and Artificial Intelligence - Kirkuk	
Module Leader			**e-mail**		
Module Leader's Acad. Title			**Module Leader's Qualification**		
Module Tutor			**e-mail**		
Peer Reviewer Name			**e-mail**		
Scientific Committee Approval Date	2/11/2026		**Version Number**	1.0	

Relation with other Modules العلاقة مع المواد الدراسية الأخرى			
Prerequisite module	Computer Networks & Operating Systems	**Semester**	3
Co-requisites module	Cryptography & Wireless Security / Penetration Testing	**Semester**	

Module Aims, Learning Outcomes and Indicative Contents أهداف المادة الدراسية ونتائج التعلم والمحتويات الإرشادية	
Module Aims أهداف المادة الدراسية	This module aims to provide students with comprehensive knowledge and technical skills in protecting computer networks and communication infrastructure. It focuses on network threat modeling, security architecture, IPsec, SSL/TLS, firewalls, Intrusion Detection/Prevention Systems (IDS/IPS), Virtual Private Networks (VPNs), Wireless Security (WPA2/WPA3, 802.1X), Email Security (PGP, S/MIME, SPF/DKIM), Network Access Control (NAC), DDoS mitigation, network forensics using Wireshark, and Zero Trust Architecture (ZTA).
Module Learning Outcomes مخرجات التعلم للمادة الدراسية	Understand fundamental network security concepts, CIA triad, threat vectors, and defense-in-depth principles. Analyze network layer security protocols including IPsec (AH, ESP, IKE) and transport layer security (SSL/TLS, HTTPS). Design and configure firewall policies, packet filtering rules (iptables/ufw), and proxy gateways. Deploy, configure, and analyze Intrusion Detection and Prevention Systems (IDS/IPS) using Snort/Suricata. Implement Virtual Private Networks (VPNs) for secure site-to-site and remote access communication. Evaluate wireless network security protocols (WPA2/WPA3, 802.11i) and enterprise authentication (RADIUS/802.1X). Perform network traffic analysis, PCAP packet inspection using Wireshark, and configure Network Access Control (NAC) & DDoS defenses.
Indicative Contents المحتويات الإرشادية	The module will cover the following key areas: Introduction to Network Security, Security Attacks, Services, and Mechanisms (CIA Triad, OSI Security Architecture) Network Layer Security: IPsec Architecture, Authentication Header (AH), Encapsulating Security Payload (ESP), and IKE Transport Layer Security: SSL/TLS Protocols, TLS Handshake, Record Protocol, Certificate Authorities (CA), and HTTPS Firewalls: Packet Filtering, Stateful Inspection, Application Gateways, Firewall Topologies, and Policy Configuration Intrusion Detection and Prevention Systems (IDS/IPS): Signature vs Anomaly-based IDS, Snort Architecture, and Rules Writing Virtual Private Networks (VPNs): Tunneling Protocols, Site-to-Site, Remote Access VPNs (OpenVPN, WireGuard, IPsec VPN) Wireless Security: WPA2, WPA3, 802.11i, EAP Protocols, RADIUS Server, and Rogue AP Detection Email Security: PGP, S/MIME, SPF, DKIM, and DMARC Verification Network Access Control (NAC), AAA Architecture (Authentication, Authorization, Accounting), TACACS+, RADIUS Denial of Service (DoS/DDoS) Attacks: SYN Flooding, UDP Amplification, and DDoS Mitigation Strategies DNS Security (DNSSEC), BGP Routing Security, Network Forensics, Wireshark PCAP Analysis, and Zero Trust Architecture (ZTA)

Learning and Teaching Strategies استراتيجيات التعلم والتعليم	
Strategies	The module will employ a combination of strategies including: Lectures: To provide theoretical foundations on network security protocols, cryptographic implementations, and defense architectures. Group Discussions: To analyze real-world network breach case studies and evaluate firewall policy configurations. Problem-Solving Sessions: To trace cryptographic handshakes (TLS/IPsec), calculate packet overheads, and design secure topologies. Practical Lab Sessions: Hands-on experience configuring firewalls, deploying IDS (Snort), packet analysis (Wireshark), and VPN setups. Tutorials: To practice writing IDS signature rules, iptables configurations, and analyzing PCAP traffic captures. Mid-term and final exams: To evaluate theoretical understanding and technical problem-solving capabilities. Preparatory Week: To give students time to revise and clarify any difficulties before the final exam.

Student Workload (SWL) الحمل الدراسي للطالب محسوب لـ ١٥ اسبوعا			
Structured SWL (h/sem) الحمل الدراسي المنتظم للطالب خلال الفصل	87	**Structured SWL (h/w)** الحمل الدراسي المنتظم للطالب أسبوعيا	2
Unstructured SWL (h/sem) الحمل الدراسي غير المنتظم للطالب خلال الفصل	63	**Unstructured SWL (h/w)** الحمل الدراسي غير المنتظم للطالب أسبوعيا	
Total SWL (h/sem) الحمل الدراسي الكلي للطالب خلال الفصل	150		

Module Evaluation تقييم المادة الدراسية					
		Time/Number	**Weight (Marks)**	**Week Due**	**Relevant Learning Outcome**
Formative assessment	**Quizzes**	2	5% (5)	5, 10	LO #1, 3 and 5
	Assignments	2	5% (5)	2, 12	LO #2, 4 and 6
	Projects / Lab.	1	10% (10)	Continuous	LO #7
	Report	1	10% (10)	13	LO #3, 5 and 7
	Midterm Exam	2 hr	20% (20)	8	LO #1 - 4

Summative assessment	**Final Exam**	2hr	50% (50)	16	All
Total assessment			100% (100 Marks)		

Delivery Plan (Weekly Syllabus) المنهاج الاسبوعي النظري	
	Material Covered
Week 1	Introduction to Network Security: Threat Models, Attack Vectors, Security Services (CIA Triad), and Defense-in-Depth.
Week 2	Network Protocol Security Foundations: Vulnerabilities in TCP/IP Suite (ARP Spoofing, IP Spoofing, TCP Hijacking).
Week 3	Network Layer Security (IPsec) I: IPsec Architecture, Security Associations (SA), Security Parameter Index (SPI).
Week 4	Network Layer Security (IPsec) II: Authentication Header (AH), Encapsulating Security Payload (ESP), Tunnel vs Transport Modes, IKE.
Week 5	Transport Layer Security (SSL/TLS) I: SSL/TLS Architecture, TLS Handshake Protocol, Cryptographic Suite Negotiation.
Week 6	Transport Layer Security (SSL/TLS) II: TLS Record Protocol, Public Key Infrastructure (PKI), Certificate Authorities, HTTPS.
Week 7	Firewall Technologies I: Types of Firewalls (Packet Filtering, Stateful Inspection, Application-Level Gateways).
Week 8	Mid-term Exam (الفصل منتصف اختبار) & Firewall Technologies II: Firewall Topologies (DMZ), Network Address Translation (NAT) Security, Policies.
Week 9	Intrusion Detection Systems (IDS): Signature-Based vs Anomaly-Based Detection, Network-Based IDS (NIDS) Architecture.
Week 10	Intrusion Prevention Systems (IPS): Inline Deployment, Prevention Mechanisms, Snort Architecture, and Custom Rule Writing.
Week 11	Virtual Private Networks (VPNs): Site-to-Site & Remote Access VPNs, OpenVPN, WireGuard, IPsec Tunneling.
Week 12	Wireless Network Security: 802.11 Security Vulnerabilities (WEP), WPA2, WPA3, 802.11i, Enterprise RADIUS/802.1X.

Week 13	Email Security Protocols: PGP (Pretty Good Privacy), S/MIME, SPF (Sender Policy Framework), DKIM, and DMARC.
Week 14	Network Access Control (NAC) & AAA Framework: RADIUS, TACACS+, Identity-Based Access Control.
Week 15	Denial of Service (DoS/DDoS) & Network Forensics: SYN Floods, Amplification Attacks, Scrubbing Centers, Wireshark PCAP Forensics.
Week 16	**Zero Trust Architecture (ZTA), Software-Defined Network (SDN) Security & Final Examination (النهائي الاختبار).**

Delivery Plan (Weekly Lab. Syllabus) المنهاج الاسبوعي للمختبر	
	Material Covered
Week 1	Lab 1: Wireshark Network Traffic Analysis & PCAP Inspection (Capturing HTTP, FTP, Telnet Cleartext Credentials).
Week 2	Lab 2: Configuring Packet Filtering Firewalls (iptables / ufw) and Network Access Control Lists (ACLs).
Week 3	Lab 3: Deploying and Custom Rule Configuration for Intrusion Detection Systems (Snort / Suricata).
Week 4	Lab 4: Setting up Encrypted Tunneling & Virtual Private Networks (OpenVPN / IPsec IKEv2 / WireGuard).
Week 5	Lab 5: SSL/TLS Certificate Authority (CA) Setup, HTTPS Web Server Configuration, and OpenSSL CLI Inspection.
Week 6	Lab 6: Network Scanning, Vulnerability Assessment (Nmap / OpenVAS), and DDoS Attack Simulation & Mitigation.
Week 7	Lab 7: Revision, Network Security Lab Project Presentation, Practical Exam, and Course Assessment.

Learning and Teaching Resources مصادر التعلم والتدريس		
	Text	**Available in the Library?**
Required Texts	Stallings, W. (2017). "Network Security Essentials: Applications and Standards" (6th ed.). Pearson.	Yes
Recommended Texts	Kurose, J. F., & Ross, K. W. (2021). "Computer Networking: A Top-Down Approach" (8th ed.). Pearson.	Yes
Websites	Yes	

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.