Air University

Student ID: 231888

Final Semester Examinations: Spring 2025

Subjective Part
(To be solved on Answer Books only)

Subject: Network Security
Class: BSCYS-F-23
Section(s): A
Course Code: CY-223

Time Allowed: 180 Minutes
Max Marks: 100
FM's Name: Ms. Laraib Javed
FM's Signature:

INSTRUCTIONS

- Attempt responses only in the answer book.
- Nothing is to be written on the question paper.
- Rough work or writing on the question paper will be considered as the use of unfair means.
- Tables/calculators are not allowed.

	Q. No. 1 (CLO1)	Marks
	An e-commerce platform faced a Distributed Denial of Service (DDoS) attack, which disrupted their payment gateway. Traffic analysis revealed volumetric flooding at multiple protocol layers. **Question:** Investigate the types of DDoS techniques used in layered attacks. Discuss the vulnerabilities targeted at each layer (L3, L4, L7) and correlate them with specific protocol weaknesses. Provide examples of tools used by attackers and explain how they exploit these vulnerabilities.	20
	Q. No. 2 (CLO2)	
	A medium-sized company has deployed a Unified Threat Management (UTM) system to improve its network security posture. However, due to improper configuration, several malicious activities have gone undetected, including the attempted download of harmful files from anonymized sources. **Question:** Prepare a complete configuration strategy for the UTM system to ensure strong, layered protection against such threats. Your response should include update management, traffic control logic, scanning policies, and response behaviour. Simulate a scenario in which the configured system successfully detects and blocks a suspicious file download and explain how your configuration contributes to preventing such incidents.	20
	Q. No. 3 (CLO3)	
	A national health organization seeks to protect its wireless infrastructure that handles sensitive patient data. The network is currently based on legacy Wired Equivalent Privacy (WEP) and has suffered repeated unauthorized access incidents.	20

	Question: Design a secure wireless communication architecture that includes encryption standards, authentication protocols, and key management strategies. Explain how your design mitigates legacy vulnerabilities and sustains compliance with data confidentiality requirements.	
	Q. No. 4 (CLO4)	
	A Security Operations Center (SOC) is struggling with unclear incident grading and slow response to cyberattacks. Evaluate current SOC models and incident response frameworks, such as NIST or MITRE ATT&CK, and identify the main issues. Propose a better SOC structure with precise incident classification, response steps, and use of automation, and explain how this would improve response time and overall security operations.	20
	Q. No. 5 (CLO2)	
	A group of students at your university is researching cybercrime marketplaces hosted on the dark web. They use the Tor browser over campus Wi-Fi and begin exploring various .onion domains. Within a few days, the IT department notices network latency, unidentifiable outbound traffic spikes, and IP blocks from academic content providers. The university has asked your team to review and recommend a secure way to support research access to these hidden services without compromising institutional security or violating legal boundaries. **Question:** Design a technical solution to allow controlled access to hidden services (.onion) for academic research. Evaluate the use of tools like Tor and VPNs in this setup and identify their limitations when used in university environments. Justify how your approach balances research freedom with network protection.	20