Air University

Student ID: 231

Mid 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: 120 Minutes
Max Marks: 50
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
A multinational organization reports unauthorized access to its internal systems despite implementing firewalls and intrusion detection systems. Log analysis reveals multiple failed login attempts followed by successful authentication using privileged accounts. i. Classify exploit techniques that adversaries could use to escalate privileges within a networked system. ii. Compare layered defense strategies that should be evaluated to mitigate unauthorized access attempts. iii. Discuss security vulnerabilities in authentication mechanisms that could enable an attacker to bypass access controls.	15
Q. No. 2 (CLO2)	
An organization has implemented Next-Generation Firewalls (NGFWs) to enhance its network security. Despite this, the network has experienced unauthorized access attempts and malware infiltrations. Security analysts have identified potential misconfigurations in the firewall rule base and inadequate traffic inspection mechanisms. As a network security engineer, you are tasked with optimizing the firewall configurations to strengthen the organization's security posture. i. Analyze how access control lists (ACLs) and stateful packet inspection (SPI) should be configured to effectively mitigate unauthorized access attempts without impacting legitimate traffic. ii. Analyze how the firewall rule base should be structured to optimize security without affecting legitimate business traffic.	15

	Q. No. 3 (CLO3)	
	A major online banking platform is experiencing persistent Man-in-the-Middle (MITM) attacks, where attackers intercept and manipulate communications between customers and the bank's servers. Security analysts suspect weaknesses in encryption and authentication mechanisms. i. Express SSL/TLS encryption method to prevent MITM attacks and compare it to IPsec in securing network communications. ii. Determine the role of Public Key Infrastructure (PKI) and Digital Certificates in verifying the authenticity of online banking transactions. iii. Discuss additional security mechanisms that should be implemented to mitigate the risk of MITM attacks in an online banking environment.	20