Air University

(Final-Term Examination: Spring 2025)

Department of Cyber Security

Subject: Network Security
Course Code: CY223
Class: BSCYS F23
Section: B

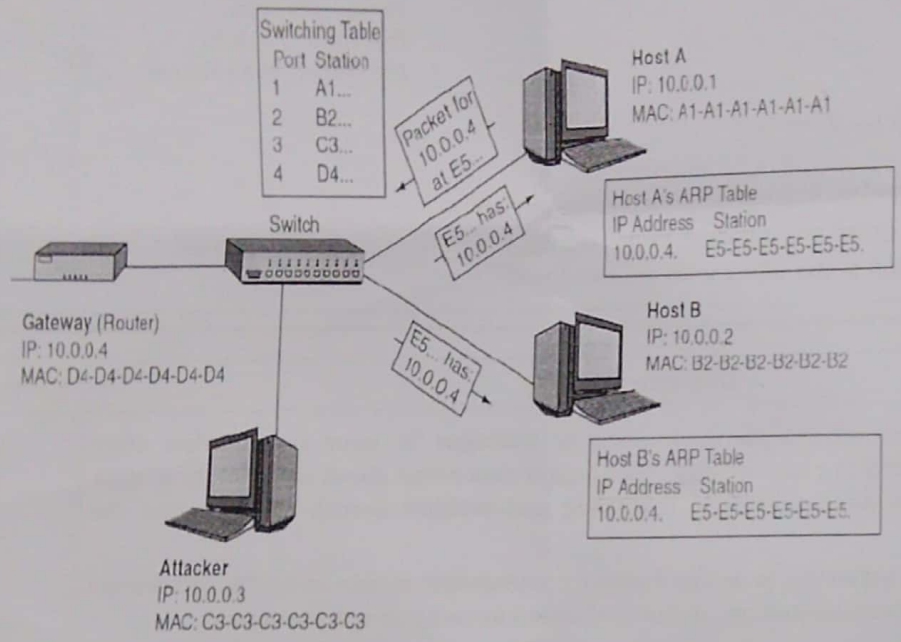
Total Marks: 100
Date: -06-2025
Duration: 3 Hours
FM Name: Hina Batool

Instructions:

- This question paper has 4 questions and page count is 3
- Understanding of questions is part of examination.
- **Return the question paper along with answer sheet.**

Question 1 (CLO 2)	Marks
You have been promoted to Network Security Manager in your organization after demonstrating strong skills in cybersecurity. Your boss is concerned about the security of data exchanged between the headquarters in Islamabad and multiple branch offices across the country. To address this, he has asked you to design a secure communication plan using IPSec to protect against data tampering, eavesdropping, and unauthorized access during transmission. Your task is to briefly explain: a) What is the difference between Authentication Header (AH) and Encapsulating Security Payload (ESP) in IPSec? (10) b) Which protocol—AH or ESP—would you recommend for ensuring data confidentiality during transmission? Justify your answer with relevant arguments. (5) c) What type of IPSec protocol mode you will recommend to your boss for a remote location considering advantages and disadvantages of each: Tunnel mode or Transport mode? Support your answer with strong arguments. (10)	25

Question 2 (CLO 2)	Marks
You are working as a security consultant engineer in an IT company. Management has requested a thorough assessment of the company's network security posture. Provided is a network architecture diagram along with an attack scenario shown in the figure below. Additionally, you have been given a set of parameters to configure the network firewall and apply security settings aimed at protecting the corporate network from identified threats. a) Consider the attack from the Fig given below. Highlight and explain in detail the Address Resolution Protocol (ARP) Poisoning attack. Also propose (at least 3) possible countermeasures (20)	40



b) Configure the ACL according to the following scenario to secure your organization's network from attacks. (20)

i. Consider outbound traffic, configure an ACL rule for "Block ICMP traffic to 192.168.20.0/24"

ii. Consider inbound traffic, configure an ACL rule for "Allow HTTP traffic only from host 203.0.113.5"

iii. Consider outbound traffic, configure an ACL rule for "Permit FTP control traffic from 172.16.0.0/16"

iv. Consider inbound traffic, configure an ACL rule for "Deny traffic from 10.0.5.0/24 except host 10.0.5.100"

Question 3 (CLO 3)	Marks
You have done a great job in highlighting security issues related to ARP poisoning and proposing your solutions. Now your boss has assigned you a critical task of redesigning the company's network infrastructure to enhance security while considering the following requirements and challenges: i. It was observed that employees are connecting their external devices (cell phone, USB, etc.) with office systems. ii. You have the option to use latest security technologies in design. iii. Your design should not leak sensitive information out from organization.	20

iv. No new device should be granted network access without proper authentication. **Your task is to:** a) Keeping in mind the above specifications/scenarios, propose a secure organizational network design. (7) b) Explain each security technology, you are using in network design, with proper headings and examples for clarification to boss. (7) c) How will you manage these security and network devices wisely? Propose a state-of-the art solution to manage all devices. (6)	
Question 4 (CLO 1)	**Marks**
Answer the following: a) Why is Unified Threat Management (UTM) preferred over Next Generation Firewall for small and medium businesses? Support your answer with technical reasoning. (7) b) What is a Peer-to-Peer (P2P) Distributed Denial-of-Service (DoS) attack? How does it work? (8)	15

********** End of Examination Paper **********