Strathmore
UNIVERSITY

SCHOOL OF COMPUTING AND ENGINEERING SCIENCES (SCES)
BACHELOR OF SCIENCE IN COMPUTER NETWORS AND CYBER SECURITY
END OF SEMESTER EXAMINATION
CNS 3105 : NETWORK SECURITY

DATE: 22nd April 2026 Time: 2 Hours

Instructions

1. This examination consists of **FIVE** questions.
2. Answer **Question ONE (COMPULSORY)** and any other **TWO** questions.

QUESTION ONE (30 MARKS)

Case study : AlphaMed Healthcare Network (AHN)

AlphaMed Healthcare Network is a regional medical provider with 5 hospitals and 12 outpatient clinics connected through a wide-area network. AHN recently digitized patient records and deployed a cloud-based telemedicine platform. After a cybersecurity assessment, several security issues were identified:
Hospital networks are connected using MPLS, but internal LANs are flat and unsegmented.
Electronic Health Records (EHR) systems use password-only access and have no session timeout controls.
Medical devices (MRI, infusion pumps, monitors) run outdated operating systems and cannot be patched easily.
Telemedicine servers in the cloud share the same virtual network as public web interfaces.
Backup servers are on the same internal network as production servers, and data is not encrypted.
Wi-Fi networks for staff and visitors share the same controller, with weak WPA2 passwords.
Remote doctors connect to internal systems via a simple VPN login without multi-factor authentication.
No centralized log management or SIEM monitoring exists.
There is no incident response plan or disaster recovery documentation.

Recently, a ransomware attack encrypted one of the clinic's networks.
AHN wants to enhance confidentiality of patient data, comply with HIPAA requirements, and reduce attack surfaces across hospitals.

Required

a)
   i. From the case study, identify four major security vulnerabilities. (4 marks)
   ii. Explain the potential impact of each vulnerability on patient safety and data security. (3 marks)

b)
   i. Hospitals require strict network segmentation. Recommend and justify three segmentation approaches that AHN should implement. (3 marks)
   ii. Draw or describe a segmented network architecture suitable for hospital environments. (3 marks)

c)
   i. Authentication is critical for Electronic Health Records. Explain why password-only authentication is insufficient. (2 marks)
   ii. Propose four strong authentication controls that should replace the current system. (4 marks)

d)
   i. AHN recently suffered a ransomware attack. Describe how ransomware typically spreads in flat networks. (4 marks)
   ii. Propose a ransomware defense strategy including detection, isolation, and recovery. (3 marks)

e)
   i. Wi-Fi networks for staff and guests share the same controller and use weak WPA2 passwords. Explain the threats introduced by this configuration. (3 marks)
   ii. Recommend a secure wireless design for clinical environments. (3 marks)

QUESTION TWO (15 MARKS)

a) Explain the difference between IDS and IPS and where each is deployed. (6 marks)
b) Describe how a TCP SYN flood attack works and give two mitigation techniques. (6 marks)
c) What is the principle of least privilege? (3 marks)

QUESTION THREE (15 MARKS)

a) Explain the concept of Public Key Infrastructure (PKI) and its components. (6 marks)
b) Compare MAC filtering and WPA3 security in wireless networks. (6 marks)
c) List three functions of a VPN (3 marks)

QUESTION FOUR (15 MARKS)

Case Study: Bank Network Security Breach
A financial institution experiences suspicious activities: unauthorized withdrawals, slow network speeds, and abnormal outbound traffic to unknown IPs. Their logs show repeated failed login attempts and malware alerts.

a) Identify five possible attack vectors in this scenario. (8 marks)
b) What indicators of compromise (IoCs) should the security team look for? (7 marks)

QUESTION FIVE (15 MARKS)

a) Explain how Artificial Intelligence and Machine Learning can be integrated into hospital cybersecurity operations. (7 Marks)
b) Design a Zero Trust Security Model for a healthcare network, including at least five core components and explaining how each improves security. (8 Marks)