COURSE CODE: CIT 855
COURSE TITLE: Advanced Cyber-security
COURSE CREDIT: 2 Units
TIME ALLOWED: 2 Hours
INSTRUCTIONS: Answer Question **ONE** (1) and any other **Two** (2) Questions

Question 1: (Compulsory, 30 Marks)
Question 1: (30 Marks)
   i) Explain the CIA triad in cyber security? **(5 marks)**
   ii) Describe three types of malware and their impact on a system. **(5 marks)**
   iii) What is a Man-in-the-Middle attack, and how can it be prevented? **(5 marks)**
   iv) Discuss the role of encryption in ensuring data confidentiality. **(5 marks)**
   v) Compare and contrast qualitative and quantitative risk analysis in cyber-security. **(5 marks)**
   vi) Describe the steps involved in responding to a cyber-security incident. **(5 marks)**

Question 2: (20 Marks)
   a) What are the primary objectives of cyber-security policies? **(3 marks)**
   b) Explain the principle of least privilege and its importance in cyber-security. **(3 marks)**
   c) Describe the process of conducting a cyber-security risk assessment. **(9 marks)**
   d) How does blockchain technology enhance cyber-security? **(3 marks**)
   e) Explain the concept of zero trust security model **(2 marks)**

Question 3: (20 Marks)
   a) What are the main components of an effective incident response plan? **(3 marks)**
   b) Explain the concept of multi-factor authentication (MFA) and its benefits. **(3 marks)**
   c) Describe the role of penetration testing in cyber-security. **(6 marks)**
   d) How does AI contribute to cyber-security defenses? **(3 marks)**
   e) How do cyber threat intelligence (CTI) and threat hunting improve an organization's security posture? **(5 marks)**

Question 4: (20 Marks)
   a) Discuss the challenges associated with securing IoT devices. **(4 marks)**
   b) Explain the difference between symmetric and asymmetric encryption. **(4 marks)**
   c) Describe the significance of data backups and the 3-2-1 backup rule. **(6 marks)**
   d) What are the potential risks of using cloud services for data storage? **(3 marks)**
   e) What are the benefits of using a VPN (Virtual Private Network)**? (3 marks)**

Question 5: (20 Marks)
   a) What are the primary functions of a firewall in network security**? (2 marks)**
   b) Explain the concept of social engineering and provide two examples. **(6 marks)**
   c) Describe the importance of security policies and standards in an organization. **(8 marks)**
   d) How does tokenization help in securing sensitive data? **(4 marks)**