KASNEB

CICT PART III SECTION 6

SYSTEMS SECURITY

THURSDAY: 24 November 2016. **Time Allowed: 3 hours.**

Answer ALL questions. Marks allocated to each question are shown at the end of the question.

QUESTION ONE

(a) Discuss three common wireless security protocols and the encryption methods they support. (6 marks)

(b) Examine six characteristics that make it difficult to eliminate malware. (6 marks)

(c) Describe the application of the following resources in the Open Systems Interconnection (OSI) model:

(i) Network address translation. (2 marks)

(ii) Shielded twisted pair (STP). (2 marks)

(iii) Internet protocol security (IPsec). (2 marks)

(iv) Secure socket layer (SSL). (2 marks)

(Total: 20 marks)

QUESTION TWO

(a) Discuss three factors that influence computer criminals to access unauthorised system assets and information. (6 marks)

(b) Justify why auditing access controls to a system is necessary in an organisation. (4 marks)

(c) For applications such as banking, it might be argued that security is a major concern when implementing a database system.

Required:
Assess five security features that should be included when designing a database system. (5 marks)

(d) Explain five techniques used by cyber criminals to gain unauthorised access to information systems. (5 marks)

(Total: 20 marks)

QUESTION THREE

(a) Discuss three standard applications used to secure email communication. (6 marks)

(b) The government security command intends to share electronic information through public networks, among several hundreds of stations and logistic units spread across the country. The security organ would like to be advised on the best way of ensuring that confidentiality is maintained at the source, during transmission and at the recipient.

Required:
Analyse two techniques of securing the information to ensure confidentiality. (4 marks)

(c) ABC Insurance Company intends to invest in protecting its information, which is a major asset to its business. Being a consultant in this area, you have been invited to advise on the risk analysis process phases that would assist in determining the threats that the company is exposed to.

Required:
Describe five phases of the risk analysis process for ABC Insurance Company. (5 marks)

(d) An organisation intends to install a system that will be used to authenticate and validate data and all entities.

Examine five components of the system described above. (5 marks)

(Total: 20 marks)

QUESTION FOUR

(a) Discuss three types of firewall implementation techniques for data transmission protection. (6 marks)

(b) Analyse four prerequisites for reviewing or assessing a network infrastructure security controls. (8 marks)

(c) Propose six practices that would help in defending against non-physical computer network threats. (6 marks)

(Total: 20 marks)

QUESTION FIVE

(a) Professional and ethical responsibility issues are recognised as being of considerable importance within the development of computerised information systems.

Required:
In relation to the above statement, describe four ethical issues to be considered by systems developers. (4 marks)

(b) Explain three malicious software tools that an attacker could use to obtain information from an ICT system. (6 marks)

(c) Describe the technique used by virtual private network (VPN) in securing information. (2 marks)

(d) Ann Kamau, a manager in XYZ Company has approached you as an ICT specialist to help in gathering evidence from one of the employees' computer suspected to have been used in committing a fraud and later sabotaged.

Required:
Assess four standard digital forensic phases to apply in retrieving the evidence from the sabotaged computer.
(8 marks)

(Total: 20 marks)

.....