kasneb

CICT PART III SECTION 6

SYSTEMS SECURITY

THURSDAY: 20 May 2021. **Time Allowed: 3 hours.**

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

QUESTION ONE

(a) Confidentiality, integrity and availability are the three principles of Information Security.

Required:
Citing appropriate counter measures, analyse each of the above principles. (6 marks)

(b) Describe the following terms in relation to business continuity:

(i) Recovery point objective (RPO). (2 marks)

(ii) Recovery time objective (RTO). (2 marks)

(iii) Work recovery time (WRT). (2 marks)

(iv) Maximum tolerable downtime (MTD). (2 marks)

(c) (i) Stating its function, identify the firewall that operates at the session layer of the OSI model. (2 marks)

(ii) Highlight two advantages and two disadvantages of the firewall described in (c) (i) above. (4 marks)

(Total: 20 marks)

QUESTION TWO

(a) Highlight three basic security events (log) entries that should be logged-in to enable effective tracking of activities. (3 marks)

(b) (i) Evaluate four functions of professional Code of Ethics with specific reference to computing industry. (4 marks)

(ii) One of the clauses of Code of Practice for computer professionals relate to privacy, security and integrity.

Discuss four major contributions of the ICT professionals on the above Code of Practice. (4 marks)

(c) Describe how you could mitigate attacks propagated through use of rainbow table. (3 marks)

(d) Hackers penetrate systems illegally to steal information, modify data or harm the system.

Assess six techniques that hackers may apply to penetrate into a system. (6 marks)

(Total: 20 marks)

QUESTION THREE

(a) An organisation has tasked you to develop an effective information classification program to enable it to meet the ISO 27000 standards.

Required:
Outline the three steps that are necessary for a proper classification program. (3 marks)

(b) Describe the purpose of Digital Signatures. (2 marks)

(c) Highlight three conditions that could cause convert channel. (3 marks)

(d) Differentiate between data diddling and salami techniques. (4 marks)

(e) Describe functions of four protocols that make up the IPSec suite. (4 marks)

(f) Differentiate between "message digest" and "digital signature". (4 marks)

(Total: 20 marks)

QUESTION FOUR

(a) Differentiate between residual risk and total risk stating how their values are determined. (4 marks)

(b) Discuss the three types of security policies in Systems Security. (6 marks)

(c) Justify why it is important to have a Network Interface Card (NIC) configured in a promiscuous mode. (2 marks)

(d) During the business impact analysis, the business continuity committee needs to identify the threats and map them to various characteristics in an organisation.

Required:
Outline five of such characteristics. (5 marks)

(e) Highlight three counter-measures that need to be put in place to mitigate against wormhole attack. (3 marks)

(Total: 20 marks)

QUESTION FIVE

(a) A large telecommunication company that has integrated its financial disbursement application with several financial institutions puts a lot of emphasis on the overall security of its network and transactions on individual employees and third party agents.

Required:
Discuss two administrative controls that the management could use to minimise security exposures that could be attributable to the employees. (4 marks)

(b) Discuss four roles of the person who has the due care responsibilities and may be held responsible for any act of negligence that results in corruption or disclosure of the data. (4 marks)

(c) Discuss the four approaches that could be used to eliminate data remanence. (4 marks)

(d) Differentiate between the two modes of encryption that could be implemented in various networking technologies. (4 marks)

(e) Enumerate four steps used when conducting forensic evidence examination in a storage media. (4 marks)

(Total: 20 marks)

.....