KASNEB

CICT PART III SECTION 6

SYSTEMS SECURITY

THURSDAY: 26 November 2015. **Time Allowed: 3 hours.**

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

QUESTION ONE

(a) Citing an example, discuss a strategy for preventing cross-site scripting security attack. (4 marks)

(b) Documenting evidence is important in handling incidences that affect the normal operations of an information communication technology (ICT) system.

Required:

(i) Explain two reasons for the importance of documenting evidence. (2 marks)

(ii) Highlight two aspects that should be recorded during evidence documentation process. (2 marks)

(c) An organisation is looking for a firewall that could protect it from attacker's exploits such as buffer overflow.

Required:

(i) Describe the type of firewall required to be implemented. (2 marks)

(ii) Explain an advantage and a disadvantage of the firewall identified in (c) (i) above. (2 marks)

(d) Describe the security controls which fall under the following categories:

(i) What they do. (4 marks)

(ii) What they are. (4 marks)

(Total: 20 marks)

QUESTION TWO

(a) Assess four security concerns in cloud computing. (4 marks)

(b) The risk to information processing facilities in an organisation emanating from business processes that involve external third parties should be identified and appropriate controls implemented before granting access.

Required:

Summarise six issues to be considered when identifying risks related to external third party access to an organisation's information system. (6 marks)

(c) A financial institution with several branch networks across Africa intends to exchange data between different servers located in various branches. The institution has sought for your advice in implementing encryption to enable them achieve confidentiality, integrity and non-repudiation by either the sender or recipient.

Required:

Discuss how the type of encryption that you recommend would assist in achieving confidentiality, integrity and non-repudiation. (4 marks)

(d) A financial institution with branches across the country has requested you to look into their network with an aim of eliminating the cyber attacks that have been reported in the recent past. The network should deny inbound access applications and allow some type of remote access.

Required:

Explain the applications and technologies that could be configured to achieve the required security. (6 marks)

(Total: 20 marks)

QUESTION THREE

(a) (i) Describe a technique used by intruders to compromise integrity of audit trails. (3 marks)

(ii) Explain two ways of protecting the integrity of audit trails. (2 marks)

(b) Propose five physical access controls which an organisation could employ to protect its data. (5 marks)

(c) Discuss six processes that are necessary for an effective forensic audit. (6 marks)

(d) Highlight two threats posed to a central database system by each of the following parties:

(i) Users. (2 marks)

(ii) Programmers. (2 marks)

(Total: 20 marks)

QUESTION FOUR

(a) Analyse four methods of testing a disaster recovery plan (DRP). (4 marks)

(b) Computer forensics is an investigative process.

Required:

(i) Explain why the initial response to computer security incident is crucial for a forensic auditor. (2 marks)

(ii) Summarise six activities for securing a suspected computer incidents scene. (6 marks)

(c) As technology improves, users need to be constantly aware of the emerging risks to an organisation information system.

Required:

(i) Analyse four risks associated with owning smart gadgets and use of smart solutions. (4 marks)

(ii) Suggest four viable solutions to the risks identified in (c) (i) above. (4 marks)

(Total: 20 marks)

QUESITION FIVE

(a) Explain how information communication technology could be used by terror groups. (3 marks)

(b) Summarise four activities that could be considered unethical if carried out by a system programmer. (4 marks)

(c) You have been provided with a router, firewall, intrusion detection and prevention system to secure a company's network.

Illustrate how you would place these items in the network to enable secure internet access. (4 marks)

(d) Explain four security threats to web-servers. (4 marks)

(e) (i) Differentiate between "law" and "ethics" as related to systems security. (4 marks)

(ii) Citing a reason, state which one should be held higher between law and ethics. (1 mark)

(Total: 20 marks)

.....