KASNEB

CICT PART III SECTION 6

SYSTEMS SECURITY

THURSDAY: 26 May 2016. **Time Allowed: 3 hours.**

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

QUESTION ONE

(a) A large company with different departments intends to design and implement a computer network that will ensure maximum data security within and across the departments. The company has assigned you this task.

Required:

(i) Describe the measures you would take in designing the network, citing the areas that would be vulnerable to attacks. (2 marks)

(ii) Outline the protective measures that you would put in place. (3 marks)

(b) (i) Describe how a firewall designed to operate in both the network and transport layers of the open systems interconnection (OSI) model works. (2 marks)

(ii) Highlight an advantage and a disadvantage of the network in (b)(i) above. (2 marks)

(c) Explain two security goals that could be achieved by using a symmetric encryption. (4 marks)

(d) Discuss the four strategic choices that are available to an organisation that is faced with risks in its information system. (4 marks)

(e) A financial institution intends to install a point of sale system at the counters to be used by the cashiers to receive and payout money to customers.

Suggest the hardware and software configurations suitable for the point of sale system. (3 marks)

(Total: 20 marks)

QUESTION TWO

(a) ABC Company Ltd. engages purely in an e-commerce mode of carrying out business transactions. The company has a central server at its headquarters located in Nairobi city. The server connects to remote work stations country-wide via the internet infrastructure.

Required:

Discuss three passive attacks that could be used to gather information on the above network infrastructure. (6 marks)

(b) ABC Ltd. is a small financial institution that has no ability to invest in expensive information communication technology (ICT) infrastructure and has decided to outsource all its ICT activities to a third party.

Discuss the security challenges that the company might face in outsourcing this function. (5 marks)

(c) Assess five areas that an organisation needs to analyse and document in a local area network (LAN). (5 marks)

(d) Describe two types of attacks a user would be prone to when carrying out transactions over an instant messaging (IM) platform. (4 marks)

(Total: 20 marks)

QUESTION THREE

(a) Differentiate between "rogue software" and "time bomb software" in the context of system security. (2 marks)

(b) Justify why transmission control protocol (TCP) is harder to spoof than user datagram protocol (UDP). (2 marks)

(c) Explain why fibre optic cable is considered more secure than a twisted-pair cable. (4 marks)

(d) Summarise six items that should be included in a contingency plan. (6 marks)

(e) Wireless local area networks (WLANs) have become common in enterprises.

Describe three threats faced by WLANs and state their corresponding counter measure. (6 marks)

(Total: 20 marks)

QUESTION FOUR

(a) Using an example in each case, discuss the relationship between a threat, vulnerability and a risk in the context of systems security. (6 marks)

(b) Assess how continued evolution of computer hardware and software technology affect an information system auditor's ability to:

(i) Understand controls. (2 marks)

(ii) Collect evidence on the reliability of controls. (2 marks)

(c) Computer ethics and computer laws could be used to reduce criminal and unethical behaviour.

Compare and contrast "computer ethics" and "computer law" in the creation of a healthy computer society. (6 marks)

(d) You are the Chief Information Security Officer (CISO) of ABC Bank which has just developed an information security policy.

Examine four strategies you would use to ensure successful implementation of the policy. (4 marks)

(Total: 20 marks)

QUESTION FIVE

(a) Discuss how certification authority, digital signatures and hash functions relate to create a secure means of communication. (6 marks)

(b) Assume that the likelihood of a risk on an information system is once every five years and the estimated loss is Sh.5 million.

Calculate the maximum cost of a counter measure you would recommend. (4 marks)

(c) Highlight four stenography tools used by hackers. (4 marks)

(d) The internet of things (IOT) system has brought several security challenges.

With reference to the above statement, outline six security challenges associated with IOT systems. (6 marks)

(Total: 20 marks)

.....