kasneb

CICT PART III SECTION 6

SYSTEMS SECURITY

THURSDAY: 24 May 2018. **Time Allowed: 3 hours.**

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

QUESTION ONE

(a) Appraise the use of the following techniques employed in modern non voice telecommunications and digital computer applications:

(i) Block ciphers. (2 marks)

(ii) Stream ciphers. (2 marks)

(b) A sniffer may turn a network card to a promiscuous mode to sniff sensitive information from a network.

With respect to the above statement, assess two major types of sniffing that could be applied while sniffing sensitive data. (4 marks)

(c) Describe two tools a potential hacker might use to analyse traffic on a network and dissect information in transit. (4 marks)

(d) A hacker intends to carry out reconnaissance attacks on an ICT installation.

Discuss two techniques that the hacker is likely to use to establish the existing vulnerabilities. (4 marks)

(e) Being a member of an incident response team, outline the four primary responsibilities that should be undertaken when an incident is reported. (4 marks)

(Total: 20 marks)

QUESTION TWO

(a) Describe four categories of access control services that support the phases of access control implementation. (4 marks)

(b) Asha and Sarah's daily assignment involves exchanging sensitive electronic information that requires maximum protection. The information requires to be verified that it has actually originated from the approved source and has not been tampered with.

Examine the algorithm that Asha and Sarah should apply to ensure that the above requirements are met. (4 marks)

(c) (i) Describe three denial of services attacks. (3 marks)

(ii) Highlight a countermeasure you need to implement to mitigate each of the attacks mentioned in (c) (i) above. (3 marks)

(d) XYZ Insurance Company has identified ICT infrastructure as one of the various business processes that could affect its bottom line in a given financial year. The company needs to carry out a risk assessment on this infrastructure.

Discuss the various phases of the risk assessment that the company plans to undertake in order to safeguard its ICT infrastructure. (6 marks)

(Total: 20 marks)

QUESTION THREE

(a) XYZ Ltd. is a company with three branches in Nairobi town. The general manager of the company has requested you as a security expert to conduct an audit across all systems in the organisation and give a comprehensive report.

Prepare a security checklist with three areas that would guide your audit process. (3 marks)

(b) Mr. Bean, a computer teacher who also offers cyber services in town centre, has been accused of helping in forgery of legal documents using electronic means.

Propose three possible services one could use to take meaningful forensic data for investigation. (3 marks)

(c) XYZ Airport intends to install a security system that will ensure that "something that you are" is used to gain access to sensitive installations within its premises.

Required:
Discuss how you will determine the best device to use in relation to its Cross Error Rate (CER). (8 marks)

(d) An organisation intends to deploy a firewall between its private network and a link to the internet to control malicious traffic from interfering with its operations. The firewall should be able to examine the packet header information from the network to the application layer of the OSI model.

With reference to the above statement:

(i) State the firewall that should be deployed by the organisation. (1 mark)

(ii) Outline the factors that this type of firewall uses to make decisions. (2 marks)

(iii) Describe two strengths and a weakness of this firewall. (3 marks)

(Total: 20 marks)

QUESTION FOUR

(a) An organisation intends to install layer3 virtual private network to secure the information transmission across its branches located in various counties.

Required:
Discuss the layer3 virtual private network (VPN) protocol citing:

- Why it is a popular protocol.
- The different modes that it can operate in.
- Its two primary components or functions.

(6 marks)

(b) Discuss the four components that should be in place for the public key infrastructure (PKI) to function. (8 marks)

(c) Examine four issues that should be addressed to ensure that an organisation's email is used effectively and in accordance to the organisation's expectations. (4 marks)

(d) Explain how creeping privileges could be controlled in an information system. (2 marks)

(Total: 20 marks)

QUESTION FIVE

(a) An organisation intends to set up an Enterprise Resource Planning (ERP) system that will have several users in various locations. They have approached you for advice on the best authentication method to apply in order to secure the ERP system.

Required:
Citing in each case a weakness and a strength, discuss three different types of authentication methods. (6 marks)

(b) Explain an advantage and a disadvantage of the following systems:

(i) Centralised access control system. (2 marks)

(ii) Decentralised access control system. (2 marks)

(c) Cyber security greatly depends on physical security. Attackers who gain physical access to a computer can further the attack.

Discuss four challenges inherent to lack of integration between physical access and cyber security. (4 marks)

(d) XYZ Ltd. plans to set up a data centre that will be used as a cloud computing centre hosting data from various firms that include financial, insurance and manufacturing among others. The management of the company have hired you as a physical security consultant to design the security for this environment.

Citing examples in each case, discuss the functional order of the physical controls that should be put in place. (6 marks)

(Total: 20 marks)

....