kasneb

CICT PART III SECTION 6

SYSTEMS SECURITY

FRIDAY: 27 November 2020. **Time Allowed: 3 hours.**

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

QUESTION ONE

(a) The term "system hardening" is commonly used when there is a need to enhance the security of information systems that are accessed through the internet.

Discuss three things that you need to do to harden a system. (3 marks)

(b) Policy weakness is a catchall phrase for company policies that inadvertently lead to security threats to the network system.

Evaluate six policy issues that could negatively impact on a business's computer system. (6 marks)

(c) Before opening any email attachment, it is advisable you know the source and if not, take some precautions.

Outline four precautions to observe when opening an email attachment. (4 marks)

(d) Malware could be classified in different ways according to different criteria.

Describe two types of malicious software that do not need a host file for propagation. (2 marks)

(e) Describe an example of each of the following e-commerce threats:

(i) Active content. (1 mark)

(ii) Active x object. (1 mark)

(iii) Malicious active content. (1 mark)

(iv) Cyber vandalism. (1 mark)

(v) Javascript. (1 mark)

(Total: 20 marks)

QUESTION TWO

(a) Data storage and retrieval is an important aspect in ensuring the security of an organisation's information.

Examine five database vulnerabilities that should be considered to avert disclosure risks, maintain confidentiality, and ensure data integrity. (5 marks)

(b) In undertaking risk analysis in an organisation, there is a need to provide a standard, quantifiable measure of the impact that a realised threat has on an organisation's assets.

Required:

Discuss the elements that would be used to quantify the impact of the loss when a threat exploits the existing vulnerabilities. (6 marks)

(c) Discuss three types of authentication in the context of system security. (3 marks)

(d) A new organisation, with branches in several counties, has invested in servers and end-user devices. Due to the urgency in securing the ICT installation, the management has requested for implementation of technical security solutions without having standards, procedures and guidelines.

Required:

(i) Outline the three likely outcomes of the technical security solutions in the above scenario. (3 marks)

(ii) Citing three reasons, justify the use of standards, procedures and guidelines in an organisation. (3 marks)

(Total: 20 marks)

QUESTION THREE

(a) Cookies may be used to compromise systems security.

Differentiate between persistent and non-persistent cookies. (2 marks)

(b) Outline three reasons why a security policy is necessary. (3 marks)

(c) (i) Discuss two types of biometric errors in system security. (4 marks)

(ii) Describe a way you could use to determine the type of biometric that provides best protection. (1 mark)

(d) (i) Describe the term "chain of custody" in terms of the forensic evidence. (1 mark)

(ii) Explain five types of information which is normally kept in an evidence log. (5 marks)

(e) Differentiate between residual risk and total risk. (4 marks)

(Total: 20 marks)

QUESTION FOUR

(a) Justify the reason for classifying information as high risk, confidential or public. (2 marks)

(b) Explain the behavior of the following computer viruses:

(i) Boot sector. (2 marks)

(ii) Stealth. (2 marks)

(iii) Polymorphic. (2 marks)

(c) (i) Explain four reasons that make it mandatory to carry out information systems audit. (4 marks)

(ii) Highlight four defense strategies employed in information systems security and audit. (4 marks)

(d) Security attacks are generally classified into four categories namely; interruption, interception, modification and fabrication.

Assess four aspects of the information security attacked in each of the above cases. (4 marks)

(Total: 20 marks)

QUESTION FIVE

(a) In cryptography, a sending party uses cipher to encrypt a secret plaintext into a cipher text, which is sent over an insecure communication channel to the receiving party.

Assess four types of cryptographic attacks. (4 marks)

(b) Explain two work area recovery sites following a disaster. (2 marks)

(c) Intellectual properties may be copyrighted thus the author of the work controls what could be done with the work.

(i) Explain the meaning of "fair use" in relation to copyright. (2 marks)

(ii) Appraise two other rights the property author holds against the copyrighted work. (2 marks)

(d) Assess two issues that need to be addressed when considering adoption of Internet of Things (IoT) devices. (2 marks)

(e) XYZ Microfinance Limited intends to set up a data centre in their six storey building. The management have invited you to advise them on the appropriate location of the data centre and the physical security required to ensure that the equipment are protected adequately.

Required:

(i) Outline three key physical infrastructures that need to be addressed to meet the basic requirements of a data centre. (3 marks)

(ii) State the most appropriate location of the data centre. (1 mark)

(f) Explain two parameters that are used to determine qualitative risk analysis values. (2 marks)

(g) Describe two approaches that could be used to eliminate data remanence. (2 marks)

(Total: 20 marks)

.....