kasneb

CICT PART III SECTION 6

SYSTEMS SECURITY

THURSDAY: 2 September 2021. **Time Allowed: 3 hours.**

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

QUESTION ONE

(a) Outline three advantages and three disadvantages of using an internal auditor in conducting system conformity. (6 marks)

(b) Determine eight stages of an information security audit process. (4 marks)

(c) A company is in the process of developing their business continuity plan (BCP) and disaster recovery plan (DRP).

Required:
Discuss the three recovery sites that the company requires to consider to enable them continue with their operations within the set mean tolerable downtime. (6 marks)

(d) Outline four phases a computer forensics expert needs to undertake during a common investigation process. (4 marks)

(Total: 20 marks)

QUESTION TWO

(a) Mrs Joan, a newly appointed Chief Executive Officer (CEO) in a financial institution has realised the benefits of maintaining accurate data.

Advise Mrs Joan on five strategies that might be applied in an institution to ensure clean data. (5 marks)

(b) Wi-Fi Protected Access (WPA) was developed to provide more sophisticated data encryption and better user authentication than Wired Equivalent Privacy (WEP).

Enumerate five steps a client uses to connect to a WAP secured access point. (5 marks)

(c) You have been appointed by XYZ Limited in a panel to formulate a cryptographic hash function to be applied in message transmission.

Required:

(i) Explain to the panel the meaning of cryptographic hash function. (2 marks)

(ii) Advise the panel on four main properties of a good cryptographic hash function. (4 marks)

(d) Citing four features, justify why IPV6 is more secure than IPV4. (4 marks)

(Total: 20 marks)

QUESTION THREE

(a) Analyse six key objectives of a disaster recovery plan. (6 marks)

(b) Assess six challenges likely to be encountered during an information security risk assessment. (6 marks)

(c) Distinguish the following terms in relation to information security policy:

(i) "Standards" and "practices". (4 marks)

(ii) "Guidelines" and "procedures". (4 marks)

(Total: 20 marks)

QUESTION FOUR

(a) The implementation of information security policy could be achieved in two ways, either using the top-down approach or a bottom-up approach.

Using an organisation structure diagram, assess the two implementation approaches. (6 marks)

(b) Securing an organisation information resources involve developing corporate-wide strategies that you need to employ to better posture the organisation for incident responses.

Assess six strategies an organisation should put in place to ensure effective incidence response. (6 marks)

(c) Describe four ethical behaviours that IT professionals need to commit to. (4 marks)

(d) Giving an example, explain why passive attacks are difficult to detect. (2 marks)

(e) Pretty Good Privacy (PGP) provides the confidentiality and authentication service used for electronic mail and file storage applications.

Suggest two reasons for the wide application of PGP. (2 marks)

(Total: 20 marks)

QUESTION FIVE

(a) (i) Using a sketch, discuss how a smurf attack might be carried out. (3 marks)

(ii) Outline the countermeasure that is needed to address the smurf attack. (1 mark)

(b) Discuss the functionalities of the OSI Layer 4 Security Protocol that uses both symmetric and asymmetric encryption. (4 marks)

(c) Differentiate between certification, accreditation and assurance in the context of systems security. (3 marks)

(d) Mary, a cybercrime investigator and prosecutor at the National Criminal Investigation (NCI) unit, has been called upon to prosecute a case in a court of law based on the previous investigations of a cybercrime committed in a financial system. During the preliminary hearings the magistrate has demanded that she classifies the expected evidence to enable the defence lawyers prepare for the case.

Required:
Describe five types of evidence that Mary could present to the court of law. (5 marks)

(e) Discuss two types of attack that a hacker could use to illegally get information through the web. (4 marks)

(Total: 20 marks)

....