kasneb

CICT PART III SECTION 6

SYSTEMS SECURITY

WEDNESDAY: 27 November 2019. **Time Allowed: 3 hours.**

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

QUESTION ONE

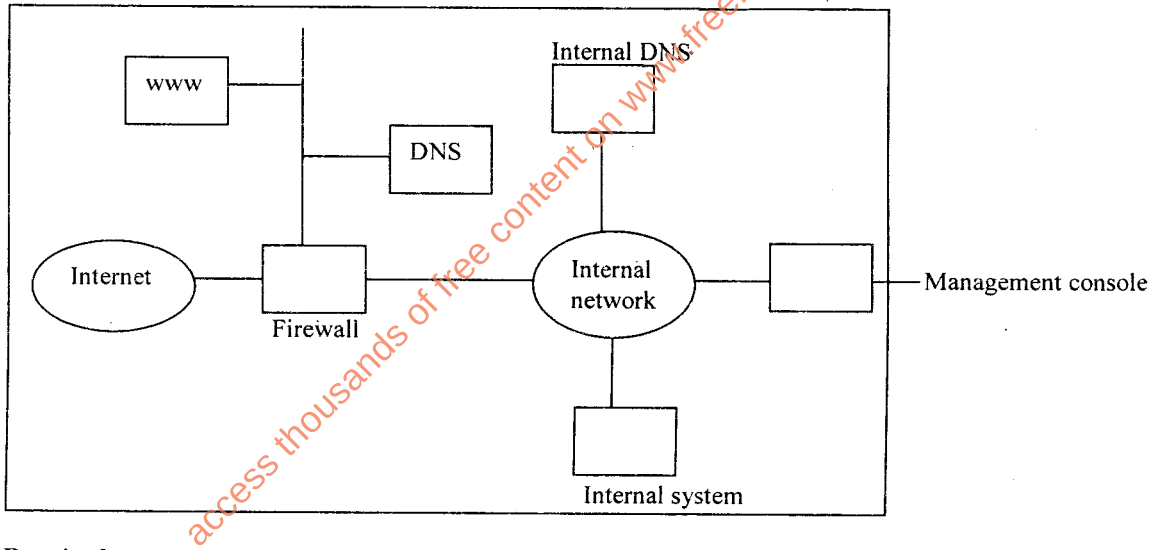
(a) Ethical issues in information systems security could be classified into four categories; property, accuracy, privacy and access.

Formulate a question addressed under each of the above stated classifications. (4 marks)

(b) Risk analysis seeks to assess the expected loss caused by a particular threat.

Citing four benefits, justify the importance of risk analysis tool in preparation for creating a security plan. (4 marks)

(c) Study the given scenario and answer the questions that follow:



Required:

(i) State the network security features that have been used to secure the network. (2 marks)

(ii) List two security features that could have been enforced to enhance security in the above network structure. (2 marks)

(iii) Explain the purpose of the DNS as used in the network structure above. (2 marks)

(iv) Describe how a hacker could gain network intrusion through the domain name system (DNS) reconnaissance technique. (2 marks)

(d) Explain how data encryption is achieved using the following encryption methods:

(i) One time pad cipher. (2 marks)

(ii) Poly-alphabetic system. (2 marks)

(Total: 20 marks)

QUESTION TWO

(a) Propose two policy statements for each of the following:

(i) Access control policy. (2 marks)

(ii) Virus prevention policy. (2 marks)

(b) Your company is expanding with the addition of a new building located across a busy highway from the existing building. The management are not interested in obtaining licensing for radio communication. However security and high transmission rates are highly desirable.

Justify with a reason the transmission medium you would recommend for the company. (2 marks)

(c) Describe two types of intrusion detection system (IDS) that could be used in a corporate network. (2 marks)

(d) Differentiate between mandatory access control and discretionary access control. (4 marks)

(e) Examine the impact of shadow IT in systems security. (3 marks)

(f) Discuss the importance of involving the following departments in the development and enforcement of the security policy in an organisation:

(i) Human resource. (3 marks)

(ii) Legal. (2 marks)

(Total: 20 marks)

QUESTION THREE

(a) Giving an example, explain the term "payload" in system security. (2 marks)

(b) Discuss how you could achieve confidentiality, integrity and non repudiation in encryption. (4 marks)

(c) Describe three areas that certified information security officer needs to consider in implementing a layered physical security. (6 marks)

(d) Discuss two factors that are used to determine risks and vulnerabilities. (4 marks)

(e) A security audit is to be carried out to determine the violation of the laid down policies and procedures.

Discuss four violation factors that should be considered during a system security audit. (4 marks)

(Total: 20 marks)

QUESTION FOUR

(a) An organisation intends to enhance its systems security by ensuring that the Human Resource Department is part and parcel of ensuring that the security policy is adhered to.

Required:

Discuss five human resource management strategies that could be applied to reinforce systems security within the organisation. (5 marks)

(b) ABC Secondary School intends to open a new branch in a different town but the school is going to be managed centrally. You have been invited by the principal to advise on a cipher to be used during data transmission from one branch to another.

Propose five characteristics of a good cipher that you would recommend to the principal. (5 marks)

(c) As an ICT expert, you have been given a tender to supply and install a honey pot in a local county government office.

Required:

(i) Describe honey pot as used in systems security. (2 marks)

(ii) Citing three reasons, argue the case for installing honey pots in the county. (3 marks)

(d) The system security officer in XYZ Sacco has received complaints from different offices regarding some system privileges assigned to them being implemented by other officers. On further analysis, he discovered that there was privilege escalation.

Formulate five strategies required to reduce the problem. (5 marks)

(Total: 20 marks)

QUESTION FIVE

(a) Incident response is an organised approach to addressing and managing the aftermath of a security breach or cyber attack.

Evaluate five criteria that should be considered when deciding whether to include law enforcement in an incident response. (5 marks)

(b) XYZ Financial Services intends to carry out a penetration test to ensure that they have conformed with the ISO 27001 requirements. Being a certified ethical hacker, you have been entrusted to lead the team to undertake the task.

Required:

(i) Describe the three types of scanning that you will be required to undertake. (3 marks)

(ii) State the objectives of undertaking the scanning in (b)(i) above. (2 marks)

(c) (i) Discuss five techniques that attackers could use to penetrate an information system in order to steal, modify the information or to harm the system. (5 marks)

(ii) Propose five methods to counter the attacks stated in (c) (i) above. (5 marks)

(Total: 20 marks)

.....