KASNEB

CICT PART III SECTION 6

SYSTEMS SECURITY

THURSDAY: 25 May 2017. **Time Allowed: 3 hours.**

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

QUESTION ONE

(a) Systems Security covers a wide range of technical issues and behavioural factors in an organisation. Suggest an example of each of the following aspects of systems security:

(i) Prevention. (1 mark)

(ii) Detection. (1 mark)

(iii) Deterrence. (1 mark)

(iv) Recovery. (1 mark)

(b) (i) Using an illustration, describe a model of conventional encryption. (3 marks)

(ii) Identify two problems associated with the model described in (b)(i) above. (2 marks)

(c) ABC Company Ltd. has consulted you as a systems security student to assist in identifying the source of a fraud that has been committed through the internet.

Analyse three common network forensic analysis tools you would apply. (6 marks)

(d) The Accounts Department in your organisation was tasked to work late into the night to meet the financial reporting deadline. You receive a call from an auditor of the organisation informing you that one of the computers has been used to commit fraud.

Required:
As the team leader of the computer incidence reporting team (CIRT), analyse the process that you would follow to restore the operations. (5 marks)

(Total: 20 marks)

QUESTION TWO

(a) Information technology systems are used by multiple individuals in an organisation. This makes it a challenge for a system security manager to trace the source of security policy violations.

Required:

(i) Appraise three audit and accountability control measures that could be enforced in a system to curb the above challenge. (3 marks)

(ii) Assess three identification and authorisation control measures that could be enforced in a system to curb the above challenge. (3 marks)

(b) Discuss four security measures that a company using e-commerce should put in place to ensure safety of the customers during payments. (4 marks)

(c) ICT risk management is not limited to information security, it concerns all ICT related risks.

Identify three areas that could be categorised as IT related risks. (3 marks)

(d) Explain three security related challenges to internet of things (IoTs). (3 marks)

(e) Discuss four issues that distinguish computing professionals' ethics from other professional ethics. (4 marks)

(Total: 20 marks)

QUESTION THREE

(a) Explain the following computer crimes:

(i) Salami slicing. (2 marks)

(ii) Spoofing. (2 marks)

(iii) Piggy backing. (2 marks)

(b) Wireless communications are inherently more difficult to secure than wired transmissions.

(i) Justify the above statement. (4 marks)

(ii) Examine six approaches to mitigate the security issues associated with wireless communications. (6 marks)

(c) A government installation is seeking your expertise in setting up high security system.

Discuss two important administrative aspects that should be taken into consideration. (4 marks)

(Total: 20 marks)

QUESTION FOUR

(a) Assess four goals that should be achieved by a password authentication scheme. (4 marks)

(b) In setting up a distributed system, data transmission is a critical issue that needs to be well addressed by the system security analyst.

Propose four typical requirements of a secure distributed computing system. (4 marks)

(c) XYZ bank is on pilot project to provide its customers with a wireless local area network (WLAN) access within the bank building. The bank manager however is concerned that this move puts the bank at risk from hackers.

Required:
Examine four possible steps that an attacker might use to penetrate to bank system through the customers Wi-Fi. (4 marks)

(d) A new entrant in the financial market intends to develop an ICT security policy that will assist it to achieve defense-in-depth.

Required:
Highlight four policies that are required to be developed for a comprehensive ICT security policy. (4 marks)

(e) Assess the impact that use of computers might have on the evidence attributed to an information system (IS) audit. (4 marks)

(Total: 20 marks)

QUESTION FIVE

(a) Citing two countermeasures in each case, explain the following attacks on an IT infrastructure:

(i) Dictionary attack. (3 marks)

(ii) Brute force attack. (3 marks)

(iii) Spoofing at login. (3 marks)

(b) Outline the steps required in carrying out vulnerability analysis. (3 marks)

(c) XYZ Bank Limited which has over ten million customers runs various services like ATMs, mobile money transfers, agent banking, among others. Taking into consideration the inherent terrorist attack risks across the world, the bank intends to test its disaster recovery plan (DRP) to confirm that it could be implemented in case of a disaster.

Required:
Analyse four types of tests that an organisation could adopt to ascertain that the DRP meets its objective. (8 marks)

(Total: 20 marks)

....