www.masomomsingi.com

kasneb

CICT PART III SECTION 6

SYSTEMS SECURITY

THURSDAY: 23 May 2019. **Time Allowed: 3 hours.**

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

QUESTION ONE

(a) Define the term "wrapping attack" in the context of cloud computing. (2 marks)

(b) Outline the two processes involved in digital signature algorithm. (2 marks)

(c) You have been tasked to recommend a protocol that could be used to secure a remote client server communication.

Required:

(i) Discuss the security options that your proposed protocol is likely to offer. (2 marks)

(ii) State two network attacks that the solution in (c) (i) above would protect the organisation from. (2 marks)

(d) Outline four responsibilities of a Business Continuity Plan team. (4 marks)

(e) Examine why holistic security approach is crucial in Internet of Things (IOT). (2 marks)

(f) Describe how a software developer could secure an application from buffer overflow and convert channel. (2 marks)

(g) (i) State two web application attacks. (2 marks)

(ii) Propose a preventive attack mechanism associated with the web application attacks stated in (g) (i) above. (2 marks)

(Total: 20 marks)

QUESTION TWO

(a) Describe how cookies could be an information security threat in an e-commerce platform. (2 marks)

(b) Explain the contribution of the following informed consent models in protecting individual privacy and information rights of internet users:

(i) Opt-out-model. (2 marks)

(ii) Opt-in-model. (2 marks)

(c) Citing four reasons, support the proposition that protecting information systems is generally difficult. (4 marks)

(d) Assess three ways that a hacker could use to determine if there is a firewall in an organisation's network. (3 marks)

(e) Discuss a strength and a weakness of the encryption method that is vulnerable to the man-in-the middle attack. (3 marks)

(f) A security breach has been reported in a financial institution that need to be investigated and legal action taken on the culprits.

Outline the chain of evidence. (4 marks)

(Total: 20 marks)

QUESTION THREE

(a) Examine four risks associated with the use of smart TVs in organisations. (4 marks)

(b) During a forensics investigation process, there are essential information and information sources that should be reviewed to direct conclusions about the computer user culpability.

Examine four information sources in a forensic audit process. (4 marks)

(c) System security is generally guided by best practice and industry standards.

Enumerate four system security standards. (4 marks)

(d) Ethical behaviour among staff may not just be directed by the existing policies but also by other professional standards.

Describe four ethical behaviours by staff that could support information security management. (4 marks)

(e) Discuss four non-discretionary access control techniques that a system administrator may apply to allow or restrict the access to an organisation's information assets. (4 marks)

(Total: 20 marks)

QUESTION FOUR

(a) ABC Bank intends to reduce or eliminate the risk of its core banking system going down due to cyber attack or any other cause that will affect the CIA triad.

Required:
Discuss the two factors that should be taken into consideration in selecting a safeguard required to mitigate the risks that are likely to affect the system. (4 marks)

(b) Discuss two symmetric encryption algorithms. (4 marks)

(c) Describe two wireless security protocols. (4 marks)

(d) Outline three criteria that an organisation may include in the implementation of the two-man rule technique as a physical security. (3 marks)

(e) A compromised system is a hazard not only to the current user but also to everyone else.

Highlight five malicious activities that could be carried out using a compromised system. (5 marks)

(Total: 20 marks)

QUESTION FIVE

(a) Firewalls monitor and control all communication into and out of an intranet.

Describe three types of controls that it must accomplish in order to effectively achieve its objective. (3 marks)

(b) Describe how IT risk management fits and serves in at least three stages of an information system life cycle. (3 marks)

(c) List three metrics for evaluating data protection. (3 marks)

(d) Enumerate four design guidelines that would guarantee the design of secure systems for an e-commerce transaction. (4 marks)

(e) Recommend three strategic antivirus components that should be inherent in antivirus software tool. (3 marks)

(f) Protection domain is a set of rights for each resource in an IT infrastructure.

Examine two implementations for protection domain citing a limitation in each case. (4 marks)

(Total: 20 marks)

.....

www.masomomsingi.com