TECHNICAL UNIVERSITY OF MOMBASA

INSTITUTE OF COMPUTING AND INFORMATICS

UNIVERSITY EXAMINATION FOR:

BACHELOR OF SCIENCE COMPUTER SCIENCE

BSCS/SEP2023/J-FT

CIT 4209 : COMPUTER SYSTEMS SECURITY
END OF SEMESTER EXAMINATION
SERIES: DECEMBER 2024
TIME :2 HOURS
DATE: Pick Date Dec 2024

Instructions to Candidates
You should have the following for this examination
-Answer Booklet, examination pass and student ID
This paper consists of **FIVE** questions. Attempt question ONE (Compulsory) and any other TWO questions.
Do not write on the question paper.

Question ONE

a) Explain the difference between the following terms: (6 MARKS)
   i) Physical security and Personnel security
   ii) Communications security and Operations security
   iii) Data Integrity and system Integrity

b) State two similarities and two differences between "Information security" and "Cybersecurity" (4 MARKS)

c) Explain the following terms:
   i) Information assets
   ii) Risk
   iii) Threat
   iv) Vulnerability
   v) Hacker (5 MARKS)

c) Explain the roles of the following specialist in information
   i) Intrusion Detection Specialist

ii) Computer Security Incident Responder
iii) Source Code Auditor
iv) Cryptanalyst
v) Penetration Tester (5 MARKS)

d) Smartphones with advanced capabilities of personal computers, are appearing in more people's pockets. Smartphones' popularity and relatively lax security have made them attractive targets for attackers who have been exploiting this expanding market by using old techniques along with new ones.

Required:

Outline any five mobile security issues related to their vulnerabilities. (5 MARKS)

e) Describe any five steps you can take to protect your mobile phone against security threat. (5 MARKS)

Question TWO

a) Describe the following controls for protecting information assets:
i) Logical security controls
ii) Physical and environmental security controls
iii) Information management
iv) Evaluating the effectiveness of the overall security system (8 MARKS)

b) "Authentication and non-repudiation are tools that system designers can use to maintain system security with respect to confidentiality, integrity, and availability. Understanding each of these five concepts and how they relate to one another helps security professionals design and implement secure systems."

Required:

Using suitable examples related to Technical University of Mombasa, explain the five principles of cybersecurity. (10 MARKS)

Question THREE

a) You have been awarded a tender to protect IT systems from cyberattacks.

Required:

Explain to management the difference between the following terms:
i) Firewall and "Intrusion Detection System"
ii) "Host-based Intrusion Detection System" and "Network-based Intrusion Detection System"
iii) "Stateful Inspection Firewall" and "Dynamic Packet Filtering Firewall" (12 MARKS)

b) With an aid of a diagram, describe how you will configure the network and setup the organization's De-Militarized Zone (DMZ). (8 MARKS)

c) Explain the term "Cybersecurity incident" (2 MARKS)

Question FOUR

a) Using Technical University of Mombasa organization hierarchy as case study, explain the role of each layer management regarding cybersecurity.
(8 MARKS)

b) Explain the following types of Cyber Attacks
i) Botnets
ii) Denial of Service
iii) Man-In-The-Middle
iv) Password Cracking
v) Ransomware
vi) Spyware (6 MARKS)

c) Risk handling/mitigation is the application of controls, and counter measures appropriate to the risk, subject to constraints – such as available funds. Explain the following risk handling strategies
i) Risk Avoidance
ii) Risk Retention
iii) Risk Reduction
iv) Risk Transfer (8 MARKS)

Question FIVE
a) Outline the six stages of incident response (12 MARKS)

b) If the business is not kept running in the short-term, then long-term recovery will not be relevant and therefore immediate standby arrangements are critical to the organization's chances of disaster recovery and to the overall costs involved. Explain the following standby arrangements that an organization can put in place:
i) Hot site facilities
ii) Cold site facilities (2 MARKS)

c) Unlike information technology systems in a traditional data center, in cloud computing, responsibility for mitigating the risks that result from these software vulnerabilities is shared between the cloud service provider (CSP) and the cloud consumer.
Explain the following vulnerabilities as a result of a CSP's implementation of cloud computing:
i) Consumers Have Reduced Visibility and Control.
ii) On-Demand Self Service Simplifies Unauthorized Use.
iii) Internet-Accessible Management APIs can be Compromised (6 MARKS)