

UGANDA MARTYRS UNIVERSITY

FACULTY OF SCIENCE

DEPARTMENT OF COMPUTER SCIENCE & INFORMATION SYSTEMS

END OF SEMESTER FINAL ASSESSMENT

SEMESTER I, 2021/2022

SECOND YEAR EXAMINATION FOR BSC IT
(Nkozi, Rubaga, Masaka)

Information Security

CSC 2102

DATE: Thursday, 20th JAN 2022

TIME: 9:30am - 12:30 pm

DURATION: 3HRS

Instructions:

1. Carefully read through ALL the questions before attempting
2. All question carry 25marks
3. Attempt ANY FOUR questions from section B
4. No names should be written anywhere on the examination book.
5. Ensure that your **Reg number** is indicated on all pages of the examination answer booklet.
6. Ensure your work is clear and readable. Untidy work shall be penalized
7. Any type of examination Malpractice will lead to automatic disqualification
8. Do not write anything on the questions paper

Question One

- a) Mention five reasons that Motivate the Rising Cyber-Attacks (10 Marks)
- b) Mention any five advantages of cyber security? (10 marks)
- c) Explain the advantage of the following to the organization as regard to security. (5 Marks)
 - i. Detection Systems
 - ii. Intrusion Prevention Systems.

Question Two

Once Vulnerabilities are not identified in a Network, they put an organization's at risk.

- a) Mention any five common vulnerabilities that Organizations should focus on in order to strengthen their network. (10 marks)
- b) The following are popular models that are designed to develop security policies. Explain what each letter stands for in each model (10 marks)
 - i. CIA Model
 - ii. AAA model
- c) Give examples where each of the above models is applicable in network? (5 marks)

Question Three

- a) Most modern cyberattacks are considered to be blended attacks. Explain how the following attacks occur (12 marks).
 - i. Social Engineering
 - ii. Malware
 - iii. Denial Of Service Attacks
 - iv. SQL Injection
- b) Social Engineer attack can be in multiple, explain how these social engineering attacks may occur in an organization. (13 marks)
 - i. Phishing
 - ii. Vishing
 - iii. Baiting
 - iv. Pretexting
 - v. Scareware
 - vi. Shoulder surfing

Question Four

- a) What do you understand by the term malware? (3 marks)
- b) Explain any five malwares that can disrupt, damage, or gain unauthorized access to a computer system. (10 marks)
- c) What is Distributed Denial of service (DDoS) (3 marks)
- d) Explain the three types of DDoS that can be used to cut off users from a server or network resource (9 marks)

Question Five

- a) What is the use of the following in the network? (10 marks)
 - i. IP address
 - ii. MAC address
 - iii. Network Public IP
 - iv. DNS
 - v. The gateway IP of your network.
- b) What do you understand by the term network attack? (2 marks)
- c) Differentiate between an active and passive attacks (4 marks)
- d) Write notes about the following tool which is used for finding networks and in security auditing. (9 marks)
 - i. Nmap
 - ii. Wire shark
 - iii. Angry IP?

Question Six

- a) As an information security analyst, advice Uganda Martyrs University and other organization that have changed to online delivery on how to improve cyber security? (give 10 ways) (20 marks)
- b) As an information security officer, what techniques would you use in preventing a brute force login attack? (5 marks)

-END-