

**FINAL  
ALTERNATIVE ASSESSMENT**

(COVER PAGE)

Session : April 2021

Programme : Diploma In Computer Science (DCS)

Course : DCS2110: Cybersecurity Fundamentals

Date of Examination : July 26, 2021 (Monday)

Time : 8.00am – 11.00am Reading Time : Nil

Duration : 3 Hours

**Special Instructions :**

This paper consists of **FOUR (4)** questions. Answer **ALL** the questions. **Write ALL your answers** in the foolscap papers.

---

**Note:** 30 minutes is added into the duration of the examination to factor in any connectivity matters and for you to scan and upload your scripts.

Materials permitted : Nil

---

Materials provided : Nil

---

Examiner(s) : Andrew Ho

---

Chief Moderator : Mr Victor Raj

---

*This paper consists of 3 printed pages, including the cover page*

DIPLOMA IN COMPUTER SCIENCE PROGRAMME (DCS)  
DCS2110: CYBERSECURITY FUNDAMENTALS  
FINAL ALTERNATIVE ASSESSMENT: APRIL 2021 SESSION

**Instructions:** This paper consists of **FOUR (4)** questions. Answer all **FOUR (4)** questions. All questions carry equal marks.

**Question 1**

- (a) Define Cybersecurity framework. List the **FIVE (5)** functions commonly included into a Cybersecurity framework. (7 marks)
- (b) Briefly explain **SEVEN (7)** networking countermeasures that can be practiced to defend against cyber network attacks. (7 marks)
- (c) One example of Social Engineering technique is eavesdropping attack.
- (i) List and discuss **TWO (2)** types of eavesdropping attack. (5 marks)
- (ii) Identify and describe **THREE (3)** ways to safeguard against eavesdropping attack. (6 marks)
- (Total: 25 marks)**

**Question 2**

- (a) Identify and briefly explain **SIX (6)** types of cybersecurity risk management treatments. (12 marks)
- (b) Malware is any software intentionally designed to cause damage to a computer, server, client, or computer network.
- (i) Name **SIX (6)** classifications of malware. (6 marks)
- (ii) Describe **FOUR (4)** reasons on why malware infection is widespread over Information System. (4 marks)
- (c) Differentiate the aim of ethical hacking from penetration testing. (3 marks)
- (Total: 25 marks)**

**Question 3**

- (a) With the aid of a diagram, draw and name the **FIVE (5)** phases of ethical hacking.  
(5 marks)
  - (b) Identify and describe **THREE (3)** *physical security* controls mechanisms that is essential for the setup of a physical networking server room.  
(6 marks)
  - (c) List and explain **FOUR (4)** security vulnerabilities of the Operating System.  
(10 marks)
  - (d) Recommend **FOUR (4)** authentication methods that can used to replace password as a more secure authentication approach.  
(4 marks)
- (Total: 25 marks)**

**Question 4**

- (a) List the **THREE (3)** authentication factors.  
(3 marks)
  - (b) Phishing attack techniques are extremely effective in obtaining unauthorized access to sensitive Personal Identifiable Information (PII) of employees in a business organization.
    - (i) Name **TWO (2)** PII that is unique to an employee in a business organization.  
(2 marks)
    - (ii) As the Cybersecurity Manager in your company, recommend and explain **FOUR (4)** countermeasures to protect PII of employees against phishing attack techniques.  
(10 marks)
  - (c) Identify and explain **FOUR (4)** goals of a modern cryptography system.  
(10 marks)
- (Total: 25 marks)**

~ The End ~

*DCS2110 (Final)/April2021*