FINAL
ALTERNATIVE ASSESSMENT

(COVER PAGE)

Session	:	**August 2021**
Programme	:	Diploma in Computer Science (DCS)
Course	:	**DCS2110: Cybersecurity Fundamentals**
Date of Examination	:	6 December 2021 (Monday)
Time	:	8.00am – 10.30am Reading Time : Nil
Duration	:	2 Hours 30 Minutes

Special Instructions :

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

Material permitted :

Non-Programmable Scientific Calculator

Materials provided :

Nil

Examiner(s)	:	**Vasuky Mohanan**
Chief Moderator	:	Victor Raj

*This paper consists of **4** printed pages, including the cover page*

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

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

Question 1

(a) Describe how each Cyber Security framework components work together to address a Cyber Security event. (10 marks)

(b) List **FIVE (5)** types of authentications for a server. (5 marks)

(c) Nowadays, it has become increasingly popular to use Ransomware as a cyber-attack tool.

(i) Ransomware is a special type of malware. Explain **TWO (2)** ways Ransomware is different compared to other types of malwares. (4 marks)

(ii) There are **TWO (2)** types of mechanism that Ransomware uses to execute a cyber-attack. **List and differentiate BOTH.** (4 marks)

(iii) WannaCry is a ransomware attack that spread to 150 countries in 2017. It exploited a particular vulnerability. Describe how this type of vulnerabilities can be minimized / avoided. (2 marks)

(*Total: 25 marks*)

Question 2

(a) One example of Social Engineering technique is Social Networking Sites attack.

(i) Using Facebook as an example, list **FIVE (5)** information that a hacker can gather about a person from their profile. (5 marks)

(ii) Describe a possible scenario how the information collected from part (i) above can be used to initiate a Social Networking Sites attack. (6 marks)

(iii) Suggest **TWO (2)** methods that you would recommend to avoid the scenario described in part (ii) above. (4 marks)

(b) Sniffing is a common method used to attack network communications.

(i) List the **TWO (2)** types of network sniffing

(2 marks)

(ii) Network sniffing can be used for both valid and malicious ways. Describe **TWO (2)** ways network sniffers can be used in a positive manner. (4 marks)

(iii) How can network sniffing lead to spoofing. (4 marks)

(*Total: 25 marks*)

Question 3

(a) Explain the process of Operating System (OS) hardening and why it is necessary. (5 marks)

(b) List **FIVE (5)** techniques used to implement OS hardening. (5 marks)

(c) There are **FIVE (5)** phases in an ethical hacking process. List and describe each phase. (10 marks)

(d) In the company that he works for, Mr John Smith is busy recovering data like documents, photos, and emails from computer hard drives and other data storage devices, such as zip and flash drives for signs of manipulation and documenting it. Is Mr John Smith an ethical hacker, insider threat or a digital forensics investigator? Justify your choice. (5 marks)

(*Total: 25 marks*)

Question 4

(a) Network security is essential in protecting a company's data. Internet Engineering Task Force (IETF) has deprecated Secure Socket Layer (SSL) and replaced it with Transport Layer Security (TLS).

(i) List the modification implemented in TLS and describe why these enhancements were important for network security. (6 marks)

(ii) Other than encryption, Certificate Authorities (CAs) can also authenticate the identity of the owner of a website, adding another layer of security called digital certificate. Explain how a Digital Certificate can provide security for a company's network. (4 marks)

(b) List and describe **FIVE (5)** ways to hack passwords (10 marks)

(c) Explain why physical security is an important aspect in cybersecurity. Give **ONE (1)** example of a physical security measure. (5 marks)

(*Total: 25 marks*)

~THE END~