SULIT

KEMENTERIAN PENDIDIKAN TINGGI
JABATAN PENDIDIKAN POLITEKNIK DAN KOLEJ KOMUNITI

BAHAGIAN PEPERIKSAAN DAN PENILAIAN
JABATAN PENDIDIKAN POLITEKNIK DAN KOLEJ KOMUNITI
KEMENTERIAN PENDIDIKAN TINGGI

JABATAN TEKNOLOGI MAKLUMAT & KOMUNIKASI

PEPERIKSAAN AKHIR

SESI I : 2025/2026

DFC20313 : CYBERSECURITY FUNDAMENTALS

TARIKH : 03 DISEMBER 2025
MASA : 8.30 PAGI - 10.30 PAGI (2 JAM)

Kertas soalan ini mengandungi **DUA PULUH TUJUH (27)** halaman bercetak.
Bahagian A: Objektif (30 soalan)
Bahagian B: Struktur (2 soalan)
Dokumen sokongan yang disertakan : Tiada

JANGAN BUKA KERTAS SOALAN INI SEHINGGA DIARAHKAN

(CLO yang tertera hanya sebagai rujukan)

SECTION B : 55 MARKS

BAHAGIAN B : 55 MARKAH

INSTRUCTION:

This section consists of **TWO (2)** structured questions. Answer **ALL** questions.

ARAHAN:

*Bahagian ini mengandungi **DUA (2)** soalan berstruktur. Jawab **SEMUA** soalan.*

QUESTION 1

SOALAN 1

CLO1 (a) List **TWO (2)** types of cybersecurity studies.

*Senaraikan **DUA (2)** jenis kajian keselamatan siber.*

[2 marks]

[*2 Markah*]

CLO1 (b) Based on the scenario shown in Figure B1(b), answer the following questions.

Berdasarkan senario yang ditunjukkan dalam Rajah B1(b), jawab soalan yang berikut.

Leen Company is a growing e-commerce platform that stores customer data, including personal details, payment information, and purchase history. Recently, the company experienced several suspicious incidents:

- An unknown individual attempted to access the admin portal using stolen credentials.
- A malicious code was found injected into the website's checkout page.
- One of the employees accidentally leaked some customer records through an unsecured email.

The management is now concerned about the company's information security and potential attacks.

Syarikat Leen ialah sebuah platform e-dagang yang sedang berkembang dan menyimpan data pelanggan termasuk maklumat peribadi, maklumat pembayaran, serta sejarah pembelian. Baru-baru ini, syarikat tersebut mengalami beberapa insiden mencurigakan:

- *Seorang individu yang tidak dikenali cuba mengakses portal pentadbir menggunakan kelayakan (credentials) yang dicuri.*
- *Kod hasad telah disuntik ke dalam halaman pembayaran (checkout page) dalam laman web.*
- *Seorang pekerja tanpa sengaja membocorkan rekod pelanggan melalui emel yang tidak selamat.*

Pihak pengurusan kini bimbang tentang keselamatan maklumat syarikat dan potensi serangan.

Figure B1(b) / *Rajah B1(b)*

i. Explain **ONE (1)** information security goal that has been violated.

*Jelaskan **ONE (1)** matlamat keselamatan maklumat yang telah dilanggar.*

[2 marks]

[2 *Markah*]

ii. Explain the type of hacker most likely to be responsible for malicious code injection with **TWO (2)** supporting reasons.

*Jelaskan jenis penggodam yang berkemungkinan melakukan penyuntikan kod hasad beserta **DUA (2)** alasan.*

[4 marks]

[4 *Markah*]

iii. Explain **TWO (2)** types of security threats faced by Leen Company.
*Huraikan **DUA (2)** jenis ancaman keselamatan yang dihadapi oleh Syarikat Leen.*

[4 marks]
[4 *Markah*]

CLO1 (c) Based on the scenario shown in Figure B1(c), answer the following questions.
Berdasarkan senario yang ditunjukkan dalam Rajah B1(c), jawab soalan yang berikut.

> A local university's IT department recently detected unusual activities in its network. First, several employees received phishing emails pretending to be from the IT helpdesk asking for their login credentials. Later, an attacker used the stolen credentials to access confidential research files. The attacker also attempted to overload the university's server with multiple traffic requests, causing temporary service disruption. The security team suspects that this attack followed a cyber kill methodology.
>
> *Jabatan IT di sebuah universiti tempatan telah mengesan beberapa aktiviti luar biasa dalam rangkaian mereka. Pertama, beberapa staf menerima emel pancingan data yang menyamar sebagai pihak meja bantuan IT dan meminta mereka memberikan butiran log masuk. Kemudian, seorang penyerang menggunakan kelayakan yang dicuri untuk mengakses fail penyelidikan sulit. Penyerang itu juga cuba membanjiri pelayan universiti dengan permintaan trafik yang banyak, menyebabkan gangguan sementara pada perkhidmatan. Pasukan keselamatan mengesyaki bahawa serangan ini mengikut metodologi 'cyber kill'*

Figure B1(c) / *Rajah B1(c)*

i. List **FOUR (4)** stages of Cyber Kill Methodology in the correct order.
*Senaraikan **EMPAT (4)** peringkat dalam metodologi 'Cyber Kill' mengikut urutan yang betul.*

[4marks]
[*4 Markah*]

ii. Based on the scenario in Figure B1(c), explain **TWO (2)** types of security attacks that occurred.

*Berdasarkan senario dalam Rajah B1(c), terangkan **DUA (2)** serangan keselamatan yang berlaku.*

[4 marks]

[4 *Markah*]

iii. Based on the scenario in Figure B1(c), phishing emails were used as part of social engineering. Explain **TWO (2)** prevention measures for phishing email attacks.

*Berdasarkan senario dalam Rajah B1(c), emel pancingan data telah digunakan sebagai sebahagian daripada kejuruteraan sosial. Jelaskan **DUA (2)** langkah pencegahan serangan emel pancingan data.*

[5 marks]

[*5 Markah*]

QUESTION 2

SOALAN 2

CLO1 (a) Based on the scenario shown in Figure B2(a), answer the following questions.
Berdasarkan senario dalam Rajah B2(a), jawab soalan yang berikut.

GlobalTech Company is migrating to a new IT system to support its daily operations. The system involves the use of a database server, financial applications and the company's internal network. Recently, the IT administration discovered several challenges:

- Some computers have not been updated with the latest security patches.
- The network segment lacks a strong firewall, leading to intrusion attempts.
- There are also risks to physical equipment such as servers that are exposed to fire hazards and power disruptions.

Syarikat GlobalTech sedang beralih ke sistem IT baharu untuk menyokong operasi hariannya. Sistem ini melibatkan penggunaan pelayan pangkalan data, aplikasi kewangan dan rangkaian dalaman syarikat. Baru-baru ini, pentadbiran IT mendapati beberapa cabaran:

- *Beberapa komputer belum dikemas kini dengan tampalan keselamatan terkini.*
- *Bahagian rangkaian tidak mempunyai perlindungan 'firewall' yang kukuh, menyebabkan beberapa cubaan pencerobohan.*
- *Terdapat juga risiko terhadap peralatan fizikal seperti pelayan yang terdedah kepada kebakaran dan gangguan kuasa.*

Figure B2(a) / *Rajah B2(a)*

i. Classify the **FOUR (4)** types of IT infrastructures.
*Kelaskan **EMPAT (4)** jenis infrastruktur IT.*

[4 marks]
[4 *Markah*]

ii. From the scenario in Figure B2(a), explain **TWO (2)** common infrastructure security measures that could be applied to protect the company's system.
*Berdasarkan senario dalam Rajah B2(a), terangkan **DUA (2)** langkah keselamatan infrastruktur biasa yang boleh digunakan untuk melindungi sistem syarikat.*

[5 marks]
[*5 Markah*]

iii. GlobalTech's system still faces risks from both malware and physical damage to equipment. Explain **TWO (2)** appropriate protection methods that can address these risks.
*Sistem GlobalTech masih berisiko daripada perisian hasad dan kerosakan fizikal terhadap peralatan. Jelaskan **DUA (2)** kaedah perlindungan yang sesuai untuk menangani risiko tersebut.*

[4 marks]
[*4 Markah*]

CLO1 (b) i. Describe **TWO (2)** methods of application security hardening that can be implemented to strengthen software protection.
*Huraikan **DUA (2)** kaedah pengukuhan keselamatan aplikasi yang boleh dilaksanakan untuk memperkukuh perlindungan perisian.*

[5 marks]
[*5 Markah*]

ii. An organization requires stronger access control to protect its sensitive files and systems. Apply **TWO (2)** methods of protecting data that can support this need.

*Sebuah organisasi memerlukan kawalan capaian yang lebih kukuh untuk melindungi fail dan sistem sensitifnya. Laksanakan **DUA (2)** kaedah perlindungan data yang boleh menyokong keperluan ini.*

[5 marks]

[*5 Markah*]

iii. The IT administrator at GlobalTech's system notices that employees often struggle to remember multiple login credentials for various internal systems.

Apply the most appropriate privilege management approach with justification to address this issue.

Pentadbir IT di Sistem GlobalTech mendapati pekerja sering menghadapi kesukaran untuk mengingati pelbagai bukti kelayakan log masuk bagi sistem dalaman yang berbeza.

Laksanakan pendekatan pengurusan keistimewaan yang paling sesuai beserta justifikasi untuk menangani masalah ini.

[3 marks]

[*3 Markah*]

CLO1

(c) Information Assurance (IA) focuses on ensuring that information is reliable, available and protected through five pillars.
Jaminan Maklumat (IA) memastikan maklumat sentiasa boleh dipercayai, mudah diakses apabila diperlukan dan dilindungi melalui lima tonggak utama.

i. State **TWO (2)** of the pillars in Information Assurance.
*Nyatakan **DUA (2)** tonggak dalam Jaminan Maklumat.*

[2 marks]
[*2 Markah*]

ii. Explain **ONE (1)** difference between Information Assurance and Information Security with an example.
*Huraikan **SATU (1)** perbezaan antara Jaminan Maklumat dan Keselamatan Maklumat beserta satu contoh.*

[2 marks]
[*2 Markah*]

SOALAN TAMAT