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 II : 2024/2025

DFC20313 : CYBERSECURITY FUNDAMENTALS

TARIKH : 21 MEI 2025
MASA : 8.30 PAGI - 10.30 PAGI (2 JAM)

Kertas soalan ini mengandungi **DUA PULUH DUA (22)** 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)(i) List **FOUR (4)** sources of security threats.
*Senaraikan **EMPAT (4)** sumber ancaman keselamatan.*

[4 marks]
[4 markah]

CLO1 (a)(ii) Describe **TWO (2)** types of security threats.
*Terangkan **DUA (2)** jenis ancaman keselamatan.*

[3 marks]
[3 markah]

CLO1 (b)(i) List **THREE (3)** types of attack. [3 marks]
Senaraikan 3 jenis serangan. *[3 markah]*

CLO1 (b)(ii) Explain **TWO (2)** types of social engineering with an example. [5 mark]
*Terangkan **DUA (2)** jenis kejuruteraan sosial beserta contoh.* *[5 markah]*

CLO1 (c)(i) List **TWO (2)** roles of a firewall in network security.
*Senaraikan **DUA (2)** peranan firewall dalam keselamatan rangkaian.*

[2 marks]
[2 markah]

CLO1 (c)(ii) Explain about **TWO (2)** security hardening in application
*Terangkan tentang **DUA (2)** pengerasan keselamatan dalam aplikasi*

[4 marks]
[4 markah]

CLO1 (c)(iii) Discuss the cybersecurity implications and law enforcement challenges related to the misuse of VPNs that can be exploited for malicious activities, such as cybercrime.
Bincangkan implikasi keselamatan siber dan cabaran penguatkuasaan undang-undang berkaitan dengan penyalahgunaan VPN yang boleh dieksploitasi untuk aktiviti jahat, seperti jenayah siber.

[4 marks]
[4 markah]

QUESTION 2

SOALAN 2

(a) A company, WebPanel Solutions, provides a web panel service that allows customers to manage their online accounts and access various features. As part of their security assessment, the company needs to identify potential risks that could affect their service and customer data.

Syarikat WebPanel Solutions, menyediakan perkhidmatan panel web bagi membolehkan pelanggan untuk menguruskan akaun di atas talian dan juga capaian kepada pelbagai ciri. Dalam sebahagian daripada penilaian keselamatan, syarikat tersebut perlu mengenalpasti potensi risiko yang boleh mempengaruhi perkhidmatan dan data pelanggan mereka.

CLO1 (a)(i) Identify the **TWO (2)** methods the company could use to identify risks.
*Kenal pasti **DUA (2)** kaedah yang boleh digunakan oleh syarikat untuk mengenal pasti risiko.*

[7 marks]
[7 markah]

CLO1 (a)(ii) Summarize **TWO (2)** types of risks that WebPanel Solutions might encounter in their operations.
*Rumuskan **DUA (2)** jenis risiko yang mungkin dihadapi oleh WebPanel Solutions dalam operasi mereka.*

[7 marks]
[7 markah]

CLO1 (a)(iii) Construct the necessity of continuous security assessments for WebPanel Solutions in the face of evolving cyber threats. In your response, discuss how the company can adapt its security measures based on assessment outcomes, focusing on the following aspects: the dynamic threat landscape, proactive risk management, regulatory compliance, and cost-effectiveness.

Bina keperluan untuk penilaian keselamatan berterusan bagi WebPanel Solutions dalam menghadapi ancaman siber yang semakin berkembang. Dalam jawapan anda, bincangkan bagaimana syarikat dapat menyesuaikan langkah-langkah keselamatannya berdasarkan hasil penilaian, dengan memberi tumpuan kepada aspek berikut: landskap ancaman yang dinamik, pengurusan risiko proaktif, pematuhan peraturan, dan keberkesanan kos.

[8 marks]
[8 markah]

CLO1 (b) A mid-sized organization has recently experienced a data breach caused by employee negligence and insufficient understanding of cybersecurity protocols. The breach exposed sensitive customer information, raising concerns about compliance with data protection laws and the need for a robust information assurance strategy. Explain **FOUR (4)** security awareness and training programs to mitigate future risks.

Sebuah organisasi bersaiz sederhana baru-baru ini mengalami pelanggaran data yang disebabkan oleh kecuaian pekerja dan pemahaman yang tidak mencukupi tentang protokol keselamatan siber. Pelanggaran itu mendedahkan maklumat pelanggan yang sensitif, menimbulkan kebimbangan tentang pematuhan undang-undang perlindungan data dan keperluan untuk strategi jaminan maklumat yang mantap.
*Terangkan **EMPAT (4)** program kesedaran dan latihan keselamatan untuk mengurangkan risiko- risiko pada masa hadapan.*

[8 marks]
[8 markah]

SOALAN TAMAT