SULIT

POLITEKNIK MALAYSIA

BAHAGIAN PEPERIKSAAN DAN PENILAIAN
JABATAN PENDIDIKAN POLITEKNIK
KEMENTERIAN PENDIDIKAN TINGGI

JABATAN TEKNOLOGI MAKLUMAT & KOMUNIKASI

PEPERIKSAAN AKHIR

SESI JUN 2016

DFP4133: INFORMATION SYSTEM SECURITY

TARIKH : 22 OKTOBER 2016
MASA : 8.30 AM - 10.30 AM (2 JAM)

Kertas ini mengandungi **DUA PULUH SATU (21)** 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 A : 45 MARKS
BAHAGIAN A : 45 MARKAH

INSTRUCTION:
This section consists of **THIRTY (30)** objective questions. Mark your answers in the OMR form provided.

ARAHAN:
*Bahagian ini mengandungi **TIGA PULUH (30)** soalan objektif. Tandakan jawapan anda di dalam borang OMR yang disediakan.*

CLO1
C1

1. | Altering or changing data to falsify information.
Mengubah atau menukar data untuk memalsukan informasi. |

Identify the term that match the statement above.
Kenalpasti terma yang menepati kenyataan di atas.

A. Information Warfare / *Peperangan Maklumat*

B. Data Modification / *Pengubahsuaian Data*

C. Information Theft / *Kecurian Maklumat*

D. File Transfer / *Pemindahan fail*

CLO1
C1

2. Select the characteristics of Closed Security Model.
Pilih ciri-ciri yang menggambarkan Model Keselamatan Tertutup.

I. User access is difficult and cumbersome
Capaian pengguna adalah sukar dan rumit

II. Network administrator requires least skills and less time to administer the network
Pentadbir rangkaian memerlukan kurang kemahiran dan masa untuk mentadbir rangkaian

III. Assuming that all users are not trustworthy
Mengandaikan bahawa semua pengguna tidak boleh dipercayai

IV. Not all security measures are implemented
Tidak semua langkah-langkah keselamatan dilaksanakan

A. III, IV
B. I, III
C. II, III
D. II, IV

CLO1 C2

3. Determine the type of threat that occurs when untrusted employee is working on the system database in the company's network?

Kenalpasti jenis ancaman yang berlaku, apabila pekerja yang tidak dipercaya bekerja menggunakan pangkalan data rangkaian syarikat

A. External threat
Ancaman luaran

B. Internal threat
Ancaman dalaman

C. Structured threat
Ancaman berstruktur

D. Unstructured threat
Ancaman tidak berstruktur

CLO1 C2

4. An organisation suspects some of its employees have leaked confidential information to its competitor.

Sebuah organisasi mengandaikan ada seorang pekerja telah membocorkan maklumat sulit kepada pihak pesaing.

Choose the right terminology based on the statement above.

Pilih terminologi yang betul berkaitan dengan kenyataan tersebut.

A. Wrong information
Maklumat yang salah

B. Information Warfare
Peperangan Maklumat

C. Accidental data loss
Kemalangan kehilangan data

D. Unstructured disclosure
Pendedahan oleh pihak tiada kebenaran

CLO1 C3

5. Identify the type of threat occur, when a disgruntle former employee attempt to access the network in order to disclose company new product design?

Kenalpasti jenis ancaman yang berlaku, apabila bekas pekerja yang tidak berpuas hati cuba mencapai rangkaian untuk mendedahkan idea rekabentuk produk baru syarikat?

A. Internal threat
Ancaman dalaman

B. External threat
Ancaman luaran

C. Structured threat
Ancaman berstruktur

D. Unstructured threat
Ancaman tidak berstruktur

CLO1 C4

6. "An attacker conducted and attacked one of Malaysia government web servers by establishing an unlimited ping request to exhaust the server."

"Penyerang mengatur dan menyerang satu pelayan sesawang kerajaan Malaysia melalui penyebaran permintaan ping tanpa had untuk melemahkan sesawang"

Based on the statement above, describe the type of attack that is happening.

Berdasarkan pernyataan diatas, nyatakan apakan jenis serangan yang berlaku.

A. Phishing Attack
Serangan Phishing

B. Recoinnaissance attack
Serangan Recoinnaissance

C. Denial of services attack
Serangan perkhidmatan dinafikan

D. Malicious Code Attack
Serangan kod mencurigakan

CLO2
C1

7. A person who breaks into other people's computers with malicious intentions. Identify the attacker.

Seseorang yang memecah masuk ke dalam komputer orang lain dengan niat jahat. Kenalpasti penyerang tersebut.

A. Hackers
Penggodam

B. Script kiddies
Skrip "kiddies"

C. Cybercriminals
Penjenayah siber

D. Cyberterrorist
Penceroboh siber

CLO2
C2

8. "This tool is used for finding problems in the network and to determine the amount of traffic on the network as a performance measurement."

Alat ini digunakan untuk mencari masalah dalam rangkaian dan untuk menentukan jumlah trafik di rangkaian sebagai ukuran prestasi."

Recognize the tool that can be used for the problem mentioned above.

Kenalpasti alatan yang boleh digunakan untuk masalah di atas.

A. Netstat tool
B. Netscan tool
C. SuperScan tool
D. Hping tool

CLO2 C1

9. Select which of the following is **NOT** a function of firewall.

*Pilih yang manakah antara berikut **BUKAN** merupakan fungsi firewall.*

A. To separate the public and private network
Untuk memisahkan antara rangkaian awam dan persendirian

B. To monitor and detect network activities
Untuk pemantauan dan mengesan aktiviti rangkaian

C. To prevent unwanted traffic
Untuk menghalang data yang tidak dikehendaki

D. To defend against attacks that go through the firewall
Untuk mempertahankan serangan yang melalui firewall.

CLO2 C1

10. This application software runs a simple game on the user's workstation. While the user is occupied with the game, the application mails a copy of itself to every user in the user's contacts email address book. The other users receive the game and then play it, thus spreading the application.

Sebuah perisian aplikasi permainan yang mudah dimainkan pada stesen kerja pengguna. Ketika pengguna leka bermain, aplikasi permainan ini telah menghantar salinannya kepada setiap pengguna dalam buku alamat e-mel kenalan pengguna. Para pengguna lain menerima permainan dan kemudian bermain, lalu terus menyebarkan aplikasi ini.

Identify the malicious code attack described in the statement above.

Kenalpasti serangan kod "malicious" yang diterangkan pada pernyataan di atas.

A. DoS
B. Worm
C. Virus
D. Trojan horse

CLO2
C2

11.

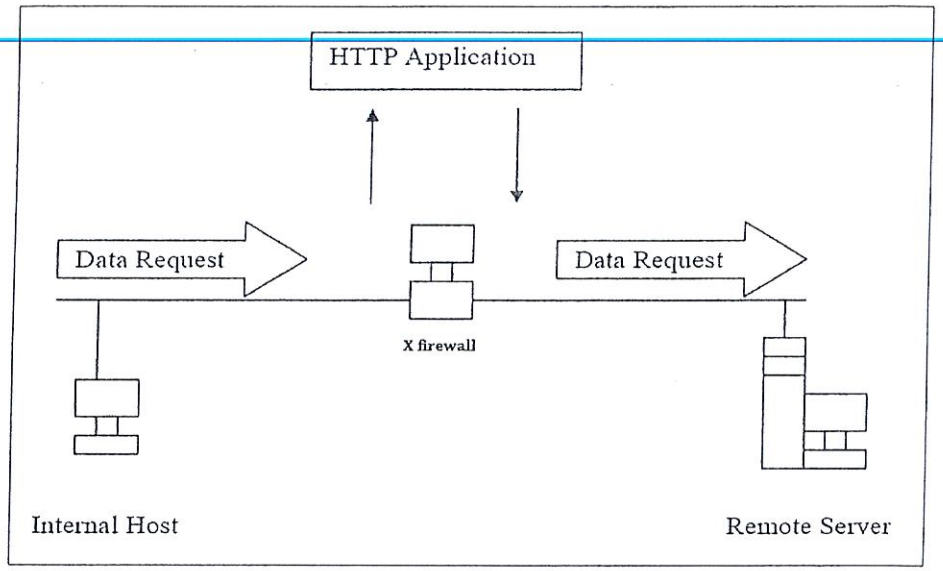

Figure A1 / *Rajah A1*

Based on Figure A1, select the type of firewall x.

Berdasarkan Rajah A1, pilih jenis firewall x.

A. Proxy
B. Application Level
C. Static Packet Filtering
D. Dynamic Packet Filtering

CLO2
C2

12. Identify the statement that shows the difference between Patches and Hotfixes.

Kenalpasti pernyataan yang menunjukkan perbezaan antara Patches dan Hotfixes.

A. Patches bring small changes while Hotfixes usually bring many changes to the software

"Patches" membawa perubahan kecil manakala "Hotfixes" biasanya membawa banyak perubahan kepada perisian.

B. Patches do not bring changes while Hotfixes usually bring many changes to the software

"Patches" tidak membawa perubahan manakala "Hotfixes" biasanya membawa banyak perubahan kepada perisian

C. Both Patches and Hotfixes bring major changes to the software

Kedua-dua "Patches" dan "Hotfixes" membawa perubahan besar kepada perisian

D. Patches bring many changes while Hotfixes usually bring small changes to the software

"Patches" membawa banyak perubahan besar manakala "Hotfixes" biasanya membawa sedikit perubahan kepada perisian.

CLO2
C3

13. It operates by monitoring and potentially blocking the input, output, or system service calls that do not meet the configured policy of the firewall. This firewall is typically built to control all network traffic on any OSI layer.

Ia beroperasi dengan memantau dan berpotensi menyekat input, output atau sistem panggilan servis yang tidak memenuhi konfigurasi polisi firewall. Firewall jenis ini biasanya dibinia untuk mengawal semua jenis trafik rangkaian pada mana-mana lapisan OSI.

Classify the firewall above.

Kelaskan firewall di atas.

A. IP Packet Filtering Firewall
Firewall Tapisan Paket IP

B. Circuit Level Gateway Firewall
Firewall Aras Litar

C. Application Level Firewall
Firewall Aras Aplikasi

D. Dynamic Packet Filtering Firewall
Firewall Tapisan Paket Dinamik

CLO2
C3

14. Recognize the actions needed to harden a host in Figure A2.

Kenalpasti tindakan yang diperlukan untuk menguatkan hos dalam Rajah A2.

> "...Device hardening is a series of actions corporations should take to make all of their hosts more difficult to attack...."
>
> *"...Memperkuatkan peranti merupakan satu siri tindakan yang perlu diambil untuk menjadikan hos lebih sukar diserang...."*

Figure A2 / *Rajah A2*

I. Provide physical security for the host
Menyediakan keselamatan fizikal pada hos

II. Install the OS with secure configuration options
Memasang pilihan konfigurasi yang selamat pada sistem pengoperasian

III. Manages access permissions
Menguruskan kebenaran capaian

IV. Turn on unnecessary services
Menghidupkan perkhidmatan yang tidak diperlukan

A. I, II, and III
B. I, II, and IV
C. I, III, and IV
D. I, II, III, and IV

CLO2
C1

15. Identify the function of Internet Information Service (IIS)?

Kenalpasti fungsi Perkhidmatan Maklumat Internet (IIS)?

A. To surf internet services
Untuk melayari perkhidmatan internet

B. To tell the users what is internet service
Untuk memberitahu pengguna apakah perkhidmatan internet

C. To make Internet Explorer function properly
Untuk memstikan Internet Explorer berfungsi dengan betul

D. To install any types of internet browser
Untuk memasang sebarang jenis pelayar internet

CLO2
C2

16. Choose the benefit of using a Linux based Proxy Server.

Pilih manfaat Server Proksi berasaskan Linux.

A. Allow HTTP proxy services.
Membenarkan perkhidmatan proksi HTTP.

B. Deny HTTP proxy services.
Menghalang perkhidmatan proksi HTTP.

C. Allow FTP service.
Menghalang perkhidmatan FTP.

D. Deny Gopher service.
Menghalang perkhidmatan "Gopher".

CLO2
C2

17. Relate the vulnerabilities issued by Internet Information Services (IIS) in their earlier version.

Kaitkan kelemahan yang menjadi isu utama kepada versi awal "Internet Information Services (IIS)"

A. Love letters
B. Red Code Agent
C. Code Red Worm
D. Denial Of Services (DOS)

CLO2
C3

18. Describe the network connectivity features used in Microsoft Security Server (ISA)

Huraikan ciri-ciri sambungan rangkaian yang digunakan dalam "Microsoft Security Server (ISA)"

A. It changes the traffic protocol based on request.
Menukarkan protokol trafik berdasarkan permintaan

B. It has HTTP proxy, FTP proxy, Direct Mapping and POP3 proxy
Ianya mempunyai konsep proksi HTTP, proksi FTP, pemetaan langsung dan proksi POP3

C. It blocks or allows transmission of packets on the basic of port, IP address and protocol.
Menghalang dan membenarkan perhantaran paket melalui laluan asas, "IP address" dan protokol.

D. It uses Network Address Translation (NAT) and Port Address Translation (PAT) in firewall technology.
Menggunakan "Network Address Translation (NAT)" dan "Port Address Translation (PAT)" dalam teknologi firewall.

CLO3
C1

19. Define cryptography.

Definisikan kriptografi.

A. Study of making the secret codes
Kajian tentang membina kod rahsia

B. Study of breaking the secret codes
Kajian tentang memecahkan kod rahsia

C. The art and science of making secret codes
Seni dan sains dalam mencipta kod rahsia

D. Research or study of making and breaking secret codes
Penyelidikan atau kajian dalam mencipta dan memecahkan kod rahsia

CLO3
C1

20. Give an example of using encryption technologies.

Berikan satu contoh penggunaan teknologi penyulitan.

A. Important in VLAN implementation
Penting dalam penggunaan VLAN

B. Transferring data from sender to receiver
Permindahan data daripada penghantar kepada penerima

C. Communication between firewall and intrusion prevention system (IPS)
Komunikasi antara "firewall" dan "Intrusion Prevention System (IPS)"

D. Important in e-commerce, online banking and online investing.
Penting dalam "e-commerce, perbankan secara talian dan pelaburan secara talian

CLO3
C2

21. Select the advantage of using symmetric encryption on large quantities of data.

Pilih kelebihan menggunakan penyulitan simetri pada kuantiti data yang besar.

A. Speed
Kelajuan

B. Nonrepudiation
Nonrepudiation

C. Uniqueness of the message digested
Keunikan penghadaman mesej

D. Anyone with the public key can decrypt the information
Sesiapa dengan kunci awam boleh didekripsi maklumat tersebut

CLO3
C2

22. Example of Symmetric Key Algorithm includes the following:
Contoh Algoritma Kunci Simetri melibatkan perkara berikut:

I DES
II. Triple-DES
III. RSA
V. DSA

A. I and II
B. II and III
C. III and IV
D. I and IV

CLO3
C2

23. Encryption scheme has several elements. Choose the **CORRECT** elements in encryption.

*Skema penyulitan mempunyai beberapa elemen. Pilih elemen yang **BETUL.***

I. Authentication / *Pengesahan*
II. Encryption Algorithm /*Algoritma penyulitan*
III. Decryption Algorithm /*Algoritma Penyahsulitan*
IV. Key /*Kunci*

A. I, II and III
B. I, II and IV
C. I, III and IV
D. II, III and IV

CLO3
C3

24. Using the Substitution Cipher method, choose the ciphertext for the message 'WE LOVE POLYTECHNICS' encrypted with the keyword "ZERO".

Dengan menggunakan kaedah 'Substitution Cipher', pilih kod sulit 'WE LOVE POLYTECHNICS' yang disulitkan menggunakan kata kunci 'ZERO'.

A. VA ILUA MLIXSBRDKFRQ

B. VA ILUA MKIXSARDLFRQ

C. VA ILUA MLIXSARDKFRQ

D. VA KLUA MIIXSARDKFRQ

CLO3
C3

25. "It referred to as a private key or secret key which is based on a single key and algorithm being shared between the parties who are exchanging encrypted information."

"Ia merujuk kepada kunci peribadi atau kekunci rahsia yang berdasarkan satu kunci dan algoritma yang dikongsi antara pihak-pihak yang bertukar-tukar maklumat yang disulitkan tersebut."

Based on the statement above, determine the class of key based on encryption algorithm.

Berdasarkan kenyataan diatas, tentukan kelas kunci algoritma enkripsi:

A. Symmetric Algorithm
Algoritma Symmetrik

B. Asymmettric Algorithm
Algoritma Asymmettrik

C. Synchronous Algorithm
Algoritma Synchronous

D. Asynchronous Algorithm
Algoritma Asynchronous

CLO3
C3

26. Tunnelling is used to describe a method of using an internetwork infrastructure to transfer a payload. Tunneling is also known as_____.

Terowong yang digunakan untuk menggambarkan satu kaedah menggunakan infrastruktur internetwork untuk memindahkan muatan. Terowong ini juga dikenalpasti sebagai _____.

A. An optional feature that increases network performance when turned on
Satu ciri pilihan yang meningkatkan prestasi rangkaian apabila dihidupkan

B. The encapsulation of packets inside packets of different protocol to create and maintain the virtual circuit.
Pengkapsulan paket dalam paket protokol yang berbeza untuk mencipta dan mengekalkan litar maya.

C. A method that use by a system administrator to detect hackers on the network
Kaedah yang digunakan oleh pentadbir sistem untuk mengesan penceroboh pada rangkaian.

D. A marketing strategy to sell VPN products cheaply in return for expensive service contracts.
Strategi pemasaran untuk menjual produk VPN dengan harga yang murah sebagai pulangan kepada kontrak perkhidmatan yang mahal.

CLO3 C1

27. A server administrator wants to install multiple hardisks and requires all of them to have the same copy. Which RAID level must be implemented?

Seorang pengurus server mahu memasang beberapa cakera keras dan perlu semua storan itu mempunyai kandungan yang sama. Tahap RAID yang mana perlu digunakan?

A. RAID 0
B. RAID 1
C. RAID 2
D. RAID 5

CLO3 C2

28. Identify the device used as an electrical equipment that provides emergency power to load when the input power source fails.

Kenalpasti peralatan yang digunakan sebagai peralatan elektrik yang memberikan kuasa tambahan untuk bebanan apabila sumber kuasa input gagal.

A. Redundant server
B. RAID
C. UPS
D. Clustering

CLO3 C2

29. The following technologies are used to handle server disaster **EXCEPT**

Teknologi berikut digunakan untuk mengendalikan server jika terjadi bencana ***KECUALI***

I. RAID
II. IIS
III. IDS
IV. Redundant server

A. I and III
B. I and IV
C. II and III
D. II and IV

CLO3
C3

30. You are trying to rearrange your backup procedures to reduce the amount of time taken for each backup. Which backup system will back up only the files that have changed since the last backup?

Anda sedang cuba untuk menyusun semula prosedur sandaran untuk mengurangkan jumlah masa yang diambil untuk setiap backup. Sistem sandaran manakah yang hanya akan menyimpan fail yang telah berubah sejak sandaran terakhir?

A. Full backup
Sandaran penuh

B. Incremental backup
Sandaran bertambah

C. Differential backup
Sandaran berbeza

D. Backup server
Server sandaran

SECTION B: 55 MARKS

BAHAGIAN B: 55 MARKAH

INSTRUCTION:
This section consists of **TWO (2)** structured questions. Answer all the questions.

ARAHAN :

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

QUESTION 1

SOALAN 1

CLO1
C1

a) i. "The goals of any security design is to provide maximum security with minimum impact on user access and productivity."

"Matlamat mana-mana reka bentuk keselamatan adalah untuk menyediakan keselamatan maksimum dengan kesan yang minimum kepada capaian pengguna dan produktiviti."

Based on the above statement, identify and explain **TWO (2)** types of general security models.

*Berdasarkan kenyataan di atas, kenalpasti dan terangkan **DUA (2)** jenis model keselamatan umum.*

[4 marks]
[*4 markah*]

CLO1
C2

ii. Explain briefly each of the following terms:
Terangkan secara ringkas setiap yang berikut:

- Data Disclosure / *Pendedahan Data*
- Data Modification / *Pengubahsuaian Data*
- Data Availability / *Ketersediaan Data*

[3 marks]
[*3 markah*]

b) i. Differentiate the following types of threats listed below:

CLO1
C1

Bezakan jenis ancaman berikut :

i) Unstructured threat / *Ancaman tidak berstruktur*

ii) Internal threat / *Ancaman dalaman*

[2 marks]
[*2 markah*]

CLO1
C4

ii.

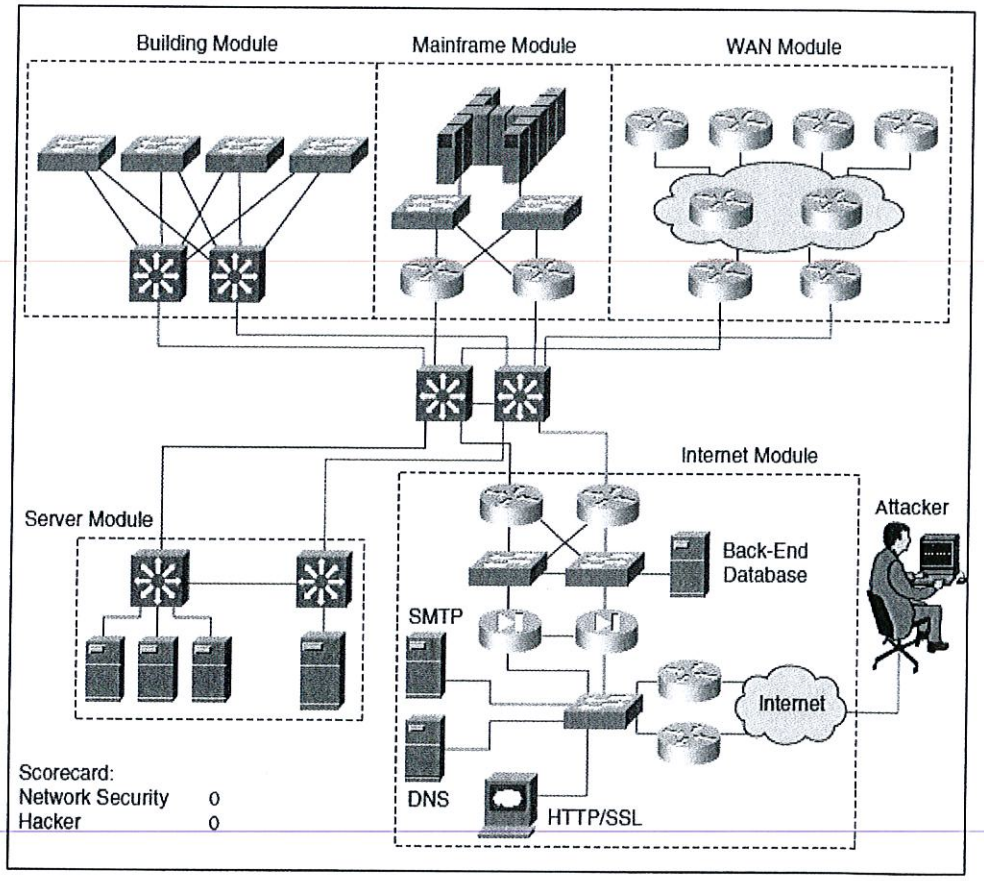

Figure B1 / *Rajah B1*

Based on Figure 2 above, describe and explain the types of attacks?

Berdasarkan Rajah 2 nyatakan dan jelaskan apakah jenis serangan.

[3 marks]
[*3 markah*]

CLO2 C2

c) Explain briefly what you understand by the term "phishing".
Terangkan secara ringkas apakah yang anda faham tentang isttilah "phishing".

[3 marks]
[*3 markah*]

CLO2 C1

d) i. State the **THREE (3)** common technologies employed in building firewall.
*Nyatakan **TIGA (3)** teknologi yang biasa digunakan dalam membina tembok api.*

[3 marks]
[*3 markah*]

CLO2 C2

ii. Explain **FIVE (5)** features of personal firewall.
*Terangkan **LIMA (5)** ciri-ciri "personal firewall".*

[5 marks]
[*5 markah*]

CLO2 C3

iii. Explain how Dynamic Packet Filtering works.
Terangkan bagaimana "Dynamic Packet Filtering" befungsi.

[3 marks]
[*3 markah*]

QUESTION 2

SOALAN 2

CLO2 C1

a) i. Explain **TWO (2)** criteria in account policy.
*Terangkan **DUA (2)** kriteria polisi akaun.*

[4 marks]
[4 markah]

CLO2 C3

ii. List **THREE (3)** differences between Packet Filter and Proxy Server.
*Senaraikan **TIGA (3)** perbezaan di antara "Packet Filter" dan "Proxy Server".*

[3 marks]
[3 markah]

CLO3 C1

b) i. Define the following cryptographic terminologies:
Takrifkan terminologi bagi kriptografi berikut:

i) Plaintext
ii) Ciphertext
iii) Encryption
iv) Decryption
v) Cryptanalyst

[5marks]
[5 markah]

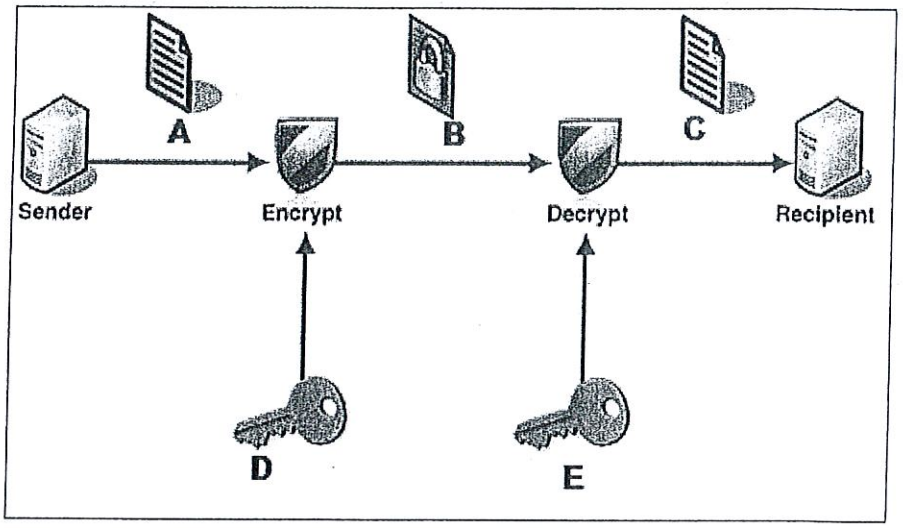

Figure B2 / *Rajah B2*

CLO3
C2

ii. Referring to Figure B1 above, identify A, B, C, D and E with the suitable terms.

Merujuk kepada Rajah B1 di atas, kenalpasti A, B, C, D dan E dengan terma yang sesuai.

[5 marks]
[*5 markah*]

CLO3
C3

iii. A Virtual Private Network (VPN) is a private network that uses a public network (the Internet) to connect users. Explain **THREE (3)** features of good VPN product.

*Virtual Private Network (VPN) adalah rangkaian persendirian yang menggunakan rangkaian umum (Internet) untuk menghubungkan pengguna. Terangkan **TIGA (3)** ciri produk VPN yang bagus.*

[5 marks]
[*5 markah*]

CLO3 C1

c) i. List **TWO (2)** characteristics of synchronous system.

*Senaraikan **DUA (2)** ciri-ciri synchronous system.*

[2 marks]

[*2 markah*]

CLO3 C2

ii. Uninterruptible Power Supply (UPS) is also known as battery backup to provide emergency power supply when utility power is not available. Choose and explain **THREE (3)** common power problems.

*Uninterruptible Power Supply (UPS) juga dikenali sebagai sandaran bateri untuk menyediakan bekalan kuasa kecemasan apabila kuasa utiliti tidak boleh didapati. Pilih dan terangkan **TIGA (3)** masalah kuasa yang sering berlaku.*

[3 marks]

[*3 markah*]

CLO3 C3

iii. Redundant Array of Independent Disk (RAID) is a group of disk drives which utilizes two or more hard drives. There are several levels of RAID. Illustrate RAID level 5.

Redundant Array of Independent Disk (RAID) adalah sekumpulan pemacu cakera yang menggunakan dua atau lebih pemacu keras. Terdapat beberapa tahap RAID.
Lukiskan RAID tahap 5.

[2 marks]

[*2 markah*]

SOALAN TAMAT