19

SULIT

POLITEKNIK MALAYSIA

BAHAGIAN PEPERIKSAAN DAN PENILAIAN
JABATAN PENDIDIKAN POLITEKNIK
KEMENTERIAN PENDIDIKAN TINGGI

JABATAN TEKNOLOGI MAKLUMAT & KOMUNIKASI

PEPERIKSAAN AKHIR

SESI DISEMBER 2017

DFN6223 : NETWORK SECURITY

TARIKH : 01 APRIL 2018
MASA : 8.30 PAGI - 10.30 PAGI (2 JAM)

Kertas ini mengandungi **LAPAN BELAS (18)** 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)

SULIT

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.*

1. Identify the importance of security for networking system.
Kenalpasti kepentingan keselamatan untuk sistem rangkaian.

CLO1
C1

A. As a backup when network system fails.
Sebagai sandaran apabila sistem rangkaian mengalami masalah.

B. As an assurance that the network has been detected by the management.
Sebagai jaminan bahawa rangkaian telah dikesan oleh pihak pengurusan.

C. To ensure all data in the network cannot be detected by hackers.
Untuk memastikan semua data dalam rangkaian tidak dapat dikesan oleh penggodam.

D. To implement applications that can protect the network from unauthorized access.
Untuk melaksanakan aplikasi yang boleh melindungi rangkaian daripada capaian yang tidak dibenarkan.

CLO1
C1

2. Select an example of information theft.
Pilih satu contoh pencurian maklumat.

A. Sending virus that reformats a computer's hard drive.
Menghantar virus yang memformat cakera keras computer.

B. Leaking confidential information such as new product plan to competitor.
Membocorkan maklumat sulit seperti pelan produk baru ke pesaing.

C. Stealing an organization's propriety information such as research and development data.
Mencuri maklumat milik organisasi seperti maklumat penyelidikan dan pembangunan.

D. Getting private information such as identification number, without any permission.
Mendapatkan maklumat sulit contoh nombor peribadi tanpa kebenaran.

CLO1
C2

3. Select the characteristics of Open Security Model.

Pilih ciri-ciri Model Keselamatan Terbuka.

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

II. Users do not have the access to all areas.
Pengguna tidak dapat memasuki semua bahagian.

III. Assume that all users are to be trusted.
Mengandaikan bahawa semua pengguna boleh dipercayai

IV. All security measures are implemented.
Semua langkah-langkah keselamatan dilaksanakan.

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

CLO1
C4

4. Mr. Wong got a private information (pin Number) without the owner permission. Based on the given situation, determine the type of threat involved.

En Wong telah memperolehi maklumat peribadi (nombor pin) tanpa kebenaran pemiliknya. Berdasarkan situasi ini, tentukan jenis ancaman yang terlibat.

A. Data Modification / P*engubahsuaian data*

B. Information Theft / *Kecurian maklumat*

C. Information Warfare / *Peperangan maklumat*

D. Unauthorized disclosure / *Pendedahan yang tidak dibenarkan*

CLO1
C1

5. Identify the type of threat that occurs when competitors attempt to gain access to your network.

Kenal pasti jenis serangan yang berlaku apabila pesaing cuba mendapatkan akses kepada rangkaian anda

A. Internal threat / *Ancaman dalaman*

B. External threat / *Ancaman luaran*

C. Structured threat / *Ancaman berstruktur*

D. Unstructured threat / *Ancaman tidak berstruktur*

CLO1
C4

6. A network engineer for company ARENA Sdn. Bhd. has been assigned to configure a new purchase firewall from their IT Vendor. During the configuration time, he sets the username and password for the admin to access the firewall as below:

username : ARENA
Password : ARENA123

Analyzed on the above situation. Determine the type of weakness that occurred.

Seorang jurutera rangkaian untuk ARENA Sdn. Bhd. telah ditugaskan untuk mengkonfigurasi firewall baru yang dibeli daripada penjual IT mereka. Semasa konfigurasi, dia menetapkan nama pengguna dan kata laluan untuk admin untuk mengakses firewall seperti seperti di bawah:

username : ARENA
kata laluan : ARENA123

Analisis situasi di atas. Tentukan jenis kelemahan yang berlaku.

A. Self-Weakness / *Kelemahan diri*
B. Security Policy Weakness / *Kelemahan polisi keselamatan*
C. Technology Weakness / *Kelemahan teknologi*
D. Configuration Weakness / *Kelemahan konfigurasi*

CLO2
C2

7. An attacker conducted and attacked one of Malaysian government web servers by establishing an unlimited ping request to the server. Based on the statement above, identify the type of attack.

Penyerang mengatur dan menyerang satu daripada pelayan sesawang Kerajaan Malaysia melalui penyebaran permintaan ping tanpa had kepada pelayan digunakan.
Berdasarkan penyataan di atas, kenalpasti jenis serangan yang telah berlaku.

A. Phishing Attack / *Serangan Phishing*
B. Reconnaissance Attack / *Serangan peninjauan*
C. Malicious Code Attack / *Serangan kod mencurigakan*
D. Denial of Service Attack / *Serangan perkhidmatan dinafikan*

CLO2
C2

8. Explain how to identify that you are a victim of Denial-of-Service (DoS) attack.
Terangkan bagaimana anda kenal pasti bahawa anda adalah mangsa kepada serangan Denial-of-Service (DoS).

A. Too many numbers of open ports.
Banyak bilangan port yang terbuka.
B. Power failure.
Kegagalan kuasa.
C. Dramatic increase in the number of spam emails received.
Peningkatan mendadak bilangan e-mel spam yang diterima.
D. Inability to access any websites.
Kegagalam mengakses mana-mana laman web.

CLO1
C2

9. Summarize the process of tightening down or increasing the security of an individual host in network security with appropriate security approach below.
Simpulkan proses mengetatkan atau meningkatkan keselamatan hos individu dalam keselamatan rangkaian dengan pendekatan keselamatan yang sesuai di bawah.

A. Device hardening / *Sekatan peranti*
B. Server management / *Pengurusan pelayan*
C. Network security / *Keselamatan rangkaian*
D. Software hardening / *Sekatan aplikasi*

CLO1
C3

10. Ilham Bena Sdn Bhd wants to keep their network from unwanted visitors while still giving their legitimate users the internet access. Determine the types of network protection that can be applied in the company?

Ilham Bena Sdn Bhd ingin menapis pengguna yang memasuki rangkaian mereka tetapi dalam masa yang sama membenarkan pengguna yang sah menggunakan internet tersebut. Kenal pasti jenis perlindungan rangkaian yang sesuai untuk dibina pada syarikat tersebut?

A. Gateway

B. Bastion Host

C. Application server

D. Firewall with proxy server

CLO1
C4

11 Bill wishes to communicate with Jane over the Internet, but a firewall exists on his network. Bill is not authorized to communicate with the firewall. He connects to the proxy on his network and sends the information about the connection he wishes to make to Jane. The proxy opens a connection through the firewall and facilitates the communication between Bill and Jane. From the situation, choose the type of proxy server that can be applied?

Bill berhasrat untuk berkomunikasi dengan Jane melalui Internet, akan tetapi rangkaian Bill terdapat satu firewall. Bill tidak boleh berkomunikasi dengan firewall itu sendiri. Bill melayari satu proxy dan menghantar maklumat berkenaan komunikasi yang ingin dijalankan dengan Jane. Proxy ini membuka satu laluan pada firewall bagi membolehkan mereka berkomunikasi. Dari situasi tersebut, pilih apakah jenis pelayan proxy yang digunakan?

A. SOCKS
B. Squid
C. Windows Proxy
D. The TIS Firewall Toolkit

CLO2
C2

12. Your company is very concerned about security. You have decided to install a system that monitors traffic in and out of your network and automatically alerts you when suspicious traffic patterns occur, indicating a possible unauthorized intrusion attempt. Identify the name of this system.

Syarikat anda amat menitikberatkan tentang keselamatan. Anda ingin memasang satu sistem yang memantau pergerakan data keluar dan masuk dari rangkaian dan secara automatik boleh memaklumkan pentadbir jika terdapat pergerakan data yang berbahaya, yang menunjukkan kemungkinan terjadi pencerobohan. Kenalpasti nama sistem tersebut.

A. Intrusion Alert Detector
Penggera pengesan pencerobohan

B. Defensive Alarm System
Sistem pengggera pertahanan

C. Intrusion Detection System
Sistem pengesan pecerobohan

D. Network Detection System
Sistem pengesan rangkaian

CLO2
C3

13. "The design philosophy of X is to scan network packets at the router or host-level, auditing packet information, and logging any suspicious packets into a special log file with extended information". Analyze the statement and identify X.

"Falsafah reka bentuk X ialah untuk mengimbas paket rangkaian pada penghala atau peringkat perumah mengaudit maklumat paket, membuat log untuk mana-mana paket yang mencurigakan ke dalam fail log khusus dengan maklumat lanjutan". Analisa penyataan tersebut dan kenal pasti X.

A. Host Intrusion Prevention System
Sistem Pencegahan Pencerobohan Perumah

B. Host Intrusion Detection System
Sistem Pengesanan Pencerobohan Perumah

C. Network Intrusion Detection System
Sistem Pengesanan Pencerobohan Rangkaian

D. Network Intrusion Prevention System
Sistem Pencegahan Pencerobohan Rangkaian

CLO2
C3

14.

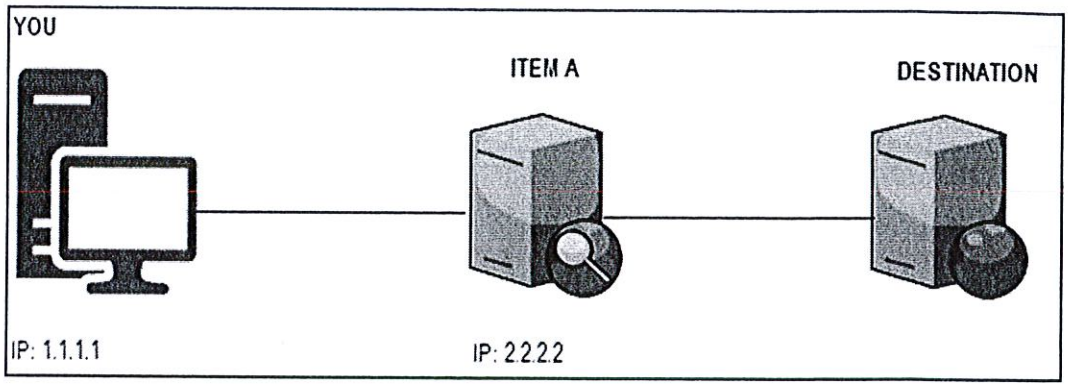

Figure A1 / *Rajah A1*

Referring to Figure A1 above, destination server will assume that the request comes from IP address 2.2.2.2. Choose the possible function of ITEM A.

Merujuk kepada Rajah A1 di atas, pelayan destinasi akan mengandaikan bahawa permintaan itu datang dari alamat IP 2.2.2.2. Pilih fungsi yang mungkin bagi ITEM A.

A. Making you anonymous / *Menjadikan anda tidak dikenali*
B. Cache the content / *Menyimpan kandungan*
C. Website filtering / *Menapis laman web*
D. Acting as middle person / *Bertindak sebagai orang tengah*

CLO2
C1

15. Identify which subset of account policy is used to prevent attackers from guessing users passwords.

Kenal pasti subset dasar akaun yang manakah digunakan untuk mencegah penyerang meneka kata laluan pengguna.

A. Audit policy / *Polisi audit*
B. Account policy / *Polisi akaun*
C. Kerberos policy / *Polisi kerberos*
D. Account lockout policy / *Polisi akaun terkunci*

CLO2
C2

16. Select an example of privileges in operating system.

Pilih satu contoh keistimewaan dalam sistem pengoperasian.

A. The ability of user to access specific folders or files.
Kebolehan untuk pengguna mengakses folder atau fail khas.
B. The ability to log on to a computer locally.
Kebolehan untuk log masuk komputer dalaman.
C. The ability to audit both successful and failed attempts at actions.
Kebolehan untuk mengaudit percubaan yang berjaya dan tidak berjaya.
D. The ability to disable user accounts if an incorrect password is entered over a specified number of times over a specified period.
Kebolehan untuk melumpuhkan akaun pengguna jika kata laluan yang salah dimasukkan dalam bilangan masa tertentu dalam tempoh tertentu.

CLO2
C2

17. In a high-security environment, only physical access may be allowed to an administrator. Identify which port should be disabled to block remote access?

Dalam persekitaran keselamatan yang tinggi, hanya akses fizikal yang dibenarkan untuk pentadbir. Kenalpasti port mana yang patut ditutup untuk menghalang capaian jauh?

A. 21
B. 23
C. 25
D. 53

CLO2
C2

18. Determine which vulnerability of IIS that allows an attacker to exploit an unchecked buffer.

Tentukan di mana kelemahan IIS yang membenarkan penyerang mengeksploitasi penimbal yang tidak terkawal.

A. Large number of open ports.
Bilangan port terbuka yang besar.

B. Windows Licence Logging Service overflows.
Limpahan Windows Licence Logging Service.

C. Default installs of operating system and applications.
Pemasangan asal sistem operasi dan aplikasi.

D. Microsof Server Message Block (SMB) vulnerability.
Kelemahan Microsof Server Message Block (SMB).

CLO2
C2

19. Identify the purpose of implementing Microsoft Security Server in a network environment.

Kenal pasti maksud kegunaan melaksanakan Microsoft Security Server dalam persekitaran rangkaian.

A. Authenticate network users.
Mengesahkan pengguna rangkaian.

B. To show all authorized users for a specific network.
Untuk menunjukkan semua pengguna yang telah diberi kuasa bagi sesebuah rangkaian.

C. Check network connectivity.
Periksa sambungan rangkaian.

D. Controlling the domain.
Mengawal domain.

CLO2
C3

20. A network administrator implemented the password policy expire in certain duration. Choose the action that a user needs to take to fulfill the requirement of network administrator.

Pentadbir rangkaian melaksanakan dasar kata laluan tamat tempoh dalam tempoh tertentu. Pilih tindakan yang perlu diambil oleh pengguna untuk memenuhi keperluan pentadbir rangkaian.

A. User cannot key in the wrong password.
Pengguna tidak boleh tersilap masukkan kata laluan.

B. The password must contain combination of alphanumeric.
Kata laluan mesti mengandungi kombinasi huruf dan nombor.

C. User's previous five password cannot be re-use.
Lima kata laluan terdahulu pengguna tidak boleh digunakan semula.

D. User needs to change the password after 90 days.
Pengguna perlu menukar kata laluan selepas 90 hari.

CLO2
C2

21. A network administrator wants to encrypt data in the file server using symmetric encryption method. Determine the **ADVANTAGE** of using symmetric encryption on large quantities of data.

*Seorang pentadbir sistem hendak menyulitkan data di dalam pelayan fail menggunakan kaedah penyulitan simetri. Tentukan **KELEBIHAN** menggunakan penyulitan simetri pada kuantiti data yang besar.*

A. Uniqueness of the message digests.

Keunikan penghadaman mesej.

B. Speed.

Kelajuan

C. Anyone with the public key can decrypt the information.

Sesiapa dengan kunci awam boleh didekripsi maklumat tersebut.

D. Nonrepudiation.

Nonrepudiation.

CLO2
C2

22. Choose various attacks that can be launched if an authentication is not implemented.

Pilih jenis serangan yang boleh berlaku jika pengeshan tidak dibina.

I. Phishing

II. Insider attack

III. Denial of Service

IV. Password discovery

A. I, II and III

B. I, II and IV

C. I, III and IV

D. I, II, III and IV

CLO2 C3

23. Select the ciphertext for the sentence 'this is secret' if using shift key =15.
Pilih tulisan rahsia "ciphertext" untuk 'this is secret' jika menggunakan shift key = 15.

A. jxyiyiiushuj
B. kyzjzjjvtivk
C. iwxhxhhtrgti
D. lwxhxhiushuj

CLO2 C3

24. Encrypt the corresponding ciphertext for 'this is secret' if we contrast the shift key = -15?
Terjemah tulisan rahsia "ciphertext" yang sama untuk 'this is secret' jika kita kontrakan shift key = -15?

A. estdtddpncpe
B. ftueueeqodqf
C. drscsccombod
D. ftueuecombod

CLO3 C1

25. State the authentication method that applied a string of characters used to verify the identity of a user.

Nyatakan kaedah pengesahan yang menggunakan sekumpulan aksara untuk mengesahkan identiti seorang pengguna..

A. card / *kad*
B. key / *kunci*
C. finger print / *cap jari*
D. password / *kata laluan*

CLO3 C1

26. Choose the features of good VPN product that protects sensitive information content from being revealed or compromised by intentional or unintentional eavesdroppers.

Pilih ciri-ciri produk VPN yang baik yang boleh melindungi kandungan maklumat sensitif yang didedahkan atau dikompromi oleh eavesdroppers dengan sengaja atau tidak sengaja.

A. Unauthorized disclosure / *Pendedahan yang tidak dibenarkan*
B. Adequate encryption / *Penyulitan yang mencukupi*
C. Strong authentication / *Pengesahan yang kuat*
D. Adherence to standard / *Mematuhi standard*

CLO3
C2

27. Arrange the **CORRECT** steps used in the asymmetric encryption.

*Susun langkah-langkah yang **BETUL** yang digunakan dalam penyulitan asimetri.*

I. User A acquires User B's public key.
Pengguna A memperoleh kunci awam pengguna B.

II. User A transmits the encrypted message.
Pengguna A menghantar mesej yang disulitkan.

III. User A uses User B's public key to encrypt a message.
Pengguna A menggunakan kunci awam pengguna B untuk menyulitkan mesej.

IV. User B uses his private key to decrypt and reveal the message.
Pengguna B menggunakan kunci persendirian untuk menyahsulit dan mendedahkan mesej.

A. I, III, II and IV

B. II, III, IV and I

C. III, II, I and IV

D. IV, III, II and I

CLO3
C3

28. Domain Name Server Security (DNSSEC) is a specification for securing certain kinds of information provided by the Domain Name System (DNS) as used in Internet Protocol (IP) networks.
In relation to the above statement, choose which of network security goal has been achieved through these standards and protocols?

Domain Name Server Security (DNSSEC) adalah spesifikasi untuk mendapatkan beberapa jenis maklumat yang diberikan oleh Domain Name System (DNS) seperti yang digunakan pada Internet Protocol (IP).
Berhubung kenyataan di atas, pilih matlamat keselamatan rangkaian yang manakah dicapai melalui piawaian dan protokol ini?

A. Integrity / *Ketelusan*
B. Availability / *Ketersediaan*
C. Confidentiality / *Kerahsiaan*
D. Non-repudiation / *Bukan penolakan*

CLO3
C3

29. Choose why RAID cannot be replaced for back-up.

Pilih mengapa RAID tidak boleh digantikan dengan sandaran.

I. If an administrator accidentally deletes a file, it will instantly be removed from both mirrored copies.
Sekiranya pentadbir secara tidak sengaja memadamkan fail, ia akan hilang dengan segera dari kedua-dua salinan yang dicerminkan.

II. If the disk is corrupted by a software bug or virus, the corruption will be done to both mirrored copies simultaneously.
Sekiranya cakera dirosakkan oleh bug perisian atau virus, kerosakan akan berlaku untuk kedua-dua salinan cermin serentak.

III. If your network is hit by a power surge, it will probably fry both disks at the same time.
Sekiranya rangkaian anda dilanda lebihan kuasa, ia mungkin akan memusnahkan kedua-dua cakera pada masa yang sama.

IV. If your office gets flooded or burned, both disks will be ruined.
Sekiranya pejabat anda banjir atau terbakar, kedua-dua cakera akan hancur.

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

CLO3
C3

30. You are trying to rearrange your backup procedures to reduce the amount of time taken for each procedure. You want it to finish quickly. Choose the system that will back up only the files that have changed since the last backup.

Anda sedang cuba untuk menyusun semula prosedur backup untuk mengurangkan jumlah masa yang diambil untuk setiap backup. Backup tersebut hendak diselesaikan secepat mungkin. Pilih sistem backup yang hanya akan backup fail yang telah berubah sejak backup terakhir.

A. Full backup

B. Incremental backup

C. Differential backup

D. Backup server

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
C1

(a) List **FIVE (5)** potential risks to network security.

*Senaraikan **LIMA (5)** potensi risiko kepada keselamatan rangkaian.*

[5 marks]
[5 markah]

CLO1
C3

b) A type of malicious code is able to replicate itself by modifying other computer programs and insert its own code. But the malicious code does nothing and threatens no one if it is not triggered.

Sejenis malicious kod boleh replikasi dirinya dengan mengubahsuai program komputer lain dan memasukkan kodnya sendiri. Tetapi, malicious kod ini tidak akan mendatangkan sebarang ancaman kepada sesiapa jika ia tidak dibuka.

Give **TWO (2)** examples of how the malicious code as stated above, can start spreading by itself.

*Berikan **DUA (2)** contoh bagaimana malicious kod yang digambarkan dalam penyataan di atas boleh mula merebak dengan sendiri.*

[2 marks]
[2 markah]

CLO1
C1

c) Give **TWO (2)** examples of configuration weaknesses.

Berikan ***DUA (2)** jenis ancaman kepada keselamatan rangkaian.*

[2marks]
[2 markah]

CLO2 C2

d) Explain **THREE (3)** steps on how an attacker performs a routine called **"ping-sweep"** in a Denial-of-Service attack.

*Terangkan **TIGA (3)** langkah bagaimana seorang penyerang melakukan satu rutin ping-sweep dalam serangan Denial-of-Service.*

[5 marks]
[5 markah]

CLO1 C2

e) Explain the **TWO (2)** commonly used technologies in building firewall.
*Terangkan **DUA (2)** teknologi yang biasa digunakan dalam membina firewall.*

[2marks]
[2 markah]

CLO1 C4

f) Analyze why firewall is the primary method keeping a computer can be secured from intruders.

Analisa mengapa dinding api adalah kaedah utama yang menjaga komputer boleh selamat daripada penceroboh

[5 marks]
[5 markah]

CLO2 C1

(g) Describe device hardening.

Terangkan sekatan peranti

[2 marks]
[2 markah]

CLO2 C2

(h) Explain how static packet filtering works.

Jelaskan bagaimana tapisan paket statik beroperasi.

[2 marks]
[2 markah]

QUESTION 2
SOALAN 2

The following phrases is created for a strong password.
Frasa berikut dicipta untuk kata laluan yang kuat.

1. 'P4T9#6@'
2. 'this_is_a_very_long_password'

CLO2 C2

a) i. Determine which password is safer.
Tentukan kata laluan yang mana adalah lebih selamat.

[2 marks]
[2 markah]

ii. Explain the reason for the selection.
Terangkan sebab pemilihan.

[3 marks]
[3 markah]

CLO2 C3

b) Explain **THREE (3)** differences between Packet Filter and Proxy Server.
*Terangkan **TIGA (3)** perbezaan di antara Packet Filter dan Proxy Server.*

[6 marks]
[6 markah]

CLO3 C1

c) Identify whose and which key to use if Bob wants to send Alice an encrypted message using asymmetric cryptography.
Kenal pasti kunci siapa dan yang mana untuk digunakan jika Bob mahu menghantar Alice mesej yang disulitkan menggunakan kriptografi asimetri.

[2 marks]
[2markah]

CLO3
C2

d) Explain **TWO (2)** primary weaknesses of symmetric encryption algorithms in securing the single key.
*Jelaskan **DUA (2)** kelemahan utama algoritma penyulitan simetri dalam menjamin keselamatan kunci tunggal.*

[6 marks]
[6 markah]

CLO3
C3

e) A Virtual Private Network (VPN) is a private networks that uses a public network (the Internet) to connect users.
Virtual Private Network (VPN) adalah rangkaian persendirian yang menggunakan rangkaian umum (Internet) untuk menghubungkan pengguna.

(i) Illustrate a diagram that shows intranet VPN connection.
Lukis satu gambarajah yang menunjukkan sambungan intranet VPN

[4 marks]
[4markah]

(ii) Suggest **THREE (3)** features of good VPN product.
*Cadangkan **TIGA (3)** kriteria produk VPN yang baik.*

[3 marks]
[3 markah]

Day	Storage Used	File Adds	File Deletes	Saved to Tape
Monday	10GB	1GB	0GB	11GB
Tuesday	11GB	1GB	3GB	1GB
Wednesday	9GB	2GB	0GB	2GB
Thursday	11GB	1GB	3GB	1GB

Table B1 / *Jadual B1*

CLO3
C2

f) Referring to Table B1, describe the problem of incremental backups if on Friday morning, you discovered that someone has performed a bit of housekeeping, deleting all the files from your 12GB drive.
Rujuk Jadual B1, huraikan masalah backup tambahan jika pada pagi Jumaat, anda mendapati bahawa seseorang yang telah melakukan sedikit pengemasan, memadam semua fail dari cakera 12GB anda.

[2 marks]
[2 markah]

CLO3
C3

g) Employ an alternative solution to the incremental backups used in Table B1.
Gunakan penyelesaian alternatif kepada backup tambahan yang digunakan dalam Jadual B1.

[2 marks]
[2 markah]

END OF QUESTION

SOALAN TAMAT