10

SULIT

POLITEKNIK MALAYSIA

BAHAGIAN PEPERIKSAAN DAN PENILAIAN
JABATAN PENDIDIKAN POLITEKNIK
KEMENTERIAN PENDIDIKAN TINGGI

JABATAN TEKNOLOGI MAKLUMAT & KOMUNIKASI

PEPERIKSAAN AKHIR

SESI JUN 2017

DFN6223 : NETWORK SECURITY

TARIKH : 23 OKTOBER 2017
MASA : 8.30 PAGI - 10.30 PAGI (2 JAM)

Kertas 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 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. When developing a secured network, there are several things to be considered. Identify the needs to be considered for developing a secured network :

   Apabila membangunkan rangkaian yang selamat, ia mempunyai beberapa perkara yang perlu dipertimbangkan. Kenalpasti keperluan untuk dipertimbangkan untuk membangunkan rangkaian yang selamat:

   A. Confidentiality
   Kerahsiaan

   B. Bandwidth
   Lebar jalur

   C. Renaming Documents
   Menamakan semula dokumen

   D. Diversionary Tactics
   Taktik Penyelewengan

CLO1
C1

2. Below are Information Security Organizations, **EXCEPT**:

   Berikut adalah organisasi keselamatan maklumat, **KECUALI**:

   A. ICSA
   ICSA

   B. Common Criteria
   Common Criteria

   C. SANS Institute
   Institut SANS

   D. IFPS
   IFPS

CLO1 C2

3. Identify which of the following statements that describes a good approach to information security in an organization.

Kenal pasti pernyataan berikut yang menerangkan pendekatan yang baik untuk keselamatan maklumat dalam sesebuah organisasi.

A. Staffs' password are shared between user group
Kata laluan Staf dikongsi dengan kumpulan pengguna

B. Security lapses are not reported except in an emergency situation
Berlaku kesilapan keselamatan tidak dilaporkan kecuali dalam keadaan kecemasan

C. Sensitive data are available to all employees
Data yang sensitif boleh dicapai oleh semua pekerja

D. Computer system are backed up on regular basis
Sistem Komputer disokong secara berkala

CLO1 C4

4. Mr. Wong obtained a private information (pin Number) without the owner's 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/ *pengubahsuaian data*

B. Information Theft/ *Kecurian maklumat*

C. Information Warfare/ Peperangan maklumat

D. Unauthorized disclosure/ Pendedahan yang tidak dibenarkan

CLO1 C1

5. The threat arises from an individual or organizations working outside of the company. Define the type of threat.

Ancaman itu timbul daripada individu atau organisasi yang bekerja di luar syarikat. Takrifkan jenis ancaman.

A. Structure threat
Ancaman struktur

B. External threat
Ancaman luaran

C. Unstructured threat
Ancaman tidak berstruktur

D. Internal threat
Ancaman dalaman

CLO1 C4

6.

A person can steal a secret information which may cause damage to an organization. This individual can penetrate the organization through job opening.

Seseorang yang boleh mencuri maklumat kritikal sesebuah syarikat dan menyebabkan kerosakan kepada syarikat tersebut. Individu tersebut memasuki syarikat tersebut melalui peluang pekerjaan yang ditawarkan.

Figure A1/ Rajah A1

As a Human Resources Manager of the company, suggest a way to prevent an attack represented in Figure A1.

Sebagai Pengurus Sumber Manusia, cadangkan cara untuk mengelak jenis serangan berdasarkan situasi dalam Rajah A1.

A. It is impossible to block these attacks
Adalah mustahil untuk menghalang serangan ini.

B. Hire the people through third-party job agencies who will vet them for you
Mengupah seseorang melalui agensi pekerjaan pihak ketiga yang akan melakukan penyamaran untuk anda

C. Investigate their social networking profiles
Menyiasat profil rangkaian sosial pekerja mereka.

D. Conduct thorough background checks before you engage them
Melakukan pemeriksaan latar belakang yang teliti sebelum anda melibatkan mereka dalam syarikat.

CLO2
C2

7. Identify the malware that is capable of altering its form in order to avoid discovery by certain virus detection programs.

Kenalpasti perisian hasad yang mampu mengubah bentuk untuk mengelakkan dikesan oleh program pengesanan virus.

A. Logic Bomb
Bom Logik

B. Stealth Virus
Stealth Virus

C. Port Scanning
Imbasan Port

D. Traps Door
Pintu Perangkap

CLO2
C2

8. A hacker contacted you by phone or email and attempted to acquire your password. This action is referred as:

Seseorang penggodam menghubungi anda melalui telefon atau e-mel dan cuba untuk memperoleh kata laluan anda. Tindakan ini dipanggil sebagai:

A. Spoofing
Perdayaan

B. Phishing
Memancing data

C. Spamming
Penspaman

D. Bugging
Pepijat

CLO1
C2

9. NMAP scan of a server shows that port 25 is open. Predict the risk it could pose to a network

Imbasan NMAP menunjukkan port 25 adalah terbuka. Jangka risiko yang boleh terjadi kepada rangkaian.

A. Open printer sharing
Perkongsian pencetakan

B. Web portal data leak
Kebocoran data pada portal web

C. Clear text authentication
Pengesahan data

D. Active mail relay
Geganti mel yang aktif.

CLO1
C3

10.

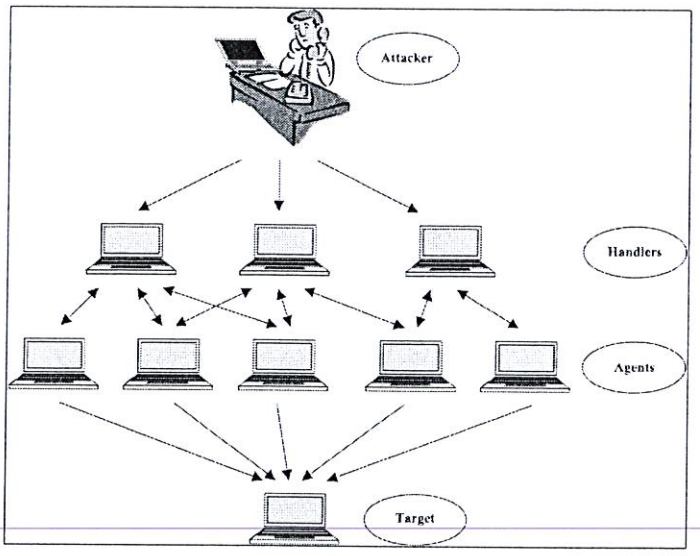

Figure A2/ Rajah A2

Refer to Figure A2, interpret the type of attack.

Rujuk Rajah A2, terjemahkan jenis serangan tersebut.

A. Ping of Death attack
B. SYN Flooding attack
C. Denial of Service attack (DoS)
D. Distributed Denial of Service attack (DDoS)

CLO1
C4

11

This application software runs in the background and users will not be aware of its existence. Upon using his/her computer, this application copies itself from system to system in the network.

Perisian ini beroperasi pada latar belakang dan pengguna tidak menyedari kewujudannya. Semasa pengguna menggunakan komputernya, aplikasi ini salin dirinya sendiri dari satu sistem ke sistem yang lain di dalam rangkaian.

Figure A3/ Rajah A3

Determine the type of malicious code as described in Figure A3.

Berdasarkan Rajah A3, tentukan ancaman yang bersesuaian.

A. DoS

B. Worm

C. Virus

D. Trojan horse

CLO2
C2

12.

A firewall is able to examine the contents of packets as well as the headers for signs that they are legitimate

Firewall mampu untuk memeriksa kandungan paket serta headers untuk mengenalpasti bahawa paket adalah sah

Figure A4/ Rajah A4

Identify the type of technology used to build a firewall in Figure A4:

Kenal pasti jenis teknologi yang digunakan untuk membina tembuk api seperti dalam Rajah A4 :

A. Boundary
Sempadan

B. Stateful
Bersyarat

C. Stateless
Tidak bersyarat

D. Personal
Peribadi

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". Interpret the identity of 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". Terjemahkan identiti 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. Provide how inbound connections handled by default by Windows Firewall.

Beri kaedah bagaimana sambungan masuk dikendalikan oleh Firewall Windows dalam keadaan asal.

A. they are blocked by default
mereka disekat oleh standard

B. access control list (ACL) or VLAN
senarai kawalan akses (ACL) atau VLAN

C. netstat -a –b
netstat-a-b

D. block, allow, and secure
blok, membenarkan, dan selamat

CLO2 C1

15. Identify additional component required for IPSec connection security.

Kenalpasti komponen tambahan yang diperlukan untuk keselamatan sambungan IPSe

A. Access control list (ACL) or VLAN
Senarai kawalan akses(ACL) atau VLAN

B. Certificate Services
Sijil Perkhidmatan

C. IPSec connection security, 802.1x access points, VPN servers, and DHCP servers
IPSec sambungan keselamatan,titik akses802.1x, pelayan VPN, dan pelayan DHCP

D. Only compliant machines are issued IP addresses
Mesin yang sesuai sahaja yang akan memberikan alamat IP

CLO2
C2

16. Match the **CORRECT** approaches to manage security using LINUX.

Padankan pendekatan yang betul untuk mengurus keselamatan menggunakan LINUX?

i. Identify and disable unnecessary port and services
Kenal pasti dan tidak aktifkan port dan perkhidmatan yang tidak diperlukan

ii. Lock identified ports
Kunci port yang dikenalpast

iii. Carry out system hardening with Bastille
Menjalankan sistem pengerasan dengan Bastille

iv. Maintain controlling and auditing of Root Access using SUDO
Mengekalkan pengawalan dan pengauditan akses asas menggunakan SUDO

A. i, ii and iii
B. ii, iii and iv
C. i, ii and iv
D. i, ii, iii and iv

CLO2
C2

17. You have implemented an IPSec policy, using only Authentication Header (AH). You are analyzing your network traffic in Network Monitor. Determine which of the following statements is **TRUE** about your network traffic?

*Anda telah melaksanakan polisi IPSec, hanya menggunakan "Authentication Header" (AH). Anda menganalisis trafik rangkaian di rangkaian memantau. Tentukan yang mana satu kenyataan berikut adalah **BENAR** tentang trafik Rangkaian anda?*

A. You will not be able to view the data in the packets, as it is encrypted.
Anda tidak akan dapat melihat data dalam paket kerana ia telah dienkripkan.

B. You will not be able to identify the upper layer protocol.
Anda tidak akan dapat mengenalpasti protokol lapisan atas.

C. You will be able to view the unencrypted data in the packets.
Anda akan dapat melihat data tanpa enkrip dalam paket.

D. You will be able to identify the encryption algorithm in use.
Anda akan dapat mengenal pasti enkrip algoritma yang digunakan.

CLO2
C2

18. Determine which of the following is the best description for Hotfix.

Tentukan yang manakah antara berikut penerangan terbaik berkenaan "Hotfix".

A. Require the system to be shut down before installing the hotfix
Memastikan sistem dimatikan sebelum pemasangan 'hotfix'

B. Brings many changes
Membawa banyak perubahan.

C. Applied directly while the systems are still alive
Dipasang terus semasa sistem sedang berfungsi

D. Not a compulsory system update
Kemaskini tidak diwajibkan

CLO2
C2

19. Identify which of the following is **NOT** a criteria of a strong password

*Kenalpasti yang manakah antara berikut **BUKAN** kriteria katalaluan yang kuat.*

A. Sequences
Berjujukan

B. Dictionaries
Kamus

C. Personal data
Data peribadi

D. Combination
Kombinasi

CLO2
C3

20. ABC Computer Company has four departments and has a different access for its user. The manager has drafted a complete guideline about logon rights and privileges. Different level of management will have different rights and privileges to access data from database. Summarize the system policy used by the manager.

Syarikat Komputer ABC mempunyai empat bahagian dan mempunyai capaian berbeza bagi setiap bahagian. Pengurusnya telah merangka garis panduan lengkap tentang hak logon dan keistimewaan. Peringkat pengurusan yang berbeza hendaklah mempunyai hak keistimewaan yang berbeza untuk capaian data dari pengkalan data. Simpulkan polisi sistem yang digunakan oleh pengurus tersebut.

A. User Right
Hak pengguna

B. Login Right
Hak log masuk

C. Access Right
Hak capaian

D. Privilege Right
Hak keistimewaan

CLO2
C2

21. A network administrator wants to encrypt data in the file server using symmetric encryption method. Indicate 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. Tunjukkan kelebihan menggunakan penyulitan simetri pada kuantiti data yang besar.

A. Uniqueness of the message digests.
Keunikan penghadaman mesej.

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

C. Speed.
Kelajuan

D. Nonrepudiation.
Nonrepudiation.

CLO2
C2

22. Match the **CORRECT** symmetric key Algorithm that can be used by a network administrator who wants to encrypt all data in the file server

*Padankan Algoritma penyulitan simetri yang **BETUL** yang boleh digunakan oleh seorang pentadbir rangkaian yang hendak menyulitkan semua data yang ada di dalam pelayan fail*

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

A. I and II

B. II and III

C. III and IV

D. I and IV

CLO2
C3

23. Show the ciphertext for the sentence 'this is secret' if using shift key =15.

Tunjukan tulisan rahsia "ciphertext" untuk 'this is secret' jika menggunakan shift key = 15.

A. Jxyiyiiushuj

B. Kyzjzjjvtivk

C. Iwxhxhhtrgti

D. lwxhxhiushuj

CLO2
C3

24. Interpret which of the following the benefits of implementing a Virtual Private Network (VPN).

Tafsirkankan yang mana diantara berikut merupakan faedah melaksanakan Virtual Private Network (VPN)

i. Enable to transmit data securely over a public network
Membolehkan data dihantar secara selamat melalui rangkaian awam

ii. Secured from attackers
Selamat daripada penyerang

iii. IP address provided by DHCP server
Alamat IP dibekalkan oleh pelayan DHCP

iv. Can be implemented without proper deployment of precautions
Boleh dilaksanakan tanpa langkah berjaga-jaga yang betul

A. i and ii.

B. i, ii and iii

C. ii and iv

D. iii and iv

CLO3
C1

25. Select which of the following are VPN tunnelling protocols.

Kenalpasti yang manakah antara berikut merupakan protokol terowong VPN.

A. PPTP
PPTP

B. IPSec
IPSec

C. L2TP
L2TP

D. All of the above
Semua diatas

CLO3
C1

26. State the benefit of using HTTPS.

Nyatakan manfaat menggunakan HTTPS

A. Allows messages to be transmitted securely using an email
Membolehkan mesej untuk dihantar dengan selamat menggunakan e-mel

B. Allows data to be managed properly in a proper table
Membenarkan data diuruskan dengan betul dalam jadual yang sepatutnya

C. Allows files to be transferred within a network
Membenarkan fail yang hendak dipindahkan melalui rangkaian

D. Allows the secure exchange of files on the World Wide Web
Membenarkan pertukaran fail pada "World Wide Web" dengan selamat

CLO3
C2

27. Differentiate between VPNs and firewalls.

Bezakan di antara "VPN" dan "firewall.

A. Firewalls are user-configurable; VPNs cannot be configured/
Firewall senang dikonfigurasi; VPNs tidak boleh dikonfiguri

B. Firewalls blocks messages; VPNs open pathways for messages
Firewall halang mesej: VPN laluan terbuka untuk mesej

C. Firewalls are new type of VPN
Firewall adalah VPN jenis baru

D. No difference exists between firewall and VPNs
Tiada wujud perbezaan antara firewall dan VPN

CLO3
C3

28. When purchasing an off-site backup facility that will ultimately be used to store all your backup media, suggest the most important factor to be considered

Semasa membeli belah untuk kemudahan sandaran luar tapak yang pada akhirnya akan digunakan untuk menyimpan semua median sandaran anda, cadangkan faktor yang paling penting untuk dipertimbangkan.

A. The backup facility should be within 15 minutes of the original facility.
Kemudahan sandaran hendaklah dalam tempoh 15 minit dari kemudahan asal.

B. The facility should contain an adequate number of PCs and servers and have raised flooring.
Kemudahan seharusnya mengandungi jumlah PC dan pelayan yang mencukupi dan mempunyai lantai yang tinggi

C. The facility should have at least one armed guard.
Kemudahan seharusnya mempunyai seorang pengawal bersenjata.

D. The facility should have protection against unauthorized access and entry.
Kemudahan yang mempunyai pelindungan dari akses tanpa kebenaran.

CLO3
C3

29. When data is lost or damaged, it will need to be recovered. Explain which one of the following would **NOT** need to be considered as part of the recovery procedure?

*Apabila data telah hilang atau musnah, ia perlu dibaikpulih. Terangkan pernyataan manakah yang **TIDAK** perlu dipertimbangkan sebagai sebahagian daripada proses baikpulih*

A. Staff should be available at short notice to recover the data.
Kakitangan perlu sentiasa bersiap sedia sekiranya dipanggil untuk membaikpulih data.

B. There must be hardware and software capable of running the data
Perlu ada perkakasan dan perisian yang mampu menjalankan data.

C. Staff must be trained on how to recover the data
Kakitangan perlu dilatih bagaimana untuk mengesan kembali data.

D. It is necessary for staff to be trained to type in all the missing data
Kakitangan perlu dilatih untuk menaip semula data yang hilang.

CLO3
C3

30. Imaging backup is a backup of an entire hard drive by means of creating its image (also called mirror, or snapshot). The following are the advantages of imaging backup **EXCEPT:**

Salinan Berimej merupakan salinan untuk keseluruhan cakera keras yang akan mencipta imejnya sendiri (juga digelar sebagai mirror atau snapshot). Berikut merupakan kebaikan menggunakan Salinan Berimej ***KECUALI:***

A. Estimates on future system resource utilization based on the resource utilization data collected from current systems.
Menganggarkan penggunaan sumber sistem akan datang berdasarkan kepada penggunaan data sumber seperti yang dikumpul melalui sistem sekarang.

B. Estimates on future system resource utilization based on the expected value of several parameters.
Menganggarkan penggunaan sumber sistem akan datang berdasarkan kepada nilai jangkaan beberapa parameter.

C. Estimates on future system resource utilization based on the management or user requirement.
Menganggarkan penggunaan sumber sistem akan datang berdasarkan kepada pengurusan atau permintaan pengguna.

D. Estimates on future system resource utilization based on what has been happen in the current system.
Menganggarkan penggunaan sumber sistem akan datang berdasarkan kepada apa yang telah berlaku kepada sistem sekarang.

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]

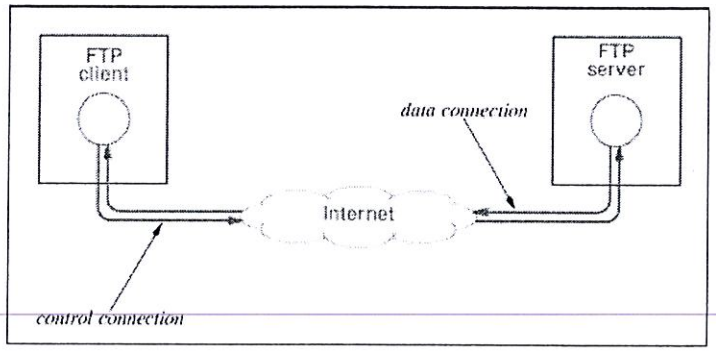

Figure B1/Rajah B1

CLO1
C3

b. Based on figure B1,
Berdasarkan rajah B1

i. Interpret internet service that is being used
Tafsirkan perkhidmatan internet yang digunakan

[1 marks]
[1 markah]

ii. Explain the internet service in b(i)

Jelaskan perkhidmatan internet pada b(i)

[1 marks]

[1 markah]

CLO1 C1

c. State **ONE (1)** difference between worms and virus.

*Nyatakan **SATU(1)** perbezaan di antara worms dan virus.*

[2 marks]

[2 markah]

W32.MyDoom@mm
Troj/ CEMS-8112

Figure B2/Rajah B2

CLO2 C2

d. Student reported that when he scanned his computer by using Trend Micro Antivirus, the following alerts shown in Figure B2 appeared. Based on the scenario,

Pelajar melaporkan apabila dia mengimbas komputer menggunakan Trend Micro Antivirus, mesej seperti di rajah B2 dipaparkan. Berdasarkan senario tersebut,

i. Determine type of attack that has been experienced by this student.

Tentukan jenis serangan dihadapi oleh pelajar tersebut.

[1 marks]

[1 markah]

ii. Describe the attack in d(i).

Jelaskan serangan pada d.(i)

[2 marks]

[2 markah]

iii. Classify W32.MyDoom@mm and W32/Troj CEMS-8112.

Kelasifikasikan W32.MyDoom@mm dan W32/Troj CEMS-8112.

[2 marks]

[2 markah]

CLO1 C2

e. Differentiate between static packet filtering and dynamic packet filtering.
Bezakan antara penapisan paket statik dan penapisan paket dinamik.

[2 marks]
[2 markah]

CLO1 C4

f. "Firewall is a primary method of keeping a computer secured from an intruder". Based on the statement given, prepare your answer on why a firewall is a primary method to keep a computer secured from intruders.
"Firewall adalah kaedah utama untuk memastikan komputer selamat daripada penceroboh". Berdasarkan pernaytaan tersebut, nyatakan kenapa firewall adalah kaedah utama untuk memastikan computer selamat daripada penceroboh.

[5 marks]
[5 markah]

CLO2 C1

g. List **TWO (2)** firewall components.
Senaraikan **DUA (2)** komponen firewall.

[2 marks]
[2 markah]

CLO2 C2

h. Determine **TWO** (2) features of network-based IDS.
*Tentukan **DUA (2)** ciri IDS berasaskan rangkaian.*

[2 marks]
[2 markah]

QUESTION 2

SOALAN 2)

CLO2 C2

a. Describe **TWO (2)** types of system policy.
*Huraikan **DUA (2)** jenis polisi system.*

[5 marks]
[5 markah]

CLO2 C3

b. Lack of written security policy and lack of continuity action are the common security policy weaknesses. Suggest how both weaknesses can be exploited.
Kurangnya polisi keselamatan secara bertulis dan kurangnya kesinambungan tindakan merupakan kelemahan yang biasa didalam polisi keselamatan. Cadangkan bagaimana kelemahan-kelemahan ini boleh dieksploitasi.

[6 marks]
[6 markah]

CLO3 C1

c. List **TWO (2)** types of cryptographic terminology.
*Senaraikan **DUA (2)** jenis terminology 'cryptographic'.*

[2 marks]
[2 markah]

CLO3 C2

d. Differentiate between symmetric key encryption and asymmetric key encryption.
Bezakan antara penyulitan kekunci simetri dan penyulitan kekunci assimetri.

[6 marks]
[6 markah]

CLO3
C3

e. A Virtual Private Network (VPN) is a private network 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 Point-to-Point Tunneling Protocol (PPTP)
Lukis satu gambarajah yang menunjukkan sambungan intranet VPN

[2 marks]
[2 markah]

ii. Illustrate a diagram that shows Layer 2 Tunneling Protocol (L2TP)
Lukis satu gambarajah yang menunjukkan sambungan intranet VPN

[2 marks]
[2 markah]

iii. Explain types of VPN protocol in e(i) & e(ii)

[3 marks]
[3 markah]

CLO3
C2

f. List **TWO (2)** disaster category and give **ONE (1)** example for each category.
*Senaraikan **DUA (2)** kategori bencana serta berikan **SATU (1)** contoh untuk setiap kategori.*

[2 marks]
[2 markah]

CLO3
C3

g. Summarize **TWO (2)** strategies to protect or restore lost, corrupted and deleted information.
*Simpulkan **DUA (2)** strategi dalam melindungi atau mendapat kembali maklumat yang hilang, rosak dan dipadam*

[2 marks]
[2 markah]

SOALAN TAMAT