21

SULIT

POLITEKNIK MALAYSIA

BAHAGIAN PEPERIKSAAN DAN PENILAIAN
JABATAN PENDIDIKAN POLITEKNIK
KEMENTERIAN PENDIDIKAN MALAYSIA

JABATAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI

PEPERIKSAAN AKHIR

**SESI DISEMBER 2015**

# DFP4133: INFORMATION SYSTEM SECURITY

**TARIKH : 04 APRIL 2016 (ISNIN)**
**MASA : 2.30 PM – 4.30 PM (2 JAM)**

---

Kertas ini mengandungi **DUA PULUH (20)** 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.*

CLO1
C1

1. Recognize the needs for information system security.
*Kenal pasti keperluan untuk keselamatan sistem infomasi.*

i. Confidentiality / *Sulit*
ii. Affordability / *Kemampuan*
iii. Availability / *Sedia ada*
iv. Integrity / *Integriti*

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

CLO1
C1

2. Identify the **CORRECT** characteristic for Closed Security Model.
*Kenal pasti ciri Closed Security Model yang **BETUL**.*

A. Users are trusted and threats are minimal.
*Pengguna boleh dipercayai dan ancaman bertahap minima.*

B. Network administrator requires least skills and less time to administer the network.
*Penyelia rangkaian memerlukan kebolehan yang rendah dan masa yang sedikit untuk mentadbir rangkaian.*

C. Assumes that all users are not trustworthy.
*Andaian semua pengguna tidak boleh dipercayai.*

D. Not all security measures are implemented.
*Tidak semua ciri keselamatan di implementasikan.*

CLO1 C2

3. Choose the activity relates to stealing a confidential data and information from an organization network.
*Pilih aktiviti yang berkaitan kepada kecurian maklumat sulit dari rangkaian sesebuah organisasi.*

A. Accidental data loss.
*Kehilangan data secara tidak sengaja.*

B. Information warfare.
*Perang maklumat.*

C. Information theft.
*Kecurian maklumat.*

D. Unauthorized disclosure.
*Pendedahan yang tidak disahkan.*

CLO1 C1

4. Name the threat that might occur, when untrusted employee is working on the system database in the company's network.
*Namakan 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 C1

5. Select **THREE (3)** primary vulnerabilities in security environment.
*Pilih **TIGA (3)** kelemahan utama di dalam persekitaran keselamatan.*

i. Technology / *Teknologi*
ii. Configuration / *Konfigurasi*
iii. Accessibility / *Kebolehcapaian*
iv. Security policy / *Polisi keselamatan*

A. i, ii and iii

B. i, ii and iv

C. i, iii and iv

D. ii, iii and iv

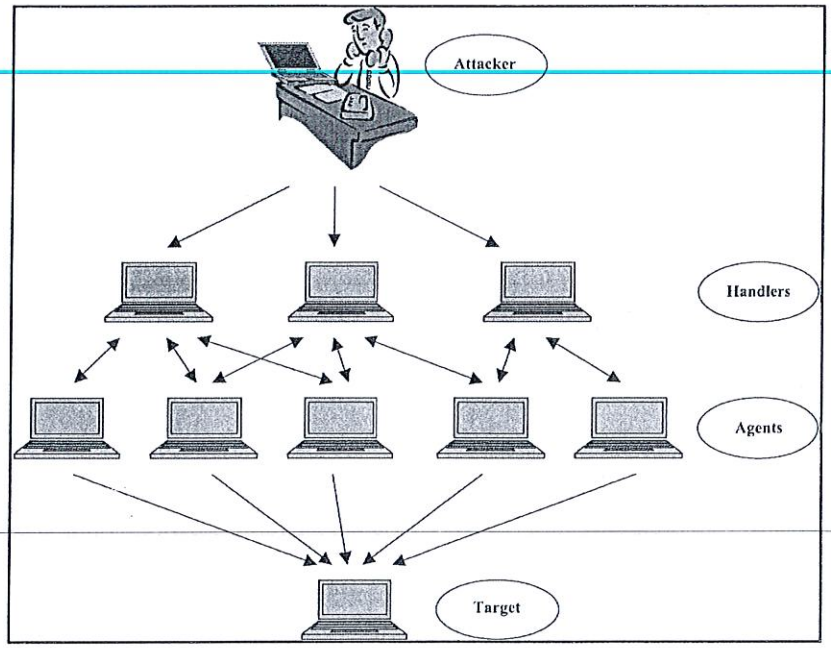


Figure A1 / *Rajah A1*

CLO1 C2

6. Referring to Figure A1, identify the type of attack.
*Merujuk Rajah A1, kenalpasti 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 C2

7. Unskilled user with the intention to damage the system has downloaded an automated hacking software (scripts) from the website.
*Pengguna tidak berkemahiran yang bertujuan merosakkan sistem telah memuat turun "hacking software (script)" daripada laman web.*

Figure A2 / *Rajah A2*

Determine the type of attacker that stated in Figure A2.
*Kenalpasti jenis penyerang yang dinyatakan dalam Rajah A2.*

A. Hackers / *Penggodam*

B. Script kiddies / *Skrip "kiddies"*

C. Cybercriminals / *Penjenayah siber*

D. Cyberterrorist / *Penceroboh siber*

CLO1 C3

8. A security administrator wants to examine the activity on the network. Choose the **CORRECT** network scanning tools to identify potential network vulnerabilitites.

*Seorang pentadbir keselamatan hendak memeriksa aktiviti di dalam rangkaian. Pilih alat pengimbasan rangkaian yang **BETUL** untuk mengenalpasti potensi kelemahan rangkaian.*

i. nslookup
ii. netstat
iii. Nmap
iv. Hping

A. i, ii and iii

B. i, ii and iv

C. i, iii and iv

D. ii, iii and iv

CLO1 C3

9. Ali tries to steal information from his company and use it for his own purpose and gain benefits.
*Ali cuba untuk mencuri maklumat dari syarikat dan menggunakannya untuk tujuan sendiri dan memperolehi keuntungan.*

Figure A3 / *Rajah A3*

Relate Ali's act as mentioned in Figure A3 with suitable terminology below.
*Kaitkan tindakan Ali seperti yang dinyatakan dalam Rajah A3 dengan terminologi yang sesuai di bawah.*

A. Information warfare / *Peperangan maklumat*

B. Accidental data loss / *Kehilangan data tidak sengaja*

C. Information theft / *Pencurian maklumat*

D. Unauthorized disclosure / *Pendedahan maklumat yang tidak sah*

CLO2 C1

10. Name the malicous code that pretend to be a useful application **BUT** could harm the computer.
*Namakan kod jahat yang kelihatan seperti berguna **TETAPI** boleh mengancam komputer.*

A. DoS

B. Worm

C. Virus

D. Trojan horse

CLO2 C1

11. A network will become vulnerable if there is misconfiguration in the device or system. Give example of configuration weaknesses.

*Sebuah rangkaian akan terdedah sekiranya terdapat kesilapan konfigurasi pada sistem atau peranti. Berikan contoh kelemahan konfigurasi.*

A. Lack of authentication
*Kekurangan pengesahan*

B. Used of default setting
*Penggunaan tetapan lalai*

C. Security policy is not enforce
*Polisi keselamatan tidak dikuatkuasakan*

D. Virus signature is not update
*Virus signature tidak dikemaskini*

CLO2 C1

12. Determine the application that controls network traffic to and from a computer.
*Tentukan aplikasi yang mengawal trafik rangkaian dari dan ke computer.*

A. Personal firewall

B. Proxy server

*C.* Antivirus

D. Patch

CLO2
C2

13. There are three type of packet filtering, which are static, dynamic and proxy. Select the **BEST** description about static packet filtering.

*Terdapat tiga jenis penapisan paket, yang terdiri daripada statik, dinamik dan proksi. Pilih pernyataan yang **TERBAIK** tentang penapis paket statik.*

A. Examines the contents of packet rather than just filtering them.
*Memeriksa kandungan paket bukan sekadar menapis sahaja.*

*B.* Considers whether a connection was started from inside.
*Mempertimbangkan paket diperiksa sama ada sambungan telah bermula dari dalam.*

*C.* Each packet checked and passed or rejected depending on a set of user-defined rules.
*Setiap paket diperiksa dan diluluskan atau ditolak bergantung kepada satu set peraturan takrifan pengguna.*

D. A reverse filter is created to allow the response packet to return.
*Satu penapis terbalik diwujudkan untuk membolehkan maklumbalas paket dihantar kembali.*

CLO2
C3

14. An administrator decided to apply a firewall type with protocol conformance and allow remote computer. Choose another characteristic that match this type of firewall.

*Seorang pentadbir membuat keputusan untuk mengaplikasikan jenis firewall dengan pematuhan protokol dan membenarkan komputer capaian jauh. Pilih satu ciri lain yang berpadanan bagi jenis firewall ini.*

A. Filter individual session
*Menapis sesi individu*

B. Examine header based on IP address
*Memeriksa 'header' berdasarkan alamat IP*

C. Monitor TCP handshaking
*Memantau TCP handshaking*

D. Sort out packet based on protocol
*Asingkan paket berdasarkan protokol*

CLO2 C1

15. Identify which is **NOT** an Internet Information Services (IIS) vulnerability.
*Kenal pasti yang mana **BUKAN** kelemahan Internet Information Services (IIS).*

A. All IIS features are disabled
*Semua fungsi IIS dimatikan*

B. Large number of open ports
*Pembukaan port dalam bilangan yang banyak*

C. Default install of operating system and applications
*Pemasangan sistem pengoperasian dan aplikasi secara lalai*

D. Microsoft Server Message Block (SMB) vulnerability
*Kelemahan Microsoft Server Message Block*

CLO2 C2

16. An administrator needs to manage open source software security for his organization. Determine one of the ways to enhance the security of a Linux Server.
*Seorang pentadbir perlu menguruskan keselamatan perisian sumber terbuka bagi organisasi beliau. Tentukankan salah satu cara untuk meningkatkan keselamatan Server Linux.*

A. Enable all features available
*'Enable' semua ciri yang ada*

B. Disable unnecessary port and services
*'Disable port' dan perkhidmatan yang tidak perlu*

C. Uninstall additional Linux Server
*'Install' Linux Server tambahan*

D. Customize Linux interfaces
*'Customize' antara muka Linux*

CLO2
C3

17. Abu Enterprise requires that every web page request from users inside its network to the internet to be transformed into anonymous web request.
*Abu Enterprise memerlukan setiap permintaan laman web dari rangkaian tempatan ke internet ditukar kepada bentuk permintaan tanpa nama.*

Figure A4 / *Rajah A4*

Select suitable technology to fulfill Abu Enterprise's requirement in Figure A4.
*Pilih teknologi yang sesuai untuk memenuhi keperluan Abu Enterprise dalam Rajah A4.*

A. Password logging facilities / *Kemudahan log katalaluan*

B. IPSec Filter / *Penapisan IPSec*

C. Bastion host / *Komputer Bastion*

D. Proxy Server / *Pelayan proxy*

CLO3
C1

18. Define the meaning of authentication.
*Takrifkan maksud bagi pengesahan.*

A. Proving one's identity to someone else.
*Membuktikan identiti seorang berbanding seseorang yang lain.*

B. Accepting connection based on password and username.
*Menerima sambungan berdasarkan katalaluan dan nama pengguna.*

C. Creating connection between peer nods.
*Mencipta sambungan antara nod.*

D. Speeding up bandwidth of a network connection.
*Meningkatkan lebar jalur untuk sambungan rangkaian.*

CLO3
C1

19. Identify the purpose of authentication for information system.
*Kenalpasti tujuan pengesahan untuk sistem maklumat.*

A. To give the authenticated user a rights for certain files and directories.
*Untuk memberi pengguna yang telah disahkan hak keatas sesebuah fail dan direktori.*

B. To prove someone authorization based on unique username and password.
*membuktikan kuasa seseorang berdasarkan nama pengguna dan kata laluan yang unik.*

C. To converting data to a format that is meaningless to human being.
*Untuk menukar data ke format yang tidak difahami oleh manusia.*

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

CLO3
C2

20. Encryption is a process of encoding a message to "encrypted information".
Translate encrypted information to cryptographic terminology.
*Penyulitan adalah proses encoding mesej kepada "encrypted information".*
*Terjemahkan penyulitan maklumat kepada terminologi kriptografi.*

A. Structured Text / *Teks berstruktur*

B. Ciphertext / *Ciphertext*

C. Algorithm / *Algoritma*

D. Confidential Text. / Teks *Sulit*

CLO3 C2

21. A Virtual Private Network (VPN) is a private network that uses a public network to connect between users. Choose the criterias of **GOOD** VPN connection.

*Sebuah Virtual Private Network (VPN) adalah rangkaian peribadi yang menggunakan rangkaian umum untuk menghubungkan antara pengguna. Pilih kriteria – kriteria bagi sebuah sambungan VPN yang **BAIK.***

i. Made by well-known manufactures
*Dihasilkan oleh jenama yang terkenal*

ii. Strong authentication.
*Pengesahan yang kuat*

iii. Adequate encryption
*Kod sulit yang mencukupi*

iv. Adherence to standards
*Memenuhi piawaian yang dikehendaki*

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

CLO3 C3

22. Convert I LOVE POLYTECHNICS with keyword "FRIENDS" using substitution cipher method.

*Tukarkan I LOVE POLYTECHNICS dengan kata kunci 'FRIENDS' menggunakan kaedah Substitution Cipher.*

A. B HLVN MLHYTNIAKBIQ
B. A HLVN MLHYTNIBKAIQ
C. B HLVN MLHYTNIBKAIQ
D. A HLVN MLHYTNIAKBIQ

CLO3 C3

23. There are two types of key-based encryption algorithm. Differentiate symmetric with asymmetric encryption algorithm.

*Terdapat dua jenis algoritma penyulitan berasaskan kunci. Bandingkan algoritma penyulitan simetri dengan asimetri.*

A. Symmetric uses secret key whereas asymmetric uses public key.
*Simetri menggunakan kunci rahsia sedangkan tidak simetri menggunakan kunci awam.*

B. Symmetric uses DNSSEC protocol whereas asymmetric uses GSSAPI protocol.
*Simetri menggunakan DNSSEC protokol sedangkan tidak simetri menggunakan protokol GSSAPI.*

C. Symmetric uses cryptanalysis method whereas asymmetric uses cryptology method.
*Simetri menggunakan kaedah 'cryptanalysis' sedangkan simetri menggunakan kaedah 'cryptology'.*

D. Symmetric uses encrypted key whereas asymmetric uses semi-decrypted key.
*Simetri menggunakan kekunci yang disulitkan manakala tidak simetri menggunakan kunci yang disulitkan separa sahaja.*

CLO3 C3

24. An administrator applied VPN connection to his organization. But VPN only protects the network from outside threat. Determine how to protect the host PC's in the organization.
*Seorang pentadbir telah mengaplikasikan sambungan VPN di organisasi beliau. Tetapi VPN hanya melindungi rangkaian daripada ancaman luar. Tentukan bagaimana untuk melindungi komputer di dalam organisasi tersebut.*

A. Implement IPSec
*Melaksanakan IPSec*

B. Enable firewall
*Enable firewall*

C. Install antivirus software
*Memasang perisian antivirus*

D. Use Host-based IDS
*Mengguna Host-based IDS*

CLO3 C1

25. Disaster recovery is the process of restoring critical operations for the resumption of activities after a disaster. Identify the category of disaster.

*Pemulihan bencana adalah proses pemulihan operasi kritikal untuk penyambungan semula aktiviti selepas bencana. Kenal pasti kategori bagi bencana.*

i. Natural disaster / *Bencana semulajadi*
ii. System disaster / *Bencana sistem*
iii. Man-made disaster / *Bencana buatan manusia*
iv. Hardware disaster / *Bencana peralatan*

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

CLO3 C1

26. Identify the plan that describes ways to continue operating until normal computer operations can be restored.

*Kenalpasti rancangan yang menerangkan cara-cara untuk meneruskan operasi sehingga operasi komputer biasa boleh dipulihkan.*

A. Backup
B. Disaster recovery
C. Protection
D. Build structure

CLO3 C2

27. An administrator needs to plan a disaster prevention and recovery system for the organization. Choose the hardware technologies for disaster handlings.

*Seorang pentadbir perlu merancang satu plan mengendalikan bencana dan pemulihan sistem. Pilih teknologi perkakasan bagi mengendalikan bencana.*

A. Clustering
B. Hard disk
C. Intrusion Prevention System
D. Load Balancer

CLO3 C2

28. This disaster recovery technique that offers cost-effective and efficient solutions against recovering from a disaster.It sends multiple replication streams from multiple primary servers to a single DR server.

*Teknik pemulihan bencana yang menggunakan kos yang rendah dan berkesan. Penghantaran keseluruhan data dari server utama kepada Salinan server tunggal.*

Figure A5 / *Rajah A5*

Determine the type of disaster recovery system stated in Figure A5.

*Tentukan jenis sistem pemulihan bencana yang dinyatakan dalam Rajah A5.*

A. Synchronous system
B. Asynchronous system
C. Real time system
D. Redundant system

CLO2 C2 (e) Explain the reconnaissance attack on network environment.
*Jelaskan reconnaissance attack dalam persekitaran rangkaian.*

[2marks]
[*2 markah*]

CLO2 C1 (f) i. Describe what is device hardening.
*Terangkan apakah pengerasan peranti.*

[2marks]
[*2 markah*]

CLO2 C1 ii. List **FIVE (5)** host and server based security components and technologies in device hardening.
*Senaraikan **LIMA(5)** komponen dan teknologi keselamatan berasaskan hos dan server dalam sekatan peranti.*

[5marks]
[*5 markah*]

CLO2 C2 (g) Describe **TWO (2)** primary function of firewall.
*Terangkan **DUA(2)** peranan utama firewall.*

[2marks]
[*2 markah*]

CLO2 C3 (h) Explain how static packet filtering works.
*Jelaskan bagaimana tapisan paket statik berfungsi.*

[2marks]
[*2 markah*]

**QUESTION 2**

***SOALAN 2***

CLO2 C1 (a) (i) List **FOUR (4)** security policy of the operating system.
*Senaraikan **EMPAT (4)** polisi keselamatan bagi sistem pengoperasian.*

[2 marks]
*[2 markah]*

CLO2 C2 (ii) Explain how Microsoft Windows updates system.
*Terangkan bagaimana Microsoft Windows melaksanakan pengemaskinian sistem.*

[2 marks]
*[2 markah]*

CLO2 C3 (iii) Differentiate between a Packet Filter and a Proxy Server.
*Bezakan diantara Packet Filter dan Proxy Server.*

[3 marks]
*[3 markah]*

CLO3 C1 (b) (i) Define the following cryptographic terminologies:
*Takrifkan terminologi bagi kriptografi berikut:*

a. Plain text
b. Encryption
c. Cipher text
d. Decryption
e. Cryptanalysis

[5 marks]
*[5 markah]*

CLO3
C2

(ii) Encrypt the following text using Caesar Cipher encryption method.
*Enkripsikan teks yang berikut dengan menggunakan kaedah penyulitan Caesar Cipher.*

I LIKE INFORMATION SYSTEM SECURITY

a. Shift + 6 / *Anjakan + 6*

b. Shift − 4 / *Anjakan − 4*

[6 marks]
*[6 markah]*

CLO3
C3

(iii) A Virtual Private Network (VPN) is a private network that uses a public network (the Internet) to connect users. Explain **TWO (2)** features of good VPN products.
*Virtual Private Network ( VPN) adalah rangkaian persendirian yang menggunakan rangkaian umum ( Internet) untuk menghubungkan pengguna. Terangkan **DUA (2)** ciri produk VPN yang baik.*

[4 marks]
*[4 markah]*

CLO3
C1

(c) (i) List **FIVE (5)** disaster recovery planning.
*Senaraikan **LIMA (5)** perancangan pemulihan bencana.*

[5 marks]
*[5 markah]*

CLO3
C3

(ii)

This type of backup makes a copy of all data to another set of media, which can be tape, disk or a DVD or CD. The primary advantage to performing this backup during every operation is that a complete copy of all data is available with a single set of media.

*Jenis sandaran ini membuat salinan semua data kepada satu lagi media, sama ada pita, cakera DVD atau CD. Kelebihan utama untuk melaksanakan sandaran ini pada setiap operasi adalah supaya satu salinan lengkap keseluruhan data boleh didapati dengan satu set media.*

Figure B1 / *Rajah B1*

Illustrate the type of backup mentioned in Figure B1.
*Gambarkan jenis sandaran yang dinyatakan dalam Rajah B1.*

[2 marks]
*[2 markah]*

**SOALAN TAMAT**