SULIT

POLITEKNIK MALAYSIA

BAHAGIAN PEPERIKSAAN DAN PENILAIAN
JABATAN PENDIDIKAN POLITEKNIK
KEMENTERIAN PENDIDIKAN TINGGI

JABATAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI

PEPERIKSAAN AKHIR

SESI JUN 2015

FP611: INFORMATION SYSTEM SECURITY

TARIKH : 26 OKTOBER 2015
MASA : 8.30 AM – 10.30 AM (2 JAM)

Kertas ini mengandungi **LIMA BELAS (15)** halaman bercetak.
Bahagian A: Objektif (30 soalan)
Bahagian B: Struktur/Esei (4 soalan)
Dokumen sokongan yang disertakan : Tiada

JANGAN BUKA KERTAS SOALAN INI SEHINGGA DIARAHKAN

(CLO yang tertera hanya sebagai rujukan)

SULIT

SECTION A : 30 MARKS
BAHAGIAN A : 30 MARKAH

INSTRUCTION:
This section consists of **TWENTY (20)** objective questions. Mark your answers in the OMR form provided.

ARAHAN :
*Bahagian ini mengandungi **DUA PULUH (20)** soalan objektif. Tandakan jawapan anda di dalam borang OMR yang disediakan.*

CLO1
C1

1. Which of the following is **NOT** the reason why we need security for our network?
*Antara berikut yang manakah **BUKAN** alasan mengapa kita memerlukan keselamatan untuk rangkaian kita?*

A. Confidentiality / *Sulit*
B. Affordability / *Kemampuan*
C. Integrity / *Integrity*
D. Availability / *Kesesuaian*

CLO1
C1

2. Select the best answer that refers to the statement "A threat that occurs as a result of carelessness"?
Pilih jawapan terbaik yang merujuk kepada pernyataan "Ancaman yang berlaku disebabkan oleh kecuaian"?

A. Unauthorized Disclosure / *pendedahan tanpa kebenaran*
B. Information theft / *pencurian maklumat*
C. Accidental data loss / *kehilangan maklumat secara tidak sengaja*
D. Information warfare / *peperangan maklumat*

CLO1
C1

3. Which of the following statements is best describe characteristics of Open Security Models?
Yang manakah di antara pernyataan berikut menerangkan ciri-ciri Model Keselamatan Terbuka?

A. Easy to implement and all user is not trustworthy.
Mudah dilaksanakan dan semua pengguna tidak boleh dipercayai.
B. All user is trustworthy and easy to implement
Semua pengguna dipercayai dan mudah untuk dilaksana.
C. Maximum security level and difficult to implement.
Level keselamatan maksimum dan sukar untuk dilaksana.
D. Minimum security level and high cost to implement.
Level keselamatan minimum dan kos tinggi untuk dilaksana.

CLO1 C1

4. Hacking is a method of breaking into information system without proper authentication and permission.
"Hacking" adalah satu kaedah memecah masuk ke dalam sistem maklumat tanpa pengesahan dan kebenaran.

A. TRUE / *BETUL* B. FALSE / *SALAH*

CLO1 C1

5. " It is an inherent weakness in the design, configuration, implementation or management of a network or system that renders it to be susceptible to a threat."
"Ia adalah titik lemah dalam rekabentuk, konfigurasi, pelaksanaan atau pengurusan satu rangkaian atau sistem yang menyebabkannya terdedah kepada ancaman."

Identify the suitable terminology based on statement above.
Pilih terminology yang sesuai berdasarkan kenyataan di atas.

A. Availability / *Kebolehsediaan*
B. Resistance / *Rintangan*
C. Weaknesses / *Kelemahan*
D. Powerlessness / *Kehilangan kuasa*

CLO2 C1

6.

It appears to be a useful software but will actually do damage once installed or run.
Ia nampak seperti aplikasi yang berguna namun sebaliknya memberi kemusnahan apabila dipasang atau dijalankan.

The statement above describes…
Penyataan di atas menerangkan ...

A. Sniffing
B. Trojan Horses
C. Viruses
D. Worms

CLO2 C2

7.

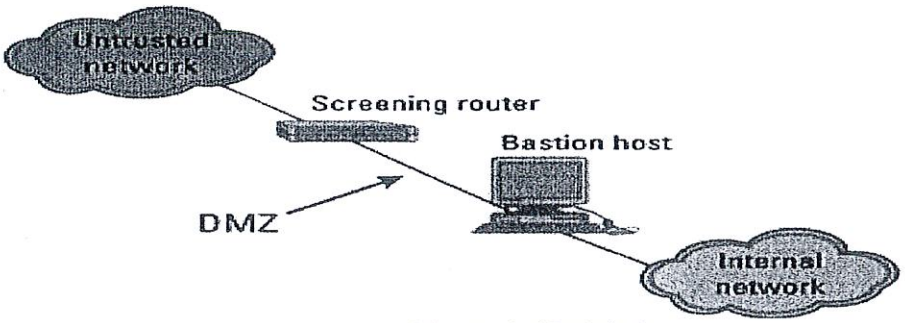

Figure 1 / *Rajah 1*

What type of firewall architecture is based on features listed in Figure 1 above?
Apakah jenis senibina "firewall" yang berasaskan pada ciri-ciri yang disenaraikan dalam Rajah 1 di atas?

A. Screened Subnet
B. Screened Host
C. Dual home host
D. Bastion Host

CLO2 C2

8. Given below are the three common technologies used in building firewalls, **EXCEPT** _____ .
*Dibawah ini adalah tiga teknologi umum yang digunakan dalam pembuatan "firewall" **KECUALI** _____ .*

A. Static packet filtering / *Penapis paket statik*
B. IP packet Filtering / *Penapis paket ip*
C. Dynamic packet filtering / *Penapis paket dinamik*
D. Proxy Filter / *penapis proxy*

CLO2 C2

9. What is the function of Dynamic Packet Filter?
Apakah fungsi Penapis Paket Dinamik?

A. Examines the role of packets rather than just filtering them.
Meneliti peranan paket bukan sekadar menapis sahaja.
B. Examines the contents of packet rather than just filtering them.
Meneliti kandungan paket bukan sekadar menapis sahaja.
C. Removes the content of packet rather than just filtering them.
Membuang kandungan paket bukan sekadar menapis sahaja.
D. Examines the contents of packets rather than just changing them.
Meneliti kandungan paket bukannya hanya menukar mereka.

CLO2 C2

10. Which **ONE (1)** of the technology employed in building firewall using filtering rules which is determine whether to deny or permit packets are permanent?
*Manakah **SATU (1)** teknologi yang digunakan dalam membangunkan "firewall" menggunakan peraturan penapisan sama ada menafikan atau membenarkan paket-paket secara kekal?*

A. Dynamic Packet filtering
Penapisan Paket Bolehubah
B. Circuit Level Gateways
Jambatan Peringkat Litar
C. Static packet filtering
Penapisan Paket Kekal
D. Proxy based firewall
Proksi sebagai dinding api

CLO2 C2

11. Which of the statement shows the difference between Patches and Hotfixes?
Yang manakah menunjukkan perbezaan Patches and 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 sementara "Hotfixes" biasanya perubahan kecil untuk perisian

CLO2 C2

12. What is the system policy used to control access to the computers and domain resources, and can override permissions that have been set on specific objects?
Apakah sistem polisi yang digunakan untuk mengawal capaian komputer dan sumber domain, dan boleh "override permission" yang telah ditetapkan pada objek tertentu?

A. Password
Katalaluan

B. Account
Akaun

C. User right
Hak pengguna

D. Audit
Audit

CLO2 C3

13. Choose the correct steps that can be implemented when securing a Windows system.
Pilih langkah-langkah yang betul untuk melaksanakan ciri keselamatan pada system Windows.

i. Keep up to date with hotfixes and installation of service packs
Sentiasa lakukan "hotfix" dan instalasi "service packs"

ii. Configure a proxy server
Mengkonfigur pelayan proxy

iii. Use NTFS on all your partitions
Gunakan NTFS pada semua partition

iv. Keep the recycle bin empty at all times
Pastikan "Recycle Bin" sentiasa kosong

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

CLO3
C3

14. In asymmetric key encryption, the decryption key is called _____ while the encryption key is called _____.
Dalam penyulitan simetri utama, penyahsulitan itu dipanggil sebagai _____ manakala kunci penyulitan dipanggil _____.

A. Private, public / *persendirian, umum*
B. Public, private / *umum, persendirian*
C. Asymmetric, non-asymmetric / *Asymmetric, bukan simetri*
D. Symmetric, non-symmetric / *Simetri, bukan simetri*

CLO3
C3

15. What is a Cryptanalysis process?
Apakah proses "Cryptanalysis"?

A. It is a process of encryption and decryption.
Ia merupakan satu proses penyulitan dan nyahpenyulitan.
B. It is a process of breaking the secret codes.
Ia merupakan satu proses untuk memecahkan kod rahsia.
C. It is an art and science of making secret codes.
Ia merupakan satu seni dan sains dalam mencipta kod rahsia.
D. It is a research and study of making and breaking secret codes.
Ia merupakan satu kajian dalam mencipta dan memecahkan kod rahsia.

CLO3
C3

16. What attack that can be launched if encryption is not implemented?
Apakah serangan yang boleh dilancarkan jika enkripsi tidak dilaksanakan?

i. Banking information disclosure
Pendedahan maklumat perbankan
ii. Interruption while transmitting data
Gangguan ketika menghantar data
iii. Unauthorized access to private data
Akses tanpa kebenaran kepada data peribadi
iv. Eavesdropping
Mencuri dengar

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

CLO3 C3 17.

	1	2	3	4	5
	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Encryption Table Grid

Transform the encryption message "**I LIKE NETWORK SECURITY**" by using Encryption Table Grid above.
*Tukarkan mesej encryption "**I LIKE NETWORK SECURITY**" dengan menggunakan Jadual "Grid encryption" di atas.*

A. 42, 13, 42, 52, 51, 33, 51, 44, 25, 43, 24, 52, 34, 51,54,24, 42, 44, 45

B. 24, 31,24, 25 ,15, 33,15, 44, 52, 34, 42, 25, 43, 15, 45, 42, 24, 44, 54

C. 42, 13, 42, 52 ,51, 43, 24, 52 34,51, 33, 51, 44, 25,54,24, 42, 44, 45

D. 24, 13, 42, 44, 25, 43, 52 ,51, 33, 51, 24, 52 34,51,54,24, 42, 44, 54

CLO3 C3 18. Based on Figure 2 below, describe what type of VPN it is referring to?
Daripada Gambarajah 2,nyatakan apakah jenis VPN yang dimaksudkan?

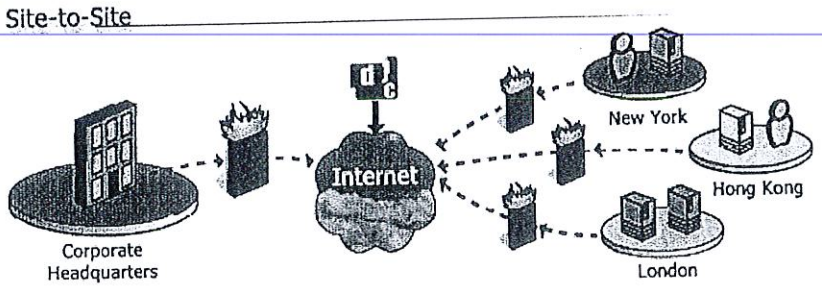

Figure 2 / *Rajah 2*

A. Intranet VPN/*VPN rangkaian dalaman*
B. Extranet VPN/*VPN rangkaian luar*
C. Remote Acess VPN/*VPN kawalan akses*
D. Local VPN/*VPN tempatan*

CLO3 C3

19. This disaster recovery system is designed to make sure that no input/output transaction can be done to the primary system until the backup system's transaction were successfully done. What type of recovery system mentioned by the above statement?
Sistem pemulihan bencana ini direka agar tiada transaksi input/output boleh dilakukan pada sistem utama sehinggalah transaksi itu telah berjaya dilakukan di storan sistem sokongan. Apakah jenis sistem pemulihan bencana yang dimaksudkan dalam pernyataan di atas?

A. Synchronous system
B. Asynchronous system
C. Primary-first system
D. Redundant system

CLO3 C3

20.

X is an electrical equipment that provides emergency power to a load when the input power source fails *X adalah peralatan elektrik yang memberikan kuasa tambahan untuk bebanan apabila sumber kuasa input gagal*

What is the device described by the above statement?
Apakah jenis peranti berdasarkan pernyataan di atas?

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

SECTION B : 70 MARKS

BAHAGIAN B : 70 MARKAH

INSTRUCTION:
This section consists of **FOUR (4)** structured questions. Answer **ALL** questions.

ARAHAN:
*Bahagian ini mengandungi **EMPAT (4)** soalan berstruktur. Jawab semua soalan.*

QUESTION 1

SOALAN 1

CLO1
C1

a) List **TWO (2)** Security Model in Information System Security.
*Senaraikan **DUA (2)** Model Keselamatan di dalam Keselamatan Sistem maklumat.*

[2 marks]
[2 markah]

CLO1
C1

b)

i) Explain the example of attacks in Information System Security for Reconnaissance Attack and Malicious Code Attack.
Terangkan contoh serangan di pangkalan Sistem Maklumat Keselamatan bagi "Reconnaissance Attack" dan "Malicious Code Attack".

[2 marks]
[2 markah]

CLO1
C1

ii) Explain briefly each of the following threat:
Jelaskan setiap ancaman yang berikut:

- Information Theft
- Information Warfare

[2 marks]
[2 markah]

QUESTION 2

SOALAN 2

CLO2 C2

a) List **TWO (2)** network scanning tools.
*Senaraikan **DUA (2)** alat pengimbas rangkaian.*

[2 marks]
[2 markah]

CLO2 C2

b) i) What is the definition of firewall?
Apakah definisi "firewall"?

[2 marks]
[2 markah]

CLO2 C2

ii) Explain the process of device hardening in host.
Terangkan process "device hardening" *pada komputer.*

[2 marks]
[2 markah]

CLO2 C2

iii) Explain how a proxy passes the network traffic.
Terangkan bagaimana proksi melalui laluan rangkaian.

[2 marks]
[2 markah]

CLO2 C2

c) Explain the following System Policy that is implemented on Microsoft Windows Operating System in terms of:
Terangkan sistem polisi yang dilaksanakan dalam sistem pengoperasian Microsoft Windows berdasarkan:

i) Audit/ *audit*
ii) User rights/*hak pengguna*

[4 marks]
[4 markah]

d)

The Director of OneTech Company wants to send a private and confidential message to his client. His IT Technician encrypts the message from plain text into cipher text.
Pengarah syarikat OneTech hendak menghantar mesej yang peribadi dan sulit kepada pelanggannya. Juruteknik IT syarikat beliau telah mengenkripsi mesej tersebut daripada "plain text" kepada "cipher text".

CLO3 C3

i) Explain the cryptography terminology "Cipher text".
Terangkan istilah kriptografi "Teks Sifer".

[2 marks]
[2 markah]

CLO3 C3

ii) List **TWO (2)** methods of encryption.
*Senaraikan **DUA (2)** kaedah penyulitan*

[2 marks]
[2 markah]

CLO3 C3

iii) Describe **TWO (2)** advantages of using encryption in network security.
*Terangkan **DUA (2)** kelebihan menggunakan penyulitan dalam keselamatan rangkaian*

[2 marks]
[2 markah]

CLO3 C3

iv) For question (iv) and (v) please refer to the statement below:
Bagi soalan (iv) dan (v) sila rujuk pernyataan dibawah:

"A class of algorithms for cryptography that uses the same cryptographic keys for both encryption of plain text and decryption of cipher text. This statement describes on _____."
"Satu kelas algoritma kriptografi untuk yang menggunakan kunci kriptografi yang sama untuk kedua-dua penyulitan dan penyahsulitan "plaintext" dan "cipher text". Kenyataan diatas menerangkan _____."

[2 marks]
[2 markah]

CLO3
C3

v) Sketch a diagram showing the statement above.
Lakarkan satu gambarajah yang menunjukkan kenyataan di atas.

[2 marks]
[2 markah]

CLO3
C3

e) i) Explain the differences between RAID 1 and RAID 2
Terangkan perbezaan diantara RAID 1 dan RAID 2.

[2 marks]
[2 markah]

CLO3
C3

ii) There are two types of disaster recovery system which is Synchronous System and Asynchronous System. Illustrate the Asynchronous System.
Terdapat dua jenis sistem pemulihan bencana iaitu Sistem Synchronous dan Sistem Asynchronous. Lukiskan Sistem Asynchronous.

[2 marks]
[2 markah]

CLO3
C3

iii) Explain the differences between Full Backup and Incremental Backup.
Terangkan perbezaan antara Sandaran penuh dan Sandaran Peningkatan.

[2 marks]
[2 markah]

QUESTION 3

SOALAN 3

CLO1 C1

a) Define the following threats:

Terangkan ancaman berikut :

i) Information Theft / M*encuri Maklumat*

ii) Unauthorized Disclosure / *Pendedahan yang tidak dibenarkan*

[6 marks]

[6 markah]

CLO1 C1

b) List **TWO (2)** characteristics of a good password.

*Senaraikan **DUA (2)** ciri-ciri kata laluan yang baik.*

[3 marks]

[3 markah]

QUESTION 4

SOALAN 4

CLO2 C2

a) Explain the meaning of attacker and hacker.

Terangkan maksud "attacker" dan "hacker".

[3 marks]

[3 markah]

CLO2 C2

b) i) Explain the features of personal firewall.

Terangkan ciri-ciri "personal firewall".

CLO2 C2

ii) Explain how Dynamic Packet Filtering works.

Terangkan bagaimana penapisan paket dinamik bekerja.

[6 marks]

[6 markah]

CLO2 C2 c) i)

The security of the operating system can be enhanced by applying security policy such as Passwords, Account, Audit and User Rights.
Keselamatan sistem pengoperasian boleh dipertingkatkan dengan menggunakan polisi keselamatan seperti kata laluan, akaun, audit dan hak pengguna.

Explain any **TWO (2)** of the security policy stated above.
*Terangkan**DUA (2)** polisi keselamatan yang dinyatakan di atas.*

[3 marks]
[3 markah]

CLO2 C2 ii) Differentiate packet filter and proxy server.
Bezakan di antara "packet filter" dan "proxy server".

[3 marks]
[3 markah]

CLO3 C3 d) i) Briefly explain decryption.
Terangkan tentang penyahsulitan.

[3 marks]
[3 markah]

CLO3 C3 ii) Sketch a diagram showing the process of asymmetric-key encryption.
Lakarkan satu gambarajah yang menunjukkan proses penyulitan simetri utama.

[3 marks]
[3 markah]

e)

- Records only those files that have changed since the last Full backup.
- Takes less time to record than a Full backup.
- Takes less time to restore than an Incremental backup.
- The restoring process requires only two tapes.

- *Merekod hanya fail-fail yang telah berubah sejak sandaran penuh terakhir*
- *Mengambil masa yang singkat untuk merekod berbanding sandaran penuh*
- *Mengambil masa yang singkat untuk menyimpan berbanding sandaran tambahan*
- *Proses penyimpanan hanya memerlukan dua pita.*

CLO3
C3

i) Based on the statement above choose which type of backup is used and briefly explain the advantages of it.
Berdasarkan kenyataan di atas pilih jenis sandaran yang digunakan dan terangkan secara ringkas kelebihannya.

[3 marks]
[3 markah]

CLO3
C3

ii) Briefly describe the activities of disaster recovery testing.
Terangkan aktiviti yang melibatkan ujian pemulihan bencana.

[3 marks]
[3 markah]

END OF QUESTION
SOALAN TAMAT