(11)

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 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]

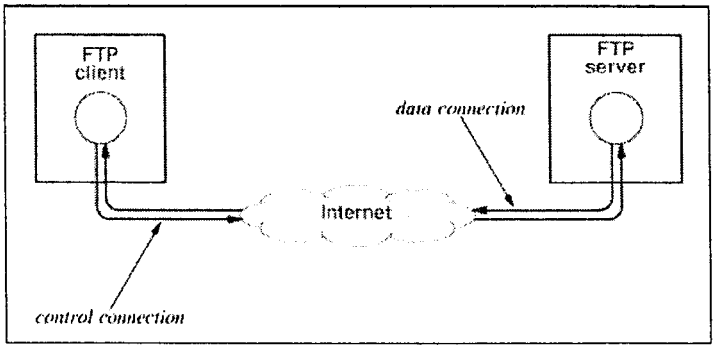

Figure B1/Rajah B1

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]

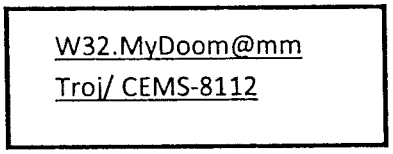

Figure B2/Rajah B2

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