SULIT

POLITEKNIK MALAYSIA

BAHAGIAN PEPERIKSAAN DAN PENILAIAN
JABATAN PENDIDIKAN POLITEKNIK
KEMENTERIAN PENDIDIKAN TINGGI

JABATAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI

PEPERIKSAAN AKHIR

SESI JUN 2015

FN612: NETWORK SECURITY

TARIKH : 21 OKTOBER 2015
MASA : 8.30 AM – 10.30 AM (2 JAM)

Kertas ini mengandungi **SEMBILAN BELAS (19)** halaman bercetak.
Bahagian A: Objektif (20 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)

SECTION B: 70 MARKS
BAHAGIAN B: 70 MARKAH

INSTRUCTION:
This section consists of **TWO (2)** structured questions and **TWO (2)** essay questions. Answer **ALL** questions in the answer booklet.

ARAHAN:
*Bahagian ini mengandungi **DUA (2)** soalan berstruktur dan **DUA (2)** soalan esei. Jawab semua soalan di dalam buku jawapan yang disediakan.*

QUESTION 1

SOALAN 1

CLO1
C1

a) Define the integrity concept in secure network system.

Nyatakan konsep integriti dalam sistem keselamatan rangkaian.

[2 marks]
[*2 markah*]

CLO1
C2

b) Based on the information in Figure B1, state the type of attack that occurred and describe the named attack.

Berdasarkan informasi di dalam Rajah B1, nyatakan jenis serangan yang berlaku dan namakan jenis serangan.

"An attacker creates a website very similar to the CIMB Clicks website. Then he traps CIMB users to use his forged website as a decoy to get their username and password." *"Penggodam mencipta laman web sama seperti laman web CIMB Click. Kemudian dia memerangkap pengguna CIMB Click menggunakan laman web palsu tersebut dan seterusnya berjaya mendapatkan nama dan kata laluan mereka".*

Figure B1/ Rajah B1

[2 marks]
[*2 markah*]

CLO1 C3

c) Most of the computing structure use firewall to protect the network environment. Illustrate the diagram that shows the location of the firewall in network infrastructure.

Kebanyakan struktur komputer menggunakan firewall untuk melindungi sistem rangkaian. Lakarkan gambarajah yang menunjukkan lokasi firewall dalam infrastruktur rangkaian tersebut.

[2 marks]
[*2 markah*]

CLO1 C2

d) Distinguish between patch and hotfix.
Bezakan antara hotfix dan patch.

[2 marks]
[*2 markah*]

CLO2 C1

e) Determine the function of Network Mapper (Nmap) as network monitoring tool software.

Tentukan fungsi Network Mapper (Nmap) sebagai perisian pemantauan rangkaian.

[2 marks]
[*2 markah*]

CLO2 C2

f) Identify the difference between static packet filtering and dynamic packet filtering.
Kenal pasti perbezaan di antara 'static packet filtering' dan 'dynamic packet filtering'.

[2 marks]
[*2 markah*]

CLO2 C1

g) In Microsoft Windows, user can perform several System Policies to manage their security approaches. List **FOUR (4)** of the System policies that can be applied.

*Dalam Microsoft Windows, pengguna boleh melakukan beberapa Polisi Sistem untuk menguruskan pendekatan keselamatan mereka. Senaraikan **EMPAT (4)** Polisi Sistem yang boleh digunakan.*

[4 marks]
[*4 markah*]

QUESTION 2

SOALAN 2

CLO2 C2

a) Describe the purpose of managing System Log Files using Log Enhancer.

Terangkan tujuan menguruskan Fail Log System menggunakan Log Enhancer.

[2 marks]
[*2 markah*]

CLO2 C2

b) Identify **TWO (2)** ways (command) how to get the system log files using LINUX.

*Kenalpasti **DUA (2)** cara (arahan) bagaimana untuk mendapatkan fail log sistem menggunakan LINUX.*

[2 marks]
[*2 markah*]

CLO2 C1

c) List **FOUR (4)** human unique characteristics that can be used for biometric identification.

*Senaraikan **EMPAT (4)** ciri unik manusia yang boleh digunakan untuk pengenalan biometrik.*

[2 marks]
[*2 markah*]

CLO3 C2

d) Assigned other name of algorithm to private key cryptography and public key cryptography.

Beri nama lain kepada algoritma kriptografi kunci 'private' dan kriptografi kunci 'public'.

[2 marks]
[*2 markah*]

CLO3 C2

e) Describe the primary weakness of symmetric algorithm.

Huraikan kelemahan utama algoritma simetri.

[2 marks]
[*2 markah*]

CLO3 C3

f) Describe **TWO (2)** types of VPN.
*Terangkan **DUA (2)** jenis VPN.*

[2 marks]
[*2 markah*]

CLO3 C3

g) Identify **TWO (2)** differences between symmetric key and asymmetric key used in encryption algorithms.
*Kenal pasti **DUA (2)** perbezaan antara kunci symmetric dan kunci asymmetric yang digunakan di dalam algoritma enkripsi.*

[4 marks]
[*4 markah*]

CLO3 C3

h) You are trying to backup on your hard drive. You want the backups to finish as quickly as possible and only backup the files that have changed since the last backup. So, the most suitable backup is_____backup.

Anda cuba melakukan salinan pendua pada cakera keras anda. Anda mahu salinan pendua itu selesai secepat mungkin dan hanya menyalin fail yang berubah pada salinan yang terakhir. Justeru itu, jenis salinan _____adalah yang paling sesuai.

[2 marks]
[*2 markah*]

QUESTION 3

SOALAN 3

M-Technology Berhad is in process to create a secure network and systems for their organization. The network administrator for the company, needs to do an analysis for their network before he proceed to develop secure networking system to the organization.

M-Technology Berhad dalam proses untuk mewujudkan satu sistem rangkaian yang selamat untuk organisasi mereka. Pentadbir rangkaian syarikat, perlu melakukan analisa untuk rangkaian mereka sebelum membangunkan sistem rangkaian selamat untuk organisasi.

CLO1
C3

a) As the network administrator for M-Technology, choose types of internet services that mostly used by an organization. Provide example each of the services.

Sebagai pentadbir rangkaian di M-Technology, pilih jenis perkhidmatan internet yang digunakan oleh kebanyakan organisasi. Berikan contoh setiap satu daripada perkhidmatan tersebut.

[3 marks]
[*3 markah*]

CLO1
C4

b) Creating secure network environment can prevent M-Technology organization from threats. Classify the threats activity that could happen in unsecured network. Give your explanations based on the answer given.

Mewujudkan persekitaran rangkaian yang selamat boleh mencegah organisasi M-Teknologi dari ancaman. Kelaskan aktiviti ancaman yang boleh berlaku dalam rangkaian yang tidak selamat. Beri penerangan anda berdasarkan jawapan yang diberikan.

[3 marks]
[*3 markah*]

CLO1
C1

c) List **THREE (3)** types of malicious codes which can cause harm for most organizations as well as individual home users.
*Senaraikan **TIGA (3)** jenis kod malicious yang boleh menyebabkan bahaya kepada organisasi dan juga kepada pengguna di rumah.*

[3 marks]
[*3 markah*]

CLO1
C1

d) Identify **THREE (3)** typical options of a firewall's base rule.
*Kenal pasti **TIGA (3)** pilihan tipikal peraturan asas sebuah firewall.*

[3 marks]
[*3 markah*]

CLO2
C2

e) Describe Intrusion Prevention System (IPS).
Terangkan Intrusion Prevention System (IPS).

[3 marks]
[*3 markah*]

CLO2
C2

f) State **ONE (1)** difference between antivirus software and personal firewall.
*Nyatakan **SATU (1)** perbezaan diantara perisian antivirus dan firewall persendirian.*

[3 marks]
[*3 markah*]

CLO2
C1

d) Transform the word **"I LOVE ENCRYPTION"** to its corresponding cipher text using Caesar Cipher method where letter of the alphabet were shifted by three positions to the right.

*Ubah perkataan **"I LOVE ENCRYPTION"** kepada cipher text yang sepadan menggunakan kaedah Caesar Cipher yang mana huruf dalam alphabet beralih dengan tiga posisi ke kanan.*

[4 marks]
[*4 markah*]

CLO3
C2

e) Explain how dynamic packet filtering technology can help in improving a firewall's performance?

Terangkan bagaimana teknologi penapisan 'packet' secara dinamik boleh membantu dalam meningkatkan prestasi firewall?

[2 marks]
[*2 markah*]

CLO3
C3

f) Describe the functions of the following technology in handling server disaster:

Huraikan fungsi teknologi berikut dalam pengendalian bencana server:

i. Redundant Array of Independent Disk (RAID)
ii. Uninterruptible Power Supply (UPS)
iii. Tape Backup

[3 mark]
[*3 markah*]

END OF QUESTION

SOALAN TAMAT

QUESTION 4
SOALAN 4

CLO2
C1

a) IP Security (IPSec) is a protocol suite for securing Internet Protocol (IP) communications. Write **TWO (2)** benefits of implementing IP Security (IPSec).
*IP Security (IPSec) adalah satu protokol untuk melindungi komunikasi Internet Protokol (IP). Tulis **DUA (2)** kelebihan melaksanakan IP Security (IPSec).*

[3 marks]
[*3 markah*]

CLO2
C2

b) Describe **THREE (3)** vulnerabilities that exist in Internet Information Services (IIS).
*Huraikan **TIGA (3)** kelemahan yang wujud dalam Internet Information Services (IIS).*

[3 marks]
[*3 markah*]

CLO2
C1

c) Refer to the figure B8 below, identify the type of encryption method being used.
Merujuk kepada rajah B8 dibawah, kenalpasti jenis kaedah enkripsi yang digunakan.

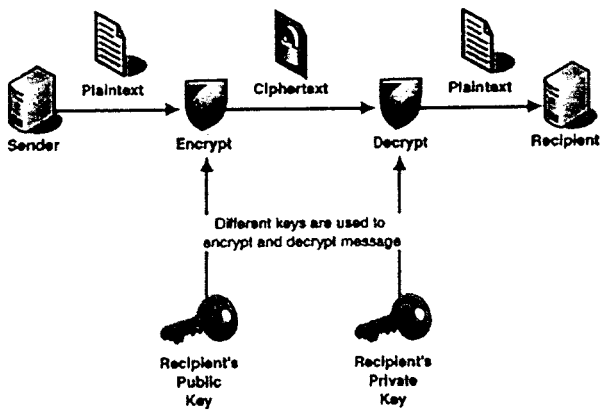

Figure B2 / *Rajah B2*

[3 marks]
[*3 markah*]