SECTION B: 55 MARKS
BAHAGIAN B: 55 MARKAH

INSTRUCTION:
This section consists of **TWO (2)** structured question. Answer **ALL** questions.

ARAHAN:
*Bahagian ini mengandungi **DUA (2)** soalan struktur. Jawab **SEMUA** soalan.*

QUESTION 1

SOALAN 1

CLO1
C3

(a) Associate the term "Penetration Testing" to the correct goal of network security. Justify your answer.

Kaitkan istilah "Ujian Penembusan" ke matlamat keselamatan rangkaian yang betul. Jelaskan jawapan anda..

[2 marks]

[*2 markah*]

CLO1
C2

(b) (i) Describe technology weaknesses in relation to security vulnerabilities.

Jelaskan kelemahan teknologi yang berkait dengan kelemahan keselamatan.

[2 marks]

[2 *markah*]

(ii) Identify **ONE (1)** example of technology weakness.

*Kenal pasti **SATU (1)** contoh kelemahan teknologi.*

[1 marks]

[1 *markah*]

CLO1
C3

(c) Practice **TWO (2)** ways to do a denial of service (DoS) attack.

*Praktikkan **DUA (2)** cara untuk membuat serangan* denial of service *(*DoS*).*

[2 marks]

[*2 markah*]

CLO1
C1

d) Write down **FOUR (4)** types of Intrusion Detection System (IDS)

*Tulis **EMPAT (4)** jenis Sistem Pengesan Pencerobohan (IDS)*

[4 marks]

[*4 markah*]

CLO1
C2

e) (i) Identify the function of a Stateful Packet Filter

Kenal pasti fungsi 'Stateful Packet Filter'

[2 marks]

[*2 markah*]

(e) (ii) Describe how Dynamic Packet Filter works to block unwanted traffic

Huraikan bagaimana 'Dynamic Packet Filter' *berfungsi untuk menyekat lalu lintas yang tidak diingini*

[2 marks]

[*2 markah*]

CLO1
C3

(f) There are various intrusion prevention strategies that can be used to prevent attacks. Implement the following strategies:

Terdapat pelbagai strategi pencegahan pencerobohan yang boleh digunakan untuk menghalang serangan. Laksanakan strategi berikut:

(i) Session Interception

Pemintasan Sesi

[3 marks]
[*3 markah*]

(ii) Gateway Intrusion Detection

Pengesanan Pencerobohan Gateway

[3 marks]
[*3 markah*]

CLO1 C4

(g) Correlate the following situation with the **CORRECT** type of VPN.

Hubung kaitkan situasi di bawah dengan jenis VPN *yang* ***BETUL****.*

i. Company FRP Sdn Bhd has three branches. They want to connect all of them together (securely) into a single network.

Syarikat FRP Sdn.Bhd. mempunyai tiga cawangan. Mereka mahu menghubungkan semua cawangan tersebut bersama (secara selamat) ke dalam satu rangkaian.

ii. Company Xylisoft Sdn Bhd wishes to connect to its partner's network. One company's LAN is connected with another company's LAN to share certain information for better business relationships.

Syarikat Xylisoft Sdn.Bhd berharap untuk berhubung dengan rangkaian rakan kongsi mereka. LAN *syarikat saling dihubungkan dengan* LAN *syarikat lain untuk berkongsi maklumat tertentu untuk hubungan perniagaan yang lebih baik.*

iii. Hamdan is working from home. He wish to connect to his Head Quarters Office using VPN.

Hamdan bekerja dari rumah. Dia berharap untuk berhubung dengan ibu pejabat menggunakan VPN.

iv. Several companies work together in a secure, shared network environment while preventing access to their intranets.

Beberapa syarikat berkerja secara bersama dalam satu persekitaran yang selamat dan terkongsi, disamping mengelakkan akses ke intranet *mereka.*

[4 marks]
[*4 markah*]

QUESTION 2

SOALAN 2

CLO1 C1 (a) State **THREE (3)** actions that can be taken to ensure the BIOS is secure.

*Nyatakan **TIGA (3)** tindakan yang boleh diambil untuk memastikan BIOS dalam keadaan selamat.*

[3 marks]

[*3 markah*]

CLO1 C2 (b) Describe each type of Rootkit Revealer as listed in the following:

Huraikan setiap jenis Rootkit Revealer *seperti yang disenaraikan di bawah:*

i. Persistent Rootkits.

ii. Memory-Based Rootkits.

iii. User-mode Rootkits

iv. Kernel Mode Rootkits

[4 marks]

[*4 markah*]

CLO1 C3 (c) Linux OS uses different mechanisms for data and network security. Apply **THREE (3)** mechanisms that will be used, by giving its explanation.

*OS Linux menggunakan mekanisme yang berbeza untuk keselamatan data dan rangkaiannya. Aplikasikan **TIGA (3)** mekanisme yang digunakan berserta penjelasan.*

[6 marks]

[*6 markah*]

CLO1 C4

(d) "Kerberos is an authentication protocol to check the authenticity of the client and computer servers in an open network". Correlate this statement with the **FIVE (5)** important advantages of the Kerberos in relation of domain security or trusts.

"Kerberos *adalah protokol pengesahan untuk memeriksa kesahihan klien dan* server *komputer di dalam rangkaian terbuka". Hubungkaitkan penyataan ini dengan **LIMA (5)** kelebihan penting* Kerberos *berkaitan dengan keselamatan* domain *atau* trusts.

[5 marks]

[*5 markah*]

CLO1 C2

(e) Identify **THREE (3)** mechanisms that could be applied to the workstations of the workers in order to maintain the physical security.

*Kenal pasti **TIGA (3)** mekanisme yang boleh diaplikasikan kepada ruang kerja pekerja untuk mengekalkan keselamatan fizikal.*

[3 marks]

[*3 markah*]

CLO1 C3

(f) Relate the methods that should be applied by the network security administrator in order to maintain the data integrity in system and backups.

Kaitkan kaedah yang perlu diterapkan oleh pentadbir keselamatan rangkaian untuk mengekalkan integriti data dalam sistem dan backup.

[5 marks]

[*5 markah*]

CLO1
C4

(g) Wireless network always exposed to attack such as, eavesdropping, denial of service and social engineering. Two of these attacks has occurred now at your company, which are eavesdropping and social engineering. As an IT Manager, solve this problem to get you company secured as before.

Rangkaian tanpa wayar selalu terdedah dengan serangan seperti eavesdropping, denial of service *dan* social engineering. *Dua daripada serangan tersebut telah berlaku sekarang di syarikat anda, iaitu* eavesdropping *dan* social engineering. *Sebagai seorang Pengurus IT, selesaikan masalah tersebut untuk melindungi syarikat anda seperti sebelum ini.*

[4 marks]

[*4 markah*]

SOALAN TAMAT