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 struktur. Jawab **SEMUA** soalan.*

QUESTION 1

SOALAN 1

CLO1
C3

(a) Employees are increasingly connecting to company networks remotely via mobile devices such as laptops and smartphones. Remote access needs to satisfy the Confidentiality, Integrity and Availability (CIA) requirements to be efficient and secure. Apply the relevant solution in terms of Confidentiality and Availability.

Semakin ramai pekerja mengakses ke rangkaian syarikat dari jarak jauh melalui peranti mudah alih seperti komputer riba dan telefon pintar. Akses jauh perlu memenuhi keperluan Kerahsiaan, Integriti dan Ketersediaan (CIA) untuk menjadi efisien dan selamat. Berikan penyelesaian yang relevan dari segi Kerahsiaan dan Ketersediaan.

[2 marks]

[*2 markah*]

CLO1
C2

(b) Briefly describe the term 'vulnerability' in the context of network security and provide **ONE (1)** example of vulnerability in a network.
*Huraikan secara ringkas istilah 'kelemahan' dalam konteks keselamatan rangkaian dan berikan **SATU(1)** contoh kelemahan di dalam rangkaian.*

[3 marks]
[*3 markah*]

CLO1
C3

(c) A vulnerability assessment involves trying to detect network and system vulnerabilities that could cause potential harm. Apply **TWO (2)** actions that could be taken in vulnerability assessment.
*Penilaian kelemahan melibatkan cara untuk mengesan kelemahan pada rangkaian dan sistem yang boleh menyebabkan kemudaratan. Aplikasikan **DUA (2)** tindakan yang boleh diambil dalam penilaian kelemahan.*

[2 marks]
[*2 markah*]

CLO1
C1

(d) State **FOUR (4)** usages of firewall in a network.
*Nyatakan **EMPAT (4)** kegunaan Firewall dalam sesebuah rangkaian.*

[4 marks]
[*4 markah*]

CLO1
C2

(e) There are serveral Virtual Private Network (VPN) tunneling protocols including Internet Protocol Security (IPSec) and Point-to-point Tunneling Protocol (PPTP). Compare both protocols.

Terdapat beberapa protokol bagi 'Virtual Private Network (VPN)' termasuk Internet Protocol Security (IPSec) dan Point-to-point Tunneling Protocol (PPTP). Bandingkan kedua-dua protokol tersebut.

[4 marks]
[*4 markah*]

CLO1
C3

(f) The system administrator wishes to monitor users' access to external websites. Illustrate how a proxy works in securing information system. Support your illustration with explanation on each process.

Pentadbir sistem ingin memantau pengguna yang akses ke laman web luaran. Lakarkan bagaimana proksi berfungsi dalam menjamin keselamatan sistem maklumat. Sokong lakaran anda dengan penjelasan pada setiap proses.

[6 marks]
[*6 markah*]

CLO1
C4

(g) KKK Bank has upgraded a new firewall with the latest technology at the network perimeter to strengthen their network security. However, the network is still exposed with security threat. Based on the understanding of firewall limitation, explain how IDS and IPS can complement the limitation of the firewall.

KKK Bank telah menaiktaraf satu firewall dengan teknologi baru di perimeter rangkaian mereka untuk mengukuhkan keselamatan rangkaian mereka. Walaubagaimanapun, rangkaian tersebut masih terdedah dengan ancaman keselamatan. Berdasarkan kefahaman kekangan firewall, terangkan bagaimana IDS dan IPS boleh melengkapkan kekangan firewall.

[4 marks]
[*4 markah*]

QUESTION 2
SOALAN 2

CLO1
C1

(a) Pluggable Authentication Module (PAM) is used in Linux security to control the function of the various applications running in the system. List **THREE (3)** components in the PAM framework.
*Pluggable Authentication Module (PAM) digunakan di dalam keselamatan Linux bagi mengawal fungsi pelbagai aplikasi yang beroperasi di dalam sistem. Senaraikan **TIGA (3)** komponen yang terdapat di dalam kerangka kerja PAM.*

[3 marks]
[3 markah]

CLO1
C2

(b) Discuss **TWO (2)** advantages and disadvantages related to Windows Registry.
*Bincangkan **DUA (2)** kelebihan dan kelemahan yang berkaitan dengan Windows Registry.*

[4 marks]
[4 markah]

CLO1
C3

(c) Applications running automatically on a system start up can be configured as Window service. Most of them are essential for the core system features but services which is usually not necessary will slow down your computer boot up process. Based on the scenario given, apply Windows services configuration needed to optimize the computer.

Aplikasi yang beroperasi semasa proses memulakan sistem boleh dikonfigurasikan sebagai perkhidmatan Windows. Kebanyakannya adalah berguna untuk menjalankan fungsi utama sistem, tetapi perkhidmatan yang tidak diperlukan akan memperlahankan operasi sistem komputer. Berdasarkan senario berikut, aplikasikan konfigurasi perkhidmatan Windows yang diperlukan untuk mengoptimumkan komputer tersebut.

i. Akram wants to encrypt her flash drives so that only he can view the contents of the removable devices.

Akram hendak menginkrip pemacu kilatnya supaya hanya dia yang dapat melihat kandungan peranti mudah alih tersebut.

ii. Aleea wants to enable the sharing of the internet connection with other computers in the network. Instead of using her computer to operate as a router, she uses a separate router to connect all the computers to the internet.

Aleea hendak membolehkan perkongsian Internet dengan komputer lain di dalam rangkaian. Dia tidak menggunakan komputernya sebagai 'router', sebaliknya dia menggunakan 'router' yang berasingan bagi menghubungkan semua komputer di dalam rangkaian.

iii. Emir needs to connect all his devices such as smartphone, speaker, mouse and camera using a Bluetooh connection so that he can access everything at ease.

Emir hendak menghubungkan semua peralatannya seperti telefon pintar, pembesar suara, tetikus dan kamera dengan menggunakan sambungan Bluetooh agar semuanya boleh dicapai dengan lebih mudah.

[6 marks]

[6 markah]

CLO1
C4

(d) A system log from a computer with IP address 192.168.1.123 shows the result as below.

Log daripada komputer dengan alamat IP 192.168.1.123 menunjukkan keputusan seperti rajah di bawah.

```
Host 192.168.1.123

[00: 00: 01]Successful Login: 015 192.168.1.123 : local

[00: 00: 03]Unsuccessful Login: 022 214.34.56.006 : RDP
192.168.1.124

[00: 00: 04]UnSuccessful Login: 010 214.34.56.006 : RDP
192.168.1.124

[00: 00: 07]UnSuccessful Login: 007 214.34.56.006 : RDP
192.168.1.124

[00: 00: 08]UnSuccessful Login: 003 214.34.56.006 : RDP
192.168.1.124
```

i. Summarize the log activities.

Rumuskan aktiviti log tersebut.

[4 marks]

[4 markah]

ii. Determine a security approach that need to be implemented to prevent unauthorized login attempt from Remote Desktop Protocol.

Tentukan pendekatan keselamatan yang perlu dilaksanakan untuk menghalang kemasukan yang tidak dibenarkan daripada protokol 'Remote Desktop'.

[1 mark]
[1 markah]

CLO1
C2

(e) A modem is a device that allows two computers to communicate via a standard telephone line. Securing a modem is as important as securing an Internet connection. Recognize **THREE (3)** security concerns that can be applied to provide a modem security in an organization.

*Modem adalah alat yang membenarkan dua komputer berkomunikasi melalui rangkaian telefon biasa. Menjaga keselamatan modem adalah sama penting seperti menjaga keselamatan rangkaian Internet. Kenalpasti **TIGA (3)** langkah keselamatan yang dapat dilaksanakan bagi menjamin keselamatan modem di dalam sesebuah organisasi.*

[3 marks]
[3 markah]

CLO1
C3

(f) A wireless networking security policy should be developed as a plan or action for handling security issues of the data, network infrastructure and users. As a network engineer of a new organization, you are required to setup a new wireless network for your company.

Construct **FIVE (5)** security policies on wireless network that can be implemented in your organization.

Polisi keselamatan rangkaian tanpa wayar seharusnya dibangunkan sebagai rancangan atau tindakan dalam menghadapi isu keselamatan berkaitan data, infrastuktur rangkaian dan pengguna. Sebagai jurutera rangkaian di sebuah organisasi yang baru dibangunkan, anda dikehendaki membangunkan rangkaian tanpa wayar bagi organisasi tersebut.

*Bangunkan **LIMA (5)** polisi keselamatan bagi rangkaian tanpa wayar yang dapat diimplementasikan di organisasi tersebut.*

[5 marks]
[5 markah]

CLO1
C4

(g) The scenario below describes the trend of computer and Internet usage in Company A. Based on your understanding of the scenario, suggest security tools that could be installed by Company A regarding the implementation of workplace security.

> Company A have limited number of computers, therefore few staffs need to share the computers amongst them. The concern is every staff might have a different level of access whereas some staff might use the computer for the general task and others might use it for the specific applications. The management have to find a suitable solution to keep the security of the sharing computer usage and at the same time to make sure staff can do their task accordingly.

Senario di bawah menghuraikan tren penggunaan komputer dan Internet di Syarikat A. Berdasarkan pemahaman anda terhadap senario tersebut, cadangkan alat keselamatan yang boleh dipasang oleh Syarikat A berkenaan dengan implementasi keselamatan tempat kerja.

> *Syarikat A mempunyai bilangan komputer yang terhad, oleh itu sebilangan pekerja perlu berkongsi komputer di antara mereka. Isu utama ialah setiap pekerja mempunyai peringkat capaian berbeza di mana sebilangan pekerja hanya menggunakan komputer untuk tugas am manakala ada pekerja yang menggunakan aplikasi tertentu. Pihak pengurusan perlu mendapatkan penyelesaian terbaik bagi keselamatan perkongsian komputer dan pada masa yang sama setiap pekerja dapat membuat tugas masing-masing.*

[4 marks]
[4 markah]

SOALAN TAMAT