SULIT

POLITEKNIK MALAYSIA

BAHAGIAN PEPERIKSAAN DAN PENILAIAN
JABATAN PENGAJIAN POLITEKNIK
KEMENTERIAN PENDIDIKAN MALAYSIA

JABATAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI

PEPERIKSAAN AKHIR

SESI DISEMBER 2013

FN612: NETWORK SECURITY

TARIKH: 15 APRIL 2014
MASA: 2.30 PM - 4.30 PM (2 JAM)

Kertas ini mengandungi **DUA PULUH LIMA (25)** halaman bercetak.
Bahagian A: Objektif (40 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 A: 50 MARKS

BAHAGIAN A: 50 MARKAH

INSTRUCTION:

This section consists of **FORTY (40)** objective questions. Mark your answers in the OMR form provided.

ARAHAN:

*Bahagian ini mengandungi **EMPAT PULUH (40)** soalan objektif. Tandakan jawapan anda di dalam borang OMR yang disediakan.*

CLO1
C1

1. Select which of the following is **NOT** the primary goal of network security?
   *Pilih antara berikut yang manakah **BUKAN** matlamat utama keselamatan rangkaian?*

   A. Assure the availability of corporate data

   Menjamin kewujudan data korporat

   B. Maintain the integrity of corporate data

   Mengekalkan integriti data korporat

   C. Protect against denial-of-service attacks

   Melindungi dari serangan DOS

   D. Protect the confidentiality of corporate data

   Melindungi kerahsiaan data korporat

2.

Mr Jack tries to steal information from his company and use it for his own purpose. *Mr. Jack cuba untuk mencuri maklumat syarikatnya dan gunakan maklumat tersebut untuk tujuan sendiri.*

Figure A2 / *Rajah A2*

CLO1
C1

Refer to the Figure A2 above, identify the threats that best describes Mr. Jack's act.
Merujuk Rajah A2 di atas, kenalpasti jenis ancaman keselamatan yang dilakukan oleh Mr. Jack.

A. Information warfare / *Peperangan Maklumat*
B. Accidental data loss / *Kehilangan data secara tidak sengaja*
C. Information theft / *Kecurian maklumat*
D. Unauthorized disclosure / *Pendedahan yang tidak dibenarkan*

CLO1
C2

3. Determine the method of attacking a computer program, in which the program is modified so as to appear to be working normally when in reality it has been modified.
Tentukan kaedah menyerang perisian komputer yang mana program itu diubahsuai supaya kelihatan berfungsi seperti normal sebaliknya program itu telah diubahsuai.

A. Sniffing
B. Spoofing
C. Hacking
D. Cracking

4. Network devices such as routers and printers often have their own reputation for security and stability. Some of these devices have default settings which provide potential security holes. Relate the above statement with the suitable vulnerability terminology.

CLO1
C2

Peralatan rangkaian seperti router dan pencetak mempunyai reputasi tersendiri berkenaan dengan isu keselamatan dan kestabilan alatan. Sesetengah alatan ini mempunyai tetapan asal yang boleh menyebabkan ia diserang. Kaitkan kenyataan di atas dengan istilah kelemahan yang bersesuaian.

A. Technology weaknesses /*Kelemahan teknologi*
B. Configuration weaknesses / *Kelemahan konfigurasi*
C. Security policy weaknesses / *Kelemahan polisi keselamatan*
D. Documentation weaknesses /*Kelemahan dokumentasi*

5. "Users who gain unauthorized access to computers for the fun of it, but do not intentionally do damage". Classify who are that users.

LO1
C3

"Pengguna yang ingin mendapatkan akses tanpa kebenaran secara suka-suka tetapi tidak berniat untuk melakukan kerosakan". Kelaskan siapakah pengguna tersebut.

A. Employees / *Pekerja*
B. Hackers / *Hacker*
C. Crackers / *Cracker*
D. Members of criminal of organization / *Ahli kumpulan penjenayah*

CLO1
C1

6. These threats come from hackers who are more highly motivated and technically competent which understand the network system designs and vulnerabilities. Recognize the name of these threats.
Ancaman ini datang dari pengodam yang bermotivasi tinggi dan mempunyai kemahiran teknikal yang tinggi yang mana mereka memahami rekabentuk dan kelemahan rangkaian. Kenali nama ancaman ini.

A. Unstructured threats /*Ancaman tidak berstruktur*
B. Internal threats /*Ancaman dalaman*
C. External threats / *Ancaman luaran*
D. Structured threats / *Ancaman berstruktur*

CLO1
C1

7. Which of the following is **NOT** an attack method on network system?
*Antara berikut yang manakah **BUKAN** kaedah untuk menyerang sistem rangkaian?*

A. Access Attack / *Serangan* access
B. Nessus Attack / Serangan Nessus
C. Eavesdropping / *Mencuri dengar*
D. Reconnaissance Attack / *Serangan Reconnaissance*

CLO1 C3

8. In Denial of Service attack (DoS), the attacker disables or corrupts network systems or services with the intent to deny the service to intended users. Discover which network security goal relates to this statement?
Dalam Denial of Service attack (DoS), penyerang melumpuhkan sistem rangkaian atau perkhidmatan dengan niat menidakkan perkhidmatan kepada pengguna yang berhak. Cari kenyataan, yang manakah berkaitan dengan tujuan utama keselamatan sistem rangkaian?

A. Confidentiality / *Kerahsiaan maklumat*
B. Integrity / *Integriti*
C. Availability / *Kebolehsediaan capaian*
D. Privacy / *Kesulitan maklumat*

CLO1 C1

9. When a new operating system is installed on a computer, the security settings are all set to the default values. Identify few common security steps that should be configured to the operating systems.
Apabila sistem pengoperasian yang baru dipasang pada sesebuah komputer, tetapan keselamatan berada pada nilai lalai. Kenalpasti beberapa langkah keselamatan umum yang sepatutnya dikonfigurasi untuk sistem-sistem pengoperasian.

I. Default usernames and passwords should be changed immediately
Nilai lalai bagi nama samaran dan kata laluan perlu ditukar dengan segera
II. Access to the system resources should be restricted to only authorized users
Akses kepada sumber sistem harus dihadkan kepada hanya pengguna yang dibenarkan
III. Any unnecessary services and applications should be turned off and uninstalled
Apa-apa perkhidmatan dan aplikasi yang tidak perlu hendaklah dipadam dan dibuang dari sistem.

A. I and II
B. I and III
C. II and III
D. I, II and III

CLO1 C2

10. Infer the solution for both situations below:
Rumuskan penyelesaian bagi kedua-dua keadaan di bawah:

I. The process of continually remaking the image in order to integrate the latest patch may become administratively time-consuming
Proses mencipta semula imej secara berterusan untuk mengintegrasikan tampalan terkini akan mengambil masa urusan pentadbiran

II. The process of pushing patches out to all systems requires that those systems be connected in some way to the network, which may not be possible
Proses mendesak tampalan kepada semua sistemmemerlukan sistem tersebut disambungkan dengan cara tertentu ke rangkaian namun ini adalah mustahil

A. update the status of latest patches
kemaskini status bagi tampalan terkini

B. perform the intrusion detection analysis and prevention
lakukan analisis pengesanan dan pencegahan pencerobohan

C. install the host antivirus software to protect against known viruses
pasang perisian antivirus bagi hos untuk melindungi daripada virus yang diketahui

D. Create a central patch server that all systems must communicate with after a set period of time
Buat pelayan tampalan berpusat yang mana semua sistem mesti saling berkomunikasi selepas satu set tempoh masa

CLO1 C2

11. Intrusion Detection System (IDS) is the ability to detect attacks against a network and provides the detection mechanism. Describe the means of detection.
Sistem Pengesanan Pencerobohan (IDS) adalah keupayaan untuk mengesan serangan terhadap rangkaian dan menyediakan mekanisme pengesanan. Terangkan cara-cara pengesanan.

A. Prevent attacks against the network
Mencegah serangan terhadap rangkaian

B. Stops the detected attack from executing.
Menghentikan serangan yang dikesan dari terlaksana.

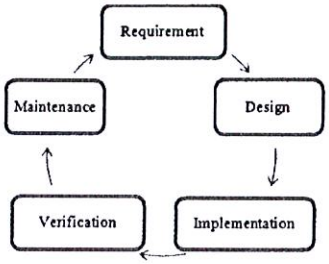
C. Immunizes the system from malicious source.
Kebalkan sistem daripada sumber berniat jahat.

D. Identifies malicious attacks on network and host resources.
Kenal pasti serangan berniat jahat pada sumber hos dan rangkaian.

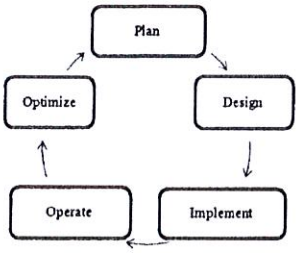
CLO1 C3

12. Which of the following is the sketch for security architecture that consist all stages of network life cycle?
Antara berikut, yang manakah ialah lakarkan bagi seni bina keselamatan yang mempunyai setiap peringkat kitar hayat rangkaian.

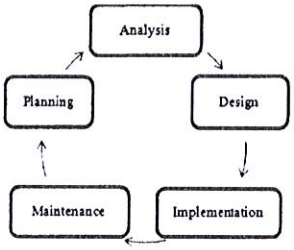
A.



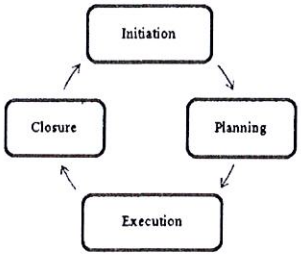
B.



C.



D.



CLO1 C3

13. Choose the following technology that plays important roles in identity solutions.
Pilih teknologi baru yang berikut yang memainkan peranan penting dalam penyelesaian identiti.

A. Firewalls
B. Digital Certificates
C. Virtual Private Network (VPN)
D. Network Intrusion Detection System (NIDS)

CLO2 C4

14. Point out the type of firewall that ensure protocol conformance?
Tunjukkan jenis firewall yang menjamin pematuhan protokol?

A. Circuit-level Gateways
B. Packet filtering firewall
C. Network Level Firewall
D. Application Level Firewall

CLO2 C4

15. Categorize the following characteristics according to the common technology employed in the dynamic packet filtering.
Kategorikan ciri-ciri berikut mengikut teknologi yang sama yang digunakan dalam dynamic packet filtering.

I. State table keeps track of all communication session between stations
Jadual keadaan menjejaki semua sesi komunikasi antara stesen

II. The most commonly used protocols such as HTTP, SMTP, FTP and Telnet
Protokol yang biasa digunakan seperti HTTP, SMTP, FTP dan Telnet

III. Only packets for current and valid communication session are allowed to pass
Hanya paket untuk sesi komunikasi yang sah yang dibenarkan untuk berlepas

IV. Each packet entering or leaving the network is checked and either passed or rejected depending on a set of user-defined rules
Setiap paket yang memasuki atau meninggalkan rangkaian diperiksa dan sama ada dilepaskan atau ditolak bergantung kepada satu set peraturan yang ditetapkan pengguna.

A. I and II
B. I and III
C. II and III
D. II and IV

CLO2 C4

16. A computer in Network A request Telnet session with a server in Network B. The firewall keeps log of the communication packet that are sent each ways. Analyze which packets are allowed back into Network A through firewall?
Sebuah komputer dalam Rangkaian A meminta sesi Telnet dengan pelayan di Rangkaian B. Firewall menyimpan log pake tkomunikasi yang dihantar kedua-dua hala. Analisa paket yang dibenarkan kembali ke dalam Rangkaian A melalui firewall?

A. Each packet allowed must have it's own proxy
Setiap paket yang dibenarkan mesti mempunyai proxy sendiri

B. Only packet that are passed the set of user-defined rules
Hanya paket yang melepasi set peraturan yang ditetapkan pengguna

C. Only packet that are a part of this current communication session
Hanya paket yang merupakan sebahagian daripada sesi komunikasi semasa

D. Each packet to be allowed must contain information of Source IP address, Destination IP address, TCP/UDP source port and TCP/UDP destination port.
Setiap paket yang dibenarkan mesti mengandungi makluma alamat Source IP address, Destination IP address, TCP/UDP source port and TCP/UDP destination port.

LO1 C1

17. Identify the function of Internet Information Service (IIS).
Kenalpasti fungsi Internet Information Service (IIS).

A. To surf internet services.
Untuk melayari perkhidmatan Internet.

B. To tell the users what is internet service
Untuk memberitahu pengguna apakah perkhidmatan Internet.

C. To make Internet Explorer functions properly.
Untuk membolehkan Internet Explorer berfungsi dengan baik.

D. To install a few types of Internet browser.
Untuk install berbagai jenis Internet browser.

CLO1
C1

18. Brings many changes to the system and requires the system to be shut down before applying them.

Membawa banyak perubahan kepada sistem, dan sistem perlu ditutup sebelum mengaplikasikan perubahan tersebut.

Figure A18 / *Rajah A18*

Locate the type of system updates match the criteria in the Figure A18 above.
Tempatkan sistem kemaskini yang memenuhi kriteria seperti penyataan dalam Rajah A18 di atas.

A. Hot fix
B. Updates
C. Patches
D. Combo pack

CLO1
C2

19. The following statements are examples of controlling and auditing of Root Access in Linux **EXCEPT**?
Penyataan berikut adalah contoh bagi kawalan dan audit Root Access dalam Linux ***KECUALI****?*

A. You should never share the root directory of a disk.
Anda tidak boleh berkongsi root directory of a disk.

B. You should share the root directory of a disk.
Anda boleh berkongsi root directory of a disk.

C. You should apply the most restrictive access necessary for a shared directory.
Anda perlu mengaplikasikan kawalan yang paling ketat bagi shared directory.

D. File systems are frequently based on hierarchical models.
Fail sistem adalah berdasarkan model berhierarki.

CLO2
C4

20. Bill wishes to communicate with Jane over the Internet, but a firewall exists on his network. Bill is not authorized to communicate through it himself. He connects to the proxy on his network and sends the information about the connection he wishes to make to Jane. The proxy opens a connection through the firewall and facilitates the communication between Bill and Jane. From the situation, investigate the type of proxy server currently deployed.
Bill berhasrat untuk berkomunikasi dengan Jane melalui Internet, akan tetapi rangkaian Bill terdapat satu firewall. Bill tidak boleh berkomunikasi dengan firewall itu secara sendiri. Bill melayari satu proxy dan menghantar maklumat berkenaan komunikasi yang ingin dijalankan dengan Jane. Proxy ini membuka satu laluan pada firewall bagi membolehkan mereka berkomunikasi. Dari situasi tersebut, kaji jenis pelayan proxy yang digunakan.

A. Squid
B. Windows Proxy
C. SOCKS
D. The TIS Firewall Toolkit

CLO1
C3

21. Choose the benefits of Linux based Proxy Server.
Pilih kelebihan Linux based Proxy Server.

I. Double-reverse lookups when access FTP sites.
II. Robust logging capabilities.
III. The host name of the requesting IP address is looked up in the DNS records.
IV. Administrator can monitor which types of Internet activity are occurring.

A. I, II, III
B. I, II, IV
C. I, III, IV
D. I, II, III and IV

CLO2 C4

22. Enquire the function of "lastlog" command in Logging Enhancers?
Siasat apakah fungsi arahan "lastlog" dalam Logging Enhancers?

A. To list the date each account logged in to the system.
Untuk menyenaraikan tarikh terakhir setiap akaun log masuk ke dalam sistem.

B. To display the data such as who is logged on to the system, who recent logged on, and when the system has rebooted.
Untuk memaparkan data pengguna yang log masuk sistem, pengguna yang baru log masuk, dan bila sistem boot semula.

C. To make a list if a password was changed and who has changed it.
Untuk membuat senarai jika kata laluan ditukar dan siapa yang menukarnya.

D. To display the users and services that have accounts on that particular machine.
Untuk memaparkan pengguna dan servis yang mempunyai akaun pada mesin tersebut.

CLO2 C3

23. One of the most important jobs of a network administrator is to review a set of files that contains information about accesses and events that have occurred on a system including attempted break-ins. Every system is set up to provide this information. Choose the type of file that is so important for the administrator to review.
Salah satu tugas penting seorang network administrator adalah menyemak fail yang mengandungi maklumat tentang akses dan acara yang berlaku pada sesebuah sistem termasuklah cubaan pencerobohan. Setiap sistem boleh menyediakan maklumat sebegini. Pilih jenis fail yang perlu disemak oleh network administrator tersebut.

A. Configuration files

B. Log files

C. Application files

D. Initialization files

CLO2
C2

29.

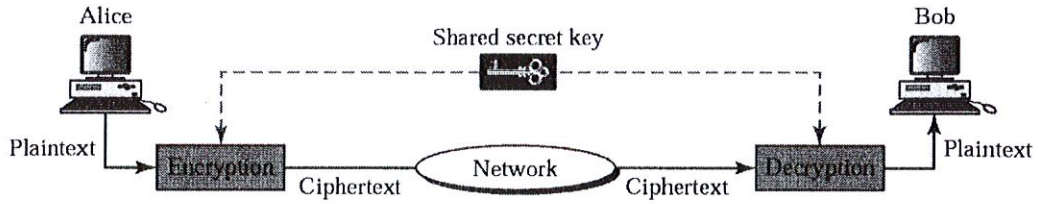


Figure A29/ *Rajah A29*

Label the class of key-based encryption algorithm in Figure A29.
Labelkan kelas algoritma penyulitan berasaskan kekunci dalam Rajah A29.

A. Shared key
B. Symmetric
C. Public-Key
D. Asymmetric

CLO2
C2

30. Convert the letters of A to its corresponding Cipher text "S" and identify the key used.
Tukar huruf A ke tulisan rahsia yang sepadan dengan "S" dan kenal pasti kekunci yang digunakan.

A. 16
B. 17
C. 18
D. 19

CLO2
C2

31. Transform the word "HELLO" to its corresponding Cipher text using classic Caesar Cipher where letter of the alphabet were shifted by three (3) positions to the right.
Ubah perkataan "HELLO" untuk tulisan rahsia yang sepadan menggunakan Caesar Cipher klasik yang mana abjad telah beralih sebanyak tiga (3) anjakan ke kanan.

A. LIPPS
B. JGNNQ
C. LGORR
D. KHOOR

CLO2 C3

32. The Secure Socket Layer protocol was created to ensure secure transactions between web servers and browsers. Arrange in sequence how it works.
Protokol Secure Socket Layer diwujudkan bagi memastikan transaksi yang selamat antara pelayan web dan pelayar. Susunkan bagaimana ia berfungsi mengikut urutan.

I. The browser checks that the certificate was issued by a trusted party (usually a trusted root CA), that the certificate is still valid and that the certificate is related to the site contacted.
II. The web server decrypts the symmetric encryption key using its private key and uses the symmetric key to decrypt the URL and http data.
III. The web server sends back the requested html document and http data encrypted with the symmetric key.
IV. The browser then uses the public key, to encrypt a random symmetric encryption key and sends it to the server with the encrypted URL required as well as other encrypted http data.
V. The web server sends its public key with its certificate.
VI. The browser decrypts the http data and html document using the symmetric key and displays the information.
VII. A browser requests a secure page (usually https://).

A. I, III, V, VI, IV, II, VII
B. II, VII, I, III, V, VI, IV
C. III, V, VI, IV, II,VII, I
D. IV, II, VII, I, III, V, VI

CLO2 C2

33. DNSSEC was designed to protect Internet resolvers from forged DNS data, such as that created by DNS cache poisoning and all answers in DNSSEC are digitally signed. Identify the network security goal that achieved using DNSSEC.

DNSSEC telah direka untuk melindungi pelanggan Internet daripada data DNS palsu, seperti yang dihasilkan oleh DNS cache poisoning *dan semua jawapan dalam DNSSEC ditandatangani secara digital. Kenalpasti matlamat keselamatan rangkaian yang dicapai dengan menggunakan DNSSEC.*

A. Integrity / Ketelusan
B. Availability / Kesediaan
C. Confidentiality / Kerahsiaan
D. Non-repudiation / Bukan penolakan

CLO1 C3

34. The following are the components to set up a Virtual Private Network (VPN) **EXCEPT**:
Berikut adalah komponen untuk mewujudkan VPN ***KECUALI****:*

A. VPN Server on end user's computer
Pelayan VPN pada komputer pengguna akhir

B. A connection from the Internet to corporate HQ
Sambungan dari Internet ke Ibu Pejabat korporat

C. A connection from the computer to the public Internet
Sambungan daripada komputer ke Internet umum

D. Server at HQ to authenticate users and decrypt their data
Pelayan di Ibu Pejabat untuk mengesahkan pengguna dan menyahsulit data mereka

CLO1 C3

35. A good VPN consists the following features **EXCEPT**:
Sebuah VPN yang baik mengandungi ciri-ciri berikut ***KECUALI****:*

A. Support multiple VPNs
Menyokong pelbagai VPN

B. Provide adequate encryption
Menyediakan penyulitan yang selamat

C. Provide strong authentication
Menyediakan pengesahan yang kukuh

D. Support adherence to standard
Menyokong pematuhan kepada piawaian

CLO1 C3

36. Apply the following technique to secure the VPN.
Aplikasikan teknik berikut untuk VPN yang selamat.

A. synchronize
B. scramble
C. block
D. filter

Refer Figure A37 for Question 37 and 38 .
Rujuk Rajah A37 untuk Soalan 37 dan 38.

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

Figure A37 / *Rajah A37* Vigenere Cipher

CLO2
C4

37. Select the encipher message for "TO BE OR NOT TO BE THAT IS THE QUESTION" using keyword RELATIONS.
Pilih mesej rahsia untuk "TO BE OR NOT TO BE THAT IS THE QUESTION" menggunakan kata kunci RELATIONS.

A. KSMFH ZBBKL SMFMP OJAGX SFJDS ELZSY

B. KSNEH ZBDLK SNEMD OGAGK SEGDS EIZSY

C. KSMEH ZBBLK SMEMP OGAJX SEJCS FLZSY

D. KSNFH ZDBKL SNFND OGAJX SEJCS EIZSY

CLO2 C4

38. List SIX (6) corresponding encipher letters to "T" in plaintext message.
Senaraikan ENAM (6) huruf rahsia yang sepadan dengan "T" dalam mesej teks biasa.

A. L, K, I, M, J and X
B. G, H, K, L, N and Y
C. L, N, K, G, X and Y
D. G, H, K, L, M and X

CLO3 C2

39. "A group of linked computers, working together closely so that in many respects they form a single computer." Match this statement with the necessary solution.
"Sebuah kumpulan komputer yang dihubungkan, bekerjasama rapat supaya membentuk sebuah komputer." Padankan kenyataan ini dengan penyelesaian yang sesuai.

A. RAID
B. UPS
C. Clustering
D. Redundant Server

CLO3 C1

40. Select which of the following is **NOT** a key concept of a RAID implementation
*Pilih yang manakah antara berikut **BUKAN** merupakan satu konsep utama pelaksanaan RAID*

A. Mirroring
B. Load-balancing
C. Stripping
D. Error checking

SECTION B : 50 MARKS
BAHAGIAN B : 50 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) Describe the following goals of network security:
Huraikan tujuan keselamatan rangkaian berikut:

(i) Confidentiality / *Kerahsiaan*

(ii) Integrity / *Integriti*

(iii) Availability / *Kebolehsediaan*

[3 marks]
[3 markah]

CLO1
C2

b) List and explain **THREE (3)** security models that can be implemented in an organization.
*Senaraikan dan terangkan **TIGA (3)** model keselamatan yang boleh diimplementasikan dalam organisasi.*

[6 marks]
[6 markah]

c) Malicious code continues to be a big security problem for most organization as well as individual home users. The term malicious code covers three different types of programs.

Malicious code menjadi ancaman keselamatan besar kepada organisasi dan juga pengguna komputer di rumah. Istilah malicious code merangkumi tiga jenis program yang berbeza.

CLO1 C1

(i) State **THREE (3)** different types of program as mentioned in the above statement?

*Nyatakan **TIGA (3)** jenis program yang disebut di atas?*

[3 marks]
[3 markah]

CLO1 C2

(ii) What are the differences between those three programs?

Apakah perbezaan diantara ketiga-tiga program tersebut?

[6 marks]
[6 markah]

CLO1 C3

d) A printed copy of a virus does nothing and threatens no one. Even executable virus code sitting on the disk does nothing. Discover what triggers a virus to start replicating?

Satu salinan virus tidak mendatangkan ancaman kepada sesiapa pun. Walaupun virus yang berada dalam cakera itu boleh bertindak ia tidak mendatangkan ancaman. Cari apakah yang menyebabkan sesuatu virus itu mula bertindak?

[2 marks]
[2 markah]

e) A team of hackers wants to attack ABC Company's network server. Mr. Jack as the network administrator needs to secure the network from unauthorized access by the hackers.
Satu kumpulan penggodam ingin menyerang pelayan rangkaian syarikat ABC. Mr. Jack bertindak sebagai pentadbir rangkaian perlu melindungi rangkaian tersebut dari akses yang tidak sah oleh kumpulan penggodam tersebut.

CLO2 C4

(i) In your opinion, what are the mechanisms that Mr. Jack can use to secure the network?
Pada pendapat anda, apakah mekanisma yang boleh Mr. Jack gunakan untuk melindungi rangkaian tersebut?

[2 marks]
[2 markah]

CLO2 C4

(ii) If the network administrator use the antivirus software to protect the network server in ABC Company from the hackers, do you think this solution is appropriate and enough to secure the network?
Pada pendapat anda, adakah sesuai dan mencukupi untuk melindungi rangkaian itu jika pentadbir rangkaian menggunakan perisian antivirus untuk melindungi pelayan rangkaian syarikat ABC dari digodam?

[3 marks]
[*3 markah*]

QUESTION 2
SOALAN 2

CLO1
C3

a) Alex, junior administrator at ABC Company confuses about packet filter and proxy server. As the system administrator, list the **FOUR (4)** similarities between a packet filter and a proxy server.

*Alex, pentadbir muda di Syarikat ABC keliru mengenai packet filter dan proxy server. Sebagai pentadbir sistem, senaraikan **EMPAT (4)** persamaan antara packet filter dan proxy server.*

[8 marks]
[8 markah]

CLO3
C1

b) Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Describe the function of the following equipment:

Rangkaian keselamatan meliputi pelbagai rangkaian komputer, kedua-dua sektor awam dan swasta, yang digunakan dalam urusan seharian seperti menjalankan urus niaga dan komunikasi di kalangan perniagaan, agensi-agensi kerajaan dan individu.
Terangkan fungsi peralatan berikut:

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

[6 marks]
[6 markah]

CLO2 C1

c) Cryptography is the strongest tool for controlling against security threats. Identify each of the cryptography terminology below:

Kriptografi adalah alat yang paling berkesan untuk mengawal sebarang ancaman keselamatan. Kenal pasti setiap istilah kriptografi di bawah:

(i) Encryption

(ii) Plain text

(iii) Ciphertext

[6 marks]
[6 markah]

CLO2 C3

d)

I Love Network Security Class

Figure B2(d) / *Rajah B2(d)*

Encrypt the message in Figure B2(d) by using the Caesar Cipher algorithm (key = 2).

Enkrip maklumat dalam Rajah B2(d) menggunakan Caesar Cipher algorithm (key=2)

[5 marks]
[5 markah]

- SOALAN TAMAT -