SULIT

POLITEKNIK MALAYSIA

BAHAGIAN PEPERIKSAAN DAN PENILAIAN
JABATAN PENGAJIAN POLITEKNIK
KEMENTERIAN PENDIDIKAN MALAYSIA

JABATAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI

PEPERIKSAAN AKHIR

SESI JUN 2014

FN612 : NETWORK SECURITY

TARIKH : 20 OKTOBER 2014
MASA : 2.30 PM - 4.30 PM (2 JAM)

Kertas ini mengandungi **DUA PULUH DUA (22)** 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)

SULIT

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. Why do we need security for our network system?
Mengapa kita memerlukan keselamatan untuk sistem rangkaian kita?

   A. To ensure all data in the network cannot be detected by any users.
   Untuk memastikan semua data dalam rangkaian tidak dapat dikesan oleh mana-mana pengguna.

   B. As a backup when during network system failure.
   Sebagai sandaran apabila sistem rangkaian mengalami masalah.

   C. To implement applications that can protect the network from unauthorized access.
   Untuk melaksanakan aplikasi yang boleh melindungi rangkaian daripada akses yang tidak dibenarkan.

   D. As an assurance that the network have been detected by the management.
   Sebagai jaminan bahawa rangkaian telah dikesan oleh pihak pengurusan.

CLO2-C4

2. Used for a number of reasons such as to filter web content, to go around restrictions such as parental blocks, to screen downloads and uploads and to provide anonymity when surfing the internet.

   Digunakan untuk beberapa sebab seperti untuk menapis kandungan web, untuk pergi sekitar sekatan seperti blok ibu bapa, untuk muat turun dan Gambar skrin dan untuk menyediakan ketanpanamaan apabila melayari internet.

   The statement above describes
   Kenyataan di atas menerangkan

   A. Firewall

   B. Proxy

   C. IDS

   D. IPS

CLO1-C2

3. Activity of stealing confidential data and information from an organization network.
Aktiviti mencuri data sulit dan maklumat dari rangkaian organisasi.

The statement above refers to _____
Kenyataan di atas merujuk kepada

A. Accidental Data Loss
Kehilangan Data secara tidak sengaja

B. Information Warfare
Peperangan Maklumat

C. Information Theft
Kecurian maklumat

D. Unauthorized Disclosure
Pendedahan yang tidak dibenarkan

CLO1-C2

4. Intrusion Prevention System (IPS) can be described as
Sistem Pencegahan Pencerobohan (IPS) boleh digambarkan sebagai

A. A system that provide IP address for all users in a network.
Satu sistem yang menyediakan alamat IP untuk semua pengguna dalam rangkaian.

B. Able to detect intrusions that will harm a network.
Dapat mengesan pencerobohan yang akan memudaratkan rangkaian.

C. Placed in-line and are able to actively prevent/blocked intrusions that are detected.
Diletakkan dalam talian dan dapat aktif mencegah / disekat pencerobohan yang dikesan.

D. A system that able to prevent users to connect to the internet.
Satu sistem yang mampu untuk menghalang pengguna untuk menyambung ke internet.

CLO1-C2

5. System that was incorrectly configured, and therefore vulnerable to attack.
Sistem yang telah dikonfigurasi dengan salah, dan oleh itu terdedah kepada serangan.

The statement above refers to _____
Kenyataan di atas merujuk kepada

A. Hardware Weakness
Kelemahan perkakasan

B. Production Weakness
Kelemahan pengeluaran

C. Technology Weakness
Kelemahan teknologi

D. Configuration Weakness
Kelemahan konfigurasi

CLO2-C1

6. What is the importance of updating Operating System Patches?
Apakah kepentingan mengemaskini Tampalan Sistem Operasi?

A. Ensure the operating system is always updated and free from vulnerabilities.
Memastikan sistem operasi yang sentiasa dikemaskini dan bebas daripada kelemahan.

B. Ensure the computer's date and times are synchronous with world clock.
Pastikan tarikh dan masa segerak dengan jam dunia komputer.

C. Ensure the operating system can always be used correctly.
Pastikan sistem operasi sentiasa boleh digunakan dengan betul.

D. Ensure the hard disk is safe and work properly.
Pastikan cakera keras adalah selamat dan berfungsi dengan baik.

CLO2-C1

7. Replicate itself on your system, creating a huge devastating effect.
Meniru sendiri pada sistem anda, mewujudkan kesan buruk yang besar.

The statement above describes _____
Pernyataan di atas menerangkan

A. Spamware

B. Trojan Horses

C. Viruses

D. Worms

CLO2-C1

8. Which of the following is not a network scanning tools?
Salah satu daripada berikut yang mana bukan alat pengimbasan rangkaian?

A. Traceroute

B. Nmap

C. Netstat

D. Hping

CLO2-C1

9. Which of the following best describe structured threats?
Apa yang anda boleh menggambarkan dengan ancaman berstruktur?

A. implemented by a technically skilled person who is trying to gain access to a network
dilaksanakan oleh orang yang mahir dari segi teknikal yang cuba untuk mendapatkan akses kepada rangkaian

B. created by an inexperienced person who is trying to gain access to your network
dicipta oleh orang yang tidak berpengalaman yang cuba untuk mendapatkan akses kepada rangkaian anda

C. occurs when someone from inside your network creates a security threat to your network.
berlaku apabila seseorang dari dalam rangkaian anda mewujudkan ancaman keselamatan untuk rangkaian anda.

D. occurs when someone outside your network creates a security threat to your network.
berlaku apabila seseorang di luar rangkaian anda mewujudkan ancaman keselamatan untuk rangkaian anda.

CLO2-C1

10. How does the Host-based IDS works?
Bagaimana IDS berasaskan Hos berfungsi?

A. Examines activity on a network.
Meneliti aktiviti pada rangkaian.

B. Examines activity on an individual computer or a host.
Memeriksa aktiviti pada komputer individu atau tuan rumah.

C. Give the hackers a notice that their action may lead to legal action.
Beri penggodam notis bahawa tindakan mereka boleh membawa kepada tindakan undang-undang.

D. Examines activity within a server.
Memeriksa aktiviti dalam pelayan.

CLO1-C3

11. Which of the following describe the Firewall?
Antara berikut yang manakah menggambarkan Firewall?

i. A hardware that give authorization for a user.
Satu perkakasan yang memberikan kebenaran untuk pengguna.

ii. Can be a software or a hardware.
Boleh menjadi satu perisian atau perkakasan.

iii. Allow or block unauthorized user to access to another network.
Membenarkan atau menghalang pengguna yang tidak dibenarkan untuk mengakses ke rangkaian lain.

iv. Allow or block unauthorized access to a network.
Membenarkan atau menyekat akses yang tidak dibenarkan kepada rangkaian.

A. i and ii

B. i,ii and iii

C. ii and iv

D. iii and iv

CLO2-C1

12. Which of the following is NOT a type of firewall?
Antara berikut yang manakah BUKAN jenis firewall?

A. Packet filtering firewall
Firewall penapisan packet

B. Circuit level gateway
Gerbang Peringkat litar

C. Network level firewall
Tahap Rangkaian firewall

D. Time-based firewall
Firewall berdasarkan masa

CLO1-C1

13.

- Easiest to be implemented than the other two security policies.
  Mudah untuk melaksanakan daripada dua dasar keselamatan lain.
- This design assume that the protected assets are minimal, users are trusted, and threats are minimal.
  Reka bentuk ini menganggap bahawa aset yang dilindungi adalah minimum, pengguna dipercayai, dan ancaman adalah minimum.
- Basic security capabilities is configured on the Existing hardware and software.
  Keupayaan keselamatan Asas dikonfigurasi pada perkakasan dan perisian sedia ada.

Which security model described in the statement above?
Model keselamatan manakah yang diterangkan di atas?

A. Easy Security Model
Model Keselamatan Mudah

B. Closed Security Model
Model Keselamatan tertutup

C. Open Security Model
Model Keselamatan terbuka

D. Restrictive Security Model
Model Keselamatan terhad

CLO2-C2

14. Which of the following are not types of firewall?
Antara berikut yang manakah bukan jenis firewall?

i. Packet firewall

ii. Router firewall

iii. Packet filtering firewall

iv. Circuit level gateway

A. i and ii

B. i,ii and iii

C. ii and iv

D. iii and iv

CLO2-C3

15. The design philosophy of **X** is to scan network packets at the router or host-level, auditing packet information, and logging any suspicious packets into a special log file with extended information.

*Falsafah reka bentuk **X** adalah untuk mengimbas paket rangkaian pada router atau host-peringkat, pengauditan maklumat paket, dan pembalakan mana-mana paket yang mencurigakan ke dalam fail log khas dengan maklumat lanjutan.*

What is **X**?
*Apakah **X**?*

A. HIPS

B. HIDS

C. NIDS

D. NIPS

CLO2-C4

16. What are the benefits of implementing VPN?
Apakah faedah VPN dilaksanakan?

i. It can transmit data securely over a public network.
Ia boleh menghantar data dengan selamat melalui rangkaian awam.

ii. Secure from attackers.
Selamat dari penyerang.

iii. IP address provided by DHCP server
Alamat IP yang disediakan oleh pelayan DHCP

iv. Can be implemented without proper deployment of precautions.
Boleh dilaksanakan tanpa penggunaan yang betul langkah berjaga-jaga.

A. i and ii

B. i,ii and iii

C. ii and iv

D. iii and iv

CLO1-C3

17. Which of the following are the characteristic of a good password?
Yang manakah antara berikut adalah ciri-ciri kata laluan yang baik?

i. Less than 6 characters for remembering easily.
Kurang daripada 6 aksara untuk mudah mengingat.

ii. Using mother's name.
Menggunakan nama ibu.

iii. Using word that is not in any dictionary.
Menggunakan perkataan yang tidak di dalam kamus.

iv. Combination of numbers and alphabets.
Gabungan nombor dan huruf.

A. i and ii

B. i,ii and iii

C. ii and iv

D. iii and iv

CLO2-C1

18. What is the importance of configuring security policy?
Apakah kepentingan mengkonfigurasi dasar keselamatan?

A. To design physical network layout in an organization.
Untuk reka bentuk susun atur rangkaian fizikal dalam sesebuah organisasi.

B. As a proper planning to tight up network security.
Sebagai perancangan yang betul untuk keselamatan rangkaian yang tegap.

C. As a contingency plan if there is any attacks to our network.
Sebagai pelan kontingensi jika terdapat sebarang serangan kepada rangkaian kami.

D. To simulate how the attackers will attack our network.
Untuk mensimulasikan bagaimana penyerang akan menyerang rangkaian kami.

CLO2-C2 19. Describe the benefit of implement IPSec.
Huraikan manfaat melaksanakan IPSec.

A. It prevents attackers to logon the operating system.
Ia menghalang penyerang untuk log masuk sistem operasi.

B. It can enhance the operating system security by updating it to avoid attack.
Ia boleh meningkatkan keselamatan sistem operasi dengan mengemas kini ia untuk mengelakkan serangan.

C. It protects against possible security exposures by protecting data while it is being transmitted over an unprotected network.
ia melindungi terhadap pendedahan keselamatan yang mungkin dengan melindungi data semasa ia sedang dihantar melalui rangkaian yang tidak dilindungi.

D. It can display vulnerabilities in our computer and network.
Ia boleh memaparkan kelemahan dalam komputer dan rangkaian kami.

CLO2-C1 20. What is the main function of Internet Information Service (IIS)?
Apakah fungsi utama Perkhidmatan Maklumat Internet (IIS)?

A. To serves internet services.
Untuk melayari perkhidmatan internet.

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

C. To make the Internet Explorer function properly.
Untuk membuat fungsi Internet Explorer dengan betul.

D. To install any types of internet browser.
Untuk memasang sebarang jenis pelayar internet.

CLO2-C3

21. What are the benefits of Linux-based proxy server?
Apakah faedah "Linux-based proxy server"?

i. It is free.
Ia adalah percuma.

ii. More secure because only root user can configure the proxy server.
Lebih selamat kerana pengguna root sahaja boleh mengkonfigurasi pelayan proksi.

iii. Can save more because the price is much cheaper than Windows-base proxy.
Boleh jimat lebih kerana harga yang lebih murah daripada "Windows-base proxy".

iv. Can be installed in mobile handheld.
Boleh dipasang di peranti mudah alih.

A. i and ii

B. i,ii and iii

C. ii and iv

D. iii and iv

CLO2-C3

22. Which of the following is NOT the feature of Microsoft Security Server (ISA)?

Antara berikut yang manakah BUKAN ciri-ciri "Microsoft Security Server" (ISA)?

A. Enhanced SMTP filter

B. Enhanced Exchange RPC filter

C. Basic authentication delegation

D. Database management system.

CLO2-C2

23. Which of the following is NOT IIS vulnerability?
Manakah antara berikut BUKAN kelemahan IIS?

A. Usage of unmanaged switches.
Penggunaan "switches" yang tidak terurus.

B. Large number of open ports.
Sebilangan besar "port" terbuka.

C. Default installs of operating system and applications
Memasang sistem operasi dan aplikasi

D. ISAPI Extension Buffer Overflows

CLO2-C1

24. _____ is a technique used to encrypt the users data.
adalah satu teknik untuk "encrypt" data pengguna.

A. Cryptography
Criptografi

B. Exception Management
Pengurusan pengecualian

C. Session Management
Pengurusan Sesi

D. Parameter Manipulation
Manipulasi parameter

CLO2-C2

25. Identify the purpose of authentication.
Kenal pasti tujuan pengesahan.

A. To give the authenticated user the rights for certain files and directories.
Untuk memberi panduan disahkan hak untuk fail direktori dan tertentu.

B. To prove a person's authorization by unique username and password.
Untuk membuktikan kebenaran seseorang dengan username dan kata laluan yang unik.

C. To convert data to a format that is meaningless to human beings.
Untuk menukar data kepada format yang bermakna kepada manusia.

D. To show all authorized users for a specific network.
Untuk menunjukkan semua pengguna yang dibenarkan untuk rangkaian tertentu.

CLO1-C1

26. What is the other name for Cipher Text?
Apakah nama lain bagi Teks Cipher?

A. Encrypted text.

B. Raw text.

C. Rich text.

D. Enhanced text.

CLO1-C4

27. A class of algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext.

Satu kelas algoritma kriptografi yang menggunakan kunci kriptografi yang sama untuk kedua-dua penyulitan plaintext dan penyahsulitan tulisan rahsia.

The statement above describes _____
Kenyataan di atas menerangkan

A. Data Algorithm.

B. Computer Algorithm.

C. Symmetric Algorithm.

D. Asymmetric Algorithm.

CLO2-C2

28. What is the function of Secure Socket Layer (SSL) ?
Apakah fungsi Secure Socket Layer (SSL)?

A. To make use of TCP as a communication layer to provide a reliable end-to-end secure and authenticated connection between two points over a network.
Untuk membuat penggunaan TCP sebagai lapisan komunikasi yang selamat dan disahkan sambungan antara dua lokasi melalui rangkaian.

B. To secure the communication between two hosts in P2P connection.
Untuk menjamin komunikasi antara dua penjuru dalam sambungan P2P.

C. To enable network connection all the time.
Untuk membolehkan sambungan rangkaian sepanjang masa

D. To make sure the network is secure from attackers.
Untuk memastikan rangkaian selamat dari penyerang.

CLO1-C4

29.

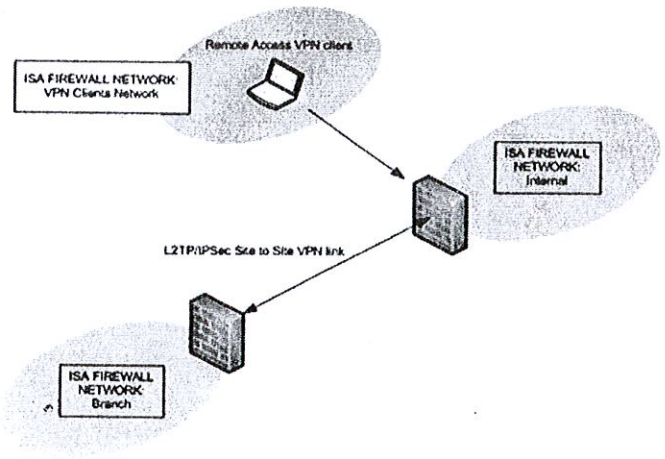


Figure above explains about _____
Rajah di atas menerangkan tentang

A. Local VPN

B. Intranet VPN

C. Remote Access VPN

D. Extranet VPN

CLO1-C1

30. Which of the following is NOT a VPN tunneling protocol?
Salah satu daripada berikut yang mana BUKAN merupakan "VPN tunneling protocol"?

A. PPPoE

B. PPTP

C. L2TP

D. IPSec

CLO3-C1

31. It takes advantage of the firewall's security mechanisms, including restricting access to the internal network. They also perform address translation; satisfy requirements for strong authentication; and serve up real-time alarms and extensive logging.

Ia mengambil kesempatan mekanisme keselamatan firewall, termasuk menyekat akses kepada rangkaian dalaman. Mereka juga melakukan terjemahan alamat; memenuhi keperluan untuk pengesahan yang kukuh; dan berkhidmat sehingga penggera masa sebenar .

Based on what does the statement above refer to?
Berdasarkan kenyataan di atas, ia merujuk kepada?

A. Dedicated Software VPN

B. Router-based VPN

C. Firewall-based VPN

D. Dedicated Hardware VPN

CLO2-C2

32. Which is NOT the feature of good VPN products?
Yang manakah BUKAN ciri produk VPN yang baik?

A. Unique serial number

B. Strong authentication

C. Adequate encryption

D. Adherence to standards

CLO3-C1

33. Which of the following are related to authentication application technology?

Antara berikut yang manakah berkaitan dengan aplikasi teknologi pengesahan?

i. Thumbprint identification

ii.. RFID identification

iii. Iris detection

iv. Face detection

A. i,ii,iii and iv

B. ii,iii and iv

C. iii only

D. i and iv

CLO3-C1

34. List the attacks that can be launched if authentication is not implemented.

Senaraikan serangan yang boleh dilancarkan jika pengesahan tidak dilaksanakan.

i. Information stealing.
Mencuri maklumat.

ii.. Interception while transmitting data.
Pemintasan ketika menghantar data.

iii. Unauthorized access to private data.
Akses tanpa kebenaran kepada data peribadi.

iv. Eavesdropping
Mencuri dengar

A. i only.

B. i and iii

C. ii and iv

D. iii and iv

CLO2-C3

35. How does cryptanalysis work?
Bagaimana "cryptanalysis" berfungsi?

A. Analyze the history of cipher text.
Menganalisa sejarah teks cipher.

B. Encrypt a text to a ciphertext.
Encrypt teks kepada tulisan rahsia.

C. Analyze and solving cipher text.
Menganalisis dan menyelesaikan teks cipher.

D. Encrypt a bulk directory.
Encrypt direktori pukal.

CLO2-C2

36. State the benefit of using HTTPS.
Nyatakan manfaat menggunakan HTTPS.

A. Allows messages to be transmitted securely using an email.
Membolehkan mesej untuk dihantar dengan selamat menggunakan e-mel.

B. Allows data to be managed properly in a proper table.
Membenarkan data diuruskan dengan betul dalam jadual yang sepatutnya.

C. Allows files to be transferred within a network.
Membenarkan fail yang hendak dipindahkan melalui rangkaian.

D. Allows the secure exchange of files on the World Wide Web.
Membenarkan pertukaran fail pada "World Wide Web" dengan selamat.

CLO3-C3 37.

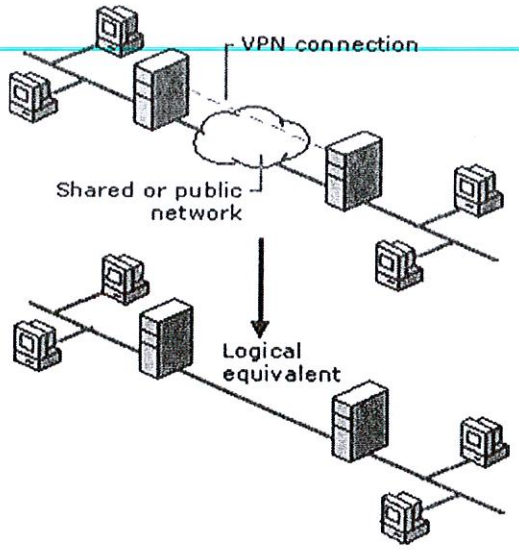


Figure above describes _____
Rajah di atas menerangkan

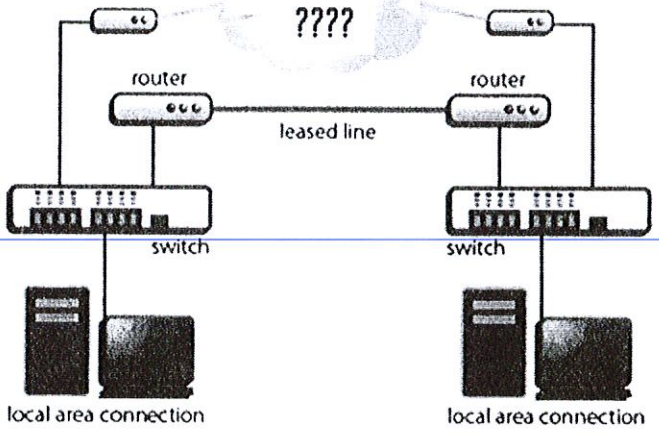
A. PPPoE

B. PPP

C. PPTP

D. L2TP

CLO3-C2 38.



The figure above explain _____ configuration.
*Rajah di atas, menerangkan konfigurasi*_____

A. Squid

B. IPTables

C. VPN

D. CUPS

CLO3-C3

39. A good VPN products must have……..?
Ciri-ciri produk VPN yang baik mesti mempunyai… ….?

i. Made by well-known manufacturers.
Dibuat oleh pengeluar terkenal.

ii.. Strong authentication.
Pengesahan yang kukuh.

iii. Adequate encryption.
Penyulitan yang bagus.

iv. Adherence to standards.
Pematuhan kepada standard.

A. i and ii

B. i,ii and iii

C. iii and iv

D. ii,iii and iv

CLO3-C2

40. Which of the following is a type of disaster recovery system?
Antara berikut yang manakah adalah jenis sistem pemulihan bencana?

A. Parallel system.

B. Serial system

C. Symmetric system

D. Synchronous system

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 struktur Jawab semua soalan.*

QUESTION 1 / SOALAN 1

(a) There are three security model commonly used to secure networking system, which are Open Security Model, Restrictive Security Model and Closed Security Model.

Terdapat tiga keselamatan model yang biasa digunakan untuk menjamin sistem rangkaian, Model Keselamatan Terbuka, Model Keselamatan Terhad dan Model Keselamatan tertutup.

CLO1-C1 i. Explain Closed Security Model.
Terangkan Model Keselamatan tertutup.

(4 Marks)
(4 Markah)

CLO1-C1 ii. Differentiate Closed Security Model and Open Security Model. (Please draw a diagram for your explanation)

Bezakan Model Keselamatan tertutup dan Model Keselamatan Terbuka. (Sila lukiskan gambarajah untuk penjelasan anda)

(6 Marks)
(6 Markah)

CLO2-C2 (b) A virus is capable of interrupting a computer system which may cause a failure to its operation and contribute to loss in business organization. Explain **TWO (2)** ways how viruses can be spread:

*Virus dapat menganggu sistem komputer sehingga boleh melumpuhkan operasi sistem komputer lantas menjejaskan pendapatan sesebuah perniagaan. Jelaskan **DUA (2)** cara bagaimana virus boleh disebarkan.*

(6 Marks)
(6 Markah)

CLO2-C3 (c) Define the goals of security policy in network system.
Terangkan matlamat dasar keselamatan dalam sistem rangkaian.

(4 Marks)
(4 Markah)

CLO3-C4 (d) Several successful Internet security attacks have used packets which carry fake source IP addresses. Describe briefly one such attack indicating why the faked source address is important, and what other conditions are required for the attack to succeed.

Beberapa serangan keselamatan Internet yang berjaya telah menggunakan paket yang membawa alamat IP dari sumber yang palsu. Terangkan secara ringkas satu serangan seperti itu yang menunjukkan mengapa sumber alamat palsu adalah penting, dan apakah syarat-syarat lain yang diperlukan bagi serangan itu untuk berjaya.

(5 marks)
(5 Markah)

QUESTION 2 / SOALAN 2

CLO1-C1 (a) Identify the function of Proxy Server?
Kenalpasti fungsi Proxy Server?

(3 Marks)
(3 Markah)

CLO2-C2 (b) What is NAT and briefly explain how it works?
Apakah NAT dan terangkan bagaimana ianya beroperasi.

(4 Marks)
(4 Markah)

CLO2-C3 (c) Explain how encryption can protect data from snooped.
Terangkan bagaimana "encryption" boleh melindungi data dari "snooped".

(4 Marks)
(4 Markah)

(d) There many type of malicious code, which is virus, worm and Trojan horse.
Ada pelbagai jenis malicious code, antaranya virus, worm dan Trojan horse.

CLO2-C2 i. Briefly explain about malicious code.
Terangkan tentang malicious code.

(3 Marks)
(3 Markah)

CLO2-C2 ii. Differentiate virus and Trojan horse
Bezakan virus dan Trojan horse.

(4 Marks)
(4 Markah)

CLO3-C3 (e) State **FIVE (5)** strategies in protecting or restoring the lost, corrupted and deleted information.

*Nyatakan **LIMA (5)** strategi dalam melindungi atau memulihkan maklumat yang hilang, rosak dan dipadam.*

(5 Marks)
(5 Markah)

CLO3-C3 (f) Identify the importance of doing backup file?
Kenalpasti kepentingan melakukan fail sampingan?

(2 Marks)
(2 Markah)

SOALAN TAMAT