16

POLITEKNIK MALAYSIA

BAHAGIAN PEPERIKSAAN DAN PENILAIAN
JABATAN PENDIDIKAN POLITEKNIK
KEMENTERIAN PENDIDIKAN TINGGI

JABATAN TEKNOLOGI MAKLUMAT & KOMUNIKASI

PEPERIKSAAN AKHIR

SESI DISEMBER 2017

DFN5033 : NETWORK SECURITY

TARIKH : 01 APRIL 2018
MASA : 8.30 PAGI - 10.30 PAGI (2 JAM)

Kertas ini mengandungi **DUA PULUH LIMA (25)** halaman bercetak.
Bahagian A: Objektif (30 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: 45 MARKS
BAHAGIAN A: 45 MARKAH

INSTRUCTION:
This section consists of **THIRTY (30)** objective questions. Mark your answers in the OMR form provided.

ARAHAN:
*Bahagian ini mengandungi **TIGA PULUH (30)** soalan objektif. Tandakan jawapan anda di dalam borang OMR yang disediakan.*

CLO1
C1

1. Identify the features of restrictive security model.

   Kenalpasti ciri-ciri model keselamatan terhad

   A. Assumes the protected assets and threats are minimal, users are trusted.
   Andaikan aset dan ancaman dilindungi adalah minimum, pengguna dipercayai.

   B. Assumes the protected assets are precious, all users are trustworthy and threats minimal.
   Andaikan aset terlindung adalah berharga, semua pengguna boleh dipercayai dan ancaman minimum.

   C. Assumes the protected assets are substantial, some users and threats are not trustworthy.
   Anggap aset yang dilindungi adalah besar, sesetengah pengguna dan ancaman tidak boleh dipercayai.

   D. Assumes the protected assets are premium, all users are not trustworthy, and threats are frequent.
   Andaikan aset terlindung adalah premium, semua pengguna tidak boleh dipercayai, dan ancaman adalah kerap.

CLO1
C1

2. Identify the weakness which is categorized as security policy weakness.

   Tentukan kelemahan tersebut adalah kategori kelemahan polisi keselamatan.

   A. Lack of continuity
   Kekurangan kesinambungan.

   B. Unsecured user accounts
   Akaun pengguna tidak bercagar

   C. Lack of updating the system patches
   Kurang mengemas kini patch system

   D. Unsecured default settings within products
   Tetapan lalai tidak selamat dalam produk

CLO1
C1

3. "These people know system vulnerabilities and can develop exploit code and scripts"

"Mereka ini tahu tentang kelemahan sistem, boleh memahami dan boleh menjalankan eksploitasi kod dan skrip"

Identify type of threat based on the statement above.

Kenalpasti jenis ancaman berdasarkan kenyataan di atas.

A. Internal threat
Ancaman Dalaman

B. External threat
Ancaman Luaran

C. Structured threat
Ancaman Berstruktur

D. Unstructured threat
Ancaman tidak berstruktur

CLO1
C2

4.

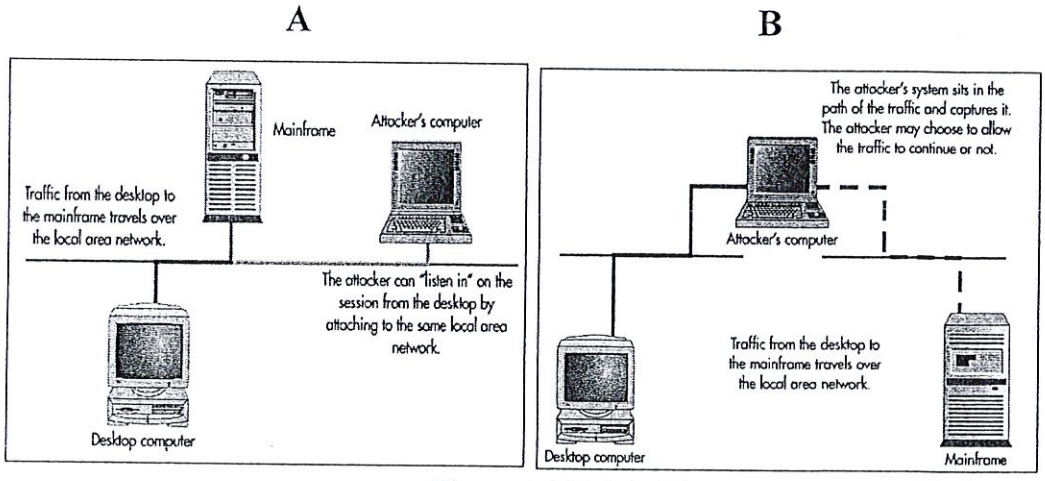

Figure A1/Rajah A1

Distinguish the attacks occur in Figure A1.

Bezakan serangan yang berlaku dalam Rajah A1.

A. A- snooping, B- poisoning
A- pengintipan, B- keracunan

B. A- interception, B- snooping
A- pemintasan, B- pengintipan

C. A- eavesdropping, B- interception
A- Mencuri dengar, B- pemintasan

D. A- interception, B- eavesdropping
A- Pemintasan. B- mencuri dengar

CLO1
C1

5. Identify the function of firewall component to capture all requests to server and tries to process the request made by the user.

Kenalpasti fungsi komponen firewall untuk merakam semua permintaan kepada server and cuba untuk proses permintaan yang dibuat oleh pengguna.

A. Packet filters
Penapis paket

B. Proxy server
Server proksi

C. Authentication system
Sistem pengesahan

D. Network address translation (NAT)
Terjemahan alamat rangkaian

CLO1
C2

6. Determine the level of implementation available for Intrusion detection system (IDS) and Intrusion Prevention System (IPS).

Tentukan aras pelaksanaan yang ada bagi Intrusion detection system (IDS) and Intrusion Prevention System (IPS).

A. Network level
Aras Rangkaian

B. Host level
Aras hos

C. Proxy server level
Aras server proksi

D. Firewall level
Aras firewall

CLO1 C3

7. Choose the **CORRECT** type of packet filtering if the network security administrator wants to filter incoming packet based on IP address and service.

*Pilih jenis penapis paket yang **BETUL** sekiranya pentadbir keselamatan rangkaian hendak menapis paket yang masuk berdasarkan alamat IP dan servis.*

A. Special

B. Dynamic

C. Stateless

D. Stateful

CLO1 C3

8. Network administrator of Bank XYZ need to protect their network from internal and external security threat. Choose the **APPROPRIATE** security devices that can be employed in order to protect their organization from both threats.

*Pentadbir rangkaian Bank XYZ perlu melindungi rangkaian mereka dari ancaman keselamatan luaran dan dalaman. Pilih peralatan keselamatan yang **SESUAI** boleh digunakan bagi melindungi organisasi mereka dari kedua-dua ancaman*

I. Proxy

II. Intrusion Detection System (IDS)

III. Firewall

IV. Demilitarized Zone (DMZ)

A. I, II

B. II, III

C. II, III, IV

D. I, II, III

CLO1
C3

9. Relate the effect towards your organization after the implementation a Demilitarized Zone (DMZ).

Kaitkan kesan terhadap organisasi anda selepas perlaksanaan Zon Bebas Ketenteraan (DMZ).

I. Local Area Network (LAN) become more secure.
LAN lebih selamat.

II. External network only access services in DMZ.
Rangkaian luar hanya capai servis yang terdapat dalam DMZ.

III. Private network isolated from Internet.
Rangkaian peribadi terpisah daripada Internet.

IV. As a firewall to protect LAN.
Sebagai firewall *untuk melindungi LAN.*

A. I, II and IV

B. I, II and III

C. II, III and IV

D. I, III and IV

CLO1
C3

10. Predict the effect if only Host-based Intrusion Detection System (IDS) is implemented rather than Network-based IDS.
Jangkakan kesan sekiranya hanya Sistem Pengesanan Pencerobohan (IDS) berasaskan hos yang dilaksanakan berbanding IDS berasaskan rangkaian.

A. Monitor only one subnet.
Memantau satu subnet sahaja.

B. Uses the resources of host.
Menggunakan sumber-sumber hos sahaja.

C. Reveal Trojan Horse.
Mendedahkan Trojan Horse.

D. Monitor local events.
Memantau kejadian setempat.

CLO1
C3

11. Arrange the steps to build a bastion host in **CORRECT** order.
*Susun langkah-langkah untuk membina hos bastion dalam turutan yang **BETUL**.*

I. Stop the unused services in the process.
Hentikan perkhidmatan yang tidak digunakan dalam proses tersebut.

II. Install or modify the services required in the process.
Pasang atau ubah suai perkhidmatan yang diperlukan dalam proses tersebut.

III. Use security audit for baseline.
Gunakan audit keselamatan untuk garis dasar.

IV. Reconfigure the machine.
Mengkonfigur semula mesin.

V. Connect the system to the network.
Sambungkan sistem ke rangkaian.

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

CLO1
C3

12. Figure A2 shows the connection of Company XYZ communication with its remote Office, Remote Worker and Business Partner. Choose the connection of A, B and C based on types of Virtual Private Network (VPN) they can use in order to secure data transfer through the internet.

Rajah A2 menunjukkan sambungan komunikasi Syarikat XYZ dengan "Remote Office", "Remote Worker" dan "Business Partner". Pilih sambungan A,B dan C berdasarkan jenis Rangkaian Persendirian Maya (VPN) yang mereka dapat gunakan untuk menjamin keselamatan pemindahan data melalui internet.

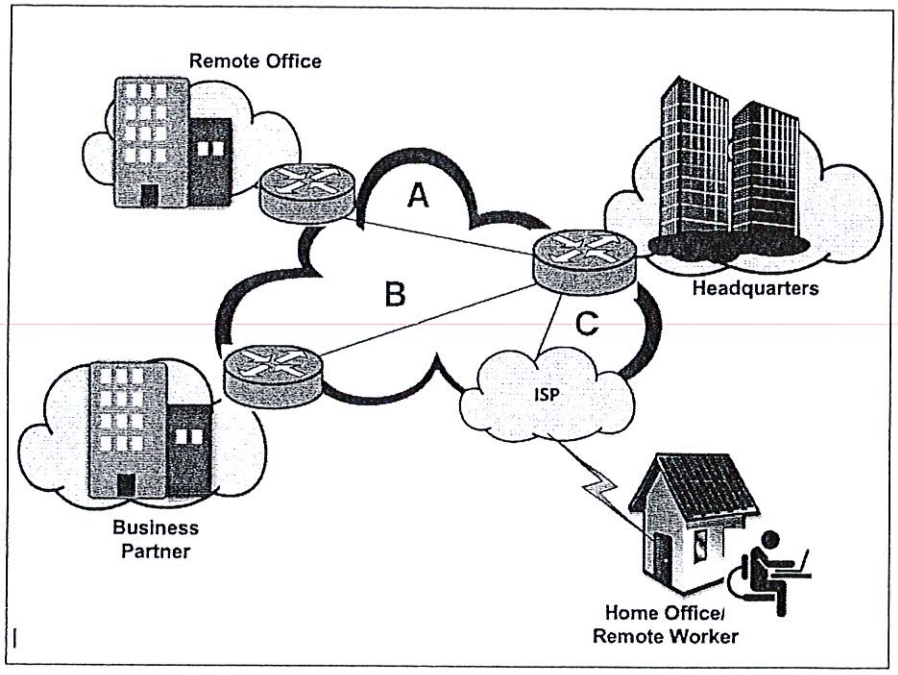

Figure A2/Rajah A2

A. A-Intranet VPN, B-Remote Access VPN, C-Extranet VPN
A-VPN Intranet, B-VPN Akses Jauh, C-VPN Extranet

B. A-Intranet VPN, B-Extranet VPN, C- Remote Access VPN
A-VPN Intranet, B- VPN Extranet, C- VPN Akses Jauh

C. A-Remote Access VPN, B-Intranet VPN, C-Extranet VPN
A- VPN Akses Jauh, B-VPN Intranet, C-VPN Extranet

D. A-Remote Access VPN, B- Extranet VPN, C- Intranet VPN
A- VPN Akses Jauh, , B - VPN Extranet, C-VPN Intranet

CLO1
C3

13.

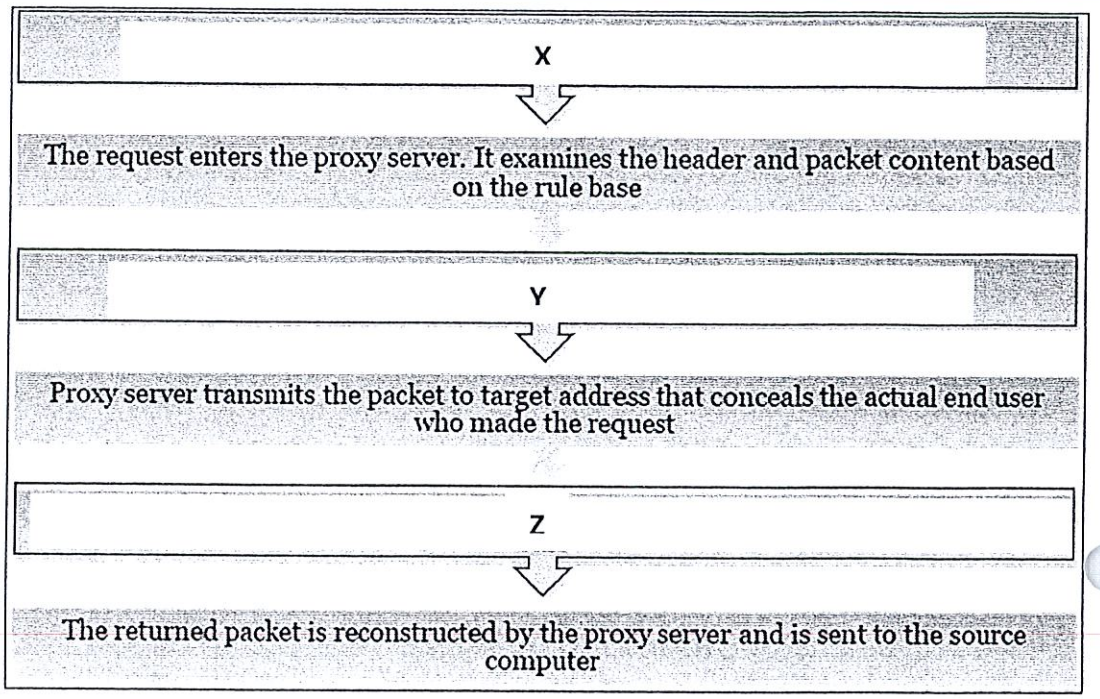

Figure A3/Rajah A3

Figure A3 shows the sequence of packet filtering process by a proxy server. Relate X, Y and Z with the following options.

Rajah A3 menunjukkan turutan proses penapisan paket oleh server proksi. Kaitkan X, Y dan Z dengan pilihan-pilihan berikut.

I. If the data packet is returned, it is resent to the proxy server to check with rule base.
Jika paket data dikembalikan, ia akan dihantar semula ke pelayan proksi untuk memeriksa dengan asas peraturan.

II. Internal host requests to process a web site.
Pemintaan hos dalaman untuk memproses laman web.

III. Server reconstructs the data packet with a different source IP Address.
Server membina semula paket data dengan IP sumber yang berlainan.

A. X = I, Y = II, Z = III
B. X = I, Y = III, Z = II
C. X = II, Y = I, Z = III
D. X = II, Y = III, Z = I

CLO1
C4

14. An administrator aims to avoid using an expensive system of leased lines for off-campus and wireless access. Determine the **BEST** practice of security architecture (SAFE) for him to adopt for his network.

*Matlamat seorang pentadbir adalah untuk mengelakkan daripada menggunakan sistem yang mahal dari talian sewaan untuk kampus luar dan akses tanpa wayar. Tentukan amalan **TERBAIK** senibina keselamatan (SAFE) kepada beliau untuk diterima pakai didalam rangkaiannya.*

A. Intrusion Detection System (IDS).
Sistem Pengesanan Pencerobohan (IDS).

B. Virtual Private Network (VPN).
Rangkaian Persendirian Maya (VPN).

C. Appliance-based firewall.
Firewall *berasaskan Perkakasan.*

D. Multiple firewalls.
Firewall *Pelbagai.*

CLO1
C1

15. Identify which of the following is referring to BIOS password.

Kenal pasti manakah diantara berikut merujuk kepada katalaluan BIOS.

A. Password for securing WIFI network
Katalaluan bagi keselamatan rangkaian WIFI

B. Password which block unwanted person from accessing BIOS system
Katalaluan yang menghalang orang yang tidak dikehendaki mengakses sistem BIOS

C. Password which block unwanted person from accessing the Internet
Katalaluan yang menghalang orang yang tidak dikehendaki mengakses internet

D. Password which allow changes on Windows Control Panel.
Katalaluan yang membenarkan perubahan pada Windows Control Panel.

CLO1 C2

16. Recognize the activity involving updating the BIOS to the latest version.

Kenal pasti aktiviti yang melibatkan mengemaskini BIOS kepada versi terkini.

A. Flash the BIOS
Mengimbas BIOS

B. Reboot the BIOS
Reboot *BIOS*

C. Configure the BIOS
Mengkonfigurasi BIOS

D. Reprogram the BIOS.
Memprogram semula BIOS.

CLO1 C3

17. Default Windows 7 settings are allow File Sharing services. Use the **CORRECT** utility to stop file sharing services in Windows 7 operating system.

*Tetapan lalai Windows 7 membolehkan perkhidmatan Perkongsian Fail. Gunakan utiliti yang **BETUL** untuk menghentikan perkhidmatan perkongsian fail dalam sistem pengoperasian Windows 7.*

A. Control Panel

B. Local Area Network Connection

C. Network Sharing Center

D. Firewall Properties

CLO1
C3

18. User X has suspected his computer been infected by a rootkit malware. Utilize **SUITABLE** software to detect the rootkit that has infected his Windows server 2003 operating system.

*Pengguna X telah mengesyaki computer beliau telah dijangkiti oleh malware rootkit. Gunakan perisian yang **SESUAI** untuk mengesan rootkit yang telah dijangkiti pada sistem pengoperasian Windows 2003 server beliau.*

A. Anti-Spyware.

B. RootkitRevealer.

C. Key Logger.

D. Remote Access Trojan (RAT) Detector.

CLO1
C3

19. Demonstrate how Rootkit Revealer works.
Tunjukkan bagaimana Rootkit Revealer berfungsi.

A. It checks the previous Windows Registry with the latest Windows Registry
Ia menyemak Registry Windows *terdahulu dengan Registry Windows terkini*

B. It checks the established connection on local netstat
Ia menyemak sambungan yang ditubuhkan pada netstat *tempatan*

C. It compares the operating system patch with the latest patch
Ia membandingkan patch sistem pengoperasian sebelumnya dengan kemaskini terkini

D. It compares result of a system scan at highest level with lower level
Ia membandingkan hasil imbasan sistem pada tahap tertinggi dengan tahap yang lebih rendah

CLO1 C3

20. Choose the **MOST** effective way to mitigate worms and fix the vulnerable system.

*Pilih cara yang **PALING** berkesan untuk mengurangkan worm dan membaiki sistem yang terdedah.*

A. Download and install operating system patches.
Memuat turun dan memasang patch sistem operasi.

B. Install personal firewall.
Memasang firewall *peribadi.*

C. Use intrusion detection system.
Penggunaan sistem pengesanan pencerobohan.

D. Use virtual private network.
Gunakan rangkaian persendirian maya.

CLO1 C3

21. System Administrator Company ZZQ wants to reduce the size of the attack surface of a Windows server within their organization.

Pentadbir Sistem syarikat ZZQ hendak mengurangkan saiz permukaan serangan terhadap pelayan Windows dalam organisasi mereka.

Based on statement above, apply the **RIGHT** way to reduce the size of surface attack on Windows Server.

*Berdasarkan pernyataan di atas, aplikasikan cara yang **BETUL** untuk mengurangkan saiz serangan permukaan pada Windows Server.*

A. Update antivirus software / *Kemaskini perisian anti-virus*

B. Install service packs / *Pasang* Service Packs

C. Disable unnecessary services / *Padamkan servis yang tidak perlu*

D. Install IDS & IPS / *Pasang IDS & IPS*

CLO1
C3

22. Kerberos authentication protocol uses Key Distribution Center (KDC) to prove identity of users. Relate the **CORRECT** statement of the KDC when the Kerberos protocol is being used.

*Protokol pengesahan Kerberos menggunakan Pusat Pengedaran Utama (KDC) untuk membuktikan identiti pengguna. Kaitkan kenyataan yang **BETUL** berkenaan KDC apabila protokol Kerberos sedang digunakan*

A. The KDC is only used to store secret keys.
KDC hanya digunakan untuk menyimpan kunci rahsia.

B. The KDC is used to capture secret keys over the network.
KDC digunakan untuk menangkap kunci rahsia melalui rangkaian.

C. The KDC is used to maintain and distribute public keys for each session.
KDC digunakan untuk mengekalkan dan mengedarkan kunci awam untuk setiap sesi.

D. The KDC is used to store, distribute, and maintain cryptographic session keys.
KDC digunakan untuk menyimpan, mengedarkan, dan menyelenggara kunci sesi kriptografi.

CLO1
C3

23. Company RYZ has installed a new Domain Controller is for running an authentication system on their organization. The Domain Controller running Kerberos as the authentication protocol. In order to ensure the connection from the client can be established between the authentication servers, the necessary inbound port is required to be open at the firewall level. Choose the combination of port number needed be open at the firewall in order for the authentication system can be running without any problem.

Syarikat RYZ telah dipasang Pengawal Domain baru untuk menjalankan sistem penyampaian maklumat pada organisasi mereka. Pengawal Domain menjalankan Kerberos sebagai protokol pengesahan. Untuk memastikan sambungan dari klien boleh ditubuhkan di antara pelayan pengesahan, port masuk yang diperlukan diperlukan untuk dibuka pada tahap firewall. *Pilih kombinasi nombor port yang perlu dibuka di* firewall *supaya sistem pengesahan dapat berjalan tanpa masalah.*

I. 88

II. 80

III. 389

IV. 8080

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

CLO1 C4

24.

- The ability to acquire multiple authorizations on high-security systems

  Keupayaan untuk mendapatkan beberapa kebenaran ke atas sistem keselamatan tinggi

- The ability to prompt the user for passwords for multiple authentication services without requiring the user to type multiple commands.

  Keupayaan untuk meminta kata laluan pengguna untuk beberapa pengesahan perkhidmatan tanpa memerlukan pengguna menaip beberapa arahan

Correlate the abilities stated above with the **CORRECT** Linux security framework.

*Hubungkaitkan kemampuan yang tertera di atas dengan kerangka kerja keselamatan Linux yang **BETUL**.*

A. Pluggable Authentication Module (PAM).

B. Virtual Private Network (VPN).

C. Security Configuration Wizard (SCW).

D. Point-to-Point Tunnelling Protocol (PPTP).

CLO1 C2

25. Select the main purpose physical access log.

Pilih tujuan utama fizikal akses log.

A. To enable authorized employee access
Untuk membolehkan akses pekerja dibenarkan

B. To show who exited the facility
Untuk menunjukkan siapa yang keluar dari bangunan

C. To show who entered the facility
Untuk menunjukkan siapa yang memasuki bangunan

D. To prevent unauthorized employee access
Untuk mengelakkan akses pekerja tanpa izin

CLO1 C3

26. Administrator of company XYZ want to strenghten their server room security. Apply the good practice for tracing the users' identities in and out from the server room.

Pentadbir syarikat XYZ ingin mengukuhkan keselamatan bilik server mereka. Aplikasikan amalan yang baik untuk mengesan identiti pengguna masuk dan keluar dari bilik server.

I. Video Cameras / *kamera video*

II. Key card door access system / *sistem akses pintu kad kunci*

III. Sign-in sheet / *borang masuk*

IV. Security guard / *pengawal keselamatan*

A. I, and III

B. I, and IV

C. II, and IV

D. I, and II

CLO1 C3

27. Company YYY provides to its employees badges that are encoded with a Private encryption key and specific personal information. The encoding is used to provide access to the organization's network. Choose the type of authentication method that being used

Syarikat YYY menyediakan lencana kepada pekerja mereka yang telah dikodkan dengan Kekunci penyulitan peribadi dan maklumat peribadi khusus. Pengekodan digunakan untuk menyediakan akses kepada rangkaian organisasi. Pilih jenis kaedah pengesahan yang digunakan

A. Token / *Token*

B. Biometric / *Biometrik*

C. Kerberos / *Kerberos*

D. Smart Card / *Kad pintar*

CLO1
C3

28. Bank ZZY has installed several network devices on their existing network. All the devices is in default state. Relate the potential security issue that might be arise when all devices are left in the default state.

Bank ZZY telah memasang beberapa peranti rangkaian pada rangkaian sedia ada mereka. Semua peranti berada dalam keadaan default. Kaitkan isu keselamatan yang mungkin muncul apabila semua peranti dibiarkan dalam keadaan default.

I. Weak Password
Kata laluan yang lemah

II. Default Account
Akaun Default

III. Data unencrypted
Data tidak di encrypt.

IV. Slowing down your internet connection.
Memperlahankan sambungan internet anda

A. I, II

B. II, III

C. II, III, IV

D. I, II, III

CLO1
C3

29. Network Administrator of Bank YYR has asked their management to limit the wireless signal of a WAP from going outside of the building. Identify the solution to limit the wireless signal from going outside of the building.

Pentadbir Rangkaian Bank YYR telah meminta pihak pengurusan mereka untuk mengehadkan isyarat wayarles WAP dari luar bangunan. Kenal pasti penyelesaian untuk mengehadkan isyarat tanpa wayar dari luar bangunan

A. Put the antenna on the exterior of the building.
Letakkan antena di bahagian luar bangunan.

B. Disable the SSID.
Matikan SSID.

C. Enable MAC filtering.
Hidupkan penapisan MAC.

D. Decrease the power levels of the WAP.
Kurangkan tahap kuasa WAP.

CLO1
C4

30. MMH Company has stored a critical information in their data center, the CEO has asked their IT Manager to improve the physical security within the data center area. The data center is already equipped with a CCTV system. Discover other related practices they can implement in order to increase the level of physical security at the data center.

Syarikat MMH tmenyimpan maklumat penting di dalam pusat data mereka, CEO telah meminta Pengurus IT mereka untuk meningkatkan keselamatan fizikal di kawasan pusat data. Pusat data sudah dilengkapi dengan sistem CCTV. Temukan praktis lain yang berkaitan yang boleh dilaksanakan untuk meningkatkan tahap keselamatan fizikal di pusat data

I. Software Based token system.
Sistem token berasaskan perisian.

II. Access control list
senarai kawalan akses

III. A mantrap.
Sebuah mantrap

IV. Biometric
Biometrik

A. I & II

B. II & III

C. III & IV

D. I, II & III

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 berstruktur. Jawab semua soalan.*

QUESTION 1

SOALAN 1

CLO1
C3

a) Company ABC is planning to upgrade their database system that is hosted in local server. List the risk assessment of the company on the existing system for them to eliminate the risk.

Syarikat ABC merancang untuk menaik taraf sistem pangkalan data mereka yang dihoskan dalam pelayan tempatan. Senaraikan penilaian risiko syarikat pada sistem yang sedia ada bagi mereka untuk menghapuskan risiko tersebut.

[2 marks]
[2 markah]

CLO1
C2

b) Describe the meaning of vulnerabilities in network security.

Huraikan maksud kelemahan dalam keselamatan rangkaian.

[3 marks]
[3 markah]

CLO1 C3

c)

> The data or message which is sent by the sender is attacked by an unauthorized individual where the message will be changed into different form or it will be used by the individual for his malicious process. So the confidentiality of the message is lost in this attack.
>
> *Data atau mesej yang dihantar oleh penghantar telah diserang oleh individu yang tidak ada kebenaran dimana mesej itu akan diubah kepada bentuk yang berbeza atau ia akan digunakan untuk proses berniat jahat. Jadi kerahsiaan mesej tersebut hilang dalam serangan ini.*

Based on the statement above, predict the type of attack that is happening in the statement and **ONE (1)** way to prevent it to be happened.

*Berdasarkan penyataan di atas, jangkakan jenis serangan yang berlaku dalam penyataan tersebut dan **SATU (1)** cara untuk mengelakkannya daripada berlaku.*

[2 marks]
[2 markah]

CLO1 C1

d) Write **FOUR (4)** components of firewall.

*Tuliskan **EMPAT (4)** komponen* firewall.

[4 marks]
[4 markah]

CLO1 C2

e) Explain the function of Demilitarize Zone (DMZ).
Terangkan fungsi Zon Demilitari (DMZ).

[4 marks]
[4 markah]

CLO1 C3

f) Explain the **TWO (2)** technologies in firewall architecture listed below.
*Jelaskan **DUA (2)** teknologi dalam senibina* firewall *yang disenaraikan di bawah.*

i. Static (Stateless Packet Filtering)
ii. Dynamic (Statefull Packet Filtering)

[6 marks]
[6 markah]

CLO1 C4

g) KKK Bank has upgraded a new firewall with latest technology at the network perimeter to strengthen their network security. However, the network is still exposed to 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 limitasi* firewall, *terangkan bagaimana IDS dan IPS boleh melengkapkan kekangan* firewall.

[4 marks]
[4 markah]

QUESTION 2
SOALAN 2

CLO1
C1

a) Define operating system hardening
Tafsirkan pengerasan sistem pengoperasian.

[3 marks]
[3 markah]

CLO1
C2

b) A computer technician has finished installing an operating system for a home user. Identify **TWO (2)** good methods to be implemented to secure that operating system.

*Seorang juruteknik komputer telah selesai memasang sistem operasi untuk pengguna rumah. Kenal pasti **DUA (2)** kaedah yang baik untuk dilaksanakan untuk memastikan bahawa sistem operasi selamat.*

[4 marks]
[4 markah]

CLO1
C3

c) Show the location directory of the following files in the Linux OS:
Tunjukkan lokasi direktori bagi fail-fail berikut di dalam OS Linux:

i. PAM application file
Fail aplikasi PAM

ii. Library modules
Modul library

iii. PAM configuration file
Fail konfigurasi PAM

[6 marks]
[6 markah]

CLO1 C4

d) Summarize the trust relationships between domains as shown in **Figure B1.**

Rumuskan hubungan kepercayaan antara domain seperti yang ditunjukkan di dalam ***Rajah B1.***

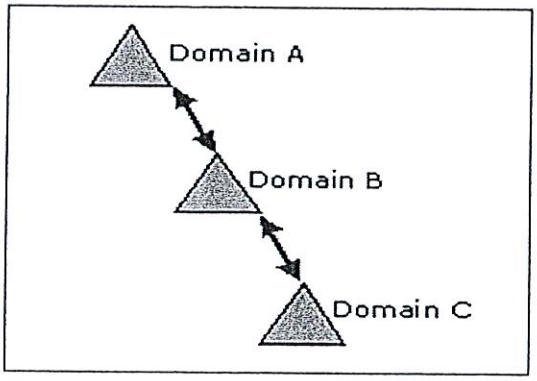

Figure B1 / ***Rajah B1***

[5 marks]

[5 markah]

CLO1 C2

e) Describe Biometric in physical security with an example.

Terangkan Biometric dalam keselamatan fizikal dengan satu contoh.

[3 marks]

[3 markah]

CLO1 C3

f) Company Airlines Surabaya has purchased a new router to replace an existing obsolete router, before the router can be placed on the production network, the router should be hardened in order to ensure the router security at the safest state. Perform the configuration that can be disabled on the router in order to secure it.

Syarikat Penerbangan Surabaya telah membeli router *baru untuk menggantikan* router *usang sedia ada, sebelum* router *dapat ditempatkan di rangkaian produksi,* router *harus dikukuhkan untuk memastikan keselamatan* router *di keadaan paling selamat. Laksanakan konfigurasi yang boleh dipadamkam pada* router *bagi memastikan ia dalam keadaan selamat.*

[5 marks]

[5 markah]

CLO1
C4

g) Distinguish between **TWO (2)** types of authentication method that are defined in IEEE 802.11 standard for protection of wireless links.

*Bezakan antara **DUA (2)** jenis kaedah pengesahan yang ditentukan dalam piawaian IEEE 802.11 untuk perlindungan pautan tanpa wayar.*

[4 marks]
[4 markah]

END OF QUESTIONS

SOALAN TAMAT