UNIVERSITI TEKNIKAL MALAYSIA MELAKA
PEPERIKSAAN AKHIR SEMESTER II
FINAL EXAMINATION SEMESTER II
SESI 2021/2022
SESSION 2021/2022
FAKULTI TEKNOLOGI MAKLUMAT DAN KOMUNIKASI

KOD KURSUS ***COURSE CODE***	**:**	**BITS 2413**
KURSUS ***COURSE***	**:**	**INFRASTRUKTUR DAN REKABENTUK KESELAMATAN RANGKAIAN** ***NETWORK SECURITY INFRASTRUCTURE AND DESIGN***
PENYELARAS ***COORDINATOR***	**:**	**KHADIJAH BINTI WAN MOHD GHAZALI**
PROGRAM ***PROGRAMME***	**:**	**BITZ**
MASA ***TIME***	**:**	**8.30 a.m.**
TEMPOH ***DURATION***	**:**	**2 JAM DAN 30 MINIT** ***2 HOURS AND 30 MINUTES***
TARIKH ***DATE***	**:**	**24 JUN 2022** ***24 JUNE 2022***
TEMPAT ***VENUE***	**:**	**EXAM HALL 3**

ARAHAN KEPADA CALON
INSTRUCTION TO CANDIDATES

1. **Sila jawab SEMUA soalan.**
   Please answer ALL questions.
2. **Kertas soalan ini mempunyai versi dwi-bahasa. Versi Bahasa Melayu bermula daripada mukasurat 2 hingga 7, manakala versi Bahasa Inggeris bermula daripada mukasurat 8 hingga 13.**
   The exam paper consists of dual-language version. The Malay version starts from page 2 to 7, whereas the English version starts from page 8 to 13.

KERTAS SOALAN INI TERDIRI DARIPADA TIGA BELAS (13) MUKA SURAT SAHAJA TERMASUK MUKA SURAT HADAPAN
THIS QUESTION PAPER CONTAINS THIRTEEN (13) PAGES INCLUSIVE OF FRONT PAGE

ARAHAN: *Jawab **SEMUA** soalan.*

SOALAN 1 (8 MARKAH)

Perlaksanakan protokol AAA *(Authentication, Authorization and Accounting)* memberikan capaian yang lebih selamat berbanding penggunaan kata laluan semata-mata. Jelaskan faedah melaksanakan AAA sebagai kaedah pengesahan setempat dan kaedah pengesahan berasaskan pelayan. Berikut ialah panduan menjawab:

- Jelaskan **DUA (2)** faedah pengesahan setempat AAA (4 markah).
- Jelaskan **DUA (2)** faedah pengesahan berasaskan pelayan AAA (4 markah).

(8 markah)

SOALAN 2 (5 MARKAH)

Rangkaian-rangkaian dalam satu domain Microsoft Windows boleh melaksanakan AAA menggunakan RADIUS *(Remote Authentication Dial-In User Service)* dalam pelayan *Network Policy Server* (NPS). Jelaskan peranan pengawal domain *Active Directory* (AD) dalam perlaksanaan ini.

(5 markah)

SOALAN 3 (4 MARKAH)

Berikan **DUA (2)** perbezaan antara ACL (*Access Control Lists*) biasa dengan ACL lanjutan.

(4 markah)

SOALAN 4 (14 MARKAH)

ACL boleh digunakan untuk mencegah serangan perdayaan. Kaji serangan perdayaan ini.

i. Apakah serangan perdayaan?

(2 markah)

ii. Senaraikan **LIMA (5)** kategori alamat IP sumber yang sepatutnya disekat oleh ACL daripada memasuki rangkaian daripada luar.

(5 markah)

iii. Bagi **DUA (2)** daripada kategori-kategori dalam soalan (ii), berikan satu contoh alamat IP bagi setiap satunya.

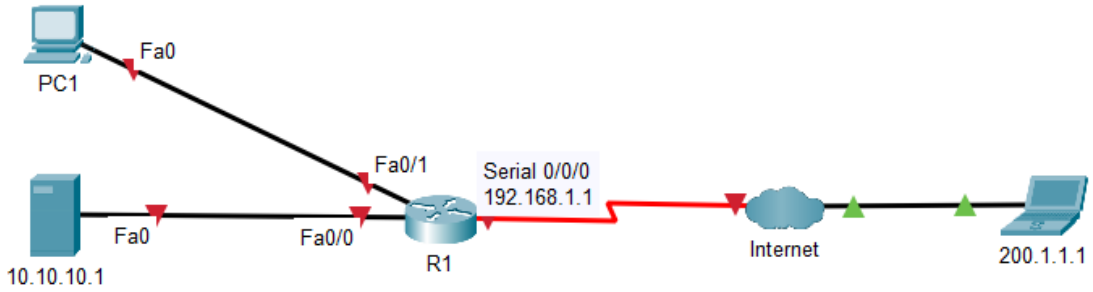
(2 markah)

iv. Jelaskan mengapa dengan menggunakan ACL untuk menyekat alamat-alamat seperti dalam soalan (ii) boleh mencegah daripada berlakunya penafian perkhidmatan.

(5 markah)

SOALAN 5 (7 MARKAH)

Rujuk kepada Rajah 2 dan Rajah 3. Rajah 2 menunjukkan satu senario rangkaian di mana ACL dilaksanakan, manakala Rajah 3 menunjukkan kenyataan ACL yang dikonfigurasikan bagi senario tersebut. Dengan mengkaji senario rangkaian dan ACL yang diberikan, tentukan penempatan ACL tersebut.



Rajah 2: Senario Rangkaian

```
R1(config)# access-list 170 permit tcp any host 10.10.10.1 eq ftp
R1(config)# access-list 170 permit tcp any host 10.10.10.1 eq smtp
R1(config)# access-list 170 permit udp any host 10.10.10.1 eq domain
R1(config)# access-list 170 permit tcp host 200.1.1.1 host 192.168.1.1 eq 22
R1(config)# access-list 170 permit udp host 200.1.1.1 host 192.168.1.1 eq smtptrap
R1(config)# access-list 170 permit udp host 200.1.1.1 host 192.168.1.1 eq syslog
```

Rajah 3: ACL

i. Nyatakan kategori ACL yang ditunjukkan dalam Rajah 3.

(1 markah)

ii. Apakah kesan ACL dalam Rajah 3 kepada senario rangkaian dalam Rajah 2.

(2 markah)

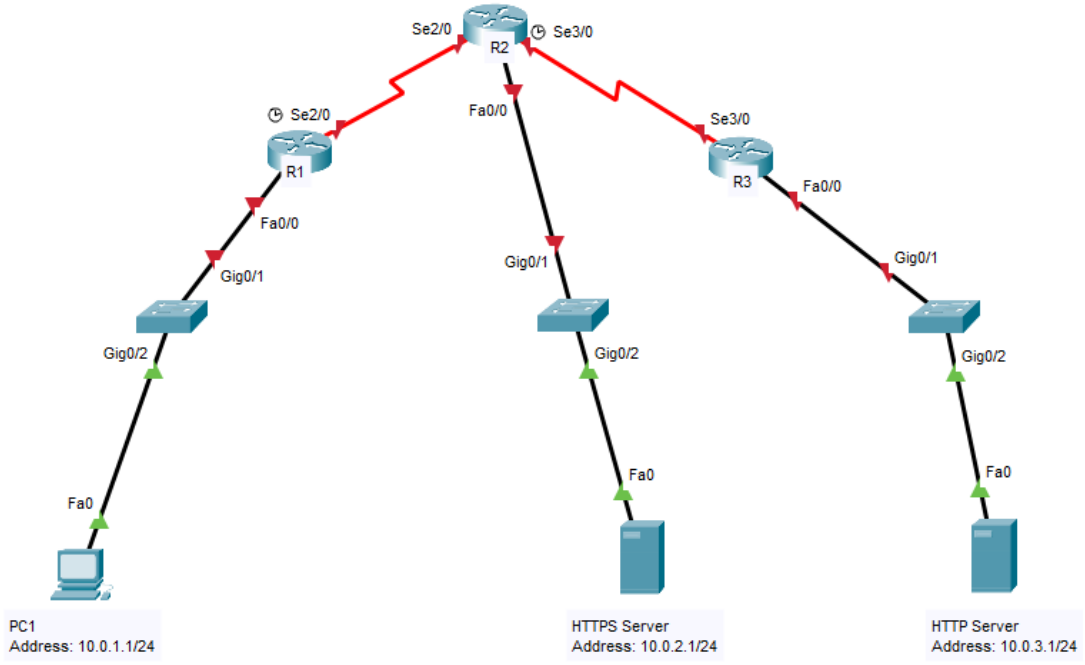
iii. Di bahagian rangkaian yang manakah ACL dalam Rajah 3 boleh diletakkan? Di lokasi tersebut, apakah arah ACL itu? Justifikasikan pemilihan tempat anda.

(4 markah)

SOALAN 6 (13 MARKAH)

Rujuk Rajah 4. Anda dikehendaki mengkonfigurasi ACL yang akan membenarkan PC1 mancapai laman-laman web dari kedua-dua pelayan HTTPS dan HTTP tetapi akan menyekat *ping* dari PC1 ke pelayan-pelayan itu. Pertimbangkan perkara-perkara di bawah semasa membina ACL anda:

- Pembolehubah-pembolehubah yang betul dinyatakan dalam ACL (5 markah).
- Sintaks ACL yang betul (5 markah).
- Penempatan dan arah ACL yang betul (3 markah).



Rajah 4: Senario Rangkaian

(13 markah)

SOALAN 7 (12 MARKAH)

Anda bekerja sebagai penganalisa keselamatan kanan di Bestlah Inc, sebuah syarikat teknologi yang sedang berkembang, milik Melon Usk. Untuk maju ke skala yang lebih besar, Bestlah perlu menaik taraf infrasturuktur keselamatannya daripada tembok api yang sedang digunakan sekarang. Tuliskan rekomendasi anda bagi perlaksanaan keselamatan yang lebih baik bagi melindungi rangkaian syarikat dari pencerobohan. Berikan butiran-butiran berikut.

- Kelebihan dan kekurangan IDS (4 markah).
- Kelebihan dan kekurangan IPS (4 markah).
- Solusi pilihan anda dan justifikasinya (4 markah).

(12 markah)

SOALAN 8 (4 MARKAH)

"Mengkonfigurasikan keselamatan pada hos-hos rangkaian dan rangkaian dalaman adalah sama pentingnya dengan melaksanakan peralatan keselamatan khusus seperti tembok api, IDS, IPS dan VPN."

Sokong kenyataan di atas dengan menjelaskan **DUA (2)** hujah.

(4 markah)

SOALAN 9 (12 MARKAH)

Penyerang boleh mengeksploitasi kelemahan dalam lapisan kedua rangkaian. Huraikan **SATU (1)** serangan terhadap suis rangkaian, dengan memberi perincian seperti berikut:

- Nama serangan (1 markah).
- Persekitaran rangkaian di mana serangan mungkin boleh dilancarkan (3 markah).
- Bagaimana kelemahan dalam persekitaran rangkaian itu boleh dieksploitasikan oleh serangan ini (4 markah).
- Strategi mitigasi bagi menghadapi serangan ini (4 markah).

(12 markah)

SOALAN 10 (12 MARKAH)

Dengan pertambahan kapasiti perkhidmatan Internet, keperluan untuk menyambung kepada sesuatu organisasi secara jarak jauh juga bertambah. Satu kaedah popular untuk melakukan perkara ini ialah dengan menggunakan VPN (*Virtual Private Network*).

Berdasarkan perkhidmatan VPN yang tersedia di pasaran kini, bincangkan **TIGA (3)** faedah dan **TIGA (3)** risiko menggunakan VPN untuk bekerja dan belajar secara jarak jauh. Terangkan setiap butiran jawapan anda. Berikut ialah panduan menjawab:

- Berikan **TIGA (3)** faedah menggunakan VPN (3 markah).
- Bagi setiap faedah, berikan penerangan (3 markah).
- Berikan **TIGA (3)** risiko menggunakan VPN (3 markah).
- Bagi setiap risiko, berikan penerangan (3 markah).

(12 markah)

SOALAN 11 (9 MARKAH)

Satu carian Google yang ringkas pada kata kunci “VPN” akan menghasilkan rekomendasi kepada produk-produk seperti “VPNExpress” dan “NordVPN”. Kenal pasti kategori produk-produk VPN ini. Bandingkan produk-produk VPN dalam kategori ini dengan *Site-to-Site VPN* yang telah anda pelajari dalam subjek ini. Berikut ialah panduan menjawab:

- Nyatakan kategori VPN yang manakah produk-produk VPN seperti “VPNExpress” dan “NordVPN” (1 markah).
- Berikan **EMPAT (4)** perbandingan antara kategori VPN yang anda nyatakan di atas dengan *Site-to-Site VPN* (4 markah).
- Bagi setiap butiran perbandingan, berikan penjelasan (4 markah).

(9 markah)

-SOALAN TAMAT-

INSTRUCTION: *Answer **ALL** questions.*

QUESTION 1 (8 MARKS)

Implementing Authentication, Authorization, and Accounting (AAA) protocol provides more access security than using passwords alone. Explain the benefits of implementing AAA as local authentication and as server-based authentication. Below is your answering guide:

- Explain **TWO (2)** benefits of AAA local authentication (4 marks).
- Explain **TWO (2)** benefits of AAA server-based authentication (4 marks).

(8 marks)

QUESTION 2 (5 MARKS)

Networks in a Microsoft Windows domain may implement AAA using RADIUS (Remote Authentication Dial-In User Service) in its Network Policy Server (NPS). Explain the roles of Active Directory (AD) domain controller in this implementation.

(5 marks)

QUESTION 3 (4 MARKS)

Give **TWO (2)** comparisons between standard ACL (Access Control Lists) and extended ACL.

(4 marks)

QUESTION 4 (14 MARKS)

ACLs can be used to prevent spoofing attacks. Study this spoofing attack.

i. What is spoofing attack?

(2 marks)

ii. List **FIVE (5)** categories of source IP addresses of incoming traffics that should be blocked by ACL to prevent spoofing attacks.

(5 marks)

iii. For **TWO (2)** of the categories in question (ii), give an example of IP address for each.

(2 marks)

iv. Explain why using an ACL to block the addresses in question (ii) can prevent Denial of Service from taking place.

(5 marks)

QUESTION 5 (7 MARKS)

Refer to Figure 2 and Figure 3. Figure 2 shows a network scenario where an ACL is implemented, whereas Figure 3 shows the ACL statements that are configured for the scenario. By studying the network scenario and ACL given, determine the placement of the ACL.

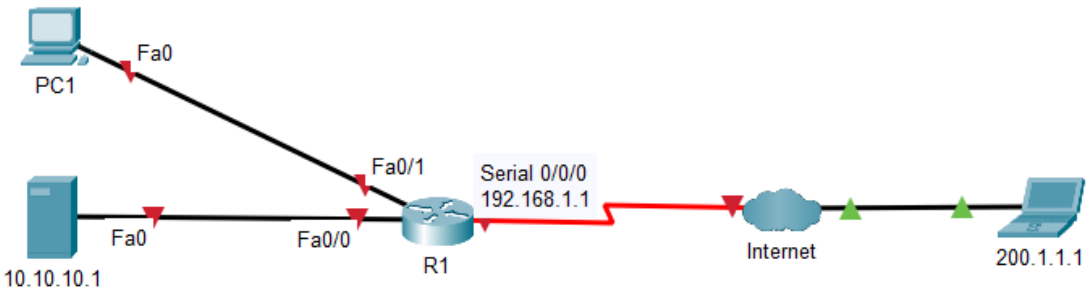


Figure 2: A Network Scenario

```
R1(config)# access-list 170 permit tcp any host 10.10.10.1 eq ftp
R1(config)# access-list 170 permit tcp any host 10.10.10.1 eq smtp
R1(config)# access-list 170 permit udp any host 10.10.10.1 eq domain
R1(config)# access-list 170 permit tcp host 200.1.1.1 host 192.168.1.1 eq 22
R1(config)# access-list 170 permit udp host 200.1.1.1 host 192.168.1.1 eq smtptrap
R1(config)# access-list 170 permit udp host 200.1.1.1 host 192.168.1.1 eq syslog
```

Figure 3: ACL

i. State the category of the ACL shown in Figure 3.

(1 mark)

ii. What are the effects of ACL in Figure 3 to the network scenario in Figure 2.

(2 marks)

iii. In which part of the network should the ACL in Figure 3 be applied? In that location, what would be its direction? Justify your placement choice.

(4 marks)

QUESTION 6 (13 MARKS)

Refer to Figure 4. You are required to configure an ACL that will allow PC1 to access websites in both HTTPS Server and HTTP Server but will block ping from PC1 to the servers. Consider the following when building the ACL:

- Correct variables stated in the ACL (5 marks).
- Correct syntax of the ACL (5 marks).
- Correct placement and direction of the ACL (3 marks).

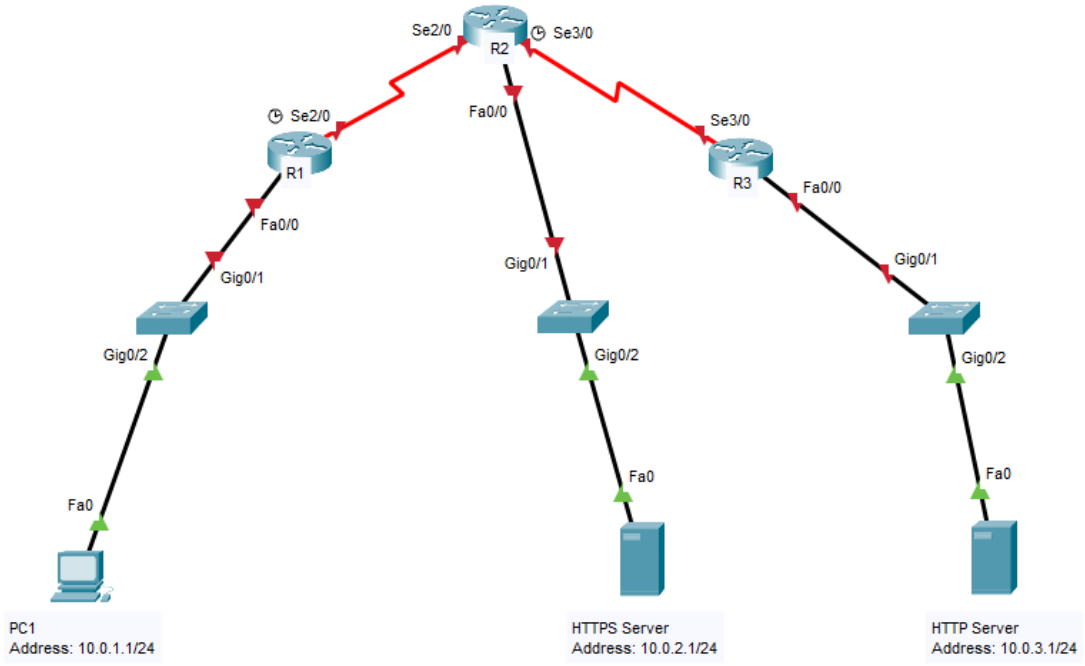


Figure 4: A Network Scenario

(13 marks)

QUESTION 7 (12 MARKS)

You work as a senior security analyst in Bestlah Inc., a growing tech company lead by an entrepreneur Melon Usk. To progress to a larger scale, Bestlah should upgrade its security infrastructure from the current firewall it is using. Write your recommendation of the better security deployment to protect the company's network from intrusion. Give the following points.

- The advantages and disadvantages of IDS (4 mark).
- The advantages and disadvantages of IPS (4 mark).
- The solution of your choice and justification (4 mark).

(12 marks)

QUESTION 8 (6 MARKS)

"Securing the network hosts and internal networks are equally as important as deploying the specific security tools such as firewalls, IDSs, IPSs, and VPNs."

Support the statement above by explaining **TWO (2)** arguments.

(4 marks)

QUESTION 9 (10 MARKS)

Attackers can exploit vulnerabilities in layer two of a network. Elaborate **ONE (1)** switch attack, by giving details as follows:

- The name of the attack (1 mark).
- The network environment where the attack can possibly be launched (3 marks).
- How the vulnerabilities in the network environment can be exploited by this attack (4 marks).
- The mitigation strategy for this attack (4 marks).

(12 marks)

QUESTION 10 (12 MARKS)

As the Internet services increases its capacity, the need to remotely connect to an organization network also increases. A popular method for doing this is by using Virtual Private Network (VPN).

Based on the existing VPN services available in the market now, discuss **THREE (3)** benefits and **THREE (3)** risks of using VPN for remote working and learning. Explain each of your point. Below is your answering guide:

- Give **THREE (3)** benefits of using VPN (3 marks)
- For each benefit, give an explanation (3 marks)
- Give **THREE (3)** risks of using VPN (3 marks)
- For each risk, give an explanation (3 marks)

(12 marks)

QUESTION 11 (9 MARKS)

A quick Google search for "VPN" keyword will result on recommendations for products such as "VPNExpress" and "NordVPN". Identify which category of VPN are these products. Compare the VPN products in this category to the Site-to-Site VPN that you learned in this subject. Below is your answering guide:

- State which category of VPN are the VPN products like "VPNExpress" and "NordVPN". (1 mark)
- Give **FOUR (4)** comparisons between the VPN category you stated above with Site-to-Site VPN (4 marks)
- For each comparison point, give an explanation (4 marks)

(9 marks)

-END OF QUESTIONS-