



UNIVERSITI TEKNIKAL MALAYSIA MELAKA

PEPERIKSAAN AKHIR SEMESTER I

FINAL EXAMINATION SEMESTER I

SESI 2023/2024

SESSION 2023/2024

FAKULTI TEKNOLOGI MAKLUMAT DAN KOMUNIKASI

**KOD MATAPELAJARAN**  
**SUBJECT CODE**

:BITS 3613

**MATAPELAJARAN**  
**SUBJECT**

:TEKNIK PENGGODAMAN DAN PENCEGAHAN  
*HACKING TECHNIQUES AND PREVENTION*

**PENYELARAS**  
**COORDINATOR**

: MOHD ZAKI MAS'UD

**KURSUS**  
**COURSE**

: 3 BITZ

**MASA**  
**TIME**

: 09:00 Pagi  
09:00 A.M

**TEMPOH**  
**DURATION**

: 2 JAM  
2 HOURS

**TARIKH**  
**DATE**

: 29 JANUARI 2024

UNIVERSITI TEK29 JANUARY 2024 A MELAKA

**TEMPAT**  
**VENUE**

: DK 5 & DK 6 KOMPLEKS DEWAN KULIAH  
DK 5 & DK 6 , LECTURE HALL COMPLEX

**ARAHAN KEPADA CALON**  
**INSTRUCTION TO CANDIDATES**

1. Kertas soalan ini mengandungi DUA (2) Bahagian. Sila Jawab SEMUA soalan di kedua-dua Bahagian  
*The exam paper consists of TWO (2) PARTS. Please ALL the questions in both part*
2. Kertas soalan ini mempunyai versi dwi-bahasa.  
*The exam paper consists of dual-language version.*

**KERTAS SOALANINI TERDIRI DARIPADA SEMBILAN BELAS (19) MUKA SURAT SAHAJA**  
**TERMASUK MUKA SURAT HADAPAN**

*THIS QUESTION PAPER CONTAINS NINETEEN (19) PAGES INCLUSIVE OF FRONT PAGE*

**BAHAGIAN A: SOALAN BERSTRUKTUR (40 MARKAH)**

**ARAHAN:** Sila jawab **SEMUA** soalan

- (a) Serangan siber yang dilakukan oleh penggodam boleh mengakibatkan kerosakan pada pelayan. Terangkan apa itu penggodam dan apakah yang menjadi motivasi untuk mereka menggodam?

**(2 markah)**

- (b) Berikan **DUA (2)** perbezaan antara penggodam dan penggodam beretika

**(2 markah)**

- (c) Penggodam boleh dikategorikan kepada beberapa jenis, senaraikan **EMPAT (4)** jenis penggodam.

**(4 markah)**

- (d) Berikan definisi kepada terma-terma penggodaman di bawah:-

i. *Vulnerability*

**(1 markah)**

ii. *Zero-day attack*

**(1 markah)**

iii. *Foot Printing*

**(1 markah)**

iv. *Enumeration*

**(1 markah)**

- (e) Etika bermaksud piawaian perbuatan yang salah dan betul manakala Undang-undang ditakrifkan sebagai peraturan kepada kelakuan atau tindakan yang dikuatkasakan secara rasmi oleh pihak berkuasa yang mempunyai bidang kuasa terhadap mereka.

Nyatakan **EMPAT (4)** lagi perbezaan antara Etika dan Undang-undang.

**(4 markah)**

- (f) Nyatakan **EMPAT (4)** undang-undang siber di Malaysia yang telah diluluskan oleh Parlimen Malaysia bagi melindungi rakyat dari jenayah siber.

**(4 markah)**

- (g) Agen Lisa telah berjaya memintas komunikasi di antara tentera US dan Rusia dalam Perang Dunia ke II dan beliau percaya, mereka menggunakan kaedah *Caesar Cipher* untuk menyulitkan mesej mereka. Sebagai *cryptanalyst* kepada Agen Lisa, cari kunci dan nyahsulit teks sifer berikut.

NVVKFVBNBLZAPA

(5 markah)

- (h) Senaraikan mana-mana **LIMA (5)** langkah dalam Metodologi *cyber kill chain* yang digunakan dalam menyerang infrastruktur rangkaian.

(5 markah)

- (i) Senaraikan mana-mana **TIGA (3)** ancaman dari sumber rangkaian.

(3 markah)

- (j) Setelah fasa *foot printing* dan *enumeration* selesai, fasa seterusnya dalam proses penggodaman ialah penggodaman sistem dan ia terdiri daripada lima peringkat. Senaraikan mana-mana **TIGA (3)** daripada peringkat penggodaman sistem.

(3 markah)

- (k) Ujian Penerobosan boleh dilaksanakan sama ada melalui pendekatan dari dalam organisasi atau luar organisasi. Terangkan setiap pendekatan tersebut serta senaraikan kelebihan dan kekurangan untuk setiap satu pendekatan.

(4 markah)

**BAHAGIAN B: SOALAN BERSTRUKTUR (60 MARKAH)**

**ARAHAN:** Sila jawab **SEMUA** soalan

**SOALAN 1 (20 MARKAH)****Kajian Kes 1:**

Esther adalah seorang penggodam *blackhat* yang telah berjaya mengeksplotasi dan menembusi komputer pelayan milik syarikat Baithori Corporation Berhad (BCB). Sebagai Pengurus Kanan Keselamatan Komputer BCB, anda telah diminta untuk melakukan siasatan ke atas kejadian tersebut. Berdasarkan penyiasatan pada log rangkaian yang ditangkap dari komputer pelayan seperti di *Appendix 1*, pencerobohan keselamatan dilakukan menggunakan kaedah penggodaman. Bincangkan penyiasatan anda tentang insiden tersebut berdasarkan metodologi penggodaman untuk dijelaskan kepada pengurusan atasan,

Untuk membantu penyiasatan anda, jawab soalan berikut berdasarkan metodologi penggodaman:

- (a) Kejuruteraan Sosial adalah salah satu kaedah yang licik untuk memanipulasi kecenderungan semulajadi manusia untuk mempercayai seseorang dan merupakan salah satu pendekatan untuk mengumpulkan maklumat dari sasaran. Terangkan secara ringkas kaedah kejuruteraan sosial berikut. Bagi setiap kaedah tersebut, berikan contoh tindakan yang boleh dilakukan.
- Pishing* (2 markah)
  - Quid Pro Quo* (2 markah)
  - Baiting* (2 markah)

- (b) Cari komunikasi yang disyaki berlaku antara mesin Esther dengan salah satu pelayan BCB dalam log trafik rangkaian *Appendix 1*.

Berdasarkan log trafik rangkaian di *Appendix 1*:

- Kenalpasti alamat IP penggodam. (1 markah)

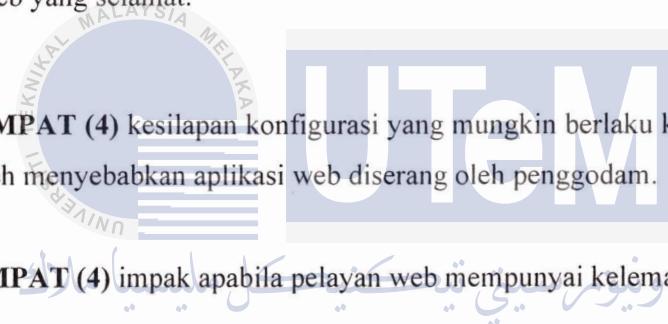
- ii) Apakah kaedah *port scanning* yang digunakan? Nyatakan alasan anda. **(2 markah)**
- iii) Kenalpasti **DUA (2)** port yang terbuka dan **DUA (2)** port yg tertutup semasa aktiviti *scanning* ini. **(4 markah)**
- iv) Berikan **DUA (2)** jenis perkhidmatan yang mungkin sedang berfungsi dalam pelayan tersebut. **(2 markah)**
- v) Berdasarkan aktiviti *scanning* tersebut ada beberapa port yang terbuka, cadangkan **DUA (2)** langkah pengukuhan yang boleh dilakukan oleh pengurus keselamatan dalam memperkuuhkan keselamatan pelayan tersebut. **(2 markah)**
- (c) Dari maklumat yang dijumpai dalam soalan (b), cadangkan **TIGA (3)** jenis serangan yang mungkin dilakukan terhadap pelayan BCB. **(3 markah)**



**SOALAN 2 (20 MARKAH)****Kajian Kes 2:**

Mysoft Sdn. Bhd. ialah sebuah syarikat perisian yang terkenal dan berkepakaran dalam membangunkan aplikasi web. Antara tatacara piawai syarikat ini adalah menganalisis setiap kod yang dibangunkan oleh pengaturcara untuk memastikan ia ditulis dengan selamat dan melakukan penilaian tahap keselamatan pelayan wab yang menempatkan sistem. Sebagai pengaturcara kanan anda perlu menyediakan kriteria amalan pembangunan sistem dalam talian yang selamat berserta ciri-ciri konfigurasi pelayan web yang selamat kepada pengaturcara muda. Bincangkan dengan terperinci kriteria pembangunan perisian selamat dan konfigurasi pelayan web selamat dalam memastikan keselamatan sistem aplikasi atas talian.

Untuk membantu membincangkan keselamatan sistem aplikasi dalam talian, jawab soalan berikut berdasarkan amalan piawai syarikat tentang menganalisis pembangunan kod dan konfigurasi pelayan web yang selamat.



- (a) Cadangkan **EMPAT (4)** kesilapan konfigurasi yang mungkin berlaku kepada pelayan web yang boleh menyebabkan aplikasi web diserang oleh penggodam. **(4 markah)**
- (b) Kenalpasti **EMPAT (4)** impak apabila pelayan web mempunyai kelemahan. **(4 markah)**
- (c) Senaraikan **DUA (2)** kaedah serangan yang boleh dilakukan kepada pelayan web tersebut. **(2 markah)**
- (d) Tentukan nama bagi setiap serangan aplikasi web dibawah dan berikan **SATU (1)** kaedah untuk mencegah serangan untuk senario tersebut berdasarkan senarai kelemahan aplikasi web OWASP.
  - i) Pada tahun 2020, platform persidangan video popular Zoom mempunyai kelemahan pada keselamatan utama yang membenarkan penyerang mendapat akses tanpa kebenaran ke mesyuarat Zoom dengan menggunakan ID mesyuarat rawak dan meneka kata laluan mesyuarat. **(2 markah)**

- ii) Pada 2019, Capital One, salah satu bank terbesar di Amerika Syarikat, mengalami pelanggaran data yang mendedahkan maklumat peribadi lebih 100 juta pelanggan dan pemohon. Pelanggaran itu disebabkan oleh kelemahan dalam tembok api aplikasi web Capital One, yang membenarkan penyerang mendapat akses kepada data sensitif termasuk nama, alamat, skor kredit dan nombor Keselamatan Sosial. Kelemahan itu disebabkan oleh kesalahan di dalam konfigurasi tembok api aplikasi web yang membenarkan eksploitasi dihantar ke pelayan web.

**(2 markah)**

- iii) Pada 2018, British Airways, syarikat penerbangan terbesar di UK, mengalami kebocoran data yang mendedahkan maklumat peribadi dan kewangan kira-kira 380,000 pelanggan. Kebocoran itu disebabkan oleh kelemahan yang terdapat dalam kod skrip pihak ketiga yang digunakan di laman web British Airways dan diperkenalkan melalui serangan rantaian bekalan. Penyerang dapat menjejaskan skrip dan menyuntik kod hasad yang menangkap maklumat kad pembayaran pelanggan semasa mereka memasukkannya di laman web British Airways.

**(2 markah)**

- iv) Pada 2018, aplikasi kecergasan popular MyFitnessPal mengalami kebocoran data yang mendedahkan maklumat peribadi lebih 150 juta pengguna. Kebocoran data itu terdapat dalam halaman log masuk MyFitnessPal, yang tidak mengendalikan percubaan log masuk yang gagal dengan betul. Khususnya, apabila pengguna memasukkan nama pengguna atau kata laluan yang salah, mesej ralat yang dikembalikan oleh halaman log masuk mengandungi token sesi yang boleh digunakan untuk membuat capaian ke akaun pengguna tanpa kata laluan. Penyerang dapat menggunakan kelemahan ini untuk mendapatkan capaian kepada maklumat peribadi berjuta-juta pengguna MyFitnessPal, termasuk nama pengguna, alamat e-mel dan kata laluan.

**(2 markah)**

- (e) Semasa sesi demonstrasi serangan aplikasi web, log pelayan web telah menangkap beberapa aktiviti yang luar biasa yang dilakukan terhadap pelayan web. Rajah 1 menunjukkan log pelayan web tersebut.

```

192.168.254.172 - - [09/Apr/2022:00:18:50 -0400] "GET
/dvwa/vulnerabilities/fi/?page=include.php HTTP/1.1" 200 4083
"http://192.168.254.133/dvwa/vulnerabilities/sqli/?id=3&Submit
=Submit" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36"
192.168.254.172 - - [09/Apr/2022:00:18:50 -0400] "GET
/dvwa/vulnerabilities/fi/?page=include.php HTTP/1.1" 200 4083
"http://192.168.254.133/dvwa/vulnerabilities/sqli/?id=3&Submit
=Submit" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36"
192.168.254.172 - - [09/Apr/2022:00:18:58 -0400] "GET
/dvwa/vulnerabilities/fi/?page=../../../../etc/passwd
HTTP/1.1" 200 5717 "-" "Mozilla/5.0 (X11; Linux x86_64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74
Safari/537.36"
192.168.254.172 - - [09/Apr/2022:00:23:21 -0400] "GET
/dvwa/vulnerabilities/sqli/ HTTP/1.1" 200 4333
"http://192.168.254.133/dvwa/vulnerabilities/fi/?page=../../../../
../../../../etc/passwd" "Mozilla/5.0 (X11; Linux x86_64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74
Safari/537.36"

```

Rajah 1: Log Pelayan Web

Berdasarkan Rajah 1,

- Namakan jenis serangan aplikasi web yang telah dilaksanakan oleh penyerang.  
**(1 markah)**
- Cadangkan **SATU (1)** mekanisma pertahanan yang boleh digunakan untuk mencegah serangan begini.  
**(1 markah)**

**SOALAN 3 (20 MARKAH)****Kajian Kes 3:**

UP Defence Sdn. Bhd. (UDSB) telah diberikan tanggungjawab oleh Xhi Resources Sdn. Bhd. (XRSB) untuk melaksanakan ujian penembusan terhadap infrastruktur dan infostruktur ICT. Sebagai penguji penembusan kanan dalam UDSB, anda perlu mencadangkan skop ujian penembusan kepada Ketua Pegawai Maklumat XRSB, bincangkan secara terperinci ujian tersebut berdasarkan metodologi ujian penembusan.

Perbincangan anda perlu merangkumi perkara-perkara berikut:

- (a) **TIGA (3)** kategori penilaian keselamatan. **(3 markah)**
- (b) **TIGA (3)** sebab kenapa Pengujian Penembusan perlu dilakukan ke atas infrastrukutur ICT XRSB. **(3 markah)**
- (c) **EMPAT (4)** ruang lingkup ujian penembusan yang perlu dilakukan untuk menjamin keselamatan infrastruktur dan infostruktur ICT di syarikat XRSB. **(4 markah)**
- (d) **DUA (2)** teknik yang boleh digunakan dalam mengesan SSID tanpa wayar. **(2 markah)**
- (e) **EMPAT (4)** langkah yang mungkin dilakukan oleh pasukan UDSB dalam menembusi AP tanpa wayar yang dipercayai dikonfigurasikan dengan pengesahan WEP. **(4 markah)**
- (f) **EMPAT (4)** langkah yang boleh dicadangkan kepada XRSB dalam mencegah serangan terhadap rangkaian tanpa wayar pada masa akan datang. **(4 markah)**

**-SOALAN TAMAT-**

**PARTA: STRUCTURED QUESTIONS (40 MARKS)****INSTRUCTION:** Answer **ALL** questions.

- (a) A cyberattack carried out by a hacker may result in a breach on a server. Explain what is a hacker and what motivates them to hack?

(2 marks)

- (b) Give **TWO (2)** differences between hackers and ethical hackers?

(2 marks)

- (c) Hackers nowadays can be categorized into several types of hackers, list **FOUR (4)** different types of hackers.

(4 marks)

- (d) Define the following hacking terminology: -

i. Vulnerability

(1 mark)

ii. Zero-day attack

(1 mark)

iii. Foot Printing

(1 mark)

iv. Enumeration

(1 mark)



- (e) Ethics is defined as the standard of right and wrong, whereas Law is defined as a set of rules on conduct or action prescribed or formally recognized as binding or enforced by a controlling authority. State another **FOUR (4)** differences between ethics and law.

(4 marks)

- (f) State **FOUR (4)** Malaysian Cyberlaw that have been approved by Malaysia's parliament in protecting the citizen from cyber related crime.

(4 marks)

- (g) Agent Lisa has successfully intercepted a communication between US Army and Russia in the World War II and believed to be using Caesar cipher to encrypt their message. As a cryptanalyst for Agent Lisa, decrypt and find the key for the ciphertext below.

NVVKFVBNBLZAPA
----------------

**(5 marks)**

- (h) List any **FIVE (5)** steps involve in Cyber kill chain methodology that might be used in attacking a network infrastructure.

**(5 marks)**

- (i) List **THREE (3)** any network threat.

**(3 marks)**

- (j) Once foot printing and enumeration phase is complete, the next phase in a hacking process is system hacking and it consists of five stages. List any **THREE (3)** of the system hacking stages.

**(3 marks)**

- (k) Penetration Testing can be performed either from the internal site or external site. Describe each of the approaches and list their advantages and disadvantages.

**(4 marks)**

**PART B: STRUCTURED QUESTIONS (60 MARKS)**

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

**QUESTION 1 (20 MARKS)****Case Study 1:**

Esther is a **black hat hacker** who has successfully exploited and penetrated a server owned by Baithori Corporation Berhad (BCB). As the Computer Security Senior Manager of BCB you are asked to do an investigation on this security breach. Based on the investigation on the **network log** captured from the server as shown in **Appendix 1**, the security breach was done using standard hacking methodology. Discuss your investigation of the incident based on the hacking methodology to explain to the top management.

To guide your investigation, answer the following questions based on hacking methodology:

- (a) Explain each of the social engineering method based on an example of an action plan to trace the hacking activities.

i) Phishing

(2 marks)

ii) Quid Pro Quo

(2 marks)

iii) Baiting

(2 marks)



اونیورسیتی تکنیک ملیسیا ملاک

- (b) Find the suspected communication between Rogayah97's machine and ZCB's server from the network traffic log in **Appendix 1**.

i) The attacker's IP address.

(1 mark)

ii) Type of port scanning method used and state your reason.

(2 marks)

iii) **TWO (2)** open and **TWO (2)** close ports during this scanning activity.

(4 marks)

iv) **TWO (2)** types of services that might be running on the server.

(2 marks)

v) Propose **TWO (2)** actions the security administrator can take to harden the server security based on the open port found in the scanning activity.

(2 marks)

- (c) Suggest **THREE (3)** types of attack that might be launched to attack the BCB's server based the finding in (b).

**(3 marks)**



**QUESTION 2 (20 MARKS)****Case Study 2:**

Mysoft Sdn. Bhd. is a software development company which is expert in developing online applications. Among the standard practice by the company before deploying an online system are analysing each code developed by the programmers to make sure it is written securely and evaluating the security level of web server that hosting the system. As a senior programmer you need to provide **criteria of a secure online system development practice** to the junior programmer as well as the characteristic of good web server configuration. Discuss in detail the criteria of a secure software development and a secure web server configuration in ensuring the security of an online application system.

To guide your discussion in ensuring the security of an online application system, answer the following questions based on company standard practices on analysing code development and secure web server configuration.

- (a) Suggest **FOUR (4)** vulnerabilities on a web server that can lead to a web server breach. **(4 marks)**
- (b) Identify **FOUR (4)** impacts of a vulnerable webserver. **(4 marks)**
- (c) List any **TWO (2)** of the attack methods to attack webserver. **(2 marks)**
- (d) Determine the correct name of web application attack and give **ONE (1)** method to prevent the attack for the scenario based on OWASP top 10 web application vulnerabilities.
- i) In 2020, the popular video conferencing platform Zoom experienced a major security flaw that allowed attackers to gain unauthorized access to Zoom meetings by using random meeting IDs and guessing the meeting password. **(2 marks)**

- ii) In 2019, Capital One, one of the largest banks in the United States, experienced a data breach that exposed the personal information of over 100 million customers and applicants. The breach was caused by a vulnerability in Capital One's web application firewall, which allowed the attacker to gain access to sensitive data including names, addresses, credit scores, and Social Security numbers. The flaw is caused by a misconfigured web application firewall that allowed an exploit to be sent to the web server.

**(2 marks)**

- iii) In 2018, British Airways, the UK's largest airline, suffered a data breach that exposed the personal and financial information of approximately 380,000 customers. The breach was caused by a vulnerability present in the code of a third-party script used on the British Airways website and was introduced through a supply chain attack. The attackers were able to compromise the script and inject malicious code that captured customers' payment card information as they entered it on the British Airways website.

**(2 marks)**

- iv) In 2018, the popular fitness app MyFitnessPal suffered a data breach that exposed the personal information of over 150 million users. The vulnerability was present in MyFitnessPal's login page, which did not properly handle failed login attempts. Specifically, when a user entered an incorrect username or password, the error message returned by the login page contained a session token that could be used to access the user's account without a password. Attackers were able to use this vulnerability to gain access to the personal information of millions of MyFitnessPal users, including usernames, email addresses, and hashed passwords.

**(2 marks)**

- (e) During the demonstration session on web application attack, the webserver log had captured some unusual activity done towards the server. Figure 1 shows the webserver log.

```

192.168.254.172 - - [09/Apr/2022:00:18:50 -0400] "GET
/dvwa/vulnerabilities/fi/?page=include.php HTTP/1.1" 200 4083
"http://192.168.254.133/dvwa/vulnerabilities/sqli/?id=3&Submit=Sub
mit" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/99.0.4844.74 Safari/537.36"
192.168.254.172 - - [09/Apr/2022:00:18:50 -0400] "GET
/dvwa/vulnerabilities/fi/?page=include.php HTTP/1.1" 200 4083
"http://192.168.254.133/dvwa/vulnerabilities/sqli/?id=3&Submit=Sub
mit" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/99.0.4844.74 Safari/537.36"
192.168.254.172 - - [09/Apr/2022:00:18:58 -0400] "GET
/dvwa/vulnerabilities/fi/?page=../../../../etc/passwd HTTP/1.1"
200 5717 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36"
192.168.254.172 - - [09/Apr/2022:00:23:21 -0400] "GET
/dvwa/vulnerabilities/sqli/ HTTP/1.1" 200 4333
"http://192.168.254.133/dvwa/vulnerabilities/fi/?page=../../../../
../../../../etc/passwd" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36"

```

Figure 1: web server log

Based on Figure 1,

- i) Name the type of web application attack that has been executed by the attacker.  
**(1 mark)**
- ii) Suggest **ONE (1)** defense mechanism that can be used to prevent this attack.  
**(1 mark)**

**QUESTION 3 (20 MARKS)****Case Study 3:**

UP Defence Sdn. Bhd. (UDSB) is hired by Xhi Resources Sdn. Bhd. (XRSB) to perform penetration testing towards its ICT infrastructure and info structure. As a senior Pen Tester in UDSB you need to propose the scope of penetration testing to the Chief Information Officer of XRSB. Discuss the proposal in detail based on the penetration testing methodology.

Your discussion must include the following:

- (a) **THREE (3)** categories of Security Assessment.

**(3 marks)**

- (b) **THREE (3)** reasons why Penetration Testing needs to be performed on XRSB ICT infrastructure.

**(3 marks)**

- (c) **FOUR (4)** scopes of penetration testing needs to be done to secure the XRSB's ICT infrastructure and info structure.

**(4 marks)**

- (d) **TWO (2)** techniques that can detect the availability of wireless SSID in the organization to start a penetration testing on a wireless network infrastructure.

**UNIVERSITI TEKNIKAL MALAYSIA MELAKA**

**(2 marks)**

- (e) **FOUR (4)** steps the UDSB team might apply in penetrating the wireless Access Point (AP), which is believed to be configured with WEP authentication and has the potential to be exploited because of the wireless AP vulnerability in the configuration setting.

**(4 marks)**

- (f) **FOUR (4)** recommended countermeasures that XRSB can apply to the wireless network for future attack prevention.

**(4 marks)**

**-END OF QUESTION-**

## APPENDIX I

The network traffic captured during the hacking incidents in BCB

No.	Source	scport	Destination	Dt port	Prtcl	Info
1	192.168.254.172	36436	192.168.254.132	445	TCP	36436 > microsoft-ds [SYN]
2	192.168.254.132	445	192.168.254.172	36436	TCP	microsoft-ds > 36436 [SYN, ACK]
3	192.168.254.172	42420	192.168.254.132	80	TCP	42420 > http [SYN]
4	192.168.254.172	54766	192.168.254.132	135	TCP	54766 > epmap [SYN]
5	192.168.254.132	80	192.168.254.172	42420	TCP	http > 42420 [SYN, ACK]
6	192.168.254.132	135	192.168.254.172	54766	TCP	epmap > 54766 [SYN, ACK]
7	192.168.254.172	42230	192.168.254.132	139	TCP	42230 > netbios-ssn [SYN]
8	192.168.254.172	36436	192.168.254.132	445	TCP	36436 > microsoft-ds [ACK]
9	192.168.254.132	139	192.168.254.172	42230	TCP	netbios-ssn > 42230 [SYN, ACK]
10	192.168.254.172	42420	192.168.254.132	80	TCP	42420 > http [ACK]
11	192.168.254.172	54766	192.168.254.132	135	TCP	54766 > epmap [ACK]
12	192.168.254.172	53720	192.168.254.132	25	TCP	53720 > smtp [SYN]
13	192.168.254.172	42230	192.168.254.132	139	TCP	42230 > netbios-ssn [ACK]
14	192.168.254.132	25	192.168.254.172	53720	TCP	smtp > 53720 [RST, ACK]
15	192.168.254.172	38686	192.168.254.132	3306	TCP	38686 > mysql [SYN]
16	192.168.254.132	3306	192.168.254.172	38686	TCP	mysql > 38686 [SYN, ACK]
17	192.168.254.172	47218	192.168.254.132	21	TCP	47218 > ftp [SYN]
18	192.168.254.172	38686	192.168.254.132	3306	TCP	38686 > mysql [ACK]
19	192.168.254.132	21	192.168.254.172	47218	TCP	ftp > 47218 [SYN, ACK]
20	192.168.254.172	46770	192.168.254.132	110	TCP	46770 > pop3 [SYN]
21	192.168.254.172	47218	192.168.254.132	21	TCP	47218 > ftp [ACK]
22	192.168.254.132	110	192.168.254.172	46770	TCP	pop3 > 46770 [RST, ACK]
23	192.168.254.172	43844	192.168.254.132	443	TCP	43844 > https [SYN]
24	192.168.254.132	443	192.168.254.172	43844	TCP	https > 43844 [SYN, ACK]
25	192.168.254.172	48756	192.168.254.132	22	TCP	48756 > ssh [SYN]
26	192.168.254.132	22	192.168.254.172	48756	TCP	ssh > 48756 [RST, ACK]
27	192.168.254.172	36436	192.168.254.132	445	TCP	36436 > microsoft-ds [RST, ACK]
28	192.168.254.172	43844	192.168.254.132	443	TCP	43844 > https [ACK]
29	192.168.254.172	42420	192.168.254.132	80	TCP	42420 > http [RST, ACK]
30	192.168.254.172	54766	192.168.254.132	135	TCP	54766 > epmap [RST, ACK]
31	192.168.254.172	42230	192.168.254.132	139	TCP	42230 > netbios-ssn [RST, ACK]
32	192.168.254.172	38686	192.168.254.132	3306	TCP	38686 > mysql [RST, ACK]
33	192.168.254.172	47218	192.168.254.132	21	TCP	47218 > ftp [RST, ACK]

34	192.168.254.172	43844	192.168.254.132	443	TCP	43844 > https [RST, ACK]
35	192.168.254.172	42632	192.168.254.132	143	TCP	42632 > imap [SYN]
36	192.168.254.132	143	192.168.254.172	42632	TCP	imap > 42632 [RST, ACK]
37	192.168.254.172	39424	192.168.254.132	53	TCP	39424 > domain [SYN]
38	192.168.254.132	53	192.168.254.172	39424	TCP	domain > 39424 [RST, ACK]
39	192.168.254.172	33856	192.168.254.132	161	TCP	33856 > snmp [SYN]
40	192.168.254.132	161	192.168.254.172	33856	TCP	snmp > 33856 [RST, ACK]
41	192.168.254.172	42936	192.168.254.132	123	TCP	42936 > ntp [SYN]
42	192.168.254.132	123	192.168.254.172	42936	TCP	ntp > 42936 [RST, ACK]
43	192.168.254.172	50564	192.168.254.132	20	TCP	50564 > ftp-data [SYN]
44	192.168.254.132	20	192.168.254.172	50564	TCP	ftp-data > 50564 [RST, ACK]

