UNIVERSITI TEKNIKAL MALAYSIA MELAKA

UNIVERSITI TEKNIKAL MALAYSIA MELAKA
PEPERIKSAAN AKHIR SEMESTER I
FINAL EXAMINATION SEMESTER I
SESI 2019/2020
SESSION 2019/2020

FAKULTI TEKNOLOGI MAKLUMAT DAN KOMUNIKASI

KOD KURSUS ***COURSE CODE***	**: BITS 3613** ***BITS 3613***
KURSUS ***COURSE***	**: TEKNIK PENGGODAMAN DAN PENCEGAHAN** ***HACKING TECHNIQUES AND PREVENTION***
PENYELARAS ***COORDINATOR***	**: MOHD ZAKI MAS'UD**
PROGRAM ***PROGRAMME***	**: 3 BITZ**
MASA ***TIME***	**: 2.15 PTG** ***2.15 PM***
TEMPOH ***DURATION***	**: 2 JAM 30 MINIT** ***2 HOURS 30 MINUTES***
TARIKH ***DATE***	**: 6 JANUARI 2020** ***6 JANUARY 2020***
TEMPAT ***VENUE***	**: DEWAN SEMINAR FTMK** ***FTMK SEMINAR HALL***

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. **Sila jawab di dalam buku jawapan yang disediakan.**
   Please answer in the answer booklet provided.
3. **Kertas soalan ini mempunyai versi dwi-bahasa.**
   The exam paper consists of dual-language version.

KERTAS SOALAN INI TERDIRI DARIPADA (19) MUKA SURAT SAHAJA (TERMASUK MUKA SURAT HADAPAN)
THIS QUESTION PAPER CONTAINS (19) PAGES INCLUSIVE OF FRONT PAGE

PERINGATAN
REMINDER:

PELAJAR TIDAK DIBENARKAN SAMA SEKALI MEMBAWA APA-APA BUKU, KERTAS, SURATAN, GAMBAR, NOTA, SEBARANG ALAT YANG DI DALAM ATAU DI ATASNYA TERDAPAT CATATAN BERTULIS, 'PROGRAMMABLE CALCULATOR', TELEFON MUDAH ALIH ATAU SEBARANG ALAT KECUALI YANG DIBENARKAN OLEH PENGAWAS KE DALAM ATAU KELUAR DARI SESUATU DEWAN PEPERIKSAAN ATAU MENERIMA APA-APA BUKU, KERTAS, SURATAN, GAMBAR, NOTA, SEBARANG ALAT YANG DI DALAM ATAU DI ATASNYA TERDAPAT CATATAN BERTULIS, 'PROGRAMMABLE CALCULATOR', TELEFON MUDAH ALIH ATAU SEBARANG ALAT DARI MANA-MANA ORANG LAIN SEMASA DI DALAM DEWAN PEPERIKSAAN KECUALI SESEORANG PELAJAR SEMASA IA BERADA DI DALAM DEWAN PEPERIKSAAN ITU MENERIMA DARIPADA PENGAWAS APA-APA BUKU, KERTAS, DOKUMEN/GAMBAR ATAU LAIN-LAIN ALAT YANG DIBENARKAN OLEH NAIB CANSELOR ATAS SYOR PEMERIKSA ATAU FAKULTI.

STUDENTS ARE NOT ALLOWED TO BRING IN ANY BOOKS, PAPERS, DOCUMENTS, PHOTOGRAPHS, NOTES, ANY TOOLS WHICH THERE ARE WRITTEN RECORDS, MOBILE PHONES, OR ANY OTHER DEVICES WITHOUT THE PRIOR PERMISSION OF THE INVIGILATORS INTO OR OUT OF THE EXAMINATION HALL, OR RECEIVE ANY PAPERS, BOOKS, DOCUMENTS, PHOTOGRAPHS, NOTES, ANY DEVICES IN OR ON WHICH THERE ARE WRITTEN RECORDS, 'PROGRAMMABLE CALCULATORS', OR TOOLS FROM OTHER PERSON(S) PRESENT IN THE EXAMINATION HALL; EXCEPT MATERIALS OR DEVICES PROVIDED BY THE INVIGILATORS AND PERMITTED BY THE VICE CHANCELLOR ON THE RECOMMENDATIONS OF THE EXAMINERS OR FACULTIES.

PART A: STRUCTURED QUESTIONS (25 MARKS)

INSTRUCTION: *Answer ALL questions.*

(a) Define what is Hacking?

(2 marks)

(b) Hackers can be categorized as White Hat, Black Hat, Script kiddies and State sponsored. Describe each of the hacker category.

(4 marks)

(c) Law is defined as a rule of conduct or action prescribed or formally recognized as binding or enforced by a controlling authority which implies imposition by a sovereign authority and the obligation of obedience on the part of all subjects to that authority. List **FIVE (5)** of Malaysia's Cyberlaw acts.

(5 marks)

(d) Intellectual property (IP) rights is a right for a person or company to have an exclusive rights to use its own plans, idea or other intangible assets without any worries for competition. These rights include Copyright, Patent, Trademark and Trade Secrets. Briefly explains these **FOUR (4)** IP rights.

(4 marks)

(e) There are four methods to break an encrypted message. List and briefly describes any **TWO (2)** methods to break an encrypted message.

(4 marks)

(f) Agent Smith successfully intercept a communication between the Soviet army in the World War II and believe they are using Caesar cipher to encrypt their message. As the cryptanalyst to Agent Smith. Decrypt and find the key for the ciphertext below.

SIOH UCFC NWIH ALUN OFUN CIHM

(6 marks)

PART B: STRUCTURED QUESTIONS (75 MARKS)

INSTRUCTION: *Answer ALL questions.*

QUESTION 1 (25 MARKS)

Case Study 1:

MarkOV is a black hat hacker that has successfully exploited and penetrated a server owned by Adzmir Technology Resources Bhd (ATRB). As the Computer Security Senior Manager of ATRB you are asked to do an investigation on this security breach. Your first task is to explain to the top management of the general scenario of how a hacking is done.

Based on the Case Study 1, answer the following questions.

(a) List all the phases involved in a hacking process.

(9 marks)

(b) Social Engineering is one of the clever manipulation of the natural human tendency to trust and it is one of the approaches to gather information from a target. Briefly describe the following social engineering methods and give an example of an action plan that can be done using each of the method.

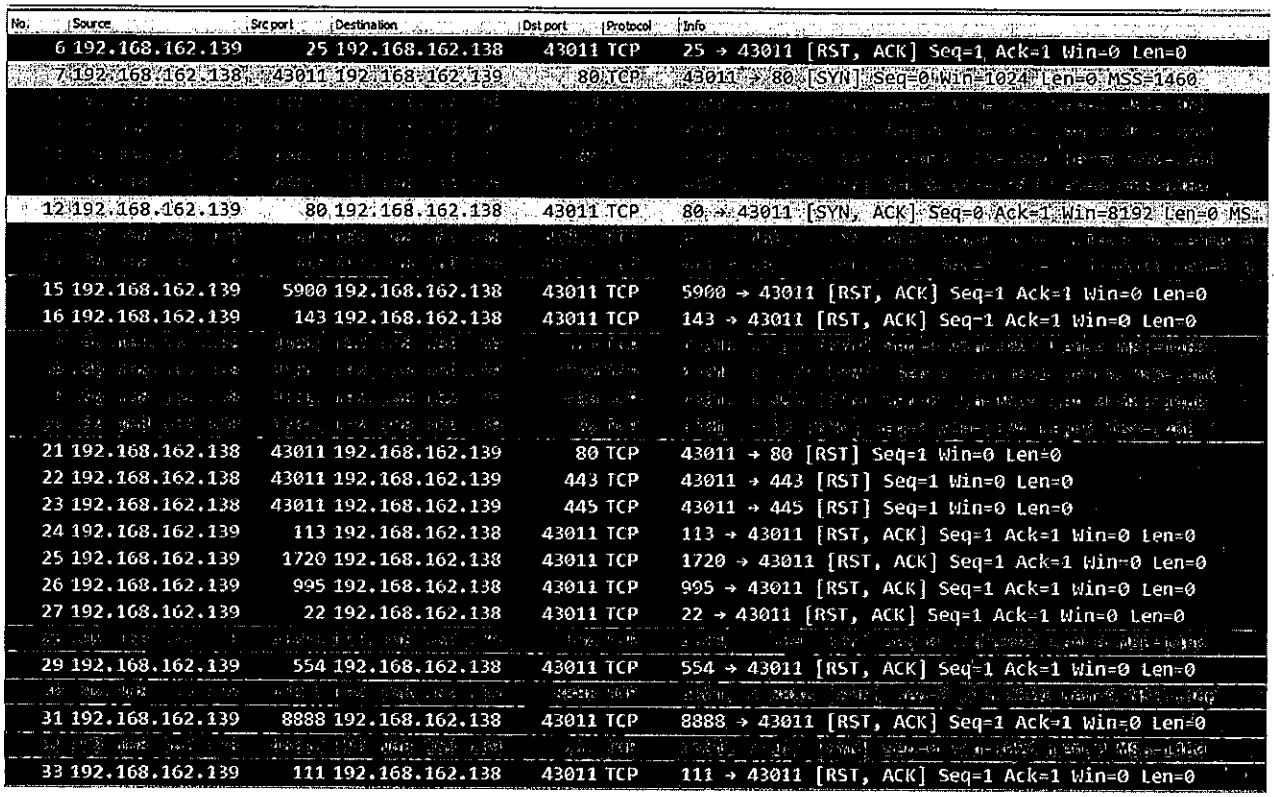
i. Quid Pro Quo

ii. Diversion theft

iii. Pretexting

(6 marks)

(c) During the incident, one of the network monitoring tool in ATRB's network infrastructure has successfully captured a series of network traffic, suspected to be a communication between MarkOv's machine and one of ATRB's server. The network traffic captured is shown in Figure 1.



No.	Source	Src port	Destination	Dst port	Protocol	Info
6	192.168.162.139	25	192.168.162.138	43011	TCP	25 → 43011 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7	192.168.162.138	43011	192.168.162.139	80	TCP	43011 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
12	192.168.162.139	80	192.168.162.138	43011	TCP	80 → 43011 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MS…
15	192.168.162.139	5900	192.168.162.138	43011	TCP	5900 → 43011 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
16	192.168.162.139	143	192.168.162.138	43011	TCP	143 → 43011 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
21	192.168.162.138	43011	192.168.162.139	80	TCP	43011 → 80 [RST] Seq=1 Win=0 Len=0
22	192.168.162.138	43011	192.168.162.139	443	TCP	43011 → 443 [RST] Seq=1 Win=0 Len=0
23	192.168.162.138	43011	192.168.162.139	445	TCP	43011 → 445 [RST] Seq=1 Win=0 Len=0
24	192.168.162.139	113	192.168.162.138	43011	TCP	113 → 43011 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
25	192.168.162.139	1720	192.168.162.138	43011	TCP	1720 → 43011 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
26	192.168.162.139	995	192.168.162.138	43011	TCP	995 → 43011 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	192.168.162.139	22	192.168.162.138	43011	TCP	22 → 43011 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
29	192.168.162.139	554	192.168.162.138	43011	TCP	554 → 43011 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
31	192.168.162.139	8888	192.168.162.138	43011	TCP	8888 → 43011 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33	192.168.162.139	111	192.168.162.138	43011	TCP	111 → 43011 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Figure 1: The network traffic captured during the hacking incidents in ATRB

Based on the network traffic captured

i. Suggest a tool that might be used by the hackers.

(1 mark)

ii. Identify the server's IP address

(1 mark)

iii. What type of scanning method the hackers use?

(1 mark)

iv. What are the **TWO (2)** open port on ATRB's server?

(2 marks)

(d) In an attempt to cover the attack track, `MarkOv` is believed to have used some types of covering track tools to delete several logs in the server. List **FIVE (5)** possible tools that `MarkOv` might have used to cover his/her tracks.

(5 marks)

QUESTION 2 (25 MARKS)

Case Study 2:

PENTABYTES Sdn. Bhd. is a renounce software house company that is expert in developing web applications. Among the standard procedures this company practise is analysing each code developed by the programmer to make sure it is written securely. As a senior programmer you need to brief the junior programmer on the task and responsibilities to write a secure code for any web application project the company is developing.

Base on the Case Study 2, answer the following questions.

(a) In a web application infrastructure, several components exist and each of them serve a specific function. Each has its own vulnerabilities as well. Explain **FOUR (4)** components that can possibly expose a web application and web server to a possible exploitation.

(8 marks)

(b) There are several methods to attack a web application. Give any **FOUR (4)** of the attack methods.

(4 marks)

(c) In order to show an example of a vulnerable coding in a web application, you have chosen a coding snippet as shown in Figure 2 to your junior programmer.

```
Line 1. # Define POST variables
Line 2. uname = request.POST('username')
Line 3. passwd = request.POST('password')
Line 4. sql = "SELECT id FROM users WHERE username='" + uname + "' AND password='" + passwd
+ "'"
Line 5. # Execute the SQL statement
Line 6. database.execute(sql)
```

Figure 2: Example of web application source code with flaws

i. Based on the Figure 2, identify line of the code that can be exploited.

(1 mark)

ii. Suggest the type of web application attack that can be used to attack the line of code in c(i).

(1 mark)

iii. Suggest **TWO (2)** attack payloads that you can use as an input to the application.

(2 marks)

iv. Describe **TWO (2)** malicious impact from the attack in c(iii) towards the application and the server holding the web application?

(2 marks)

v. Suggest **ONE (1)** solution to improve this code.

(1 mark)

(d) During the demonstration session on web application attack, you showed a sample of a web application that can be exploited through its GET request in the command URL as shown in Figure 3.

```
http://Grandbazzar.com/payment.php?noitem=5&amount=6000
```

Figure 3: GET request in URL

i. How does an attacker can exploit this flaw?

(1 mark)

ii. Suggest one tool that you can use to exploit this flaws.

(1 mark)

(e) A web application needs a web server platform to run and the security of the web server is equally important as developing a secure web application. Give any **FOUR (4)** methods that can be applied to the web servers in order to defend against Web Server Attacks.

(4 marks)

QUESTION 3 (25 MARKS)

Case Study 3:

ZAMSS Sdn. Bhd. is hired by Nazri Tech and Resources Sdn. Bhd. (NTRSB) to perform a penetration testing to its ICT infrastructure and info structure. Among the scope that needs to be covered by the pen tester is social engineering, wireless network, wired network infrastructure, Web server and its application. As a senior Pen Tester in ZAMSS you need to explain to the Chief Information Officer of NTRSB the issues and scope related to the penetration testing.

Based on the Case Study 3, answer the following questions.

(a) List and Explain **THREE (3)** categories of Security Assessment .

(6 marks)

(b) List **FOUR (4)** Penetration Testing scopes ZAMSS can suggest to NTRSB.

(4 marks)

(c) To start the pentest on the wireless network infrastructure your team need to first identify all the open wireless access point in the campus. State **FOUR (4)** techniques to detect wireless networks.

(4 marks)

(d) From the open wireless acces point (AP) survey done on (c), your team found two wireless AP that have a potential to be exploited due to the wireless AP vulnerability in the configuration setting. Suggest **FOUR (4)** countermeasure NTRSB can apply to the wireless network for preventing future attack.

(4 marks)

(e) List **THREE (3)** vulnerability scanner that ZAMSS can use in the penetration testing on a web application server.

(3 marks)

(f) Penetration Testing can be done either by Blackbox or Whitebox approach. Describe each of the approach and list the advantage and disadvantage of each of the approach.

(4 marks)

-END OF QUESTIONS-

BAHAGIAN A: SOALAN BERSTRUKTUR (25 MARKAH)

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

(a) Takrifkan Pengodaman?

(2 markah)

(b) Penggodam boleh dikategorikan sebagai *White Hat*, *Black Hat*, *Script Kiddies* dan *State sponsored*. Terangkan setiap kategori penggodam tersebut.

(4 Markah)

(c) Undang-undang ditakrifkan sebagai peraturan kepada kelakuan atau tindakan yang dilakukan oleh seorang individu. Ia ditetapkan atau diiktiraf secara rasmi oleh pihak berkuasa yang mempunyai bidang kuasa terhadap mereka yang dikawalselia dibawah kuasa mereka. Senaraikan **LIMA (5)** akta undang-undang siber di Malaysia.

(5 markah)

(d) Hak Harta Intelek (IP) adalah hak ekslusif yag diberikan kepada individual atau syarikat untuk menggunakan pelan, idea atau reka cipta tanpa perlu bimbang kepada persaingan. Hak yang dimaksudkan dalam IP adalah Hak Cipta, Paten, Cap Dagangan dan Rahsia Perdangan. Terangkan secara ringkas **EMPAT (4)** Hak IP tersebut.

(4 markah)

(e) Ada empat metadologi untuk memecah sesuatu mesej nyahsulit. Senarai dan terangkan secara ringkas **DUA (2)** metadologi yang boleh diambil oleh seorang penyerang untuk memecahkan mesej yang dinyahsulit.

(4 markah)

(f) Agen Smith telah berjaya memintas komunikasi antara tentera Soviet dalam perang dunia ke II dan beliau percaya, mereka ada menggunakan sifer *Caesar* untuk menyulitkan mesej mereka. Sebagai *cryptanalyst* kepada Agent smith dekripsi dan cari kunci untuk kod sifer di bawah.

SIOH UCFC NWIH ALUN OFUN CIHM

(6 markah)

BAHAGIAN B: SOALAN BERSTRUKTUR (75 MARKAH)

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

SOALAN 1 (25 MARKAH)

Kajian Kes 1:

MärkOv adalah seorang penggodam *blackhat* yang telah berjaya mengeksploitasi dan menembusi komputer pelayan milik syarikat Sumber Teknologi Adzmir Bhd (ATRB). Sebagai Pengurus Kanan Keselamatan Komputer ATRB anda telah diminta untuk melakukan siasatan ke atas kejadian tersebut. Tugas pertama anda adalah untuk menjelaskan kepada pihak pengurusan tertinggi senario umum tentang bagaimana penggodaman itu berlaku.

Berdasarkan kajian kes 1, jawab semua soalan berikut.

(a) Senaraikan semua fasa godam yang telibat dalam kejadian penggodaman tersebut.

(9 markah)

(b) Kejuruteraan Sosial adalah salah satu kaedah yang licik untuk memanipulasi kecenderungan semulajadi manusia untuk mempercayai seorang dan merupakan salah satu pendekatan untuk mengumpulkan maklumat dari sasaran. Terangkan secara ringkas kaedah kejuruteraan sosial berikut dan berikan contoh tindakan yang boleh dilakukan menggunakan setiap kaedah tersebut.

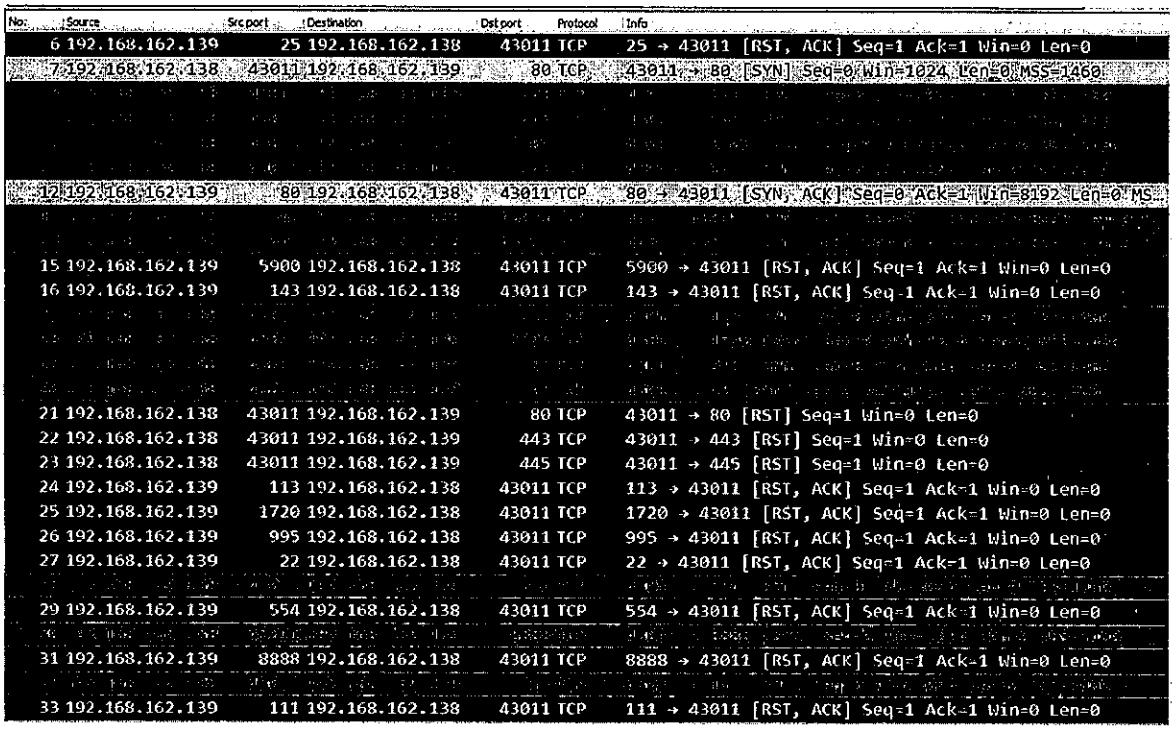
i. Quid Pro Quo

ii. Diversion Theft

iii. Pretexting

(6 markah)

(c) Semasa kejadian, salah satu alat pemantauan rangkaian dalam infrastruktur rangkaian ATRB berjaya menangkap satu siri trafik rangkaian yang disyaki menjadi komunikasi antara mesin `MarkOv` dengan salah satu pelayan ATRB. Trafik rangkaian ditangkap ditunjukkan pada Rajah 1?



No.	Source	Src port	Destination	Dst port	Protocol	Info
6	192.168.162.139	25	192.168.162.138	43011	TCP	25 → 43011 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7	192.168.162.138	43011	192.168.162.139	80	TCP	43011 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
12	192.168.162.139	80	192.168.162.138	43011	TCP	80 → 43011 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MS
15	192.168.162.139	5900	192.168.162.138	43011	TCP	5900 → 43011 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
16	192.168.162.139	143	192.168.162.138	43011	TCP	143 → 43011 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
21	192.168.162.138	43011	192.168.162.139	80	TCP	43011 → 80 [RST] Seq=1 Win=0 Len=0
22	192.168.162.138	43011	192.168.162.139	443	TCP	43011 → 443 [RST] Seq=1 Win=0 Len=0
23	192.168.162.138	43011	192.168.162.139	445	TCP	43011 → 445 [RST] Seq=1 Win=0 Len=0
24	192.168.162.139	113	192.168.162.138	43011	TCP	113 → 43011 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
25	192.168.162.139	1720	192.168.162.138	43011	TCP	1720 → 43011 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
26	192.168.162.139	995	192.168.162.138	43011	TCP	995 → 43011 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	192.168.162.139	22	192.168.162.138	43011	TCP	22 → 43011 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
29	192.168.162.139	554	192.168.162.138	43011	TCP	554 → 43011 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
31	192.168.162.139	8888	192.168.162.138	43011	TCP	8888 → 43011 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33	192.168.162.139	111	192.168.162.138	43011	TCP	111 → 43011 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Rajah 1: Trafik rangkaian yang ditangkap semasa kejadian penggodaman di ATRB

Berdasarkan trafik rangkaian di Rajah 1:

i. Cadangkan perisian yang mungkin digunakan oleh penggodam.

(1 markah)

ii. Kenal pasti alamat IP penggodam

(1 markah)

iii. Apakah jenis kaedah pengimbasan yang digunakan penggodam?

(1 markah)

iv. Apakah **DUA (2)** port terbuka pada pelayan ATRB??

(2 markah)

(d) Dalam usaha untuk menutupi jejak aktiviti penggodaman, `MarkOv` dipercayai telah menggunakan beberapa jenis perisian yang boleh memadam beberapa log di dalam komputer pelayan tersebut. Senaraikan **LIMA (5)** perisian yang `MarkOv` mungkin gunakan untuk menutupi kesan-kesan penggodaman tersebut.

(5 markah)

SOALAN 2 (25 MARKAH)

Kajian Kes 2:

PENTABYTES 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. Sebagai pengaturcara kanan anda telah ditugaskan untuk memberi taklimat kepada pengaturcara junior mengenai tugas dan tanggungjawab untuk menulis kod selamat untuk mana-mana projek aplikasi web yang sedang dibangunkan.

Bedasarkan Kajian Kes 2, jawab soalan-soalan berikut.

(a) Beberapa komponen penting wujud dalam infrastruktur aplikasi web, setiap komponen mempunyai fungsi yang tertentu. Setiap komponen juga mempunyai beberapa kelemahan, Jelaskan **EMPAT (4)** komponen yang boleh mendedahkan aplikasi web dan pelayan web kepada eksploitasi.

(8 markah)

(b) Terdapat beberapa kaedah untuk menyerang aplikasi web. Berikan mana-mana **EMPAT (4)** kaedah serangan.

(4 markah)

(c) Untuk menunjukkan contoh kelemahan dalam pengekodan aplikasi web, anda menunjukkan keratan aturcara seperti di Rajah 2 kepada pengaturcara junior anda.

```
Line 1. # Define POST variables
Line 2. uname = request.POST('username')
Line 3. passwd = request.POST('password')
Line 4. sql = "SELECT id FROM users WHERE username='" + uname + "' AND password='" +
passwd + "'"
Line 5. # Execute the SQL statement
Line 6. database.execute(sql)
```

Rajah 2: Contoh kod aplikasi web yang lemah.

i. Berdasarkan Rajah 2, kenalpasti baris kod yang boleh dieksploitasi.

(1 markah)

ii. Cadangkan jenis serangan aplikasi web yang boleh digunakan untuk menyerang kod di c(i).

(1 markah)

iii. Cadangkan **DUA (2)** muatan serangan yang anda boleh masukkan ke dalam aplikasi ini.

(2 markah)

iv. Apakah **DUA (2)** kesan buruk yang boleh berlaku kepada aplikasi web dan pelayan web akibat daripada serangan dalam c (iii)?

(2 markah)

v. Cadangkan **SATU (1)** penyelesaian untuk meningkatkan keselamatan kod ini.

(1 markah)

(d) Semasa sesi demonstrasi serangan aplikasi web, anda telah menunjukkan contoh aplikasi web yang boleh dieksploitasi melalui permintaan *GET* dalam URL arahan, seperti ditujukkan dalam Rajah 3.

```
http://Granbazzar.com/payment.php?noitem=5&amount=6000
```

Rajah 3: GET dalam URL

i. Nyatakan **SATU (1)** Jenis serangan yang boleh mengeksploitasi kelemahan ini ?

(1 markah)

ii. Cadangkan satu perisian yang boleh digunakan untuk mengeksploitasi kelemahan ini.

(1 markah)

(e) Aplikasi web memerlukan platform pelayan web untuk menjalankan perkhidmatannya dan platform pelayan web juga memerlukan tahap keselamatan yang sama seperti pembangunan aplikasi web. Berikan **EMPAT (4)** kaedah yang boleh diaplikasikan kepada platform pelayan web bagi mempertahankan aplikasi web dari serangan.

(4 markah)

SOALAN 3 (25 MARKAH)

Kajian Kes 3:

ZAMSS Secure Sdn. Bhd. telah diberikan tanggungjawab oleh Nazri Tech and Resources Sdn. Bhd. (NTRSB) untuk melaksanakan ujian penerobosan terhadap infrastruktur dan info struktur ICT. Antara skop yang perlu diuji adalah kejuruteraan sosial, infrastruktur rangkaian tanpa wayar dan berwayar serta keselamatan pelayan Web dan aplikasi web. Sebagai penguji penerobosan kanan dalam ZAMSS, anda perlu menjelaskan kepada Ketua Pegawai Maklumat JTRSB menegenai isu dan skop yang berkaitan dengan ujian tersebut.

Berdasarkan Kajian Kes 3, jawab soalan-soalan berikut.

(a) Jelaskan **TIGA (3)** kategori penilaian keselamatan.

(6 markah)

(b) Senaraikan **EMPAT (4)** Skop Pengujian Penembusan yang ZAMSS boleh dicadangkan kepada NTRSB.

(4 markah)

(c) Untuk memulakan pengujian penerobosan pada infrastruktur rangkaian tanpa wayar, pasukan anda perlu mengenal pasti terlebih dahulu semua pusat akses tanpa wayar di dalam kampus. Nyatakan **EMPAT (4)** teknik untuk mengesan rangkaian tanpa wayar yang terbuka.

(4 markah)

(d) Dari pemerhatian yang dijalankan di (c), pasukan anda mendapati dua pusat akses tanpa wayar masih mempunyai ruang untuk dieksploitasi disebabkan oleh konfugirasi keselamatan yang lemah. Cadangkan **EMPAT (4)** langkah untuk keselamatan yang NTRSB boleh laksanakan terhadap rangkaian tanpa wayar untuk mengelakkan dari serangan pada masa akan datang.

(6 markah)

(e) Senaraikan **TIGA (3)** perisian pengimbasan kelemahan yang boleh digunakan oleh ZAMSS dalam ujian penembusan pada pelayan aplikasi web.

(3 markah)

(f) Ujian Penerobosan boleh dilakukan secara Kotak Hitam dan Kotak Putih. Bincangkan kedua-dua pendekatan tersebut serta nyatakan kelebihan dan kekurangan setiap pendekatan.

(4 markah)

-SOALAN TAMAT-