UNIVERSITI TEKNIKAL MALAYSIA MELAKA

UNIVERSITI TEKNIKAL MALAYSIA MELAKA
PEPERIKSAAN AKHIR SEMESTER II
FINAL EXAMINATION SEMESTER II
SESI 2020/2021
SESSION 2020/2021

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***	**: 14:15 Hingga 16:15**
TEMPOH ***DURATION***	**: 2 JAM** ***2 HOURS***
TARIKH ***DATE***	**: 6 JULAI 2021**
TEMPAT ***VENUE***	**:HALL 5**

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 SOALAN INI TERDIRI DARIPADA (17) MUKA SURAT SAHAJA
(TERMASUK MUKA SURAT HADAPAN)
THIS QUESTION PAPER CONTAINS (17) PAGES INCLUSIVE OF FRONT PAGE

BAHAGIAN A: SOALAN BERSTRUKTUR (25 MARKAH)

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

(a) Teknologi Internet telah berkembang secara drastik dalam beberapa tahun kebelakangan ini dan sekarang ini lebih banyak peranti telah disambungkan ke internetmenyebabkan lebih banyak peranti terdedah kepada ancaman siber. Huraikan peranan seorang Penggodam Beretika dalam mengurangkan ancaman siber?

(4 markah)

(b) Penggodam boleh dikategorikan kepada beberapa jenis penggodam, bincangkan **TIGA (3)** jenis penggodam berdasarkan tahap pengetahuan penggodaman mereka, tahap kesan penggodaman yang dilakukan terhadap sesebuah organisasi dan sejauh mana aktiviti mereka disahkan oleh undang-undang.

(12 Markah)

(c) Etika bermaksud piawai 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. Senaraikan **EMPAT (4)** perbezaan antara Etika dan Undang-undang.

(4 markah)

(d) Agen Smith telah berjaya memintas komunikasi di antara tentera Soviet dalam Perang Dunia ke I dan beliau percaya, mereka menggunakan kaedah *Caesar Cipher* untuk menyulitkan mesej mereka. Sebagai *cryptanalyst* kepada Agen Smith, cari kunci dan nyahsulit teks sifer berikut.

YMJK PJQU WNHJ BNQQ NSHW JFXJ YTWH KTZW GDSJ CYBJ JP

(5 markah)

BAHAGIAN B: SOALAN BERSTRUKTUR (75 MARKAH)

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

SOALAN 1 (25 MARKAH)

Kajian Kes 1:

Fariq78 adalah seorang penggodam *blackhat* yang telah berjaya mengeksploitasi dan menembusi komputer pelayan milik syarikat Malik Technology Resources Bhd (MTRB). Sebagai Pengurus Kanan Keselamatan Komputer MTRB anda telah diminta untuk melakukan siasatan ke atas kejadian tersebut. Tugas pertama anda adalah untuk menjelaskan kepada pihak pengurusan tertinggi senario umum tentang bagaimana sesuatu penggodaman itu berlaku.

Berdasarkan kajian kes 1, jawab semua soalan berikut.

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

(9 markah)

(b) 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.

i. *Phishing*

ii. *Piggybacking*

iii. *Vishing*

(6 markah)

(c) Semasa kejadian, salah satu alat pemantauan rangkaian dalam infrastruktur rangkaian MTRB berjaya menangkap satu siri trafik rangkaian yang disyaki menjadi komunikasi antara mesin Fariq78 dengan salah satu pelayan MTRB. Trafik rangkaian yang ditangkap ditunjukkan pada Rajah 1.

Source	source port	Destination	Dest port	Protocol	Info
192.168.254.131	48614	192.168.254.130	25	TCP	48614 > smtp [SYN] Seq=0
192.168.254.131	48614	192.168.254.130	80	TCP	48614 > http [SYN] Seq=0
192.168.254.131	48614	192.168.254.130	53	TCP	48614 > domain [SYN] Seq=
192.168.254.131	48614	192.168.254.130	123	TCP	48614 > ntp [SYN] Seq=0 W
192.168.254.131	48614	192.168.254.130	67	TCP	48614 > bootps [SYN] Seq=
Vmware_7f:08:97		Broadcast		ARP	Who has 192.168.254.131?
Vmware_e8:52:0a		Vmware_7f:08:97		ARP	192.168.254.131 is at 00:
192.168.254.130	67	192.168.254.131	48614	TCP	bootps > 48614 [RST, ACK]
192.168.254.130	54915	192.168.254.255	54915	UDP	Source port: 54915 Desti
192.168.254.131	48615	192.168.254.130	123	TCP	48615 > ntp [SYN] Seq=0 W
192.168.254.131	48615	192.168.254.130	53	TCP	48615 > domain [SYN] Seq=
192.168.254.130	123	192.168.254.131	48615	TCP	ntp > 48615 [RST, ACK] Se
192.168.254.130	53	192.168.254.131	48615	TCP	domain > 48615 [RST, ACK]
192.168.254.131	48615	192.168.254.130	80	TCP	48615 > http [SYN] Seq=0
192.168.254.131	48615	192.168.254.130	25	TCP	48615 > smtp [SYN] Seq=0
192.168.254.130	80	192.168.254.131	48615	TCP	http > 48615 [SYN, ACK] S
192.168.254.130	25	192.168.254.131	48615	TCP	smtp > 48615 [SYN, ACK] S
192.168.254.131	48615	192.168.254.130	80	TCP	48615 > http [RST] Seq=1
192.168.254.131	48615	192.168.254.130	25	TCP	48615 > smtp [RST] Seq=1
192.168.254.130	54915	192.168.254.255	54915	UDP	Source port: 54915 Desti
192.168.254.130	54915	192.168.254.255	54915	UDP	Source port: 54915 Desti
192.168.254.130	25	192.168.254.131	48614	TCP	smtp > 48614 [SYN, ACK] S
192.168.254.130	80	192.168.254.131	48614	TCP	http > 48614 [SYN, ACK] S
192.168.254.131	48614	192.168.254.130	25	TCP	48614 > smtp [RST] Seq=1

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

Berdasarkan trafik rangkaian di Rajah 1:

i. Kenalpasti alamat IP penggodam.

(1 markah)

ii. Apakah kaedah *Port scanning* yang digunakan? Nyatakan alasan anda.

(2 markah)

iii. Kenalpasti satu port yang terbuka dan satu port yg tertutup semasa aktiviti *scanning* ini?

(2 markah)

iv. Berikan **DUA (2)** kaedah port scanning lain yang boleh digunakan dalam serangan ini?

(2 markah)

(d) Dalam cubaan untuk menutupi jejak aktiviti penggodaman, Fariq78 dipercayai telah menggunakan beberapa jenis perisian yang boleh memadam beberapa log di dalam komputer pelayan tersebut. Senaraikan **TIGA(3)** perisian yang boleh digunakan oleh Fariq78 untuk menutupi kesan-kesan penggodaman tersebut.

(3 markah)

SOALAN 2 (25 MARKAH)

Kajian Kes 2:

SoftHouse 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 muda mengenai tugas dan tanggungjawab untuk menulis kod selamat untuk mana-mana projek aplikasi web syarikat yang sedang dibangunkan.

Bedasarkan Kajian Kes 2, jawab soalan-soalan berikut.

(a) Nyatakan **EMPAT (4)** kesilapan konfigurasi yang mungkin berlaku kepada pelayan web yang boleh menyebabkan aplikasi web diserang oleh penggodam .

(4 markah)

(b) Bincangkan secara ringkas **DUA (2)** kesan apabila pelayan web mempunyai kelemahan.

(4 markah)

(c) Terdapat beberapa kaedah boleh digunakan untuk menyerang pelayan web. Berikan mana-mana **EMPAT (4)** kaedah tersebut.

(4 markah)

(d) Penyataan dibawah merujuk kepada definasi serangan yang boleh dilakukan kepada aplikasi web atas talian, namakan serangan aplikasi web yang tepat untuk setiap definasi serangan berikut dan berikan **SATU (1)** kaedah yang boleh dilakukan untuk menghalang serangan tersebut.

i. Serangan yang mengeksploitasi pengesahan dan pengurusan sesi yang sering dilaksanakan dengan cara yang salah, ini membolehkan penyerang menyalahgunakan kata laluan, token sesi, atau mengeksploitasi kelemahan pelaksanaan lain untuk mengambil alih identiti pengguna lain secara sementara atau kekal.

(2 markah)

ii. Serangan yang mana penyerang menghantar data palsu kepada pentafsir sebagai sebahagian daripada arahan atau pertanyaan. Penyerang boleh menipu pentafsir supaya melaksanakan arahan yang tidak sepatutnya atau membuat capaian data tanpa kebenaran yang wajar.

(2 markah)

iii. Serangan yang membolehkan penyerang melaksanakan skrip dalam pelayar mangsa yang boleh merampas sesi pengguna, mengubah laman web, atau mengalihkan pengguna ke laman web lain yang berniat jahat.

(2 markah)

iv. Serangan di mana penyerang mengeksploitasi konfigurasi lalai yang tidak selamat, konfigurasi tidak lengkap atau secara *ad hoc*, penyimpanan awan terbuka, kepala HTTP yang salah, dan mesej ralat kesalahan yang mengandungi maklumat sensitif.

(2 markah)

(e) Semasa sesi demonstrasi serangan aplikasi web, anda telah menangkap satu permintaan http yang boleh dieksploitasi melalui permintaan *GET* L, seperti yang ditunjukkan dalam Rajah 3.


```
GET /account/main_user.php?id=450120338654&ammount=5000 HTTP/1.1
Host: moibank.gov.my
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
Firefox/78.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://moibank.gov.my/login.php
Connection: keep-alive
Cookie: PHPSESSID=u62evbcltm2ou27ea0oqgdmhi3
Upgrade-Insecure-Requests: 1
```

Rajah 3: GET dalam URL

Berdasarkan Rajah 3,

i. Kenalpasti bagaimana kelemahan ini dieksploitasi oleh penyerang?

(1 markah)

ii. Cadangkan **SATU (1)** perisian yang boleh digunakan untuk mengeskploitasi kelemahan ini.

(1 markah)

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

(3 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. Sebagai penguji penerobosan kanan dalam ZAMSS, anda perlu menjelaskan kepada Ketua Pegawai Maklumat NTRSB mengenai isu dan skop yang berkaitan dengan ujian tersebut.

Berdasarkan Kajian Kes 3, jawab soalan-soalan berikut.

(a) Terangkan **DUA (2)** kategori penilaian keselamatan.

(4 markah)

(b) Senaraikan **TIGA (3)** sebab kenapa Pengujian Penembusan perlu dilakukan ke atas infrastrukutur ICT NTRSB.

(3 markah)

(c) Cadang dan Jelaskan **EMPAT (4)** ruang lingkup ujian penembusan yang perlu dilakukan untuk menjamin keselamatan infrastruktur dan info struktur ICT disyarikat ZAMSS.

(8 markah)

(d) Pasukan pengujian penerobosan ZAMSS menjumpai dua pusat capaian tanpa wayar yang masih mempunyai ruang untuk dieksploitasi disebabkan oleh konfigurasi keselamatan yang lemah. Cadangkan **EMPAT (4)** langkah balas yang boleh diaplikasikan oleh NTRSB terhadap rangkaian tanpa wayar untuk mencegah serangan pada masa akan datang.

(4 markah)

(e) Ujian Penerobosan boleh dilaksanakan samada melalui pendekatan dari dalam organisai dan juga pendekatan dari luar organisasi. Bincangkan kedua-dua pendekatan tersebut serta nyatakan kelebihan dan kekurangan setiap satunya.

(6 markah)

-SOALAN TAMAT-

PART A: STRUCTURED QUESTIONS (25 MARKS)

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

(a) Internet technology has evolved drastically in recent years and nowadays more devices are connected to the internet, thus exposing more devices to cyber threats. Describe the role of an Ethical Hacker in reducing the cyber threats.

(4 marks)

(b) Hackers nowadays can be categorized into several types of hackers, Discuss **THREE (3)** different types of hackers based on the level of their hacking knowledge, level of severity they can cause an organization and legality of their hacking activity.

(12 marks)

(c) Ethic 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 **FOUR (4)** differences between Ethics and Law.

(4 marks)

(d) Agent Smith successfully intercepted a communication between the Soviet army in the World War I and were using Caesar cipher to encrypt their message. As a cryptanalyst for Agent Smith, decrypt and find the key for the ciphertext.

YMJK PJQU WNHJ BNQQ NSHW JFXJ YTWH KTZW GDSJ CYBJ JP

(5 marks)

PART B: STRUCTURED QUESTIONS (75 MARKS)

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

QUESTION 1 (25 MARKS)

Case Study 1:

Fariq78 is a black hat hacker that has successfully exploited and penetrated a server owned by Malik Technology Resources Bhd (MTRB). As the Computer Security Senior Manager of MTRB you are asked to do an investigation on this security breach. Your first task is to explain to the top management on the general scenario of how a hacking is done. Based on Case Study 1, answer the following questions.

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

(9 marks)

(b) Social Engineering is one of the clever manipulations 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. For each of them, give an example of an action plan that can be done.

i. Phishing
ii. Piggybacking
iii. Vishing

(6 marks)

(c) During the incident, one of the network monitoring tools in MTRB's network infrastructure has successfully captured a series of network traffic, suspected to be a communication between Fariq78's machine and one of MTRB's server. The network traffic captured is shown in Figure 1.

Source	source port	Destination	Dest port	Protocol	Info
192.168.254.131	48614	192.168.254.130	25	TCP	48614 > smtp [SYN] Seq=0
192.168.254.131	48614	192.168.254.130	80	TCP	48614 > http [SYN] Seq=0
192.168.254.131	48614	192.168.254.130	53	TCP	48614 > domain [SYN] Seq=
192.168.254.131	48614	192.168.254.130	123	TCP	48614 > ntp [SYN] Seq=0 W
192.168.254.131	48614	192.168.254.130	67	TCP	48614 > bootps [SYN] Seq=
Vmware_7f:08:97		Broadcast		ARP	Who has 192.168.254.131?
Vmware_e8:52:0a		Vmware_7f:08:97		ARP	192.168.254.131 is at 00:
192.168.254.130	67	192.168.254.131	48614	TCP	bootps > 48614 [RST, ACK]
192.168.254.130	54915	192.168.254.255	54915	UDP	Source port: 54915 Desti
192.168.254.131	48615	192.168.254.130	123	TCP	48615 > ntp [SYN] Seq=0 W
192.168.254.131	48615	192.168.254.130	53	TCP	48615 > domain [SYN] Seq=
192.168.254.130	123	192.168.254.131	48615	TCP	ntp > 48615 [RST, ACK] Se
192.168.254.130	53	192.168.254.131	48615	TCP	domain > 48615 [RST, ACK]
192.168.254.131	48615	192.168.254.130	80	TCP	48615 > http [SYN] Seq=0
192.168.254.131	48615	192.168.254.130	25	TCP	48615 > smtp [SYN] Seq=0
192.168.254.130	80	192.168.254.131	48615	TCP	http > 48615 [SYN, ACK] S
192.168.254.130	25	192.168.254.131	48615	TCP	smtp > 48615 [SYN, ACK] S
192.168.254.131	48615	192.168.254.130	80	TCP	48615 > http [RST] Seq=1
192.168.254.131	48615	192.168.254.130	25	TCP	48615 > smtp [RST] Seq=1
192.168.254.130	54915	192.168.254.255	54915	UDP	Source port: 54915 Desti
192.168.254.130	54915	192.168.254.255	54915	UDP	Source port: 54915 Desti
192.168.254.130	25	192.168.254.131	48614	TCP	smtp > 48614 [SYN, ACK] S
192.168.254.130	80	192.168.254.131	48614	TCP	http > 48614 [SYN, ACK] S
192.168.254.131	48614	192.168.254.130	25	TCP	48614 > smtp [RST] Seq=1

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

(d) Based on Figure 1.

i. Identify the attacker's IP address

(1 mark)

ii. What type of port scanning method is used? State your reason.

(2 marks)

iii. Identify **ONE (1)** open and **ONE (1)** close port during this scanning activity.

(2 marks)

iv. Give **TWO (2)** other port scanning methods that can be used in this attack.

(2 marks)

(e) In an attempt to cover the attack track, Fariq78 is believed to have used some types of covering track tools to delete several logs in the server. List **THREE (3)** possible tools might be used by Fariq78 to cover his/her tracks.

(3 marks)

QUESTION 2 (25 MARKS)

Case Study 2:

SoftHouse Sdn. Bhd. is a software development company which is expert in developing web applications. Among the standard practise by the company is analysing each code developed by the programmers 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 company's web application project development.

Based on Case Study 2, answer the following questions.

(a) State **FOUR (4)** misconfiguration in a web server that can lead to web application attacked by hacker.

(4 marks)

(b) Briefly discuss **TWO (2)** impacts of a vulnerable webserver.

(4 Marks)

(c) There are several methods to attack a webserver. Give any **FOUR (4)** of the attack methods.

(4 marks)

(d) The following definition refer to a specific web application attack, name the correct web application attack for each of the definition and give **ONE(1)** method to prevent the attack.

i. An attack which exploits the authentication and session management that are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.

(2 marks)

ii. An attack which an attacker sends an untrusted data to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter

into executing unintended commands or accessing data without proper authorization.

(2 marks)

iii. An attack where an attacker can execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

(2 marks)

iv. An attack where the attacker exploits the insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information.

(2 marks)

(e) During the demonstration session on web application attack, you had captured http request that can be exploited through GET request as shown in Figure 3.

```
GET /account/main_user.php?id=450120338654&ammount=5000 HTTP/1.1
Host: moibank.gov.my
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://moibank.gov.my/login.php
Connection: keep-alive
Cookie: PHPSESSID=u62evbcltm2ou27ea0oqgdmhi3
Upgrade-Insecure-Requests: 1
```

Figure 3: HTTP request

Based on Figure 3,

i. How can an attacker exploit this flaw?

(1 mark)

ii. Suggest **ONE(1)** tool that can be used to exploit this flaw.

(1 mark)

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

(3 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. 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 Case Study 3, answer the following questions.

(a) Explain **TWO (2)** categories of Security Assessment .

(4 marks)

(b) List **THREE (3)** reasons why Penetration Testing need to be performed on NTRSB ICT infrastructure.

(3 marks)

(c) Proposed and explain **FOUR (4)** scopes of penetration testing need to be done to secure the ZAMSS's ICT infrastructure and info structure .

(8 marks)

(d) ZAMSS penetration test team found two wireless Acees Point (AP) that have a potential to be exploited due to the wireless AP vulnerability in the configuration setting. Suggest **FOUR (4)** countermeasures NTRSB can apply to the wireless network to prevent future attacks.

(4 marks)

(e) Penetration Testing can be performed either from the internal site or external site. Describe each of the approach and list the advantage and disadvantage of each of them.

(6 marks)

-END OF QUESTION-