UTHM
Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER I
SESSION 2022/2023

COURSE NAME	:	COMPUTER SECURITY
COURSE CODE	:	BEJ 42703
PROGRAMME CODE	:	BEJ
EXAMINATION DATE	:	FEBRUARY 2023
DURATION	:	3 HOURS
INSTRUCTION	:	1. ANSWER ALL QUESTIONS 2. THIS FINAL EXAMINATION IS CONDUCTED VIA **CLOSED BOOK.** 3. STUDENTS ARE **PROHIBITED** TO CONSULT THEIR OWN MATERIAL OR ANY EXTERNAL RESOURCES DURING THE EXAMINATION CONDUCTED VIA CLOSED BOOK.

THIS QUESTION PAPER CONSISTS OF **SEVEN (7)** PAGES

PART A: Objective Questions

Q1 What can be done to secure a wireless network?

(A) Decrease power transmission level to cover only the intended area.
(B) Use a wireless encryption standard such as 802.3
(C) Change the DHCP-supplied default gateway address.
(D) Configure wireless router admin access to use HTTP.

(1 mark)

Q2 Which standard requires stations to authenticate before gaining network access?

(A) 802.11a
(B) 802.11b
(C) 802.1x
(D) 802.3

(1 mark)

Q3 SNMP is a protocol used for ....

(A) Secure e-mail
(B) Secure encryption of network packets
(C) Remote access to user workstations
(D) Remote access to network infrastructure

(1 mark)

Q4 A university student has a wired network connection to a restrictive university network. At the same time, the student connected to a Wi-Fi hotspot for a nearby coffee shop that allows unrestricted Internet access. What potential problem exists in this case?

(A) The student computer could link coffee shop patrons to the university network.
(B) The student computer could override the university's default gateway setting.
(C) Encrypted university transmissions could find their way onto the Wi-Fi network.
(D) Encrypted coffee shop transmissions could find their way onto the university network.

(1 mark)

Q5 Users store company files on USB flash drives so that they can work from various computers outside of the corporate network. What should you do to secure this data?

(A) Generate file hashes for USB flash drive content.
(B) Scan USB flash drives for viruses.
(C) Encrypt USB flash drives.
(D) Digitally sign files on USB flash drives.

(1 mark)

Q6 Bob is a lawyer in Kuala Lumpur. He requires secure, high-quality voice communication with Indonesian clients. What can he do?

(A) Use VOIP with packet encryption over the Internet.
(B) Use cell phone voice encryption.
(C) Use only landline telephones.
(D) Use his cell phone on a special voice network for a legal professional.

(1 mark)

Q7 Your IT manager asks you to ensure e-mail messages and attachments do not contain sensitive data that could be leaked to competitors. What type of solution should you propose?

(A) Antivirus software
(B) NIDS
(C) DLP
(D) HIDS

(1 mark)

Q8 Discovered in 1991, the Michelangelo malware was said to be triggered to overwrite the first 100 hard disk sectors with null data each year on March 6, the date of the Italian artist's birthday. What type of malware is Michelangelo?

(A) Zero-day
(B) Worm
(C) Trojan
(D) Logic bomb

(1 mark)

Q9 A piece of malicious code uses dictionary attacks against computers to gain access to administrative accounts. The code can link compromised computers together to receive remote commands. What term best applies to this malicious code?

(A) Exploit
(B) Botnet
(C) Logic Bomb
(D) Backdoor

(1 mark)

Q10 What will prevent frequent repeated malicious attacks against user account passwords?

(A) Minimum password age
(B) Password hints
(C) Password history
(D) Account lockout

(1 mark)

Q11 Your organization hosts a website with a back-end database. The database stores customer data, including credit card numbers. Which of the following is the BEST way to protect credit card data?

(A) Full database encryption
(B) Whole disk encryption
(C) Database column encryption
(D) File-level encryption

(1 mark)

Q12 The Nuclear Power Plant has created an online application teaching nuclear physics. Only students and teachers in the Batu Pahat secondary School can access this application via the cloud. What type of cloud service model is this?

(A) IaaS
(B) PaaS
(C) SaaS
(D) Public

(1 mark)

Q13 Which security role is responsible for establishing access to data and enforcing related policies, laws and regulations?
(A) Custodian
(B) Data Owner
(C) Data User
(D) Database administrator

(1 mark)

Q14 Database administrators have created a database used by a web application. However, testing shows that the application is taking a significant amount of time to access data within the database. Which of the following actions is MOST likely to improve the overall performance of a database?

(A) Normalization
(B) Client-side input validation
(C) Server-side input validation
(D) Obfuscation

(1 mark)

Q15 Your organization is preparing to deploy a web-based application, which will accept user input. Which of the following will BEST test the reliability of this application to maintain availability and data integrity?

(A) Model verification
(B) Input validation
(C) Error handling
(D) Dynamic analysis

(1 mark)

Q16 Which concepts expose employees to varying job roles to increase their overall knowledge of the business?

(A) Mandatory vacations
(B) Least privilege
(C) Separation of duties
(D) Job rotation

(1 mark)

Q17 Which of the following best describes security fuzzing?

(A) Providing random data to test application security.
(B) Conducting a quick overview security audit.
(C) Jamming Wi-Fi radio frequencies to prevent rogue access points.
(D) Injecting spoofed packets on a network.

(1 mark)

Q18 A military division uses portable computing units to aid in flight take-off and landings at ad hoc landing strips. How can the military track the position of these portable units?

(A) SSL
(B) GPS
(C) TPM
(D) Bluetooth

(1 mark)

Q19 A tour disaster recovery plan requires the quickest possible data restoration from backup tape. Which strategy should you employ?

(A) Weekly full backup, daily incremental backup
(B) Daily full backup, weekly incremental backup
(C) Daily full backup
(D) Daily differential backup

(1 mark)

Q20 Users store company files on USB flash drives so that they can work from various computers outside of the corporate network. What should you do to secure this data?

(A) Generate file hashes for USB flash drive content.
(B) Scan USB flash drives for viruses.
(C) Encrypt USB flash drives.
(D) Digitally sign files on USB flash drives.

(1 mark)

PART B: Subjective Questions

Q21 (a) Analyze the following source code whether they cause a buffer overflow or not. Show your answer using a memory allocation diagram.

(i)

```
char A[5];
A[5]='a';
```

(ii)

```
int A[5];
for (int i=0; i<5; i++)
     A[i]=100;
```

(iii)

```
int A[5];
for (int i=4; i>0; i--)
     A[i]=100;
```

(iv)

```
int A[2][3];
for (int i=0; i<2; i++)
   for (int j=0; j<3; j++)
      A[j][i]=100;
```

(v)

```
char A[8];
strcpy(A, "password");
```

(10 marks)

(b) Describe **two (2)** steps to secure operating systems.

(4 marks)

Q22 (a) Discuss **three (3)** differences between EMI and EMP.

(6 marks)

(b) Besides using the password as human authentication, explain another human authentication based on the following categories.

(i) Something you have

(ii) Something you are

(iii) Somewhere you are

(iv) Something you do

(8 marks)

Q23 (a) Illustrates a diagram to show the protection of Statistical Databases from inference attacks.

(4 marks)

(b) As a computer security expert, suggest **three (3)** solutions to protect the database from any security threats.

(9 marks)

Q24 (a) In the form of a figure, investigate how El Gamal, SHA dan 3DES are used in the secure e-mail delivery process.

(5 marks)

(b) Differentiate the following malicious code:

(i) Virus vs Worm

(ii) Spyware vs Trojan Horses

(8 marks)

Q25 (a) During Covid19 Pandemic, many education institutions implement online teaching and learning. As an IT security officer, discuss policy guidelines for lecturer works outside the office.

(5 marks)

(b) Adam and Hawa are having another debate about computer and network security. Adam says that it is the job of security professionals to find all vulnerabilities and every threat and make sure the system is always 100% secure. Do you agree with Adam? You should explain your answer with **five (5)** reasons.

(6 marks)

Q26 (a) IPsec is a suite of protocols for securing networks. Briefly outline how it provides confidentiality, integrity and key management.

(6 marks)

(b) Draw a diagram to show where IPSec fits in the TCP/IP model.

(3 marks)

(c) You are the IT manager of a company that provides laptop PCs to its sales employees. You are concerned about the security implications. This is because the sales staff can store sensitive data on their laptop PCs and then use them for email.

Identify **two (2)** risks to data on a laptop PC and briefly explain how each risk can compromise the confidentiality, integrity or availability of the data.

(6 marks)

- END OF QUESTIONS -