Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER II
SESSION 2022/2023

COURSE NAME	:	COMPUTER SECURITY
COURSE CODE	:	BEJ42703/BEC41903
PROGRAMME CODE	:	BEJ
EXAMINATION DATE	:	JULY/AUGUST 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 **NINE (9)** PAGES

PART A: Objective Questions. (25 marks)

Q1 The Marvin Monroe Memorial Hospital recently suffered a serious attack. The attackers notified management personnel that they encrypted a significant amount of data on the hospital's servers and it would remain encrypted until the management paid a hefty sum to the attackers. Which of the following identifies the MOST likely threat actor in this attack?

(A) Organized crime
(B) Thieves
(C) Competitors
(D) Hacktivist

Q2 Dr. Terwilliger installed code designed to enable his account automatically if he ever lost his job as a sidekick on a television show. The code was designed to reenable his account three days after it is disabled. Which of the following does this describe?

(A) Logic bomb
(B) Rootkit
(C) Spyware
(D) Ransomware

Q3 A security administrator recently noticed abnormal activity on a workstation. It is connecting to systems outside the organization's internal network using uncommon ports. The administrator discovered the computer is also running several hidden processes. Which of the following choices BEST describes this activity?

(A) Rootkit
(B) Backdoor
(C) Spam
(D) Trojan

Q4 Lisa recently developed an application for the Human Resources department. Personnel use this application to store and manage employee data, including Personally Identifiable Information (PII). She programmed in the ability to access this application with a username and password that only she knows, so that she can perform remote maintenance on the application if necessary. Which of the following does this describe?

(A) Virus
(B) Worm
(C) Backdoor
(D) Trojan

Q5 While cleaning out his desk, Bart threw several papers containing Personally Identifiable Information (PII) into the recycle bin. Which type of attack can exploit this action?

(A) Vishing
(B) Dumpster diving
(C) Shoulder surfing
(D) Tailgating

Q6 Bart recently sent out confidential data via email to potential competitors. Management suspects he did so accidentally, but Bart denied sending the data. Management wants to implement a method that would prevent Bart from denying accountability in the future. Which of the following are they trying to enforce?

(A) Confidentiality
(B) Encryption
(C) Access control
(D) Non-repudiation

Q7 A software company occasionally provides application updates and patches via its web site. It also provides a checksum for each update and patch. Which of the following BEST describes the purpose of the checksum?

(A) Availability of updates and patches
(B) Integrity of updates and patches
(C) Confidentiality of updates and patches
(D) Integrity of the application

Q8 Bart wants to send a secure email to Lisa, so he decides to encrypt it. Bart wants to ensure that Lisa can verify that he sent it. Which of the following does Lisa need to meet this requirement?

(A) Bart's public key
(B) Bart's private key
(C) Lisa's public key
(D) Lisa's private key

Q9 Bart wants to send a secure email to Lisa, so he decides to encrypt it. He wants to ensure that only Lisa can decrypt it. Which of the following does Lisa need to decrypt Bart's email?

(A) Bart's public key
(B) Bart's private key
(C) Lisa's public key
(D) Lisa's private key

Q10 An organization requested bids for a contract and asked companies to submit their bids via email. After winning the bid, Acme realized it couldn't meet the requirements of the contract. Acme instead stated that it never submitted the bid. Which of the following would provide proof to the organization that Acme did submit the bid?

(A) Digital signature
(B) Integrity
(C) Repudiation
(D) Encryption

Q11 Your organization wants to ensure that employees do not install any unauthorized software on their computers. Which of the following is the BEST choice to prevent this?

(A) Master image
(B) Application whitelisting
(C) Anti-malware software
(D) Antivirus software

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

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

Q13 Your organization hosts a web site with a back-end database. The database stores customer data, including credit card numbers. Which of the following is the BEST way to protect the credit card data?

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

Q14 Your organization wants to increase security for VoIP and video teleconferencing applications used within the network. Which of the following protocols will BEST support this goal?

(A) SMTP
(B) TLS
(C) SFTP
(D) SRTP

Q15 Management within your company wants to restrict access to the Bizz app from mobile devices. If users are within the company's property, they should be granted access. If they are not within the company's property, their access should be blocked. Which of the following answers provides the BEST solution to meet this goal?

(A) Geofencing
(B) Geolocation
(C) GPS tagging
(D) Containerization

Q16 Attackers recently attacked a web server hosted by your organization. Management has tasked administrators with configuring the servers following the principle of least functionality. Which of the following will meet this goal?

(A) Disabling unnecessary services
(B) Installing and updating antivirus software
(C) Identifying the baseline
(D) Installing a NIDS

Q17 Your organization's security policy requires that Personally Identifiable Information (PII) data-in-transit must be encrypted. Which of the following protocols would BEST meet this requirement?

(A) FTP
(B) SSH
(C) SMTP
(D) HTTP

Q18 An organization has recently had several attacks against servers within a DMZ. Security administrators discovered that many of these attacks are using TCP, but they did not start with a three-way handshake. Which of the following devices provides the BEST solution?

(A) Stateless firewall
(B) Stateful firewall
(C) Network firewall
(D) Application-based firewall

Q19 You need to configure a UTM security appliance to restrict traffic going to social media sites. Which of the following are you MOST likely to configure?

(A) Content inspection
(B) Malware inspection
(C) URL filter
(D) DDoS mitigator

Q20 Marge needs to collect network device configuration information and network statistics from devices on the network. She wants to protect the confidentiality of credentials used to connect to these devices. Which of the following protocols would BEST meet this need?

(A) SSH
(B) FTPS
(C) SNMPv3
(D) TLS

Q21 Management within your organization wants to ensure that users understand the rules of behavior when they access the organization's computer systems and networks. Which of the following BEST describes what they would implement to meet this requirement?

(A) Acceptable Use Policy (AUP)
(B) non- disclosure agreement (NDA)
(C) bring your own device (BYOD)
(D) Data Duplicator (DD)

Q22 After a recent security audit, management has decided to upgrade the security policy. Among other items, they want to identify a policy that will reduce the risk of personnel within an organization colluding to embezzle company funds. Which of the following is the BEST choice to meet this need?

(A) AUP
(B) Training
(C) Mandatory vacations
(D) Background check

Q23 After a major data breach, Lisa has been tasked with reviewing security policies related to data loss. Which of the following is MOST closely related to data loss?

(A) Clean desk policy
(B) Legal hold policy
(C) Job rotation policy
(D) Background check policy

Q24 Your organization is planning to implement an incident response plan in response to a new incident response security policy. Which of the following items is the FIRST step in an incident response process?

(A) Preparation
(B) Identification
(C) Containment
(D) Eradication

Q25 Waylon reported suspicious activity on his computer. After investigating, you verify that his computer is infected with malware. Which of the following steps should you take NEXT?

(A) Identification
(B) Preparation
(C) Containment
(D) Eradication

PART B: Subjective Questions. (75 marks)

Q26 (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]='1';
```

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

(iii)
```
int A[5];
for (int i=4; i>-1; i--)
    A[i]=100;
```

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

(v)
```
char A[8];
strcpy(A, "pass word");
```

(10 marks)

(b) Illustrates the three (3) diagrams how viruses attach to a program.

(6 marks)

Q27 (a) Passwords are still the most common method of user authentication. Describe four (4) characteristics of weak passwords and give example password for every characteristics.

(4 marks)

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

(i) Something you have

(ii) Something you are

(iii) Something you do

(6 marks)

(c) They are many attackers that we cannot know. First consider the motives of attackers. Focusing on motive may give some idea of who might attack a networked host or user. Discover three (3) important motives.

(6 marks)

Q28 (a) The basis of operating system protection is separation. List FOUR (4) types of operating system separation.

(4 marks)

(b) Explain four (4) basic steps needed to secure the operating system?

(4 marks)

(c) Malaysian typically use a public Wi-Fi in a hotel, restaurant, coffee shop or convenient store. Explain precautions do you should take when using a public Wi-Fi.

(4 marks)

Q29 (a) Illustrates the diagram to show the protection of Statistical Database from inference attacks.

(6 marks)

(b) As an security expert, examine the solution to overcome the following database security threats.

(i) Weak audit trail

(ii) Lack of security expertise and education

(iii) DDoS attack.

(iv) SQL Injection

(v) Unmanaged Sensitive Data

(10 marks)

Q30 (a) During Covid19 Pandemic, many education institutions implement online teaching and learning. As an IT security officer, discuss a 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)

-END OF QUESTIONS -