UNIVERSITI KUALA LUMPUR
MALAYSIAN INSTITUTE OF INFORMATION TECHNOLOGY

FINAL ASSIGNMENT
MARCH 2026 SEMESTER

COURSE CODE	:	IKB21004
COURSE NAME	:	SOFTWARE VULNERABILITIES AND EXPLOITATION
PROGRAMME NAME	:	BACHELOR OF INFORMATION TECHNOLOGY (HONS) IN COMPUTER SYSTEM SECURITY
DATE	:	23 JUNE 2026
TIME	:	2:00 PM – 4:00 PM
DURATION	:	2 HOURS

INSTRUCTIONS TO CANDIDATES

1. Candidates are required to read all instructions carefully before answering the questions.
2. This question paper contains printed information on both sides of the paper.
3. This question paper consists of TWO (2) sections, namely Section A and Section B.
4. Candidates must answer ALL questions in English ONLY.
5. Write your answers in the Answer Booklet provided.

THERE ARE 8 PAGES OF QUESTIONS, EXCLUDING THIS PAGE.

TOTAL: 80 MARKS

SECTION A (30 Marks)

INSTRUCTION: Answer all questions. Write your answers in the Answer Booklet provided.

1. Which of the following best defines a vulnerability in a system?
   A. A software feature that enhances usability
   B. A protocol that improves network speed
   C. A weakness that can be exploited to compromise security
   D. A firewall rule that blocks traffic

2. Which of the following is a common goal of attackers in the Cyber Kill Chain?
   A. Strengthening security policies
   B. Exploiting vulnerabilities to gain access or control
   C. Reducing system downtime
   D. Improving encryption algorithms

3. What is the primary objective of system hacking?
   A. To optimize system performance
   B. To update operating systems
   C. To configure firewalls
   D. To gain unauthorized access and control

4. What is the goal of maintaining access?
   A. To remove all traces of the attack
   B. To maintain persistent control over the compromised system
   C. To improve system speed
   D. To check log integrity

5. Which Windows tool allows viewing and managing event logs?
   A. Task Manager
   B. Device Manager
   C. Event Viewer
   D. Disk Utility

6. What is privilege escalation?
   A. Gaining higher-level access than initially obtained
   B. Removing system patches
   C. Running antivirus scans
   D. Using guest accounts

7. Horizontal privilege escalation allows attackers to:
   A. Gain admin-level control
   B. Access accounts with similar privilege levels
   C. Modify firewall rules
   D. Delete event logs

8. Clearing logs is part of which phase of system hacking?
   A. Gaining access
   B. Escalating privileges
   C. Maintaining access
   D. Covering tracks

9. Which malware mechanism is designed to provide persistent unauthorized remote access?
   A. Ransomware
   B. Trojan
   C. Backdoor
   D. Rootkit

10. Which method helps attackers elevate privileges by replacing system files?
    A. File manipulation
    B. Log rotation
    C. Backup restoration
    D. User training

11. Which of the following is an example of passive footprinting?
    A. Ping sweep
    B. WHOIS lookup
    C. Port scanning
    D. Banner grabbing

12. The command nslookup is used to:
    A. Check system performance
    B. Crack passwords
    C. Capture network packets
    D. Resolve domain names

13. What does banner grabbing help identify?
    A. Server software and versions
    B. Email passwords
    C. Social media friends
    D. User browsing history

14. What does traceroute help identify?
    A. Application vulnerabilities
    B. System passwords
    C. Path packets take to reach a destination
    D. Website content

15. A DNS zone transfer vulnerability allows attackers to:
    A. Verify password strength
    B. Reset DNS servers
    C. Enumerate the entire DNS domain information
    D. Change TTL values

16. What is footprinting via web services commonly used for?
    A. Enumerating API endpoints
    B. Cracking passwords
    C. Disabling antivirus
    D. Formatting log files

17. A common risk of outdated WHOIS privacy records is:
    A. Slow DNS propagation
    B. Loss of domain
    C. Invalid MX records
    D. Exposure of personal contact information

18. Publishing malicious apps on official app stores relies **MOST** on:
    A. User trust in platform reputation
    B. Zero-day vulnerabilities
    C. Weak encryption
    D. Technical exploits

19. Which password policy reduces brute-force attacks **MOST** effectively?
    A. Strong passwords
    B. Password reuse
    C. Account lockout after failed attempts
    D. Writing passwords down

20. Which action **BEST** prevents identity theft?
    A. Using private Wi-Fi or avoid public Wi-Fi networks
    B. Oversharing on social media
    C. Enabling two-factor authentication
    D. Strong passwords

21. Which of the following **BEST** describes CVSS?
    A. A tool used for scanning vulnerabilities
    B. A scoring system to measure vulnerability severity
    C. A firewall configuration standard
    D. A password encryption method

22. Which factor **MOST** influences vulnerability prioritisation in an organisation?
    A. Number of vulnerabilities
    B. Colour of severity rating
    C. Business impact and asset criticality
    D. Type of operating system

23. Which of the following is an example of **active reconnaissance**?
    A. Reviewing company website
    B. Searching LinkedIn profiles
    C. Performing port scanning
    D. Reading public reports

24. What is the **PRIMARY** purpose of a vulnerability scanner like Nessus?
    A. To exploit vulnerabilities
    B. To detect and report known vulnerabilities
    C. To encrypt sensitive data
    D. To monitor user behaviour

25. Which vulnerability is **MOST** associated with APIs?
    A. Broken authentication
    B. Buffer overflow
    C. Open port scanning
    D. Disk fragmentation

26. In cloud environments (e.g., Amazon Web Services), a common misconfiguration is:
    A. Weak CPU performance
    B. Slow internet connection
    C. Large file size
    D. Publicly exposed storage buckets

27. What does the principle of least privilege mean?
    A. Users should have full admin access
    B. Users should only have access necessary for their role
    C. Users should not have passwords
    D. Users should share accounts

28. Which of the following **BEST** describes a **false positive** in vulnerability scanning?
    A. A vulnerability that does not exist but is reported
    B. A vulnerability that is confirmed exploitable
    C. A vulnerability that is patched
    D. A vulnerability that is critical

29. Why is patch management **IMPORTANT** in vulnerability management?
    A. It improves system speed
    B. It removes unused files
    C. It fixes known vulnerabilities in systems
    D. It increases storage capacity

30. Which of the following **BEST** reduces the risk of **Man-in-the-Middle (MITM)** attacks?

A. Using HTTP

B. Disabling firewall

C. Implementing HTTPS with TLS

D. Using default passwords

SECTION B (50 Marks)

INSTRUCTION: Answer all questions. Write your answers in the Answer Booklet provided.

CASE STUDY

FinServe Solutions Sdn. Bhd. is a growing fintech company in Malaysia that offers a mobile and web-based digital payment service for SMEs and individual users.

The system environment consists of:

1. A customer-facing mobile and web application
2. A RESTful API backend handling payment processing
3. A centralised database storing user credentials and financial data
4. A cloud-based hosting environment
5. A small internal IT security team responsible for system maintenance

Recently, the organisation has observed:

1. Multiple unauthorised login attempts and suspicious transactions
2. Possible misconfigurations in system security controls
3. Increasing concern from management regarding data leakage, compliance (e.g., PDPA), and customer trust
4. Management has requested a vulnerability assessment to evaluate system weaknesses and recommend improvements.

(a) Vulnerability Identification and Analysis

You have been appointed as a Security Analyst for FinServe Solutions Sdn. Bhd. Based on the case study above, prepare a vulnerability assessment and risk analysis report.

Analyse and elaborate on the following **potential vulnerabilities** identified within the system:

1. Ineffective Authentication and Authorisation Mechanisms
2. Lack of Secure Communication Protocols
3. Insufficient Input Filtering and Validation
4. Use of Unsupported or Legacy Software Components

For each vulnerability, your answer must include:

1. Description of the vulnerability in the context of the case environment (2.5m)
2. Category (e.g., Application, Network, System) (1m)
3. Possible exploitation techniques (2m)
4. Potential impact on the organisation (2m)

(30 marks)

(b) Vulnerability Assessment Reporting

Explain **FIVE (5) key components** of a professional vulnerability assessment report.
For each component:

1. Provide a clear description
2. Justify its importance for management decision-making

(20 marks)

END OF QUESTIONS