UNIVERSITI
TEKNOLOGI
PETRONAS

FINAL EXAMINATION
MAY 2024 SEMESTER

COURSE	**:**	**TEB2093/TEB2193/TEB2213/TFB2043 - COMPUTER SECURITY/INFORMATION ASSURANCE AND SECURITY/INTRODUCTION TO CYBER SECURITY**
DATE	**:**	**13 AUGUST 2024 (TUESDAY)**
TIME	**:**	**2:30 PM - 5:30 PM (3 HOURS)**

INSTRUCTIONS TO CANDIDATES

1. Answer **ALL** questions in the Answer Booklet.
2. Begin **EACH** answer on a new page in the Answer Booklet.
3. Indicate clearly answers that are cancelled, if any.
4. Where applicable, show clearly steps taken in arriving at the solutions and indicate **ALL** assumptions, if any.
5. **DO NOT** open this Question Booklet until instructed.

Note :

i. There are **NINE (9)** pages in this Question Booklet including the cover page

ii. **DOUBLE-SIDED** Question Booklet.

1. As a security analyst at TechieMart, a leading e-commerce company operating an online marketplace platform, you are responsible for conducting a comprehensive security assessment of the company's systems. Your primary objective is to identify potential threats and vulnerabilities that could compromise the platform's security services.

   a. Explain **THREE (3)** key security services that should be provided for TechieMart's platform and give an example scenario for each.

   [6 marks]

   b. Define threat in the context of computer security and provide **ONE (1)** example relevant to the TechieMart's online marketplace. Your example should include details about the threat actor, their motive, and their capability.

   [4 marks]

   c. List **TWO (2)** vulnerabilities that TechieMart's online marketplace may have and describe their potential consequences.

   [4 marks]

   d. State **TWO (2)** assets in the context of computer security that need to be protected with regards to TechieMart's online marketplace.

   [2 marks]

   e. Describe **TWO (2)** potential active attacks that could be launched against TechieMart's online marketplace.

   [4 marks]

2. You are a cryptography analyst working for a government intelligence agency. The agency has recently encountered a critical need to secure sensitive communications and data transmissions. Your task is to evaluate and recommend an appropriate encryption algorithm that can meet the agency's security requirements.

a. Explain how the Advanced Encryption Standard (AES) provides data security and why it is considered a suitable choice for encrypting sensitive communications.

[4 marks]

b. Describe the functionality of Rivest-Shamir-Adleman (RSA) algorithm in securing data transmissions and provide an example of how it can be used to protect sensitive government communications.

[4 marks]

c. Discuss the importance of key management in the context of encryption and propose one best practice for securely managing cryptographic keys in a government intelligence agency.

[4 marks]

d. Explain how digital signatures ensure the integrity and authenticity of data and describe a scenario where digital signatures would be essential for government intelligence operations.

[4 marks]

e. Compare AES and RSA in terms of performance and suitability for encrypting large volumes of data. Based on this comparison, recommend which encryption method the agency should prioritize for securing sensitive communications and justify your recommendation.

[4 marks]

3. Lakeville Medical Centre (LMC) is a medium-sized healthcare facility that has been operating for over 10 years. LMC is currently using a network environment that consists of legacy equipment and relies on basic onsite Information Technology infrastructure. Currently, LMC hosts its web and email servers in-house. Additionally, staff can access the system remotely from their homes or public workspaces. Considering these factors, LMC is looking to modernize its infrastructure and improve security.
The basic network architecture of LMC is shown in **FIGURE Q3**.

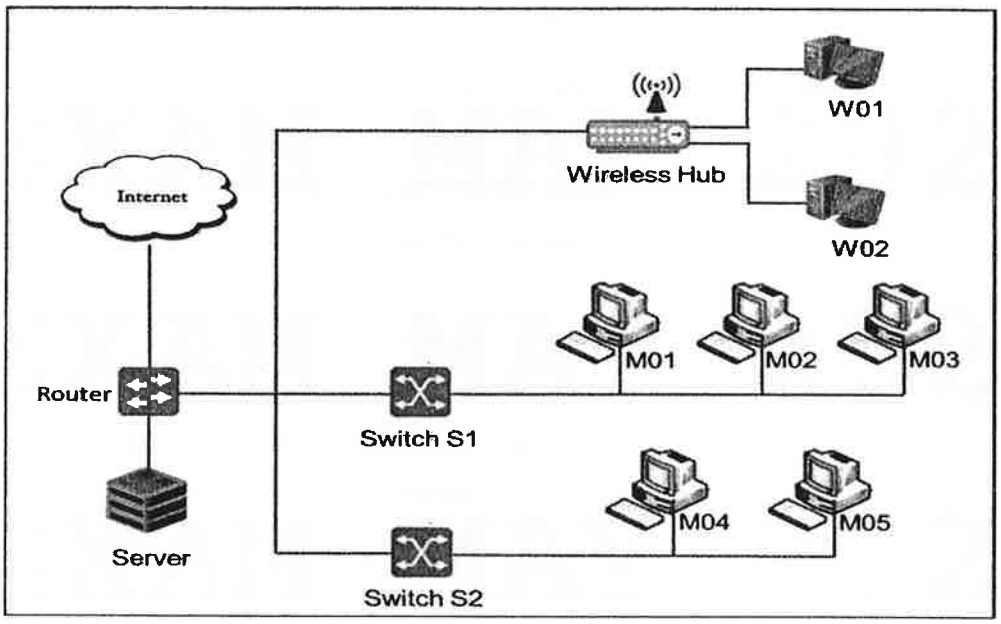

FIGURE Q3: Basic Network Architecture of LMC

a. Propose **ONE (1)** security countermeasure for protecting the hosts of LMC in **FIGURE Q3.** Justify your answer.

[2 marks]

b. Propose **TWO (2)** suitable network security countermeasures for protecting the internal network of LMC as shown in **FIGURE Q3**. Justify your answer.

[4 marks]

c. Propose **ONE (1)** suitable network security countermeasure for protecting the perimeter of the LMC's network as shown in **FIGURE Q3**. Justify your answer.

[4 marks]

d. Based on your answer in **part (b)** and **part (c),** redraw **FIGURE Q3** to depict the proposed network security countermeasures. Label the diagram accordingly.

[6 marks]

e. Recommend **ONE (1)** suitable network security countermeasure for ensuring that staff remote access to LMC's in-house systems is secured.

[4 marks]

4. Na Fa University (NFU) is a prominent university with a large student and faculty population. The university relies heavily on technology for various operations, including student information systems, research data, and communication platforms. As a security consultant, you have been tasked to conduct a risk assessment to ensure the security of the university's digital assets and safeguard against potential cybersecurity incidents. According to the historical data, the university has been attacked with malware attacks at an average four times a year. It is estimated that the average cost in damages and lost productivity due to a malware attack is RM20,000. The university decided to invest in an intelligent malware scanner which will cost RM100,000 as the countermeasure for the issue.

Your task is to assess the risks involved in the university and provide a comprehensive risk assessment report.

a. Propose **ONE (1)** approach for risk analysis in NFU. Justify your answer.

[2 marks]

b. Analyse **FOUR (4)** specific assets within NFU that may be at risk.

[4 marks]

c. Develop a risk register for the identified assets in **part (b)**.

[6 marks]

d. Propose **ONE (1)** risk treatment strategy for each identified risk in **part (c)**. Justify your answer.

[4 marks]

e. Conduct a risk quantitative analysis and return on security investment related to purchasing of the intelligent malware scanner. Justify whether the investment is reasonable.

[4 marks]

5. You are a web security analyst, tasked with investigating a recent cyber-attack on WealthGuard Systems, a fintech company specializing in wealth management services. WealthGuard Systems operates an online platform that allows clients to access their investment portfolios and facilitates secure financial transactions and account management. Recently, WealthGuard Systems fell victim to SQL Injection and Cross-Site Scripting (XSS) vulnerabilities.

You are responsible for conducting a comprehensive security analysis of WealthGuard Systems' web application, identifying the root causes of the SQL Injection and XSS vulnerabilities, and providing actionable recommendations to reinforce the company's web security defenses and prevent similar attacks in the future.

a. Define SQL Injection and discuss the impact of the attack on the WealthGuard Systems' web application.

[4 marks]

b. Write a sample SQL Injection query that could have been used by the attackers to exploit vulnerabilities of the WealthGuard Systems' web application and gain unauthorized access to the client database. Provide an explanation of how this query could compromise the security of the database.

[4 marks]

c. Based on your answer in **part (b)**, propose **TWO (2)** specific countermeasures to prevent SQL Injection.

[4 marks]

d. Explain XSS and discuss the impact of the attack on the WealthGuard Systems' web application.

[4 marks]

e. Propose **ONE (1)** strategy in safeguarding WealthGuard Systems' web application from malicious script execution and unauthorized data access. Justify your answer.

[4 marks]

-END OF PAPER-