



UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION  
SEMESTER II  
SESSION 2021/2022

- COURSE NAME : FUNDAMENTALS OF INFORMATION SECURITY
- COURSE CODE : BIT 21403
- PROGRAMME CODE : BIT
- EXAMINATION DATE : JULY 2022
- DURATION : 3 HOURS
- INSTRUCTION : 1. ANSWER ALL QUESTIONS
2. THIS FINAL EXAMINATION IS AN **ONLINE** ASSESSMENT AND 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 **EIGHT (8)** PAGES

TERBUKA

CONFIDENTIAL

**SECTION A**

**Choose the BEST answer for the following questions.**

- Q1** Trojan horse is \_\_\_\_\_.
- A. a software program designed to detect computer virus
  - B. an application software designed to decrease the quality of computer performance
  - C. a software program which provides functions within operating system
  - D. a software program that appears legitimate but contain hidden function that cause damage
- Q2** Computer viruses first appeared in the early \_\_\_\_\_.
- A. 1960s
  - B. 1970s
  - C. 1980s
  - D. 1990s
- Q3** Unsolicited bulk e-mail is referred to as \_\_\_\_\_.
- A. spam
  - B. propagating
  - C. phishing
  - D. crimeware
- Q4** What is an Email Spoofing?
- A. Adding inappropriate pictures to email.
  - B. The creation of email messages with a forged sender address.
  - C. Sending email to people you do not know.
  - D. Fast checking emails.
- Q5** Which of the following are possible signs of a malware infection?
- A. Slow system performance.
  - B. Irregular computer behavior.
  - C. Slow Internet connection.
  - D. All the above.



- Q6** What is the term used to describe malware that changes characteristics or rewrites its code between infections?
- A. Resident.
  - B. Stealth.
  - C. Polymorphic.
  - D. User mode.
- Q7** The \_\_\_\_\_ is what the virus “does”.
- A. infection
  - B. trigger
  - C. logic bomb
  - D. payload
- Q8** The attack that focuses on capturing small packets from the network transmitted by other computers and reading the data content in search of any type of information is \_\_\_\_\_.
- A. phishing
  - B. eavesdropping
  - C. scams
  - D. exploits
- Q9** A \_\_\_\_\_ uses scripting code, typically embedded in a document, and triggered when the document is viewed or edited, to run and replicate itself into other such documents.
- A. boot sector infector
  - B. file infector
  - C. macro virus
  - D. multipartite virus
- Q10** \_\_\_\_\_ is the first function in the propagation phase for a network worm.
- A. Propagating
  - B. Fingerprinting
  - C. Keylogging
  - D. Spear phishing

**Q11** During the \_\_\_\_\_ phase, the virus is idle.

- A. dormant
- B. propagation
- C. triggering
- D. execution

**Q12** The ideal solution to the threat of malware is \_\_\_\_\_.

- A. identification
- B. removal
- C. detection
- D. prevention

**Q13** Which of the following describes how a criminal starts ransomware attacks?

- A. Sending a scam email with a link that put the target's network and data at risk.
- B. Getting into the target's server through vulnerabilities and installing malware.
- C. Using infected websites that automatically download malicious software to the target's computer.
- D. All the above.

**Q14** BitDefender Antivirus provides real time protection against all viruses and ransomware. It also offers vulnerability scanning, anti-tracker, and secure VPN for complete privacy.

Which generation of anti-virus describes BitDefender?

- A. First generation.
- B. Second generation.
- C. Third generation.
- D. Fourth generation.

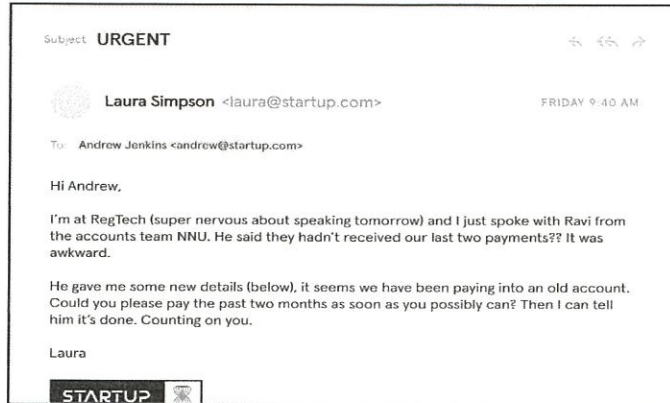
**Q15** Which of the following is a sign that suggests the email a target received from a bank is possibly forged and an attempt at phishing?

- A. The domain name of the email sender corresponds with the bank name.
- B. The bank website link is provided in the email.
- C. The email contains spelling and grammar mistakes.
- D. Registered full name and postal address in the email is same with the provided information for online banking registration.





**Q18** Based on **Figure Q18**:



**Figure Q18**

What type of phishing in **Figure Q18**?

- A. Whaling
- B. Smishing
- C. Vishing
- D. Spear phishing

**Q19** Based on **Figure Q19**:

```

Username = read_username ();
password = read_password ();
if username is "hack0r"
    return ALLOW_LOGIN;
if username and password are valid
    return ALLOW_LOGIN
else return DENY_LOGIN
    
```

**Figure Q19**

What type of malicious software in **Figure Q19**?

- A. Trapdoor.
- B. Bot.
- C. Rootkit.
- D. Zombie.

TERBUKA

*[Faint, illegible text at the bottom left corner]*

**Q20** Ahmad, a software developer was hired for providing an information system to a company. He planned X and enabled its positive conditions for the system. Due to this, the system used to crash every time the condition was met.

What is x?

- A. Adware.
- B. Rootkit.
- C. Logic bombing.
- D. Trapdoor.

(20 marks)

## SECTION B

**Q21** Consider the following scenario:

Universiti Tun Hussein Onn Malaysia (UTHM) is planning to digitalize the students' academic transcript. Assume that you want to propose the application of digital watermarking technology to the digital transcript.

(a) Define digital watermarking technology.

(2 marks)

(b) Describe **FOUR (4)** applications of watermarks to the UTHM digital academic transcript.

(12 marks)

(c) Discuss **THREE (3)** key features of digital watermarks.

(6 marks)

**Q22** Based on the following scenario:

Mr Ammar has a watch shop in Bangi and he wants to grow his business by implementing an online store. However, he still lacks an understanding concept of online payment and is worried about the security of this payment system.

(a) Explain the concept of online payment.

(8 marks)

(b) Discuss **THREE (3)** potential payment security issues.

(6 marks)

- (c) Discuss each solution for **Q22(b)**. (6 marks)

**Q23** Based on the following scenario:

Salim Bersaudara Sdn Bhd (SBSB) is a factory that produces electronic components and has 300 employees. Products will be shipped to customers throughout Malaysia. SBSB also had to provide an extensive database system to manage the information of its employees and customers. This database is managed by three IT staff and can be accessed by human resources and accounts department staff.

- (a) Discuss **FOUR (4)** security issues SBSB will face in managing their database. (8 marks)
- (b) Suggest **THREE (3)** suitable countermeasures to avoid SBSB database from SQL injection attack. (6 marks)
- (c) Explain **THREE (3)** reasons why SBSB needs to implement access control in accessing its database. (6 marks)

- Q24** (a) Explain **THREE (3)** types of computer crime based on the role that the computer plays in the criminal activity. (6 marks)
- (b) Discuss **THREE (3)** difficulties in implementing law enforcement on cybercrime. (6 marks)
- (c) Differentiate between copyright and trademark. (2 marks)
- (d) Explain **THREE (3)** forms of intellectual property that are relevant in the context of network and computer security. (6 marks)

- END OF QUESTIONS -

