CONFIDENTIAL / SULIT

UNIRAZAK
UNIVERSITI TUN ABDUL RAZAK

FINAL EXAMINATION

MARCH 2024

COURSE TITLE **INFORMATION SECURITY**

COURSE CODE **RCIT2523**

DATE/DAY **19 JUNE 2024 / WEDNESDAY**

TIME/DURATION **09:00 AM - 11:00 AM / 02 Hour(s) 00 Minute(s)**

INSTRUCTIONS TO CANDIDATES :

1. Please read the instruction under each section carefully.
2. Candidates are reminded not to bring into examination hall/room any form of written materials or electronic gadget except for stationery that is permitted by the Invigilator.
3. Students who are caught breaching the Examination Rules and Regulation will be charged with an academic dishonesty and if found guilty of the offence, the maximum penalty is expulsion from the University.

(This Question Paper consists of **8** Printed Pages including front page)

DO NOT OPEN THE QUESTION PAPER UNTIL YOU ARE TOLD TO DO SO

This question paper contains TWO (2) sections. Please answer ALL questions in the answer booklet. [70 MARKS]

SECTION A (30 Marks)

There are THIRTY (30) questions this part of the examination paper. Answer ALL questions in the answer booklet provided.

1. Availability means _____ .

   A. someone who is not authorized makes a change to intentionally misrepresent something
   B. computer power surge corrupts a file or someone authorized to make a change accidentally deletes a file or enters incorrect information
   C. information can be accessed and modified by anyone authorized to do so
   D. None of the above

2. Authentication can be achieved through _____.

   A. VOIP
   B. application software
   C. operating system setup
   D. username and password.

3. Which of the following is an unintentional threat to the security of computer networks?

   A. Sabotage
   B. Computer failure
   C. DOS Attack
   D. Virus

4. I sent a data set {A,B,C,D} to a recipient which got received as {F,P,D,X}. This is an example of _____.

   A. data security is compromised
   B. data integrity is lost
   C. confidentiality is lost
   D. data availability is compromised

5. Which of this statement best describes "Access Control"?

   A. For each information resource that an organization wishes to manage, a list of users who have the ability to take specific actions can be created such as read, write and delete access.
   B. A virus that is released into a computer system to delete files
   C. A trojan horse that enters the information system via an email attachment
   D. A data integrity problem that arises when there is a database failure

6. Describe a "cookie".

A. A rogue software that contains worms that attach itself to information system.
B. a small file that contains information about you and your Web activities, which a Web site places on your computer.
C. A large file that takes up all the computer resources
D. None of the above

7. A hackers hired by companies to reveal security weaknesses within the firm's systems is referred to as a _____ .

A. black hat hacker
B. red Hat hacker
C. white hat hacker
D. cracker

8. Encryption is a process of _____.

A. determining which users are authorized to read, modify, add, and/or delete information.
B. encoding data upon its transmission or storage so that only authorized individuals can read it
C. computer power surge corrupts a file or someone authorized to make a change accidentally deletes a file or enters incorrect information
D. having the servers available all the time without disruption

9. All of the items listed below define methods of authentication **EXCEPT**_____ .

A. biometric
B. password system
C. tokens
D. anti-virus

10. A hardware firewall is a device that is connected to the network which _____ .

A. filters the packets based on a set of rules
B. allows file transfers
C. keeps logs only
D. allows communication traffic without rules

11. To prevent computer server from shutting down due to power failure, the best method is using _____ .

A. firewall that keeps the LAN secure at all times
B. an anti-virus that detects and deletes malware
C. universal Power Supply (UPS), a device that provides battery backup
D. virus checker that checks for malicious software.

12. An important part of data recovery is _____.

    A. firewall
    B. anti-virus
    C. intrusion detection
    D. having backup.

13. Sending email messages that look like those of legitimate businesses to ask users for personal data is called_____.

    A. phishing.
    B. pharming.
    C. evil twin.
    D. spamming.

14. PGP (Pretty Good Privacy) provides a confidentiality and authentication service that can be used for _____ .

    A. intrusion detection
    B. web services
    C. file Transfer
    D. electronic mail and file storage applications

15 Adware is a type of malicious software that is used for _____.

    A. Trojan horses
    B. salting
    C. forced advertising
    D. asymmetric encryption

16. Steganography is a technique of hiding a message in _____ .

    A. mail
    B. another file
    C. webpage
    D. SSH network

17. What type of attack has an organization experienced when an employee installs an unauthorized device on the network to view network traffic?

    A. Sniffing
    B. Spoofing
    C. Phishing
    D. Spamming

18. Sending of unsolicited and commercial bulk message over the internet is known as _____ .

A. pinging
B. hacking
C. spamming
D. handshaking

19. Which methods can be used to implement multifactor authentication?

A. IDS and IPS
B. tokens and hashes
C. VPNs and VLANs
D. passwords and fingerprints

20. In the context of IT security, what does the principle of "least privilege" refer to?

A. Granting users the maximum level of access to resources by default.
B. Providing users with access to all resources within the network.
C. Assigning users only the permissions necessary to perform their tasks.
D. Allowing users to modify access control policies at their discretion.

21. Which tool is design to probe a system for open ports?

A. Port Opener
B. Port scanner
C. Virus
D. Worm

22. Bob gets an email addressed from his bank, asking for his user ID and password. He then notices that the email has poor grammar and incorrect spelling. He calls up his bank to ask if they sent the email, and they promptly tell him they did not and would not ask for that kind of information. What is this type of attack called?

A. Pharming
B. Spam
C. Phishing
D. Vishing

23. SMIME is _____ .

A. a secure feature of instant messaging
B. a secure feature of voice transmissions
C. a secure method of protecting attachments in email
D. a virus that attacks emails

24. A worm is a _____.

A. malicious, self-replicating software program (popularly termed as 'malware') which affects the functions of software and hardware programs.
B. virus that is stored in the user's computer either temporarily for that session only or permanently on the hard disk.
C. trojan horse created by a website that is stored in the user's computer either temporarily for that session only or permanently on the hard disk.
D. none of the above

25. What is the primary focus of an anomaly-based Intrusion Detection System (IDS)?

A. Detecting known attack signatures
B. Identifying novel, previously unseen attacks
C. Establishing a baseline of normal network behaviour
D. Blocking all network traffic by default

26. What are strengths of Network based IDS?

A. Cost of ownership reduced
B. Malicious intent detection
C. Real time detection and response
D. All of the mentioned

27. What are the different ways to intrude?

A. Buffer overflows
B. Unexpected combinations and unhandled input
C. Race conditions
D. All of the mentioned

28. A false positive can be defined as _____.

A. is considered to be an alert that does not represent a real security concern
B. Unexpected attack on the system
C. Unusual traffic to a particular server
D. All of the mentioned

29. Intrusion detection does all the these **EXCEPT** _____.

A. anomaly detection
B. misuse detection
C. blocks e-payment
D. monitors your inbound and outbound network traffic

30. Signature based IDS does _____.

A. compares incoming traffic packets with known signatures
B. compares traffic input and output
C. tracking of traffic anomaly
D. none of the above

SECTION B **(40 Marks)**

There are TWO (2) questions in this part of the examination paper. Answer ALL question in the answer booklet.

Question 1 (20 marks)

Explain the concept of the CIA Triad in information security. Discuss each component (Confidentiality, Integrity, and Availability) in detail, and provide real-world examples of how compromising each aspect can lead to security breaches.

Question 2 (20 marks)

Discuss the significance of cybersecurity incident response planning in modern organizations.

***** END OF QUESTION PAPER *****