AL-MUSTAQBAL UNIVERSITY, COLLEGE OF SCIENCES
CYBER SECURITY DEPARTMENT

MIDTERM TEST EXAMINATION

COURSE	**:**	**PRINCIPLES OF CYBER SECURITY**
COURSE CODE	**:**	**CYSP115**
LECTURER	**:**	**DR. MUAMER MOHAMMED**
DATE	**:**	**19 FEBRUARY 2024**
DURATION	**:**	**2 HOURS**
SEMESTER	**:**	**SEMESTER/ FALL 2023/2024**
LOCATION	**:**	**JC502 & Cyber Security Lab**

INSTRUCTIONS TO CANDIDATES:

1. This question paper consists OF **THIRTY (30)** Multiple Choice Questions. **Answer all questions**.
2. Use the bubble sheet paper provided to write your answers.

EXAMINATION REQUIREMENTS:

NONE

DO NOT TURN THIS PAGE UNTIL YOU ARE TOLD TO DO SO

This examination paper consists of **SIX (6)** printed pages including the front page.

NAME: _____ **ID NO.:** _____

FINAL MARK **[10 MARKS]**
QUESTION 1 **[30 Marks]**

MULTIPLE CHOICE QUESTIONS.

Please **Select the Correct Answer** for each of the following questions. **(1 Mark)** for each Question. **Answer All Questions.**

1. Which one the following terms is frequently used to describe the tasks of securing information that is in a **digital format**?

a. network security **b.** information security **c.** physical security
d. logical security **e.** Digital Encryption

2. Which one the following **refers to Item that it has value** in an organization?

a. Asset **b.** Vector **c.** Threat
d. Risk **e.** Liability

3. Select the information protection item that **ensures that information is correct** and no unauthorized person or malicious software has modified that data.

a. availability **b.** confidentiality **c.** integrity
d. identity **e.** Information Authentication

4. Which of the following **ensures that data is accessible** to authorized users?

a. availability **b.** confidentiality **c.** integrity
d. identity **e.** Data Encryption

5. Which of the following protections **ensures that only authorized** parties can view the information?

a. security **b.** confidentiality **c.** integrity
d. identity **e.** Authentication

6. What is the name of the process that is used to establish whether or not a **user's identity is real?**

a. Availability **b.** Accountability **c.** Authentication
d. User Authorization **e.** Access Authorization

7. Which of the following is an authentication system that uses Triple Alliance AAA?

a. RADIUS **b.** TACACS **c.** OAuth

d. Shibboleth **e.** Kerberos

8. In information security, which of the following is an **example of a threat actor**?

a. Tornado that could destroy computer equipment **b.** Using computers to secure data

c. Regular Software Updates **d.** Rules changing too often e. Antivirus Software

9. What is a **common challenge** in keeping information safe nowadays?

a. Using paper documents **b.** No simple solution **c.** Rules changing too often

d. Letting authorized person access sensitive data **e.** All are correct

10. What is a **common reason** behind successful attacks on information security?

a. Hardware limitations **b.** Configuration issues **c.** Poorly designed software

d. Widespread vulnerabilities **e.** All are correct

11. What's important for getting people to be more careful with information?

a. Punishing mistakes **b.** Ignoring employees **c.** Making security culture

d. Using computers to Only secure data **e.** All are correct

12. Which of the following human characteristic is usually used for authentication?

a. Breathing pattern **b.** Smile expression **c.** Height

d. Fingerprint **e.** Heart Beets

13. Your enterprise recently approved using fingerprint scanners to authenticate employees who access restricted areas. You are assigned to conduct a study on how secure fingerprint authentication is. Which of the following should you report?

a. Fingerprint scanning is the safest available authentication method

b. Fingerprint scanners have the lowest false acceptance rate among other authentication methods.

c. Fingerprint scanners can be used for trickery in rare cases.

d. Fingerprint scanners have the highest false rejection rate among other authentication methods.

e. Regularly updating fingerprint scanners is crucial for maintaining security

14. What is a key characteristic of multifactor authentication (MFA)?

a. It relies solely on a single form of authentication.
b. It requires users to remember complex passwords.
c. It involves the use of multiple authentication factors.
d. It is less secure than single-factor authentication.
e. It is only applicable to certain users.

15. Which authentication method involves verifying the identity of a user by sending a temporary code to their mobile device or email

a. Voice Recognition **b.** One-Time Password **c.** Single Sign-On (SSO)
d. Fingerprint Authentication **e.** Face Recognition

16. You are asked to choose a secure authentication method **other than a username and password** for the employees to access the database. Which of the following should you choose?

a. Facial recognition **b.** Voice Recognition **c.** Knowledge Authentication
d. Behavioral Authentication **e.** Smart card authentication

17. Which of the following authentication methods belongs in the "**something you have**" category?

a. Keystroke dynamics **b.** Multifactor authentication **c.** Picture password
d. Voice recognition **e.** Behavioral Authentication

18. Which of the following authentication methods belongs in the "**something you know**" category?

a. Facial recognition **b.** Multifactor authentication **c.** Username & password
d. Physiological biometrics **e.** Behavioral Authentication

19. Which of the following authentication methods belongs in the "**something you are**" category?

a. Facial recognition **b.** Multifactor authentication **c.** Username & password
d. Picture password **e.** Behavioral Authentication

20. Which of the following authentication methods belongs in the " **something you do**" category?

a. Facial recognition **b.** Voice recognition **c.** Username & password
d. Iris recognition **e.** Behavioral Authentication

21.How does the **Single Sign-On** enhance secure authentication?

a. Implementing a single sign-on will reduce the time required for authentication

b Implementing a single sign-on will use multiple passwords for accessing multiple accounts and applications

c. Implementing a single sign-on will use biometric data for authentication

d. Implementing a single sign-on will restricting access to a single network

e. Implementing a single sign-on will use single password for accessing multiple accounts and applications

22. What is a key advantage **of Single Sign-On (SSO)** in terms of user credentials?

a. Users need to remember multiple sets of credentials

b. Users have a separate password for each application

c. Users can share their credentials with others

d. Users use a single set of credentials for all integrated applications

e. All are correct

23. Threat actors **focused on financial gain** often attack which of the following main target categories?

a. Product lists **b.** Individual users **c.** social media assets
d. Other services **e.** All are correct

24. What term describes a layered security approach that provides the comprehensive protection?

a. defense-in-depth **b.** diverse-defense **c.** limiting-defense
d. comprehensive-security **e.** All are correct

25. Which of the following is **a valid fundamental security principle**? (Choose all that apply.)

a. layering **b.** Limiting **c.** diversity

d. simplicity **e.** All are correct

26. Which of the following are considered threat actors for companies.

a. administrators **b.** individuals **c.** users

d. competitors **e.** All are correct

27. A secret combination of **letters, numbers, and/or characters** that only the **user should know**, is known as a:

a. token **b.** password **c.** biometric detail

d. challenge **e.** behavioral detail

28. What is the main weakness associated with the use of passwords?

a. human memory **b.** encryption technology **c.** handshake technology

d. human reliability **e.** authentication technology

29. The use of one authentication credential to access multiple accounts or applications is referred to as which of the following?

a. individual Sign On **b.** single Sign On **c.** unilateral Sign On

d. federated Sign On **e.** personal Sign On

30. W Which fundamental security principle focuses on the idea of restricting access to only authorized individuals or systems?

a. Limiting access **b.** Defense in Depth **c.** Regular Auditing

d. Strong Authentication **e.** Security through Obscurity

END OF QUESTION PAPER