BOWEN UNIVERSITY IWO, OSUN STATE
COLLEGE OF COMPUTING AND COMMUNICATION STUDIES
CYBER SECURITY PROGRAMME
B. SC. DEGREE FIRST SEMESTER EXAMINATION SESSION: 2023/2024
COURSE CODE: CYB 201 COURSE TITLE: FUNDAMENTALS OF CYBER SECURITY II
COURSE CREDIT: 2 DATE: TIME ALLOWED: 2 HOURS
INSTRUCTION: Answer all questions in section A and three (3) in section B

SECTION A

1. What is the primary focus of Signature-Based Intrusion Detection Systems (IDS)? A. Data integrity B. Anomaly detection C. Confidentiality D. Recognizing known malicious patterns
2. In Signature-Based IDS, what is the role of the Signature Database (S)? A. Determines anomaly scores B. Contains predefined signatures C. Establishes baseline behavior D. Executes well-formed transactions
3. What does the Matching Function (M) in Signature-Based IDS compare? A. Network packet data and system log entries B. Baseline behavior and observed behavior C. Input data and predefined signatures D. Well-formed transactions and certification rules
4. Which advantage is associated with Signature-Based IDS?
A. Effective at detecting unknown attacks B. High adaptability to evolving threats
C. Low false-positive rates D. Does not require signature updates
5. What limitation is specific to Signature-Based IDS?
A. Limited to known signatures B. High false-positive rates C. Ineffective against well-defined attacks D. Doesn't require regular updates
6. What is the primary focus of Anomaly-Based Intrusion Detection Systems (IDS)? A. Recognizing known malicious patterns B. Preventing unauthorized disclosure C. Identifying deviations from normal behavior D. Ensuring the consistency of data
7. What is the role of the Anomaly Detection Function (A) in Anomaly-Based IDS?
A. Matches predefined signatures B. Compares input data with the baseline C. Executes well-formed transactions D. Generates alert based on known patterns
8. What is the primary advantage of Anomaly-Based IDS? A. Low false-positive rates B. Effectiveness against known attacks C. Requires minimal user training D. Adaptable to evolving attack techniques

9. What limitation is specific to Anomaly-Based IDS? A. Requires constant signature updates B. Ineffective against novel threats C. High false-positive rates D. Limited to well-defined attacks

10. Which security model emphasizes data integrity by preventing information contamination from lower to higher integrity levels? A. Bell-LaPadula Model B. Biba Model C. Clark-Wilson Model D. Role-Based Access Control (RBAC)

11. Which network security component focuses on monitoring traffic for malicious activity and blocking attacks? A. Firewall Policies B. Intrusion Detection Systems (IDS) C. Mobile Device Management (MDM) D. Role-Based Access Control (RBAC)

12. In cloud security, what does the Shared Responsibility Model define? A. Access control policies B. Responsibilities of both the cloud provider and the customer C. Data integrity rules D. Well-formed transactions

13. What is the primary goal of operating system (OS) security? A. Enhancing performance B. Reducing system complexity C. Protecting resources, data, and users from unauthorized access D. Ensuring backward compatibility

14. In access control, what are entities seeking access to resources called? A. Permissions B. Objects C. Subjects D. Resources

15. Which type of access control allows the owner of a resource to set access controls? A. Role-Based Access Control (RBAC) B. Mandatory Access Control (MAC) C. Discretionary Access Control (DAC) D. Access Control Lists (ACL)

16. What is the purpose of authentication in the context of OS security? A. To control access to specific resources B. To monitor system activities C. To verify the identity of a user, system, or process D. To encrypt data in transit

17. Which authentication method uses physical or behavioral characteristics for identification? A. Multi-Factor Authentication (MFA) B. Username and Password C. Biometrics D. Role-Based Authentication (RBA)

18. What is used to log security-relevant events for monitoring and reviewing system activities? A. Firewalls B. Audit Trails C. Encryption D. Intrusion Detection Systems (IDS)

19. What does encryption involve in the context of OS security? A. Monitoring network traffic B. Preventing unauthorized access C. Converting data into a secure format D. Reviewing audit trails

20. How does the Principle of Least Privilege contribute to secure configurations? A. By granting maximum access to all users B. By enforcing strong password policies C. By

providing flexibility to resource owners D. By granting users and processes the minimum access required

21. Which access control model is suitable for environments with strict security requirements and predetermined access controls? A. Role-Based Access Control (RBAC) B. Discretionary Access Control (DAC) C. Mandatory Access Control (MAC) D. Least Privilege Principle (LPP)

22. Which term refers to the randomness of an encryption, making it harder for anyone to guess the key or input? A. Complexity factor B. Cipher strength C. Key randomness D. Encryption variability

23. What is the main focus of confidentiality in cryptography objectives? A. Ensuring message integrity B. Securing data in transit C. Restricting unauthorized access to the message contents D. Verifying identities of sender and recipient

24. What does non-repudiation mean in the context of cryptography? A. Ensuring only the intended recipient can decrypt the message B. Preventing unauthorized access C. Verifying identities of sender and recipient D. Sender cannot deny their reasons for creating the message

25. In public key cryptography, how many keys are used for encryption and decryption? A. One key B. Two keys C. Three keys D. Four keys

26. What is the private key in public key cryptography used for? A. Encrypting data B. Decrypting data C. Both encrypting and decrypting data D. Authenticating sender and recipient

27. What is the primary goal of steganography? A. Securing communications from outside observers B. Preventing unauthorized access C. Hiding information within a fake message D. Verifying identities of sender and recipient

28. In Secret Key Cryptography, what happens if the secret key is compromised during message transmission? A. The message is automatically decrypted B. The message remains secure C. The message becomes inaccessible D. The sender denies sending the message

29. Which method is NOT a form of steganography? A. Audio Steganography B. Image Steganography C. Symmetric Steganography D. Text Steganography

30. What is the primary goal of Network or Protocol Steganography? A. Concealing information within an image B. Hiding data within an audio signal C. Using network protocols as cover objects D. Ensuring message integrity **30 Marks**

SECTION B

Question One

(a) i. Write an exhaustive note on Cryptography. **7 MarKs**

ii. Explain the principle of least privilege in the context of operating system security. **4 Marks**

(b) Discuss the difference between host-based and network-based intrusion detection systems. **4 Marks**

(c) Describe a scenario where an IDS alerts administrators to a potential security threat and explain the subsequent actions. **5 Marks**

Question Two

(a) i. Discuss formal security models. **7 Marks**

ii. Explain the concept of information flow control in formal security models. **4 Marks**

(b) How can the Bell-LaPadula model be applied to control information flow in a military database? **4 Marks**

(c) Compare symmetric and asymmetric encryption, highlighting scenarios where each is suitable. **5 Marks**

Question Three

(a) i. Discuss Steganography. **7 Marks**

ii. Differentiate between cover carriers and stego carriers in the context of steganography. **4 Marks**

(b) Explain how firewalls operate as a critical component of network security. **5 Marks**

(c) Outline strategies to mitigate the impact of a DDoS attack on a web server. **4 Marks**

Question Four

(a) i. Differentiate between viruses and worms, and explain how each spreads. **5 Marks**

ii. Provide recommendations to prevent the spread of malware within a corporate network. **5 Marks**

(b) Explain how the use of two-factor authentication enhances the security of online financial transactions. **5 Marks**

(c) Describe the security measures implemented in an electronic voting system to ensure the integrity of the voting process. **5 Marks**