11. The most common authentication mechanism used in operating systems.
a) Digital signature
b) Iris recognition
c) Password comparison
d) Face recognition

12. A security tool by which the executable memory is separated from data memory for each use making it harder for attacks to overwrite code.
a) Two pairs of base/bounds registers
b) Fence register
c) Base/bounds registers
d) Fixed fence

13. A type of countermeasures that can be used for the system recovery in case an intrusion does succeed.
a) Detection
b) Response
c) Prevention
d) Deflection

14. Time-based authentication can be implemented through .....
a) Fingerprint
b) Tokens
c) Passwords
d) Security questions

15. Which of the following techniques helps in implementing the authentication?
a) Symmetric encryption
b) Asymmetric encryption
c) DES
d) AES

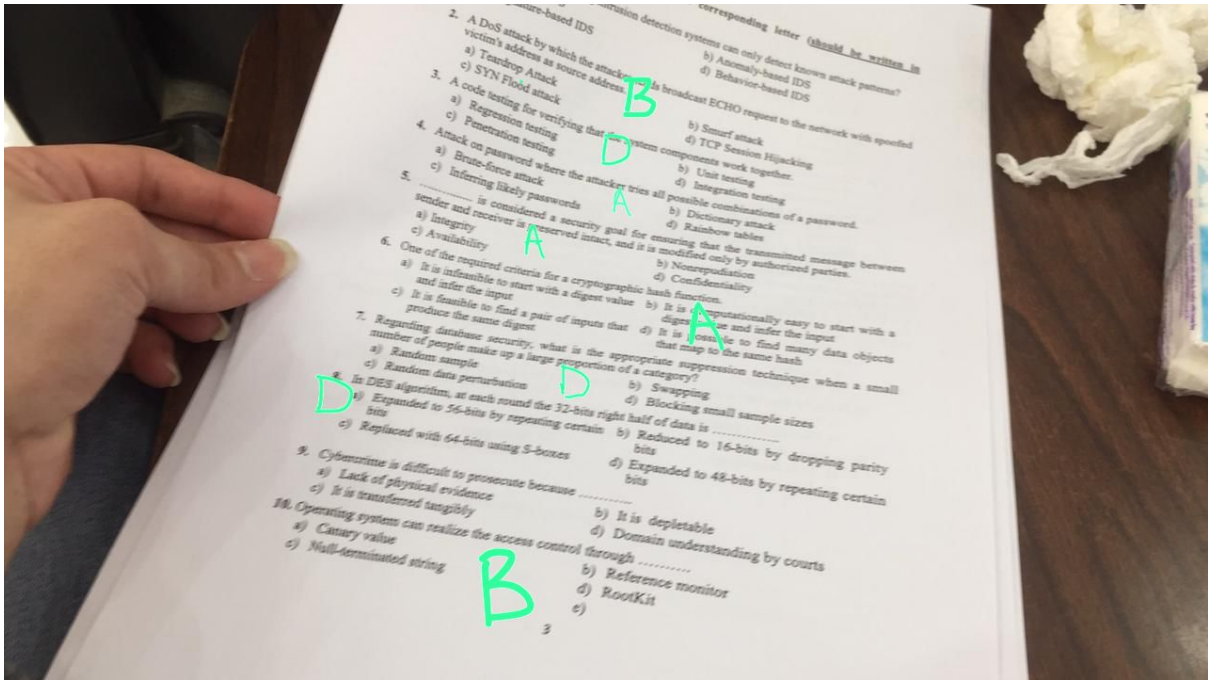
16. A measure by which the DBMS ensures that the value of a specific data field is changed onl by authorized parties.
a) Database integrity
b) Element accuracy
c) Database Reliability
d) Element integrity

17. Which of the following statements is NOT true?
a) Law is applied to everyone
b) Ethics are enforced by courts
c) Ethics are chosen personally
d) Ethics are interpreted by each indivi

18. A security tool by which the program is divided into separate logical pieces or parts, a part has its own set of access rights.
a) Sandbox
b) Paging
c) Segmentation
d) Tagged Architecture

19. In digital signature technique, the receiver can verify the signature of the sender using
a) The sender's private key
b) The receiver's private key
c) The sender's public key
d) The receiver's public key

20. A theory of ethics that is concerned with the consequences of actions to individual a
a) Rule-deontology
b) Teleological
c) The right to privacy
d) Universal natural rules



...ure-based IDS
...ruption detection systems can only detect known attack patterns?
b) Anomaly-based IDS
d) Behavior-based IDS

2. A DoS attack by which the attacker sends a broadcast ECHO request to the network with spoofed victim's address as source address
a) Teardrop Attack
b) Smurf attack
c) SYN Flood attack
d) TCP Session Hijacking

3. A code testing for verifying that system components work together.
a) Regression testing
b) Unit testing
c) Penetration testing
d) Integration testing

4. Attack on password where the attacker tries all possible combinations of a password.
a) Brute-force attack
b) Dictionary attack
c) Inferring likely passwords
d) Rainbow tables

5. _____ is considered a security goal for ensuring that the transmitted message between sender and receiver is preserved intact, and it is modified only by authorized parties.
a) Integrity
b) Nonrepudiation
c) Availability
d) Confidentiality

6. One of the required criteria for a cryptographic hash function.
a) It is infeasible to start with a digest value and infer the input
b) It is computationally easy to start with a digest value and infer the input
c) It is feasible to find a pair of inputs that produce the same digest
d) It is infeasible to find many data objects that map to the same hash

7. Regarding database security, what is the appropriate suppression technique when a small number of people make up a large proportion of a category?
a) Random sample
b) Swapping
c) Random data perturbation
d) Blocking small sample sizes

8. In DES algorithm, at each round the 32-bits right half of data is _____
a) Expanded to 56-bits by repeating certain bits
b) Reduced to 16-bits by dropping parity bits
c) Replaced with 64-bits using S-boxes
d) Expanded to 48-bits by repeating certain bits

9. Cybercrime is difficult to prosecute because _____
a) Lack of physical evidence
b) It is depletable
c) It is transferred tangibly
d) Domain understanding by courts

10. Operating system can realize the access control through _____
a) Canary value
b) Reference monitor
c) Null-terminated string
d) RootKit
e)

B
D
A
A
A
D
D
B

3