سيـــســـــــــــــــــ ١ ـــــــــــــــــكـــو

1. Which of the following type of access control seeks to discover evidence of unwanted, unauthorized, or illicit behavior or activity?
A. Preventive **B.** Deterrent **C.** Detective **D.** Corrective

2. Can you define and detail the aspects of password selection that distinguish good password choices from ultimately poor password choices?
A. Difficult to guess or unpredictable **B.** Meet minimum length requirements
C. Meet specific complexity requirements **D.** All of the above

➔**3.** Which of the following is most likely to detect DoS attacks?
A. Host-based IDS **B.** Network-based IDS
C. Vulnerability scanner **D.** Penetration testing

➔ **4.** Which of the following is considered a denial-of-service attack?
A. Pretending to be a technical manager over the phone and asking a receptionist to change their password
B. While surfing the Web, sending to a web server a malformed URL that causes the system to use 100 percent of the CPU to process an endless loop
C. Intercepting network traffic by copying the packets as they pass through a specific subnet
D. Sending message packets to a recipient who did not request them simply to be annoying

5. At which layer of the OSI model does a router operate?
A. Network layer **B.** Layer 1 **C.** Transport layer **D.** Layer 5

➔**6.** Which type of firewall automatically adjusts its filtering rules based on the content of the traffic of existing sessions?
A. Static packet filtering **B.** Application-level gateway
C. Stateful inspection **D.** Dynamic packet filtering

7. A VPN can be established over which of the following?
A. Wireless LAN connection B. Remote access dial-up connection
C. WAN link D. All of the above

➔ 8. Email is the most common delivery vehicle for which of the following?
A. Viruses B. Worms C. Malicious code D. All of the above

9. The CIA Triad is comprised of what elements?
A. Contiguous, interoperable, arranged B. Authentication, authorization,account
C. Capable, available, integral D. Availability, confidentiality, integrity

10. Which of the following is not a required component in the support of accountability?
A. Auditing B. Privacy C. Authentication D. Authorization

11. Which of the following is not a defense against collusion?
A. Separation of duties B. Restricted job responsibilities
C. Group user accounts D. Job rotation

14. Which one of the following is a layer of the ring protection scheme that is not normally implemented in practice?
A. Layer 0 **B.** Layer 1 **C.** Layer 3 **D.** Layer 4

15. What is the last phase of the TCP/IP three-way handshake sequence?
A. SYN packet **B.** ACK packet **C.** NAK packet **D.** SYN/ACK packet

16. Which one of the following vulnerabilities would best be countered by adequate parameter checking?
A. Time-of-check-to-time-of-use **B.** Buffer overflow
C. SYN flood **D.** Distributed denial of service

17. What is the value of the logical operation shown here?
X: 0 1 1 0 1 0
Y: 0 0 1 1 0 1
X ⊕ Y: ? The ⊕ symbol represents the XOR function.
A. 0 1 1 1 1 1
B. 0 1 1 0 1 0
C. 0 0 1 0 0 0
D. 0 0 1 1 0 1

18. what type of cipher are letters of plain-text message rearranged ?
A. Substitution **B.** Block **C.** Transposition **D.** One-time pad

19. What is the length of a message digest produced by the MD5 algorithm?
A. 64 bits **B.** 128 bits **C.** 256 bits **D.** 384 bits

20. If Renee receives a digitally signed message from Mike, what key does she use to verify that the message truly came from Mike?
A. Renee’s public key **B.** Renee’s private key
C. Mike’s public key **D.** Mike’s private key

21. Which of the following statements is true?
A. The less complex a system, the more vulnerabilities it has.
B. The more complex a system, the less assurance it provides.
C. The less complex a system, the less trust it provides.
D. The more complex a system, the less attack surface it generates.

22. Ring 0, from the design architecture security mechanism known as protection rings, can also be referred to as all but which of the following:
A. privileged mode **B.** supervisory mode
C. system mode **D.** user mode

28. Auditing is a required factor to sustain and enforce what?
A. Accountability **B.** Confidentiality **C.** Accessibility **D.** Redundancy

31. Which of the following represent natural events that can pose a threat or risk to an organization?
A. Earthquake **B.** Flood **C.** Tornado **D.** All of the above

➔29. …is the process of verifying or testing the validity of a claimed identity.
A. Identification B. Authentication C. Authorization D. Accountability

30. Which of the following is an example of a Type 2 authentication factor?
A. "Something you have," such as a smart card, ATM card, token device, & memory card
B. "Something you are," such as fingerprints, voice print, retina pattern, iris pattern, face shape, palm topology, and hand geometry
C. "Something you do," such as type a passphrase, sign your name, and speak a sentence
D. "Something you know," such as a password, personal identification number (PIN), lock combination, passphrase, mother's maiden name, and favorite color

31. Which is not a reason why using passwords alone is a poor security mechanism?
A. users choose easy-to-remember passwords that are easy to guess or crack.
B. Randomly generated passwords are hard to remember
C. Short passwords can be discovered quickly in brute-force attacks only when used against a stolen password database file.
D. Passwords can be stolen through many means

32. Which of the following is not a valid means to improve the security offered by password authentication?
A. Enabling account lockout controls
B. Enforcing a reasonable password policy
C. Using password verification tools and password-cracking tools against your password database file
D. Allowing users to reuse the same password

33. What can be used as an authentication factor that is a behavioral or physiological characteristic unique to a subject?
A. Account ID **B.** Biometric factor **C.** Token **D.** IQ

36. What type of detected incident allows the most time for an investigation?
A. Compromise **B.** DOS **C.** Malicious code **D.** Scanning

38. What is the point of a secondary verification system?
A. To verify the identity of a user
B. To verify the activities of a user
C. To verify the completeness of a system
D. To verify the correctness of a system

14. A network environment that uses discretionary access controls is vulnerable to which?
A. SYN flood **B.** Impersonation **C.** DOS **D.** Birthday attack

15. What is the most important aspect of a biometric device?
A. Accuracy **B.** Acceptability **C.** Enrollment time **D.** Invasiveness

16. Which of the following is not an example of a deterrent access control?
A. Encryption **B.** Auditing **C.** Awareness training **D.** Antivirus

17. Kerberos provides the security services of …… protection for authentication traffic.
A. availability and nonrepudiation **B.** confidentiality and authentication
C. confidentiality and integrity **D.** availability and authorization

18. Which of the following forms of authentication provides the strongest security?
A. Password and a PIN **B.** One-time password
C. Passphrase and a smart card **D.** Fingerprint

19. Which of the following is the least acceptable form of biometric device?
A. Iris scan **B.** Retina scan **C.** Fingerprint **D.** Facial geometry

20. Why is separation of duties important for security purposes?
A. It ensures that multiple people can do the same job.
B. It prevents an organization from losing important information when they lose important people.
C. It prevents any single security subject (person) from being able to make major security changes without involving other subjects.
D. It helps subjects concentrate their talents where they will be most useful.