**MIS5214 Mid-Term Exam**

Answer Sheet

1. Which of the following is not a characteristic of a conceptual data model:
   A. Data objects
   B. Properties of data objects
   C. Implementation details
   D. Relationships between objects and cardinalities of relationships

2. John has been told to report to the board of directors with a vendor-neutral enterprise architecture framework that will help the company reduce fragmentation that results from misalignment of IT and business processes. Which of the following frameworks should he suggest?
   A. DoDAF
   B. CMMI
   C. ISO/IEC 42010
   D. TOGAF

3. The values of an attribute of a data entity can only have the following set of operators applied to it:
   =, < >, <, >, +, -
   which one of Stevens' measurement levels best characterizes the entity's attribute?
   A. Nominal
   B. Ordinal
   C. Ratio
   D. Interval

4. An IS auditor finds out-of-range data values in some attributes of tables stored within a database. Which of the following controls should the IS Auditor recommend to avoid this situation?
   A. Log all table update transactions
   B. Implement integrity constraints in the database
   C. Implement before-and-after image reporting
   D. Use tracing and tagging

5. The database administrator (DBA) suggests that database efficiency can be improved by de-normalizing some tables. This would result in
   A. unauthorized accesses
   B. loss of confidentiality
   C. increased redundancy
   D. application malfunctions

6. Which of the following shows the OSI layer sequence as layers 2, 5, 7, 4, and 3
   A. Data link, transport, application, session, and network
   B. Data link, session, application, transport, and network
   C. Network, transport, application, session, and presentation
   D. Network, session, application, network, and transport

7. What takes place at the data link layer?
   A. End-to-end connection
   B. Dialog control
   C. Framing
   D. Data Syntax

8. A characteristic of User Datagram Protocol (UDP) in network communications is:
   A. Packets may arrive out of order
   B. Increased communication latency
   C. Incompatibility with packet broadcast
   D. Error correction may slow down processing

9. Systems that are built on the OSI framework are considered open systems. What does this mean?
   A. They are built with international protocols and standards so they can choose what types of systems they will communicate with.
   B. They are built with internationally accepted protocols and standards so they can easily communicate with other systems.
   C. They do not have authentication mechanisms configured by default.
   D. They have interoperability issues.

10. Which of the following protocols work in the following layers: application, data link, network, and transport?
    A. FTP, ARP, TCP, and UDP
    B. FTP, ICMP, IP, and UDP
    C. TFTP, RARP, IP, and ICMP
    D. TFTP, ARP, IP, and UDP

11. Which best describes the IP protocol?
    A. A connection-oriented protocol that deals with the addressing and routing of packets
    B. A connection-oriented protocol that deals with sequencing, error detection, and flow control
    C. A connectionless protocol that deals with the addressing and routing of packets
    D. A connectionless protocol that deals with dialog establishment, maintenance, and destruction

12. Which of the following OSI layers includes protocols that handle encryption, compression, and processing based on file format extensions?
    A. Layer 8 - User
    B. Layer 7 - Application
    C. Layer 6 - Presentation
    D. Layer 2 - Data Link

13. Use the following scenario to answer this question: Don is a security manager of a large medical institution. One of his groups develops proprietary software that provides distributed computing through a client/server model. He has found that some of the systems that maintain the proprietary

software have been experiencing half-open denial-of-service attacks. Some of the software is antiquated and still uses basic remote procedure calls, which has allowed for masquerading attacks to take place.

What should Don's team put in place to stop the masquerading attacks that have been taking place?

A. Dynamic packet filter firewall
B. Secure RPC
C. ARP spoofing protection
D. Disable unnecessary ICMP traffic at edge routers

14. Layer 2 of the OSI model has two sublayers. What are those sublayers, and what are two IEEE standards that describe technologies at that layer?
    A. LCL and MAC; IEEE 802.2 and 802.3
    B. LCL and MAC; IEEE 802.1 and 802.3
    C. Network and MAC; IEEE 802.1 and 802.3
    D. LLC and MAC; IEEE 802.2 and 802.3

15. An Information System (IS) auditor is reviewing an organization's disaster recovery plan (DRP) implementation. The project was completed on time and on budget. During the review, the auditor uncovers several areas of concern. Which of the following presents the greatest risk?
    A. Testing of the DRP has not been performed
    B. The business impact analysis (BIA) was conducted, but the results were not used
    C. The disaster recovery strategy does not specify use of a hot site
    D. The disaster recovery project manager for the implementation recently left the organization

16. Which of the following is the best method for determining the criticality of each application system in the production environment?
    A. Interview the application programmers
    B. Perform a gap analysis
    C. Perform a business impact analysis (BIA)
    D. Review the most recent application audits

17. Which of the following groups is the best source of information for determining the criticality of application systems as part of a business impact analysis (BIA) ?
    A. Business process owners
    B. IT management
    C. Senior business management
    D. Industry experts

18. Development of the Business Continuity Plan (BCP) focuses on the enterprises mission critical infrastructure which includes
    A. People, processes, and technology
    B. Physical, technical and administrative controls
    C. Responsible, accountable, consulted, and informed (RACI) managers
    D. Firewalls, switches, routers, and intrusion detection systems

19. According to The City of New York's Citywide Information Security Policy, the organizational role responsible for determining the appropriate value and categorization of the information generated by the owner or agency is:
    A. Data Custodian
    B. Data Steward
    C. Enterprise Risk Committee
    D. Chief Information Officer (CIO)

20. A vulnerability is:
    A. Strategy for dealing with risk
    B. Potential of loss from an attack
    C. Weakness that makes targets susceptible to an attack
    D. Potential for the occurrence of a harmful event such as an attack

21. Which of the following factors should an IS auditor primarily focus on when determining the appropriate level of protection for an information assessment?
    A. Results of a risk assessment
    B. Relative value to the business
    C. Results of a vulnerability assessment
    D. Cost of security controls

22. A poor choice of passwords and unencrypted data transmissions over unprotected communication lines are examples of:
    A. Vulnerabilities
    B. Threats
    C. Probabilities
    D. Impacts

23. An information system contains three information types, each with impact ratings listed below:
    Information Type 1 = {(Confidentiality, MODERATE), (Integrity, LOW), (Availability, LOW)}
    Information Type 2 = {(Confidentiality, LOW), (Integrity, LOW), (Availability, MODERATE)}
    Information Type 3 = {(Confidentiality, LOW), (Integrity, LOW), (Availability, LOW)}
    What is the security categorization of the information system?
        A. {(Confidentiality, MODERATE), (Integrity, LOW), (Availability, LOW)}
        B. {(Confidentiality, LOW), (Integrity, LOW), (Availability, MODERATE)}
        C. {(Confidentiality, LOW), (Integrity, LOW), (Availability, LOW)}
        D. None of the above

24. Which of the following network components is primarily set up to serve as a security measure by preventing unauthorized traffic between different segments of the network?
    A. Layer 2 switches
    B. Routers
    C. Firewalls

D. Virtual local area networks (VLANS)

25. A company is implementing a Dynamic Host Configuration Protocol (DHCP). Given that the following conditions exist, which represents the greatest concern?
    A. Most employees use laptops
    B. A packet filtering firewall is used
    C. Access to a network port is not restricted
    D. The IP address space is smaller than the number of PC's

26. During a review of intrusion detection logs, an IS auditor notices traffic coming from the Internet which appears to originate from the internal IP address of the company payroll server. Which of the following malicious activities would most likely cause this type of result?
    A. A denial-of-service (DoS) attack
    B. A man-in-the middle attack
    C. Spoofing
    D. Port scanning

27. Which of the following protocols is considered connection-oriented?
    A. ICMP
    B. TCP
    C. IP
    D. UDP

28. Use the following scenario to answer this question: Don is a security manager of a large medical institution. One of his groups develops proprietary software that provides distributed computing through a client/server model. He has found that some of the systems that maintain the proprietary software have been experiencing half-open denial-of-service attacks. Some of the software is antiquated and still uses basic remote procedure calls, which has allowed for masquerading attacks to take place.
    What type of client ports should Don make sure the institution's software is using when client-to-server communication needs to take place?
    A. Dynamic
    B. Registered
    C. Well known
    D. Free

29. When reviewing the configuration of network devices, an information system auditor should first identify:
    A. the good practices for the types of network devices deployed
    B. whether components of the network are missing
    C. the importance of the network devices in the topology
    D. whether subcomponents of the network are being used appropriately

30. Which of the following types of firewalls cannot make access decisions based on protocol commands?
    A. Packet filtering
    B. Stateful inspection
    C. Circuit-level proxy
    D. Application-level proxy

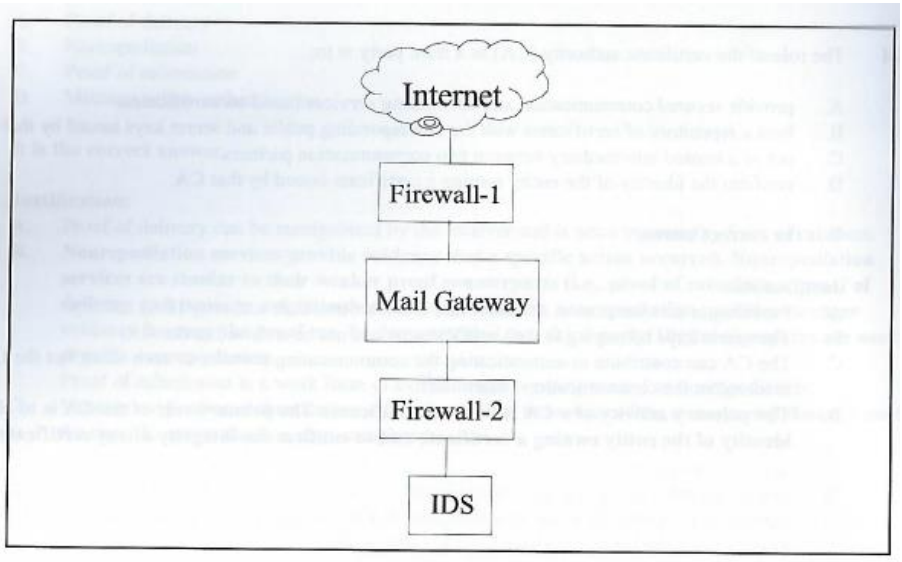
31. Which of the following types of firewalls offers the benefit of allowing any type of traffic outbound, but permits only response traffic inbound to a randomly identified port that it chooses outside the range of the well-known ports?
    A. Dynamic packet-filtering
    B. Stateful inspection
    C. Kernal proxy
    D. Next-Generation Firewall (NGFW)

32. Which of the following architectures lacks defense in depth and is a vulnerable single point of failure?
    A. DMZ
    B. Dual-Homed Firewall
    C. Screened Subnet
    D. Screen Host Firewall

33. How many security control families are described and detailed in NIST 800-53 Revision 4 “Security and Privacy Controls for Federal Information Systems and Organizations” ?
    A. 18 Control families presented mostly alphabetically
    B. 5 Control families organized into functional areas: Identify, Protect, Detect, Respond, and Recover
    C. 3 Control Families organized into classes: Management, Operational, and Technical
    D. 3 Control Families organized by impact categorization: Low, Moderate, and High

34. With respect to IT network security domains which of the following is false:
    A. Resources within each domain are working under the same security policy and managed by the same group
    B. Different domains are separated by logical boundaries created by security components that enforce security policy for each domain
    C. Logical and physical resources are available to users, processes and applications
    D. Routers are prohibited from connecting two Local Area Network security domains of different impact categorizations

35. With reference to the figure below, Email traffic from the Internet is routed via Firewall-1 to the mail gateway. Mail is routed from the mail gateway, via Firewall-2, to the mail recipients in the internal network. Other traffic is not allowed. For example, the firewalls do not allow direct traffic from the Internet to the internal network. The intrusion detection system (IDS) detects traffic for the internal network that did not originate from the mail gateway.



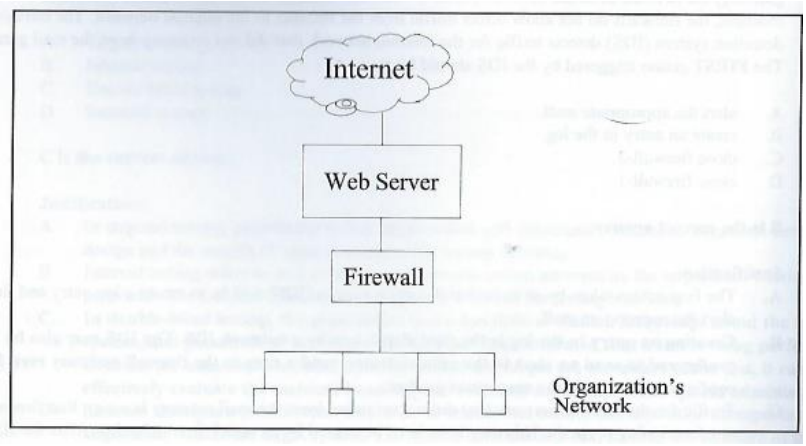

The first action triggered by the IDS should be to:

A. Close Firewall-1
B. Close Firewall-2
C. Create an entry in the log
D. Alert the appropriate staff

36. Which of the following intrusion detection systems (IDSs) will most likely generate false alarms resulting from normal network activity?
A. Signature
B. Statistical-based
C. Rule-based
D. Host-based

37. When reviewing an intrusion detection system (IDS), an IS auditor should be most concerned about which of the following?
A. Number of nonthreatening events identified as threatening
B. Attacks not being identified by the system
C. Reports/logs being produced by an automated tool
D. Legitimate traffic being blocked by the system

38. With reference to the figure below,




to detect attack attempts that the firewall is unable to recognize, an evaluator of an information system's security should recommend placing a network intrusion detection system (IDS) between the:

A. Internet and the firewall
B. Internet and the web server
C. Web server and the firewall
D. Firewall and the organization's network

39. Which of the following provides the most relevant information for proactively strengthening security settings?

A. Bastion host
B. Honeypot
C. Intrusion detection system
D. Intrusion prevention system

40. Mutual authentication can be circumvented through which of the following attacks?

A. Denial-of-service
B. Man-in-the-middle
C. Key logging
D. Brute force

41. Which of the following are important aspects of secure computer identities:

A. Diffusion and confusion
B. Uniqueness, non-descriptiveness and issuance
C. Public information and private information
D. Something you know, something you have, something you are

42. In electronic authentication, assurance is defined as all of the following, except:

A. The amount of certainty in the vetting process used to establish the identity of the individual to whom the credential was issued
B. The degree of certainty that the user has presented an identifier that refers to his or her identity

C. The degree of confidence that the individual who uses the credential is the individual to whom the credential was issued
D. The degree of certainty that the user has the authorization to access a network resource

43. What are identity authentication assurance levels used for?
    A. Providing confidentiality, integrity and availability impact categories for authentication errors
    B. Selecting controls that mitigate risks associated with impacts resulting from authentication errors in electronic transactions
    C. Mapping FIPS199 security categorization levels to e-authentication levels
    D. Providing high confidence in the asserted identity's validity

44. You have been asked to evaluate the security architecture and controls of an information system used to support the community and social services programs at a governmental agency. Your research has revealed that the information system will contain the following information types with their associated security categories:
    - Homeownership promotion: {(confidentiality, Low), (integrity, Low), (availability, Low)}
    - Community & regional development: {(confidentiality, Low), (integrity, Low), (availability, Low)}
    - Social services: {(confidentiality, Low), (integrity, Low), (availability, Low)}
    - Postal services: {(confidentiality, Low), (integrity, Moderate), (availability, Moderate)}

    Your review of the relevant NIST special publication guide (NIST SP800-60v2r1) determined that the public's trust in the agency may be lost as a result of breaches in integrity and availability of postal services information. This loss may harm the agency's programs and its ability to serve the public's interests. According to Office of Management Budget's memorandum on e-Authentication Guidance for Federal Agencies (OMB M—04-04), which level of confidence is needed for the e-authentication assurance of the information system?

    A. Level 1
    B. Level 2
    C. Level 3
    D. Level 4

45. When very high confidence is needed in the vetting process used to establish the identity of the individual to whom the credential was issued, how should the vetting process be implemented?
    A. Either in-person or remote registration, with the individual providing personally identifying information, and a government picture ID (in person) or ID number (remote), and either utility or financial account information
    B. In-person or remote registration with the individual providing personally identifying information, a government picture ID, a second government ID, and utility or financial account information, and biometric information
    C. In-person with the individual providing personally identifying information, a government picture ID, a second government ID, utility or financial account information, and biometric information
    D. In-person with the individual providing personally identifying information, a government picture ID, utility or financial account information, and biometric information

46. According to NIST special publication guide (NIST SP800-60v2r1), multi-factor e-authentication can be achieved with:
    A. Something you know and something you are
    B. Something you have and something you are
    C. Something you know, something you have, and something you are
    D. Something you have and something else you have

47. In e-Authentication the claimant authenticates to a system or application over a network by proving that he or she:
    A. Is an applicant to a Registration Authority
    B. Has credentials registering them as a subscriber of a Credential Service Provider
    C. Is in possession of a token provided by a Credential Service Provider
    D. Can provide a valid token authenticator generated from a token he or she possesses

48. On completion of the e-authentication process, the Verifier generates an assertion containing the results of the authentication and provides it to the Requesting Party. Examples of assertions include all the following, except:
    A. Symmetric key-based Kerberos tickets
    B. Cookies
    C. X.509 public key certificates
    D. Security Assertions Markup Language documents

49. Used in combination together, what is the highest e-Authentication level provided by an Out of Band Token and a Single Factor One Time Password Device?
    A. Little or no confidence in the asserted identity's validity
    B. Some confidence in the asserted identity's validity
    C. High confidence in the asserted identity's validity
    D. Very high confidence in the asserted identity's validity

50. A Multi-Factor Software Cryptographic Token can support which e-Authentication levels?
    A. Level 1, Level 2, Level 3, and Level 4
    B. Level 1, Level 2, and Level 3
    C. Level 1 and Level 2
    D. Level 3 and Level 4