MIS5214 Midterm Exam Spring-2018

Answer Sheet

1. **Conceptual Design** - Which of the following is not a characteristic of a conceptual model of an information system:
   A. Categories of components making up the system
   B. General contents or properties of system components
   C. Implementation details
   D. Relationships between components

2. **Enterprise Architecture** – Which of the following is a vendor-neutral enterprise architecture framework that helps reduce fragmentation resulting from misalignment of IT and business processes?
   A. UML - Unified Modeling Language
   B. TOGAF - The Open Data Group Architecture Framework
   C. CMMI - Capability Maturity Model Integration
   D. ISO/IEC 42010

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

5. **OSI Stack** - 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.

6. **OSI Stack** - 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

7. **OSI Stack** - 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

8. **OSI Stack** – A team of developers is creating proprietary software that provides distributed computing through a client/server model. They found that 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 the team put in place to stop the masquerading attacks that have been taking place?
   A. Dynamic packet filter firewall
   B. ARP spoof protection
   C. Secure RPC
   D. Disable unnecessary ICMP traffic at edge routers

9. **OSI Stack** - Layer 2 of the OSI model has two sublayers. What are those sublayers?
   A. LLC and MAC
   B. LCL and MAC
   C. LCL and PPP
   D. Network and MAC

10. **Risk: Vulnerabilities** - 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

11. **Risk: Assessment** - An information system contains three information types, each with impact ratings listed below:
    Information Type 1 = {(Confidentiality, LOW), (Integrity, LOW), (Availability, LOW)}
    Information Type 2 = {(Confidentiality, LOW), (Integrity, LOW), (Availability, LOW)}
    Information Type 3 = {(Confidentiality, HIGH), (Integrity, MODERATE), (Availability, LOW)}
    What is the overall security categorization of the information system?
    A. LOW
    B. HIGH
    C. Confidentiality, Integrity, Availability
    D. SENSITIVE

12. **Network Security: Firewalls** - 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)

13. **Network Security: Firewalls** - 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

14. **Exploits** - 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

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

16. **Network Security: Firewalls** – A security manager at a large medical institution oversees a group that develops a proprietary software application that provides distributed computing through a client/server model. She 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 the security manager make sure the institution's software is using when client-to-server communication needs to take place?
    A. Registered
    B. Well known
    C. Dynamic
    D. Free

17. **Network Security: Domains** - 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

18. **Network Security: Firewalls** - Which of the following types of firewalls cannot make access decisions based on protocol commands?
    A. Application-level
    B. Kernal proxy

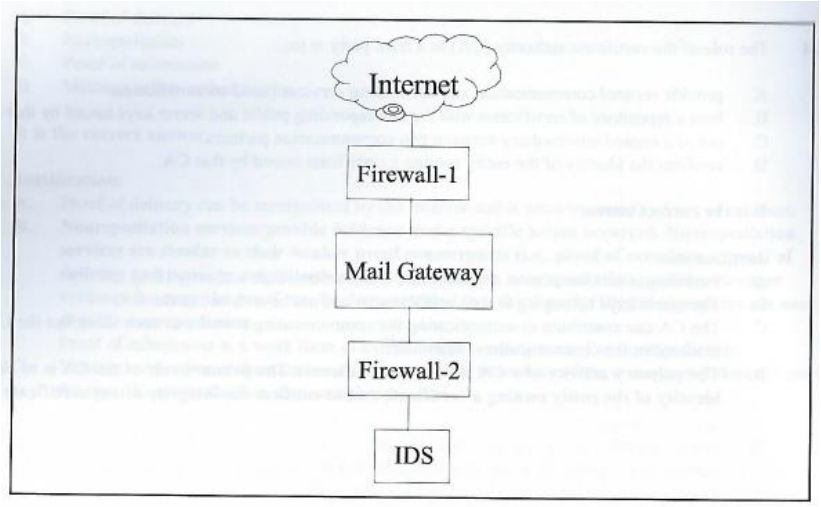
C. Circuit-level proxy
D. Next-generation

19. **Network Security: Firewalls** - 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. Stateful inspection
    B. Kernal proxy
    C. Dynamic packet-filtering
    D. Next-Generation Firewall (NGFW)

20. **Network Security: Firewalls** - 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

21. **Network Security: Domains** - 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. Routers are prohibited from connecting two Local Area Network security domains of different impact categorizations
    C. Different domains are separated by logical boundaries created by security components that enforce security policy for each domain
    D. Logical and physical resources are available to users, processes and applications

22. **Network Security: Firewalls** - 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.



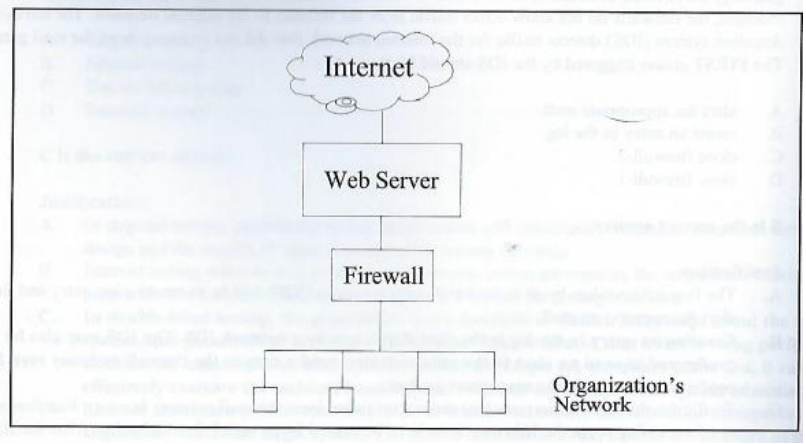
The first action triggered by the IDS should be to:

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

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

24. **Network Security: IDS -** 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

25. **Network Security: Firewalls -** 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. Firewall and the organization's network
C. Internet and the web server
D. Web server and the firewall

26. **Exploits** - 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

27. **Network Architecture: Routers** - If inadequate, which of the following would be the most likely contributor to the success of a denial-of-service (DoS) attack?
    a. Router configuration and rules
    b. Design of the internal network
    c. Updates to the router system software
    d. Audit testing and review techniques

28. **Network Architecture** – All of the following is true about the Screened Subnet Architecture except:
    a. It is used to create a DMZ.
    b. It is created using a router and two firewalls.
    c. It includes the Screened-Host Architecture.
    d. It has similar defense in depth characteristics as the Dual-Homed Firewall Architecture.

29. **Control Families** – The general classes of information system security controls identified in the National Institute of Standards and Technology's Special Publication entitled "Guide for Developing Security Plans for Federal Information Systems" are:
    a. Identification and Authentication, Access Control, Audit and Accountability, System and Communication Protection
    b. Management, Operational, Technical
    c. Security, Accreditation, Security Assessments
    d. Identify, Protect, Detect, Respond, Recover

30. **IDS** - There are several types of intrusion detection systems (IDSs). What type of IDS builds a profile of an environment's normal activities and assigns an anomaly score to packets based on the profile?
    a. State-based
    b. Statistical anomaly-based
    c. Misuse-detection system
    d. Protocol signature-based

31. **IDS:** When installing an intrusion detection system (IDS), which of the following is most important?
    a. Properly locating it in the network architecture
    b. Preventing denial-of-service (DoS) attacks
    c. Identifying messages that need to be quarantined
    d. Minimizing the rejection errors

32. **IDS -** An information system auditor reviewing the implementation of an intrusion detection system (IDS) should be most concerned if:
    a. IDS sensors are placed outside the firewall
    b. a behavior-based IDS is causing many false alarms
    c. a signature-based IDS is weak against new types of attacks
    d. the IDS is used to detect encrypted traffic

33. **IPS** - A rootkit is a set of software tools that enable an unauthorized user to gain controls of a computer system without being detected. A company determined that its web site was compromised and a rootkit was installed on the server hosting the application. Which of the following choices would have most likely prevented the incident?
    a. A firewall
    b. A host-based intrusion prevention system (IPS)
    c. A network-based intrusion detection system (IDS)
    d. Operating system (OS) patching

34. **Cloud:** There are common cloud computing service models. _____ is the software environment that runs on top of the infrastructure. _____usually requires companies to deploy their own operating systems, application, and software onto the provided infrastructure. In the _____ model the provider commonly gives the customer network-based access to a single copy of an application.
    a. Platform as a Service, Platform as Software, Application as a Service
    b. Infrastructure as a Service, Application as a Service, Software as a Service
    c. Platform as a Service, Infrastructure as a Service, Software as a Service
    d. Infrastructure as a Service, Platform as a Service, Software as a Service

35. **Cloud:** Which of the following is the most important security consideration to an organization that wants to reduce its information system infrastructure by using servers provided by a platform as service (PaaS) vendor?
    a. Require users of the new application to adopt specific, minimum-length passwords.
    b. Implement a firewall that monitors incoming traffic using the organization's standard settings.
    c. Review the need for encryption of stored and transmitted application data.
    d. Make the service vendor responsible for application security through contractual terms.

36. **Risk Assessment:** One of the primary steps in a quantitative risk analysis is to determine the annualized loss expectancy (ALE). How is the ALE calculated?
    a. Single loss expectancy / Frequency per year
    b. Single loss expectancy X Annualized rate of occurrence
    c. Asset value + (Single loss expectancy / Frequency per year)
    d. SLE X RTO

37. **Categorization:** What are the security objectives of NIST's Federal Information Processing Standards Publication 199 "Standards for Security Categorization of Federal Information and Information Systems"?
    a. LOW, MODERATE, HIGH
    b. Confidentiality, Integrity, Availability
    c. Limited, Serious, Catastrophic
    d. Limited, Serious, Severe

38. **Risk Assessment:** You are doing risk analysis as part of a company's information risk management process. You calculate that the single loss expectancy (SLE) due to a denial of service (DoS) attack

on the company's network would be $15,250.You calculate that the annualized loss expectancy (ALE) for this event is $15,250. What can you say about the annualized rate off occurrence (ARO)?

a. The ARO will be less than 1.0
b. The ARO will be greater than 1.0
c. The ARO equals 1.0
d. The ARO cannot be calculated in this case

39. An IS auditor is reviewing an organization's information security policy, which requires encryption of all data placed on universal serial bus (USB) drives. The policy also requires that a specific encryption algorithm be used. Which of the following algorithms would provide the greatest assurance that data placed on USB drives is protected from unauthorized disclosure?
    a. Secure Shell (SSH)
    b. Data Encryption standard (DES)
    c. Message digest 5 (MD-5)
    d. Advanced Encryption Standard (AES)

40. The IS auditor is reviewing prior findings from an IS audit of a hospital. One finding indicates that the organization was using email to communicate sensitive patient issues. The IT manager indicates that to address this finding, the organization has implemented digital signatures for all email users. What should the IS auditor's response be?
    a. Digital signatures are adequate to protect confidentiality
    b. Digital signatures are not adequate to protect confidentiality
    c. The IS auditor should gather more information about the specific implementation
    d. The IS auditor should recommend implementation of digital watermarking for secure email

41. The MOST important difference between hashing and encryption is that hashing:
    a. Is not reversible
    b. Output is the same length as the original message
    c. Is concerned with integrity and security
    d. Is the same at the sending and receiving end

42. Which of the following cryptography options would increase overhead/cost?
    a. The encryption is symmetric rather than asymmetric
    b. A long asymmetric encryption key is used
    c. The hash is encrypted rather than the message
    d. A secret key is used

43. The PRIMARY reason for using digital signatures is to ensure data:
    a. Confidentiality
    b. Integrity
    c. Availability
    d. Timeliness

44. The review of router access control lists should be conducted during:
    a. An environmental review

b. A network security review
c. A business continuity review
d. A data integrity review

45. A digital signature contains a message digest to:
    a. Define the encryption algorithm
    b. Confirm the identity of the originator
    c. Show if the message has been altered after transmission
    d. Enable message transmission in a digital format

46. The feature of a digital signature that ensure the sender cannot later deny generating and sending the message is called:
    a. Data integrity
    b. Authentication
    c. Nonrepudiation
    d. Replay protection

47. Which of the following is the MOST effective type of antivirus software to detect an infected application?
    a. Scanners
    b. Active monitors
    c. Hash-based integrity checkers
    d. Vaccines

48. When using public key encryption to secure data being transmitted across a network:
    a. Both the key used to encrypt and decrypt the data are public
    b. The key used to encrypt is private, but the key used to decrypt the data is public
    c. The key used to encrypt is public, but the key used to decrypt the data is private
    d. Both the key used to encrypt and decrypt the data are private

49. During an audit of an enterprise that is dedicated to e-commerce, the IS manager states that digital signatures are used when receiving communications from customers. To substantiate this, an IS auditor must prove that which of the following is used?
    a. A biometric, digitized and encrypted parameter with the customer's public key
    b. A hash of the data that is transmitted and encrypted with the customer's private key
    c. A hash of the data that is transmitted and encrypted with the customer's public key
    d. The customer's scanned signature encrypted with the customer's public key

50. Email message authenticity and confidentiality is BEST achieved by signing the message using the:
    a. Sender's private key and encrypting the message using the receiver's public key
    b. Sender's public key and encrypting the message using the receiver's private key
    c. Receiver's private key and encrypting the message using the sender's public key
    d. Receiver's public key and encrypting the message using the sender's private key