CyberRookie CSX Fundamentals - Mock Exam 3

Friday, September 13, 2019 2:59 PM

Section 3 - SECURITY ARCHITECTURE PRINCIPLES

1. Defense in depth can be defined as:

a) The depth of security in a security system model

b) Maturity of the organization cybersecurity program

c) The knowledge of security in the organization

d) The practice of layering defense to provide added protection

2. The protection of data regardless of its location is a _____ model.

a) Data-centric

b) Network or system-centric

c) Well known

d) None of the above

3. SABSA, ZACHMAN, TOGAF are examples of:

a) Frameworks

b) Standards

c) Policies

d) Procedure models

4. Encapsulation is the process of _____ to data as they are transmitted down the OSI stack:

a) Security information

b) Database code

c) Addressing information

d) None of the above

5. Organise the OSI model in the diagram below (place the letter in the box):

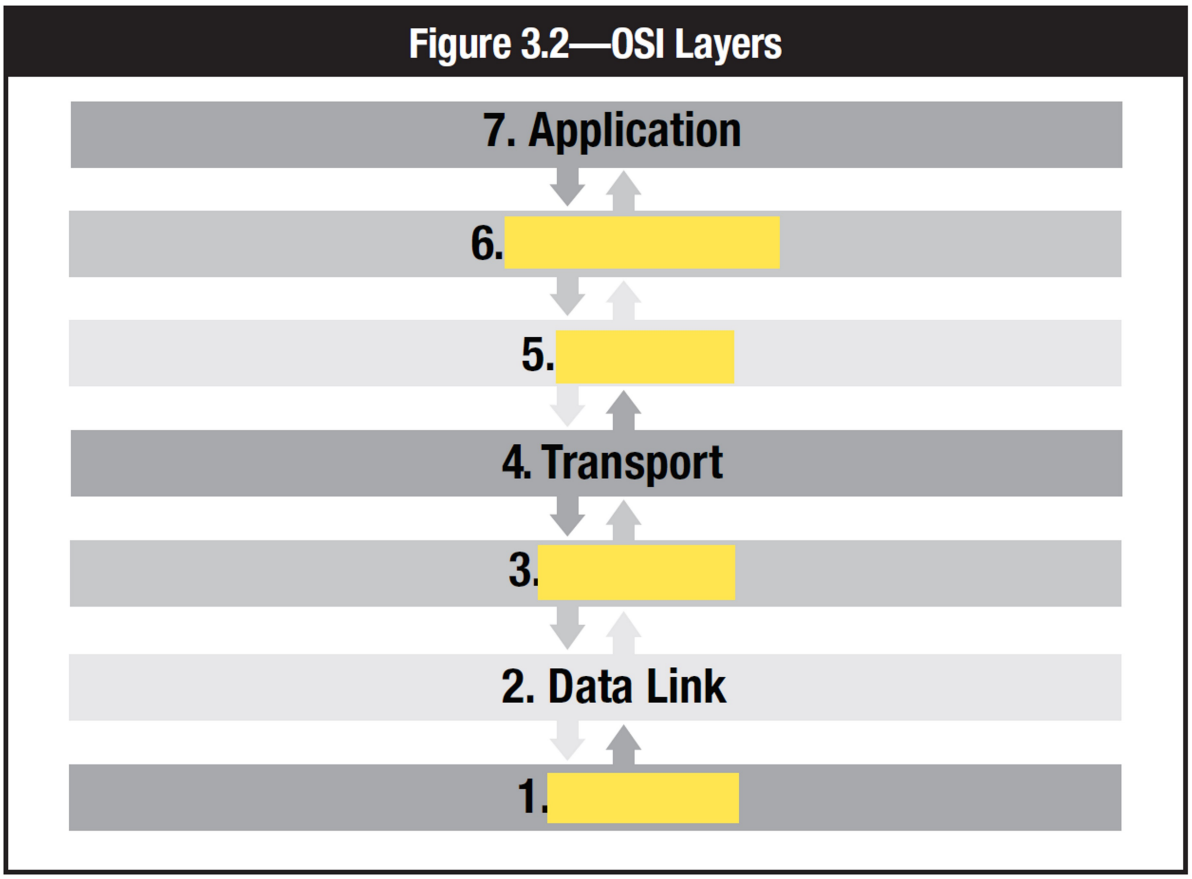
a) 1. Physical, 3. Network, 5. Session, 6. Presentation

b) 1.Presentation, a) 3. Physical, 5. Network, 6. Session

c) 1. Network, 3. Session, 5. Presentation, 6. Physical

d) 1. Session, 4. Physical, 5. Presentation, 6. Network

OSI Model (Question 5)



7. A _____ is defined as a system or combination of systems that enforces a boundary between two or more networks.

a) Software filter

b) Firewall

c) Network adaptor

d) None of the above

8. This type of firewall brings in the functionality of an intrusion prevention system (IPS) and will often inspect Secure Socket Layer (SSL) or Secure Shell (SSH) connections

a) First generation

b) Second generation

c) Third generation

d) Next generation

9. In this type of attack, the attacker fakes the IP address of either an internal network host or trusted network host:

a) Miniature fragment attack

b) IP spoofing

c) Source routing specification

d) Fake attack

10. This type of filter does not keep the state of ongoing TCP connection sessions:

a) State filtering

b) Stateful filtering

c) TCP filtering

d) Stateless filtering

11. This type of firewall implementation has two or more networks interfaces, each of which is connected to a different network

a) Dual-homed firewall

b) Demilitarized zone or screened-subnet firewall

c) Screen-host firewall

d) Multi-firewall

12. A common technique for implementing network security is to segment an organization’s network so that each segment can be separately controlled, monitored and protected. A network administrator therefore will:

a) Design a security hot site

b) Implement various operating system

c) Purchase more servers

d) Implement virtual local networks (VLANs)

13. _____ reviews can identify risk-relevant events such as compliance violations, suspicious behaviour, errors, probes or scans and abnormal activity.

a) Log

b) Personnel

c) Server

d) Firewall

14. This attack vector refers to network communications coming in:

a) Ingress

b) Direct

c) Egress

d) Perpetrator

15. _____ works in conjunction with routers and firewalls by monitoring network usage anomalies. It protects a company's IS resources from external as well as internal misuse.

a) Intrusion detection systems (IDS)

b) Packet sniffers

c) Wireshark

d) Intrusion prevention systems (IPS)

16. Select all that apply. The Internet perimeter should:

A. detect and block traffic from infected internal end points.

B. eliminate threats such as email spam, viruses and worms.

C. format, encrypt and compress data.

D. control user traffic bound toward the Internet.

E. monitor internal and external network ports for rogue activity.

17. The _____ layer of the OSI model ensures that data are transferred reliably in the correct sequence, and the _____ layer coordinates and manages user connections.

A. Presentation, data link

B. Transport, session

C. Physical, application

D. Data link, network

18. Choose three. The key benefits of the DMZ system are:

A. DMZs are based on logical rather than physical connections.

B. an intruder must penetrate three separate devices.

C. private network addresses are not disclosed to the Internet.

D. excellent performance and scalability as Internet usage grows.

E. internal systems do not have direct access to the Internet.

19. Which of the following best states the role of encryption within an overall cybersecurity program?

A. Encryption is the primary means of securing digital assets.

B. Encryption depends upon shared secrets and is therefore an unreliable means of control.

C. A program's encryption elements should be handled by a third-party cryptologist.

D. Encryption is an essential but incomplete form of access control.

20. The number and types of layers needed for defense in depth are a function of:

A. asset value, criticality, reliability of each control and degree of exposure.

B. threat agents, governance, compliance and mobile device policy.

C. network configuration, navigation controls, user interface and VPN traffic.

D. isolation, segmentation, internal controls and external controls.

21. Which activity is NOT part of the systems development lifecycle (SDLC)?

Service delivery

Feasibility study

Requirements study

Requirements definition

Post-implementation review

22. The design and coding specifications describing how the system will interact, conditions under which the system will operate and the information criteria that the system should meet are called:

Technical requirements

Functional requirements

Business requirements

Control requirements

23. The testing phase of the systems development lifecycle (SDLC) includes all of the following except:

Verification and validation that functions perform as designed

Confirmation that test units operate without adverse effect on other system components

Development methodologies and organizational requirements for testing

Deliverables for the next phase in the implementation process

24. The system development lifecycle (SDLC) process guides all phases of software development including which of the following? Select all that apply.

Acquisition

Retirement

Governance

Cost

25. The process by which changes to processes, systems, software, applications, platforms and configuration are introduced in an orderly, controlled manner is called:

Change management

System development lifecycle (SDLC)

Risk management

Compliance

26. The practice of layering defenses to provide added protection is called:

Defense in depth

Risk mitigation

Edge protection

Network foundation protection

27. The type of defense in which a series of nested layers must be bypassed in order to execute an attack is called:

Concentric rings

Overlapping redundancy

Segregation

Compartmentalization

28. Two or more controls that work in parallel to protect an asset is called:

Overlapping redundancy

Concentric rings

Segregation

Compartmentalization

29. The type of defense in which two or more processes, controls or individuals are required for access is called:

Overlapping redundancy

Concentric rings

Segregation/Compartmentalization

Horizontal defense

30. Ingress and egress are types of:

Horizontal defense

Attack vector

Vertical defense

Data

31. A virtual boundary which protects an organization from threats that come from the outside world is called a(n):

Security perimeter

Defense in depth

Virtual private network

Content filter

32. A system or combination of systems that enforces a boundary between two or more networks is called a(n):

Firewall

Application-level gateway

Circuit-level gateway

Demilitarized zone

33. A small, isolated network for an organization’s public servers, bastion host information servers and modem pools is called a(n):

Demilitarized zone (DMZ)

Virtual local area network (VLAN)

Dual-homed firewall

Screened-host firewall

34. The process of eliminating as many security risks as possible by removing all nonessential components is called:

System hardening

Stateless filtering

Stateful inspection

Isolation

35. Network segmentation does which one of the following?

Allows an organization’s network to be controlled, monitored and protected in separate zones

Blocks some or all of the traffic trying to pass between the networks

Protects the entire network by limiting break-ins to firewalls

Maps the source of an IP address of an incoming packet with the list of destination IP addresses

36. Advantages of application firewalls include which of the following? Select all that apply.

Provide security for commonly used protocols

Hide the network from untrusted networks

Easy scalability as internet usage grows

Protect the network by limiting firewall break-ins

37. A stateful inspection firewall is also known as:

Dynamic packet filtering

Screened-host firewall

Dual-homed firewall

Demilitarized zone (DMZ)

38. A key limitation of anti-malware is that it:

Is generally not effective in identifying malicious code that has yet to be identified

Is complex to administer

Is not scalable as internet usage grows

Is generally not effective for known threats

39. The art of designing, analyzing and attacking cryptographic schemes is called:

Encryption

Cryptography

Symmetric Key Encryption

Quantum Cryptography

40. Symmetric and asymmetric are types of:

Cryptographic systems

Nonrepudiation

Public key infrastructure

Encryption standards

41. All of the following are encryption techniques except:

Elliptical curve cryptography

Quantum cryptography

Advanced encryption standard

Key length

42. Which of the following are considered applied cryptographic techniques? Select all that apply.

Digital signature

Virtual private network (VPN)

Digital certificate

Registration authority

43. An authority in a network that verifies user requests for a digital certificate and tells the certificate authority (CA) to issue it is called:

Registration authority

Certificate authority

Digital certificate

Digital signature

44. Keys and hashes are used to:

Transform a string of characters into a shorter or fixed-length value

Decrypt parts of a ciphertext message

Compute the digital signature inside a certificate

Initiating the key recovery process

Back

Next

Never submit passwords through Google Forms.