CS205 FINAL TERM 2023 BY MOIN AKHTAR

MCQ No 1:

Which technique or solution can be used to analyze and block inbound email mechanisms with malicious behavior?

A. Enterprise antivirus
B. Sandboxing
C. SIEM solution
D. Firewall solution

Answer: B. Sandboxing

MCQ No 2:

OWASP Software Assurance Maturity Model (SAMM) undertakes software security testing and improvement during which phase?

A. Governance and deployment
B. Governance and verification
C. Verification and deployment
D. Construction and Governance

Answer: B. Governance and verification

MCQ No 3:

Creating awareness relating to policy and ISMS falls under which Cause?

A. Support
B. Operator
C. Performance Evaluation
D. Leadership

Answer: D. Leadership

MCQ No 4:

Assigning resources, assigning roles, and communicating roles fall under which Cause?

A. Support
B. Leadership
C. Performance Evaluation
D. Operator

Answer: B. Leadership

MCQ No 5:

The objective of COBIT is to help organizations:

A. Create optimal values from IT by balancing benefits with risk
B. Implement a strong governance of IT
C. Manage it effectively while ensuring business continuity
D. Create a single page IT dashboard

Answer: A. Create optimal values from IT by balancing benefits with risk

MCQ No 6:

In security terms, ownership of and accountability for controls lies with:

A. IT operations team
B. Business team
C. Info security or consultant
D. IT help desk team

Answer: C. Info security or consultant

MCQ No 7:

Where should source code be kept as best practice?

A. Access control system
B. Change control system
C. Version control system
D. Source control system

Answer: C. Version control system

MCQ No 8:

As per ISO27001, Operating procedures should be:

A. Confidential
B. Verbally communicated
C. Decided on an ad-hoc basis
D. Documented and maintained for those who need them

Answer: D. Documented and maintained for those who need them

MCQ No 9:

Conducting a successful security transformation project is more challenging in:

A. Large size organizations
B. Medium size organizations
C. Small-sized organizations
D. Environments where multiple sites are present

Answer: D. Environments where multiple sites are present

MCQ No 10:

Stage 2 of security transformation refers to:

A. Security Governance
B. Security Engineering
C. Security Hardening
D. Vulnerability Management

Answer: B. Security Engineering

MCQ No 11:

Which should be used to ensure that critical system files have not been altered?

A. CIS Control Pro
B. Qualys Vulnerability Scanner
C. Security Incident and Event Monitoring tools
D. File Integrity Monitoring tools

Answer: D. File Integrity Monitoring tools

MCQ No 12:

An authentic IT or security professional should always:

A. Take credit for everything
B. Never admit mistakes and ensure secrecy
C. Give credit where it is due
D. Be very strict and disciplined

Answer: C. Give credit where it is due

MCQ No 13:

Network performance degradation can be noticed in which step of VM cycle?

A. Preparing the scanner
B. Analyzing the asset
C. Running the scanner
D. Applying the patches

Answer: C. Running the scanner

MCQ No 14:

Which category indicates the highest severity in Qualys scan?

A. Level 2
B. Level 3
C. Level 4
D. Level 5

Answer: D. Level 5

MCQ No 15:

ISO31000 guidelines are centered on:

A. Organizational context
B. Leadership and commitment

C. Planning
D. Operation

Answer: A. Organizational context

MCQ No 16:

Which party plays a critical role in the success of a security transformation project?

A. IT team led by CIO
B. Business team
C. Internal team
D. Highest management

Answer: D. Highest management

MCQ No 17:

What should be deployed to limit and control which devices can be connected to the network?

A. 802.1x
B. 802.11g
C. 802.11b
D. 802.11i

Answer: A. 802.1x

MCQ No 18:

If network traffic to or from the internet must pass through, **which proxy should be used to filter unauthorized connections?**

A. Application-layer filtering proxy
B. Session-layer filtering proxy
C. Network-layer filtering proxy
D. System-layer filtering proxy

Answer: A. Application-layer filtering proxy

MCQ No 19:

In which phase of Security Assessment, assessment methods based on the report findings are decided?

A. Report finding
B. Build plan, scope, and objectives
C. Assign roles
D. Conduct assessment

Answer: B. Build plan, scope, and objectives

MCQ No 20:

Automated tools should be used to verify and compare the network device configuration with:

A. Approved security configuration
B. Recommended security configuration by vendor
C. Latest security configuration released by vendor
D. Default security configuration

Answer: A. Approved security configuration

MCQ No 21:

Under the security transformation model, which team is responsible for incident response?

A. Business team
B. IT or security team or consultant
C. IT operations team
D. IT help desk team

Answer: B. IT or security team or consultant

MCQ No 22:

The Computer Security Resource Center (CSRC) website guides users to resources related to:

A. CIS resources on computer, cyber, IT, and information security and privacy
B. SANS resources on computer, cyber, IT, and information security and privacy
C. NIST resources on computer, cyber, IT, and information security and privacy
D. PCI resources on computer, cyber, IT, and information security and privacy

Answer: C. NIST resources on computer, cyber, IT, and information security and privacy

MCQ No 23:

Complex passwords should be enforced to resist:

A. Dictionary attack
B. Injection attack
C. DoS attack
D. Phishing attack

Answer: A. Dictionary attack

MCQ No 24:

Activities related to C++ security hardening are carried out in which phase of Security Transformation Program?

A. Perform hardening of Key IT assets in Test environment
B. Understand organization and its security issues
C. Develop ISMC
D. Identify assets for various phases

Answer: A. Perform hardening of Key IT assets in Test environment

MCQ No 25:

The term "Candidness" in the context of security management means:

A. Promoting performance and merit
B. Encouraging intra-team fights among members
C. Honesty and straight talk
D. Adjusting partners in the right positions

Answer: C. Honesty and straight talk

MCQ No 26:

Which protocol is used for assigning IP addresses dynamically?

A. DCP
B. HTTP
C. DHCP
D. IP

Answer: C. DHCP

MCQ No 27:

Which team has primary ownership of vulnerability management processes?

A. IT or security team
B. IT operations team
C. Business team
D. Risk and compliance team

A. IT or security team

MCQ No 28:

Rules are mentioned related to C++ security hardening in which section?

A. Section 1
B. Section 8
C. Section 9
D. Section 10

Answer: B. Section 8

MCQ No 29:

What is the goal of performing an audit?

A. Testing security that is assumed to be secure
B. Technical assessment designed to achieve specific goals
C. To fix as many things as possible and as efficiently as possible
D. Focuses on how existing configurations compare to standards

Answer: B. Technical assessment designed to achieve specific goals

MCQ No 30:

Under security transformation model, which team is responsible for implementing controls?

A. IT operations team
B. Security consultant
C. Risk and compliance team
D. Business team

Answer: A. IT operations team

MCQ No 31:

In which assessment type does the tester have access to all internal information about the target?

A. White box assessment
B. Grey box assessment
C. Black box assessment
D. Risk assessment

Answer: A. White box assessment

MCQ No 32:

Which assessment is designed to determine whether an attacker can achieve specific goals while using your current security posture?

A. Threat assessment
B. Bug bounty hunting
C. Penetration testing
D. Red team exercise

Answer: C. Penetration testing

MCQ No 33:

What are the key benefits of security transformation project implementation to an organization?

A. IT team gains experience and awareness of security
B. Prevention of an attack
C. IT team gets certifications
D. Management becomes aware of IT team capabilities

Answer: D. Management becomes aware of IT team capabilities

MCQ No 34:

Which action is recommended for an organization having a very good security posture and scoring higher than 85%?

A. Go for risk assessment
B. Third-party security review
C. Go for ISO27001 certification
D. Implement security transformation program

Answer: C. Go for ISO27001 certification

MCQ No 35:

The version of security-related updates applied to network devices should be:

A. Latest
B. Default
C. Latest and stable
D. Oldest

Answer: C. Latest and stable

MCQ No 36:

Most of the problems associated with weak security posture are due to:

A. Lack of awareness
B. Lack of funds
C. Lack of experience
D. Lack of commitment

Answer: A. Lack of awareness

MCQ No 37:

The Information Security policy needs to be reviewed:

A. Once every three years
B. Updated once every five years
C. Locked in a drawer and kept confidential
D. Regularly reviewed and approved for changes

Answer: D. Regularly reviewed and approved for changes

MCQ No 38:

In the case of the financial sector, regulations need to be reviewed and understood to gain management support for security transformation from:

A. SBP
B. PTA
C. PEMRA
D. PEPRA

Answer: A. SBP

MCQ No 39:

History of authorized and unauthorized software control requires making a list of:

A. Authorized access and version
B. Authorized operating system and version
C. Authorized software and version
D. Unauthorized software and version

Answer: C. Authorized software and version

MCQ No 40:

Which principle should be used when setting up a user in a database?

A. Principle of normal user
B. Principle of administrative user
C. Principle of least privilege
D. Principle of highest privilege

Answer: C. Principle of least privilege