CS205 FINAL TERM 2023 BY MOIN AKHTAR (03146654464)

CS205 FINAL TERM 2023 BY MOIN AKHTAR
TIME & FATE (12 PM 2-16-2024)

1. **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

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

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

Answer D. Leadership

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

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

Answer B. Leadership

4. **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

5. **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

6. **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

7. 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

8. 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

9. ISO31000 guidelines are centered on

A. Organizational context B. Leadership and commitment C. Planning D. Operation

Answer A. Organizational context

10. 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

11. 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

12. Complex passwords should be enforced to resist

A. Dictionary attack B. Injection attack

C. Do attack D. Phishing attack

Answer A. Dictionary attack

13. 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

14. 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

Answer. IT or security team

15. 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

16. 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

17. 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

18. 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

19. 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

20. 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

21. To prevent attacks, fraud, and pilferage, what is essential for an effective information security transformation program?

a. Enhancing system aesthetics b. Ensuring server speed

c. Protecting sensitive data and ensuring system integrity d. Implementing colorful user interfaces

Correct Answer: c) Protecting sensitive data and ensuring system integrity

22. What is the recommended timeline for an effective information security transformation program?

a. 6 months b. 12 months c. 18 months d. 24 months

Correct Answer: c) 18 months

23. In the financial sector, what is crucial for raising management support for security transformation?

a) Ignoring regulations
b) Reviewing and understanding regulations
c) Avoiding security measures
d) Outsourcing security responsibilities

Correct Answer: b) Reviewing and understanding regulations

24. What is a common cause of problems associated with a weak security posture?

a) Excessive security measures
b) Strict regulatory compliance
c) Lack of awareness
d) Robust security protocols

Correct Answer: c) Lack of awareness

25. What is an open source vulnerability management tool?

A. NESSUS
B. OPENVAS
C. Wireshark
D. Snort

Correct Answer: B. OPENVAS

26. The enterprise technology governance and risk management framework is considered a combination of?

A. ITIL, ISACA, NIST
B. COBIT, ISO 27001, FAIR
C. TOGAF, HIPAA, PCI DSS
D. COSO, PMP, FISMA

Correct Answer: B. COBIT, ISO 27001, FAIR

27. Which of the following activity is part of risk treatment?

A. Risk identification
B. Risk mitigation
C. Risk assessment
D. Risk acceptance

Correct Answer: B. Risk mitigation

28. In which phase of security assessment, assessment methods based on report format are decided?

A. Initiate assessment
B. Build plan, scope and objectives
C. Execute assessment
D. Report findings and remediation

Correct Answer: B. Build plan, scope and objectives

29. What are considered types of security assessment?

A. Vulnerability assessment and penetration testing
B. Security awareness training and disaster recovery planning

C. Incident response and access control assessment
D. Risk management and network monitoring

Correct Answer: A. Vulnerability assessment and penetration testing

30. What is the goal of performing vulnerability assessment?

A. To fix as many things as possible as efficiently as possible
B. To identify and prioritize security vulnerabilities in a system
C. To create new vulnerabilities
D. To generate false positive reports

Correct Answer: B. To identify and prioritize security vulnerabilities in a system

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

A. Black-box
B. White-box
C. Gray-box
D. Zero-box

Correct Answer: A. Black-box

Short Question

Mention the names of security testing?

Answer:

1. **Vulnerability Assessment**
2. **Penetration Testing**
3. **Security Auditing**
4. **Security Scanning**
5. **Security Code Review**
6. **Security Awareness Training**
7. **Wireless Security Testing**
8. **Web Application Security Testing**