CS205 – Information Security

Final Term Papers 2025

Prepared By: Usama Farooq

Multiple Choice Questions (MCQs) Topics

- SDLC diagram (construction, employment, or verification phases)
- CIS/DISA STIGs
- Causes of information security system failures based on security engineering
- ISO 27001 clauses
- Anthem security breach details
- Layers of the Cyber Security Maturity Matrix (CSMM)

Short Questions

1. What are the compliance features of Nessus?
2. What is the name of the last layer of the Cyber Security Maturity Matrix (CSMM)?
3. List the types of vulnerability tests.
4. Which of the following are correct?
    - a. Deny permission to known malicious IP addresses
    - b. Accept all IP addresses
    - c. Deny permission to all IP addresses
5. What are the free tools and scanners provided by Qualys?
6. From a given list of Qualys scanners, identify which two are not used as scanners.
7. Which vulnerability scanner is used for both code and secure configuration vulnerabilities?
8. Given a scenario related to SDLC, identify the development approach.
9. What is the name of the first layer of the CSMM?
10. What are the alternatives to the "Is" prefix in coding?
11. How can you identify code with a holistic view function?
12. How do you rewrite code to remove side effects?
13. How do you identify static and dynamic elements from a UML diagram?
14. What are the coverage schemes of white box testing?
15. List key security frameworks and their acronyms.
16. How should the layers of the Cyber Security Maturity Matrix be arranged?
17. Which web browsers and email clients should an organization use for enhanced security?
18. What are the steps in the vulnerability management life cycle, and which teams are responsible for each?
19. List common vulnerability scanners.
20. What is the difference between remote and local exploits?
21. What is the responsibility matrix, and who is responsible for each tier?
22. Provide details of the Home Depot and Anthem security breaches.
23. What are the objectives and activities of security engineering?
24. List the different types of security testing.
25. What are the steps involved in security hardening?
26. What are the five steps for a Qualys policy compliance scan?
27. Which protocols require secondary encryption?
28. What are the security functions for asset management?
29. What are the building blocks of security governance?
30. Where should source code be stored?
31. What is the authorized scripting language for email and web applications?
32. What is used for filtering network traffic?
33. What are the ISO 31000 guidelines?
34. What are the functions of a Security Operations Center (SOC)?
35. Which management function is responsible for assigning resources and roles?
36. What is the definition of COBIT?
37. What is the function related to monitoring and measuring in security?
38. When should employee screening occur?
39. What is the verification phase of the Software Assurance Maturity Model (SAMM)?
40. What are the standards for Enterprise Technology Governance?
41. What is the second stage of the Transformation Model?
42. What types of attacks do OWASP security guidelines protect against?
43. What is the goal of performing a security audit?
44. Why are complex passwords important?
45. List the different types of security assessments.
46. What are the benefits of version control?

47. Which assessment method helps evaluate attacker success?
48. How many steps are in a Qualys policy compliance scan?
49. What is a benefit of a security transformation project?
50. Which protocol is used for dynamic address assignment?
51. When does a validation activity occur in the SDLC?
52. How many steps are in the vulnerability management process?
53. What action should be taken if compliance exceeds 85%?
54. Which CSMM layer is responsible for implementing controls?
55. What tool is used to limit network device connections?
56. What are the qualities of an effective InfoSec Head?
57. What is the method for analyzing inbound email attachments?
58. What is the highest severity level for a vulnerability scan?
59. Which team has primary ownership in vulnerability management?
60. How many security hardening rules exist for C++?
61. What is an assessment with full internal information called?
62. What was the former name of ISO 27002?
63. What are the default TCP/UDP ports for a specific tool discussed in the course?
64. Describe the tier and responsibilities diagram.
65. What is a scanner in the context of information security?
66. List the steps of a vulnerability scanner and name the second step.
67. List all layers of the Cyber Security Maturity Matrix (CSMM).
68. Name the frameworks against which the Nessus scanner provides configuration auditing features.
69. Describe the first layer of the CSMM.

Long Questions

1. Given a table of the Cyber Security Maturity Matrix, match Column A (Layer 1 to Layer 5) with Column B (Hardened, Protected, Monitor, Foundation, Fundamental).
2. Given a table, indicate whether each job (Approve, Business Commitment, Budget, Monitoring) is performed by the Board or IT Operations.
3. Match the correct activity to the responsible team:
    - Column 1 (Activity): Security Requirements, Security Design, Validating Security Controls, Security Implementation, Validating Security Requirements
    - Column 2 (Team): Information Security Team, Network/IT Security Assisted by Vendor, Information Security with Consultation
4. Explain the uses of Get/Set methods and the "Is" prefix in coding.
5. Given a scenario, explain how to identify and fix loop errors, with an example.
6. Rearrange the layers and services of the Cyber Security Maturity Matrix.
7. Rearrange a table of work and corresponding teams.
8. Assign the appropriate board or IT operation responsibilities.
9. Rearrange a table of teams and their work.
10. Write a note on the verification phase and deployment in the SDLC.
11. Arrange the information security governance blocks in the correct order:
    - Awareness Intermediate
    - Monitoring Intermediate
    - Policy Initial
    - Periodic Review Initial

Answers:

Multiple Choice Questions (MCQs) Topics

These topics are typically covered in multiple-choice format in exams. Below is a brief explanation of each to guide understanding:

1. **SDLC Diagram (Construction, Employment, or Verification Phases)**
   Focuses on the Software Development Life Cycle phases, particularly construction (coding/development), employment (deployment/operation), and verification (testing/validation). Questions may ask about activities, tools, or security practices in these phases.
2. **CIS/DISA STIGs**
   CIS (Center for Internet Security) and DISA STIGs (Defense Information Systems Agency Security Technical Implementation Guides) provide configuration standards for securing systems. Questions may cover their purpose, application, or specific controls.
3. **Causes of Information Security System Failures Based on Security Engineering**
   Examines reasons for security failures, such as poor design, inadequate testing, misconfiguration, or lack of risk management, rooted in security engineering principles.
4. **ISO 27001 Clauses**
   Refers to the clauses (4–10) of ISO/IEC 27001:2022, which outline requirements for an Information Security Management System (ISMS), including leadership, planning, and risk management.
5. **Anthem Security Breach Details**
   Questions focus on the 2015 Anthem breach, where attackers accessed 78.8 million records due to phishing and unencrypted data vulnerabilities.
6. **Layers of the Cyber Security Maturity Matrix (CSMM)**
   Tests knowledge of CSMM layers, often structured to reflect an organization's cybersecurity maturity (e.g., Initial, Managed, Defined, Quantitatively Managed, Optimized).

Short Questions

1. **What are the compliance features of Nessus?**
   Nessus, a vulnerability scanner, supports compliance auditing for standards like CIS, DISA STIGs, PCI DSS, and ISO 27001. Features include configuration audits, policy compliance checks, and customizable templates for regulatory standards.
2. **What is the name of the last layer of the Cyber Security Maturity Matrix (CSMM)?**
   The last layer is typically **Optimized** (or similar, depending on the model), focusing on continuous improvement and adaptive cybersecurity practices.
3. **List the types of vulnerability tests.**
   - Network vulnerability scanning
   - Application vulnerability scanning
   - Penetration testing
   - Configuration auditing
   - Code review/scanning
4. **Which of the following are correct?**
   - **a. Deny permission to known malicious IP addresses**: Correct (blocks known threats).
   - **b. Accept all IP addresses**: Incorrect (insecure, violates least privilege).
   - **c. Deny permission to all IP addresses**: Correct (default-deny policy enhances security).

   Answer: a and c.
5. **What are the free tools and scanners provided by Qualys?**
   Qualys offers:
   - Qualys Community Edition (limited vulnerability scanning)
   - FreeScan (basic vulnerability and compliance scans)
   - SSL Labs (SSL/TLS configuration testing)
6. **From a given list of Qualys scanners, identify which two are not used as scanners.**
   Without a specific list, common Qualys tools not used as scanners include:
   - **Qualys Policy Compliance** (evaluates configurations, not a scanner).
   - **Qualys File Integrity Monitoring** (monitors changes, not a scanner).
7. **Which vulnerability scanner is used for both code and secure configuration vulnerabilities?**
   SonarQube scans for code vulnerabilities and misconfigurations, while tools like Nessus or Qualys can also assess secure configurations.
8. **Given a scenario related to SDLC, identify the development approach.**
   Depends on the scenario. Common approaches include:
   - **Waterfall**: Linear, sequential.
   - **Agile**: Iterative, flexible.

- **DevSecOps**: Integrates security throughout development.
  Example: If the scenario describes iterative development with continuous testing, it's likely **Agile** or **DevSecOps**.

9. **What is the name of the first layer of the CSMM?**
   The first layer is typically **Initial** or **Foundation**, where processes are ad hoc and reactive.
10. **What are the alternatives to the "Is" prefix in coding?**
    Alternatives include:
    - **Has** (e.g., hasPermission)
    - **Can** (e.g., canAccess)
    - **Get** (e.g., getStatus)
    - **Check** (e.g., checkValidity)
11. **How can you identify code with a holistic view function?**
    Look for functions that:
    - Integrate multiple system components (e.g., data access, processing, and output).
    - Use modular design with clear inputs/outputs.
    - Avoid tight coupling and side effects.
      Example: A function handling user authentication across modules.
12. **How do you rewrite code to remove side effects?**
    - Use pure functions (same input, same output, no external state changes).
    - Avoid global variables; pass dependencies explicitly.
    - Use immutable data structures.
      Example: Refactor updateGlobalCounter() to returnCounterValue(input).
13. **How do you identify static and dynamic elements from a UML diagram?**
    - **Static Elements**: Classes, interfaces, attributes (shown in class diagrams).
    - **Dynamic Elements**: Interactions, state changes, sequences (shown in sequence or state diagrams).
      Analyze diagram type and notation (e.g., arrows for interactions).
14. **What are the coverage schemes of white box testing?**
    - Statement coverage
    - Branch coverage
    - Path coverage
    - Condition coverage
    - Function coverage
15. **List key security frameworks and their acronyms.**
    - ISO/IEC 27001 (Information Security Management)
    - NIST CSF (Cybersecurity Framework)
    - CIS Controls (Center for Internet Security)
    - COBIT (Control Objectives for Information and Related Technologies)
    - PCI DSS (Payment Card Industry Data Security Standard)
16. **How should the layers of the Cyber Security Maturity Matrix be arranged?**
    Typically:
    i. Initial/Foundation (ad hoc)
    ii. Managed (basic processes)
    iii. Defined (standardized policies)
    iv. Quantitatively Managed (metrics-driven)
    v. Optimized (continuous improvement)
17. **Which web browsers and email clients should an organization use for enhanced security?**
    - **Browsers**: Google Chrome, Mozilla Firefox, Microsoft Edge (with updated security patches).
    - **Email Clients**: Microsoft Outlook, Mozilla Thunderbird (with encryption and phishing protection enabled).
18. **What are the steps in the vulnerability management life cycle, and which teams are responsible for each?**
    - **Discovery**: Identify assets (IT Team).
    - **Assessment**: Scan for vulnerabilities (Security Team).
    - **Prioritization**: Rank risks (Security Team).
    - **Remediation**: Fix vulnerabilities (IT/Security Teams).
    - **Verification**: Confirm fixes (Security Team).
    - **Monitoring**: Continuous oversight (SOC Team).
19. **List common vulnerability scanners.**
    - Nessus
    - Qualys
    - OpenVAS
    - Burp Suite
    - Nikto
20. **What is the difference between remote and local exploits?**
    - **Remote Exploits**: Executed over a network without physical access (e.g., exploiting a server vulnerability).
    - **Local Exploits**: Require local access to the system (e.g., privilege escalation from a user account).

21. **What is the responsibility matrix, and who is responsible for each tier?**
    A responsibility matrix (e.g., RACI) defines roles:
    - **Tier 1 (Operational)**: IT/Security Team (executes tasks).
    - **Tier 2 (Tactical)**: Security Managers (oversee processes).
    - **Tier 3 (Strategic)**: CISO/Board (set policies, approve budgets).
22. **Provide details of the Home Depot and Anthem security breaches.**
    - **Home Depot (2014)**: Attackers used stolen vendor credentials to install malware on POS systems, compromising 56 million credit card records. Cause: Weak access controls and unsegmented networks.
    - **Anthem (2015)**: Phishing attack led to unauthorized access to 78.8 million records. Cause: Lack of encryption and poor email security.
23. **What are the objectives and activities of security engineering?**
    - **Objectives**: Ensure confidentiality, integrity, and availability (CIA triad).
    - **Activities**: Risk assessment, secure design, code reviews, penetration testing, incident response planning.
24. **List the different types of security testing.**
    - Vulnerability scanning
    - Penetration testing
    - Code review
    - Configuration auditing
    - Social engineering testing
25. **What are the steps involved in security hardening?**
    - Identify assets and risks.
    - Apply secure configurations (e.g., CIS benchmarks).
    - Remove unnecessary services/software.
    - Implement access controls.
    - Regularly patch and update systems.
26. **What are the five steps for a Qualys policy compliance scan?**
    - Define policy (compliance standards).
    - Scan assets for configurations.
    - Analyze results against policy.
    - Report non-compliance issues.
    - Remediate and re-scan.
27. **Which protocols require secondary encryption?**
    - HTTP (use HTTPS)
    - FTP (use SFTP)
    - Telnet (use SSH)
    - SMTP (use SMTPS or STARTTLS)
28. **What are the security functions for asset management?**
    - Asset inventory creation
    - Classification of assets
    - Access control enforcement
    - Monitoring and tracking
    - Secure disposal
29. **What are the building blocks of security governance?**
    - Policies and procedures
    - Risk management framework
    - Compliance monitoring
    - Security awareness training
    - Incident response planning
30. **Where should source code be stored?**
    In a secure version control system (e.g., Git with access controls, hosted on platforms like GitHub, GitLab, or Bitbucket with encryption).
31. **What is the authorized scripting language for email and web applications?**
    JavaScript (commonly used, secure when sanitized to prevent XSS).
32. **What is used for filtering network traffic?**
    Firewalls, Intrusion Detection/Prevention Systems (IDS/IPS), and Access Control Lists (ACLs).
33. **What are the ISO 31000 guidelines?**
    ISO 31000 provides a framework for risk management, including:
    - Risk identification
    - Risk assessment
    - Risk treatment
    - Monitoring and review
    - Communication and consultation
34. **What are the functions of a Security Operations Center (SOC)?**
    - Threat detection and monitoring

- Incident response
- Vulnerability management
- Log analysis
- Threat intelligence gathering

35. **Which management function is responsible for assigning resources and roles?**
    Planning (defines roles, responsibilities, and resource allocation).
36. **What is the definition of COBIT?**
    COBIT (Control Objectives for Information and Related Technologies) is a framework for IT governance and management, aligning IT with business goals and ensuring risk management and compliance.
37. **What is the function related to monitoring and measuring in security?**
    Continuous oversight of systems, logs, and metrics to detect anomalies, assess compliance, and measure security effectiveness.
38. **When should employee screening occur?**
    Before hiring, during onboarding, and periodically (e.g., background checks for role changes).
39. **What is the verification phase of the Software Assurance Maturity Model (SAMM)?**
    The verification phase involves testing and reviewing software to ensure security requirements are met (e.g., code reviews, penetration testing).
40. **What are the standards for Enterprise Technology Governance?**
    - ISO/IEC 38500 (IT governance)
    - COBIT
    - ITIL (Information Technology Infrastructure Library)
    - NIST SP 800-53
41. **What is the second stage of the Transformation Model?**
    Typically **Defined** (processes are standardized and documented).
42. **What types of attacks do OWASP security guidelines protect against?**
    - SQL injection
    - Cross-site scripting (XSS)
    - Cross-site request forgery (CSRF)
    - Broken authentication
    - Insecure deserialization
43. **What is the goal of performing a security audit?**
    To assess compliance, identify vulnerabilities, and ensure security controls are effective.
44. **Why are complex passwords important?**
    They increase resistance to brute-force and dictionary attacks, enhancing account security.
45. **List the different types of security assessments.**
    - Vulnerability assessments
    - Penetration testing
    - Risk assessments
    - Compliance audits
    - Security posture assessments
46. **What are the benefits of version control?**
    - Tracks changes and history
    - Enables collaboration
    - Facilitates rollback to stable versions
    - Enhances security through access controls
47. **Which assessment method helps evaluate attacker success?**
    Penetration testing (simulates real-world attacks to test defenses).
48. **How many steps are in a Qualys policy compliance scan?**
    Five (see question 26).
49. **What is a benefit of a security transformation project?**
    Improved security posture, reduced risk, and enhanced compliance with standards.
50. **Which protocol is used for dynamic address assignment?**
    DHCP (Dynamic Host Configuration Protocol).
51. **When does a validation activity occur in the SDLC?**
    During the **testing/verification phase**, after development, to ensure the system meets requirements.
52. **How many steps are in the vulnerability management process?**
    Six (Discovery, Assessment, Prioritization, Remediation, Verification, Monitoring).
53. **What action should be taken if compliance exceeds 85%?**
    Maintain current controls, focus on continuous improvement, and address remaining gaps.
54. **Which CSMM layer is responsible for implementing controls?**
    Managed or Defined (where controls are formalized and implemented).
55. **What tool is used to limit network device connections?**
    Firewall or Access Control Lists (ACLs).
56. **What are the qualities of an effective InfoSec Head?**

- Strategic vision
- Technical expertise
- Leadership and communication skills
- Risk management knowledge
- Compliance awareness

57. **What is the method for analyzing inbound email attachments?**
    Use sandboxing, antivirus scanning, and content filtering to detect malicious content.
58. **What is the highest severity level for a vulnerability scan?**
    Critical (based on CVSS scoring, typically 9.0–10.0).
59. **Which team has primary ownership in vulnerability management?**
    Security Team (coordinates scanning, prioritization, and remediation).
60. **How many security hardening rules exist for C++?**
    The CERT C++ Secure Coding Standard includes approximately **83 rules** (subject to updates).
61. **What is an assessment with full internal information called?**
    White-box testing (full system knowledge provided to testers).
62. **What was the former name of ISO 27002?**
    ISO/IEC 17799.
63. **What are the default TCP/UDP ports for a specific tool discussed in the course?**
    Without course context, assuming Nessus: **TCP 8834** (default for web interface). Please specify the tool for accuracy.
64. **Describe the tier and responsibilities diagram.**
    A tiered diagram outlines:
    - **Tier 1 (Operational)**: IT staff handle daily tasks (e.g., patching).
    - **Tier 2 (Tactical)**: Security managers oversee processes.
    - **Tier 3 (Strategic)**: CISO/Board sets policies and budgets.
65. **What is a scanner in the context of information security?**
    A tool that identifies vulnerabilities in systems, networks, or applications (e.g., Nessus, Qualys).
66. **List the steps of a vulnerability scanner and name the second step.**
    - Discover assets
    - **Scan for vulnerabilities** (second step)
    - Analyze results
    - Report findings
    - Recommend remediation
67. **List all layers of the Cyber Security Maturity Matrix (CSMM).**
    - Initial/Foundation
    - Managed
    - Defined
    - Quantitatively Managed
    - Optimized
68. **Name the frameworks against which the Nessus scanner provides configuration auditing features.**
    - CIS Benchmarks
    - DISA STIGs
    - PCI DSS
    - ISO 27001
    - NIST 800-53
69. **Describe the first layer of the CSMM.**
    The **Initial/Foundation** layer is characterized by ad hoc, reactive processes with minimal formal policies or controls.

Long Questions

1. **Given a table of the Cyber Security Maturity Matrix, match Column A (Layer 1 to Layer 5) with Column B (Hardened, Protected, Monitor, Foundation, Fundamental).**
    - Layer 1: **Foundation** (or Fundamental)
    - Layer 2: **Managed** (Protected)
    - Layer 3: **Defined**
    - Layer 4: **Quantitatively Managed** (Monitor)
    - Layer 5: **Optimized** (Hardened)
2. **Given a table, indicate whether each job (Approve, Business Commitment, Budget, Monitoring) is performed by the Board or IT Operations.**
    - **Approve**: Board
    - **Business Commitment**: Board
    - **Budget**: Board
    - **Monitoring**: IT Operations
3. **Match the correct activity to the responsible team.**

- **Security Requirements**: Information Security Team
- **Security Design**: Information Security with Consultation
- **Validating Security Controls**: Network/IT Security Assisted by Vendor
- **Security Implementation**: Information Security Team
- **Validating Security Requirements**: Information Security Team

4. **Explain the uses of Get/Set methods and the "Is" prefix in coding.**
   - **Get/Set Methods**: Used to access (Get) or modify (Set) private class attributes, ensuring encapsulation and controlled access. Example: getName() retrieves a name; setName() updates it.
   - **"Is" Prefix**: Used for boolean methods to indicate a true/false state (e.g., isActive() checks if a user is active).
5. **Given a scenario, explain how to identify and fix loop errors, with an example.**
   - **Scenario**: A program hangs due to an infinite loop.
   - **Identification**: Use debugging tools to trace loop execution, check loop conditions, and monitor variable changes.
   - **Fix**: Ensure the loop condition eventually evaluates to false.
   - **Example**:
     cpp
     ```
     // Buggy code
     for (int i = 0; i < 10; i--) { // Infinite loop (i decreases)
        cout << i;
     }
     // Fixed code
     for (int i = 0; i < 10; i++) { // Increment i
        cout << i;
     }
     ```
6. **Rearrange the layers and services of the Cyber Security Maturity Matrix.**
   Layers (from least to most mature):
   - Foundation: Basic security controls
   - Managed: Formal policies, basic monitoring
   - Defined: Standardized processes
   - Quantitatively Managed: Metrics-driven controls
   - Optimized: Continuous improvement, automation
7. **Rearrange a table of work and corresponding teams.**
   Example table:
   - Work: Vulnerability Scanning → Team: Security Team
   - Work: Network Monitoring → Team: SOC
   - Work: Policy Development → Team: Information Security Team
   - Work: Patching → Team: IT Operations
8. **Assign the appropriate board or IT operation responsibilities.**
   - **Board**: Strategic oversight, policy approval, budgeting.
   - **IT Operations**: Implementation, monitoring, patching, incident response.
9. **Rearrange a table of teams and their work.**
   Example:
   - Information Security Team: Policy development, risk assessment
   - SOC: Real-time monitoring, incident response
   - IT Operations: System maintenance, patching
   - Network/IT Security: Firewall management, vendor coordination
10. **Write a note on the verification phase and deployment in the SDLC.**
    - **Verification Phase**: Involves testing to ensure the system meets requirements (e.g., unit testing, integration testing, security testing). Tools like static analysis or penetration testing are used.
    - **Deployment Phase**: The system is released to production. Security tasks include secure configuration, access control setup, and monitoring activation. Both phases ensure the system is secure and functional before and during operation.
11. **Arrange the information security governance blocks in the correct order.**
    - **Policy Initial**: Establish baseline security policies.
    - **Awareness Intermediate**: Train staff on policies and threats.
    - **Monitoring Intermediate**: Implement continuous oversight.
    - **Periodic Review Initial**: Regularly assess and update policies.