

VU Learning HUB

CS205 Quiz File

Chapter-wise Solved MCQs

vulearninghub.xyz

Chapter 1: Fundamentals of Information Security

Q1. What are the three pillars (triad) of information security?

- A) Confidentiality, Integrity, Availability
- B) Speed, Cost, Power
- C) Hardware, Software, Network
- D) Users, Admins, Guests

Q2. Which role is primarily responsible for an organization's information security strategy?

- A) CISO (Chief Information Security Officer)
- B) Janitor
- C) Receptionist
- D) Driver

Q3. What does "confidentiality" mean in information security?

- A) Ensuring information is accessible only to authorized parties
- B) Making all data public
- C) Deleting backups
- D) Sharing passwords

Q4. What is "integrity" in the context of information security?

- A) Ensuring data is accurate and unaltered
- B) Making data available faster
- C) Encrypting passwords only
- D) Hiding the server room

Answer Key

1. A) The three pillars are Confidentiality, Integrity, and Availability.
2. A) The CISO is responsible for the organization's information security strategy.
3. A) Confidentiality ensures information is accessible only to authorized parties.
4. A) Integrity ensures data remains accurate and unaltered.

Chapter 2: Typical Enterprise IT Architecture & Security Overlay

Q1. In a typical enterprise IT architecture, which layer is most exposed to external threats?

- A) The perimeter/DMZ facing the internet
- B) The internal printer
- C) The cafeteria network
- D) The parking system

Q2. What is the purpose of a security overlay in enterprise architecture?

- A) To integrate security controls across all architectural layers
- B) To paint the servers
- C) To slow the network
- D) To remove firewalls

Q3. Which component segregates internal networks from untrusted external networks?

- A) Firewall at the perimeter
- B) A keyboard

- C) A mouse
- D) A monitor

Q4. What does "defense in depth" mean?

- A) Layered security controls so that if one fails, others still protect
- B) A single strong password
- C) Hiding the data center
- D) One antivirus

Answer Key

1. A) The perimeter/DMZ facing the internet is most exposed to external threats.
2. A) A security overlay integrates security controls across all architecture layers.
3. A) A perimeter firewall segregates internal networks from untrusted external networks.
4. A) Defense in depth uses layered controls so remaining layers protect if one fails.

Chapter 3: Security Transformation Stage & Hardening Methodology

Q1. What is the goal of the security transformation stage?

- A) To systematically elevate the organization's security posture
- B) To buy more computers
- C) To hire janitors
- D) To paint offices

Q2. What does "hardening" mean in system security?

- A) Reducing attack surface by disabling unnecessary services and applying secure configurations
- B) Making the case physically harder
- C) Adding more users
- D) Overclocking the CPU

Q3. Which is a hardening step?

- A) Disabling unused ports and services
- B) Enabling guest accounts
- C) Using default passwords
- D) Sharing admin credentials

Q4. Why is a hardening methodology important?

- A) It provides a repeatable, consistent process for securing systems
- B) It makes systems slower
- C) It is not important
- D) It increases costs only

Answer Key

1. A) The security transformation stage systematically elevates the organization's security posture.
2. A) Hardening reduces attack surface by disabling unnecessary services and applying secure configurations.
3. A) Disabling unused ports and services is a key hardening step.
4. A) A hardening methodology provides a repeatable, consistent process for securing systems.

Chapter 4: Vulnerability Management & Software Security

Q1. What is vulnerability management?

- A) The continuous process of identifying, evaluating, and remediating security weaknesses
- B) Ignoring bugs
- C) Writing more code
- D) Buying hardware

Q2. Which activity is part of software security?

- A) Secure code review and penetration testing
- B) Skipping testing
- C) Hardcoding passwords
- D) Disabling logging

Q3. What is a CVE?

- A) Common Vulnerabilities and Exposures — a public catalog of known security flaws
- B) A type of CPU
- C) A video format
- D) A programming language

Q4. Why should software be patched promptly?

- A) Patches fix known vulnerabilities that attackers exploit
- B) Patches change the color scheme
- C) Patches are optional
- D) Patches delete data

Answer Key

1. A) Vulnerability management continuously identifies, evaluates, and remediates security weaknesses.
2. A) Secure code review and penetration testing are core software security activities.
3. A) CVE is the public catalog of Common Vulnerabilities and Exposures.
4. A) Prompt patching fixes known vulnerabilities before attackers exploit them.

Chapter 5: Security Engineering & Critical Security Controls

Q1. What is security engineering?

- A) Designing and building systems to be secure from the ground up
- B) Repairing broken chairs
- C) Painting walls
- D) Mowing lawns

Q2. Which is an example of a critical security control?

- A) Inventory and control of hardware/software assets
- B) Free coffee
- C) Casual Fridays
- D) Open Wi-Fi without password

Q3. Why are critical security controls prioritized?

- A) They mitigate the most common and damaging attacks
- B) They are the cheapest
- C) They look impressive
- D) They are optional

Q4. What does "secure by design" mean?

- A) Security is built into the system architecture from the start
- B) Adding security after deployment only
- C) Hoping for the best
- D) Ignoring threats

Answer Key

1. A) Security engineering designs and builds systems to be secure from the ground up.
2. A) Inventory and control of hardware/software assets is a foundational critical security control.
3. A) Critical controls are prioritized because they mitigate the most common and damaging attacks.
4. A) "Secure by design" means security is built into the architecture from the start.

Chapter 6: Risk Management Frameworks & Outsourced Asset Hardening

Q1. What is the purpose of a risk management framework?

- A) To systematically identify, assess, and mitigate information security risks
- B) To avoid all work
- C) To increase risks
- D) To eliminate IT

Q2. Which is a well-known risk management framework?

- A) NIST RMF
- B) A cookbook
- C) A travel guide
- D) A phone book

Q3. When outsourcing assets (e.g., cloud), what security practice is essential?

- A) Ensuring the provider meets hardening and compliance requirements via contracts and audits
- B) Trusting blindly
- C) No contracts needed
- D) Sharing all passwords

Q4. What is "hardening" for outsourced/cloud assets?

- A) Applying secure configurations and controls to cloud resources
- B) Making clouds physically hard
- C) Ignoring the provider
- D) Deleting backups

Answer Key

1. A) A risk management framework systematically identifies, assesses, and mitigates security risks.
2. A) NIST RMF is a well-known risk management framework.
3. A) Contracts and audits ensure outsourced providers meet hardening and compliance requirements.
4. A) Hardening cloud assets means applying secure configurations and controls to cloud resources.

End of Quiz

CS205 — 24 solved MCQs
Prepared by VU Learning HUB
vulearninghub.xyz