Examen de CEG 4399 Preparation QCM generer

Lecture 1-2 : Introduction

Q1: What is the primary goal of computer security?

A) To improve system performance
B) To safeguard data, hardware, and communication networks from unauthorized access
C) To enhance user experience
D) To reduce the cost of software development
Correct answer: B) To safeguard data, hardware, and communication networks from unauthorized access

Q2: What are the three main objectives of computer security, often referred to as the CIA triad?

A) Confidentiality, Integrity, Accountability
B) Confidentiality, Integrity, Availability
C) Confidentiality, Identification, Authentication
D) Confidentiality, Accessibility, Integrity
Correct answer: B) Confidentiality, Integrity, Availability

Q3: Which of the following refers to the assurance that information is not altered except in an authorized way?

A) Availability
B) Privacy
C) Integrity
D) Confidentiality
Correct answer: C) Integrity

Q4: What is a passive attack in computer security?

A) An attack where the attacker modifies the data stream
B) An attack that involves unauthorized monitoring or eavesdropping
C) An attack that blocks legitimate access to services
D) An attack that uses a virus to damage the system
Correct answer: B) An attack that involves unauthorized monitoring or eavesdropping

Q5: What is the purpose of security policies in an organization?

A) To increase software performance
B) To define rules and practices for protecting assets and systems
C) To reduce hardware costs
D) To monitor employee productivity
Correct answer: B) To define rules and practices for protecting assets and systems

Q6: Which term refers to any situation or entity that could potentially harm computer system assets?

A) Risk
B) Threat
C) Attack
D) Vulnerability
Correct answer: B) Threat

Q7: What is a vulnerability in the context of computer security?

A) A measure used to prevent unauthorized access
B) A potential flaw or weakness in a system that can be exploited
C) A device used to monitor network traffic
D) A cryptographic method to secure data
Correct answer: B) A potential flaw or weakness in a system that can be exploited

Q8: Which of the following is a type of active attack?

A) Eavesdropping
B) Replay attack
C) Traffic analysis
D) Scanning
Correct answer: B) Replay attack

Q9: What does the term "risk" refer to in computer security?

A) The likelihood that an attack will occur and the damage it may cause
B) The process of encrypting data for security
C) A legal framework for data protection
D) The prevention of unauthorized access
Correct answer: A) The likelihood that an attack will occur and the damage it may cause

Q10: In the context of threat modeling, what does the STRIDE technique refer to?

A) A cryptographic algorithm
B) A method for identifying threats like Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege
C) A risk assessment tool used to calculate vulnerabilities
D) A programming language used in secure software development
Correct answer: B) A method for identifying threats like Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege

—----------

Lecture 3 : Review of Cryptography

Q1: What is the main purpose of encryption?

A) To increase data transfer speed
B) To encode a message so its meaning is hidden
C) To store data securely on the cloud
D) To perform mathematical calculations
Correct answer: B) To encode a message so its meaning is hidden

Q2: In symmetric encryption, which of the following is true?

A) The encryption and decryption keys are the same
B) The encryption and decryption keys are different
C) It only uses a public key for encryption
D) It is not possible to decrypt the message
Correct answer: A) The encryption and decryption keys are the same

Q3: Which type of cipher uses multiple alphabets for encryption?

A) Mono-alphabetic cipher
B) Caesar cipher
C) Poly-alphabetic cipher
D) One-time pad cipher
Correct answer: C) Poly-alphabetic cipher

Q4: What is a "one-time pad" in cryptography?

A) A type of block cipher
B) A method of encryption where the key is the same length as the message and used only once
C) A cipher that shifts the alphabet by three letters
D) An algorithm used for key generation in RSA
Correct answer: B) A method of encryption where the key is the same length as the message and used only once

Q5: What is the main objective of transposition ciphers?

A) To change the characters of the plaintext
B) To rearrange the characters of the plaintext
C) To substitute each character with another
D) To use different keys for each letter
Correct answer: B) To rearrange the characters of the plaintext

Q6: What does AES stand for in cryptography?

A) Advanced Encryption Standard
B) Asymmetric Encryption System
C) Algorithm for Encrypted Security
D) Adaptive Encryption Scheme
Correct answer: A) Advanced Encryption Standard

Q7: In a cryptographic system, what is meant by the "avalanche effect"?

A) A small change in the key causes minimal changes in the ciphertext
B) A small change in the plaintext causes a significant change in the ciphertext
C) It refers to the failure of an encryption algorithm
D) A method of breaking a cipher through statistical analysis
Correct answer: B) A small change in the plaintext causes a significant change in the ciphertext

Q8: Which encryption algorithm uses both public and private keys?

A) DES
B) AES
C) RSA
D) Caesar cipher
Correct answer: C) RSA

Q9: What is the primary weakness of the Data Encryption Standard (DES)?

A) It is too slow for practical use
B) It is not based on mathematical principles
C) It uses a short key length, making it vulnerable to brute-force attacks
D) It uses a public key for both encryption and decryption
Correct answer: C) It uses a short key length, making it vulnerable to brute-force attacks

Q10: What is the key difference between stream ciphers and block ciphers?

A) Stream ciphers encrypt one symbol at a time, while block ciphers encrypt groups of symbols
B) Stream ciphers use asymmetric keys, and block ciphers use symmetric keys
C) Block ciphers are used for faster encryption
D) Stream ciphers are more secure than block ciphers
Correct answer: A) Stream ciphers encrypt one symbol at a time, while block ciphers encrypt groups of symbols

Q11: What does RSA encryption rely on for its security?

A) The difficulty of factoring large numbers
B) The use of random keys
C) The substitution of characters
D) The speed of modern processors
Correct answer: A) The difficulty of factoring large numbers

Q12: In the context of secret sharing, what is a (t, n)-threshold scheme?

A) A system where t participants must agree to change the encryption key
B) A system where any t participants out of n can reconstruct the secret
C) A system where t shares are needed to distribute the secret to n participants

D) A system where n participants must agree to a new encryption standard
Correct answer: B) A system where any t participants out of n can reconstruct the secret

---

Lecture 4 : Security in the Software Development Life Cycle

Q1: What is the main goal of integrating security into the Software Development Life Cycle (SDLC)?

A) To reduce software development costs
B) To prevent vulnerabilities and create secure software
C) To speed up software delivery
D) To test software performance
Correct answer: B) To prevent vulnerabilities and create secure software

Q2: At which phase of the SDLC should threat modeling be conducted to identify potential security issues?

A) Design phase
B) Implementation phase
C) Testing phase
D) Deployment phase
Correct answer: A) Design phase

Q3: Which of the following is a common software vulnerability that can lead to security breaches?

A) Inadequate documentation
B) Buffer overflow
C) Code redundancy
D) Lack of user interface testing
Correct answer: B) Buffer overflow

Q4: What is the primary goal of secure coding practices during the implementation phase?

A) To minimize code size
B) To prevent common flaws like input validation issues
C) To reduce development time
D) To improve the user interface design
Correct answer: B) To prevent common flaws like input validation issues

Q5: Which of the following tools can be used for static code analysis to detect vulnerabilities before deployment?

A) OWASP ZAP
B) Burp Suite
C) SonarQube
D) Penetration testing tools

Correct answer: C) SonarQube

Q6: What is the purpose of the "disposal" phase in the SDLC?

A) To deploy the software to the production environment
B) To remove or archive data securely and perform media sanitization
C) To add new features to the software
D) To perform software performance testing
Correct answer: B) To remove or archive data securely and perform media sanitization

Q7: Which SDLC model involves overlapping steps to ensure flexibility and minimize risks?

A) Waterfall model
B) Sashimi model
C) Spiral model
D) Agile model
Correct answer: B) Sashimi model

Q8: What is the main purpose of a Configuration Management Plan (CMP) according to NIST guidelines?

A) To manage system performance
B) To control changes and ensure they don’t affect security
C) To improve software usability
D) To track software sales and licenses
Correct answer: B) To control changes and ensure they don’t affect security

Q9: Which of the following is a common attack that exploits vulnerabilities in SQL databases?

A) Cross-Site Scripting (XSS)
B) Buffer overflow
C) SQL injection
D) Cross-Site Request Forgery (CSRF)
Correct answer: C) SQL injection

Q10: What is a key benefit of using dynamic code analysis tools?

A) They detect vulnerabilities without executing the code
B) They analyze code in real-time during execution to find vulnerabilities
C) They reduce the size of the codebase
D) They improve software usability testing
Correct answer: B) They analyze code in real-time during execution to find vulnerabilities

Q11: In the context of API security, what is a common threat associated with improper use of APIs?

A) SQL injection

B) Server-Side Request Forgery (SSRF)
C) Buffer overflow
D) Code redundancy
Correct answer: B) Server-Side Request Forgery (SSRF)

Q12: Which level of the Software Capability Maturity Model (CMM) involves a controlled and measured process?

A) Initial
B) Repeatable
C) Defined
D) Managed
Correct answer: D) Managed

Lecture 5 : Access Control and Management

Q1: What is the main function of access control?

A) To monitor network traffic
B) To allow or deny permission to specific resources
C) To encrypt all data in a system
D) To control user passwords
Correct answer: B) To allow or deny permission to specific resources

Q2: Which of the following is a type of physical access control?

A) Password authentication
B) Firewalls
C) Hardware-based door locks
D) Data encryption
Correct answer: C) Hardware-based door locks

Q3: In access control, what is the process of verifying a user's identity called?

A) Authorization
B) Authentication
C) Accounting
D) Identification
Correct answer: B) Authentication

Q4: What does RBAC stand for in access control?

A) Role-Based Access Control
B) Rule-Based Access Control
C) Resource-Based Access Control
D) Risk-Based Access Control
Correct answer: A) Role-Based Access Control

Q5: Which of the following models is considered the least restrictive in terms of access control?

A) Discretionary Access Control (DAC)
B) Mandatory Access Control (MAC)
C) Role-Based Access Control (RBAC)
D) Attribute-Based Access Control (ABAC)
Correct answer: A) Discretionary Access Control (DAC)

Q6: What is the primary characteristic of Mandatory Access Control (MAC)?

A) Users have full control over access permissions
B) Permissions are set based on system policies, not user discretion
C) Users can assign their permissions to others
D) It uses attributes like user location for access decisions
Correct answer: B) Permissions are set based on system policies, not user discretion

Q7: What are labels in the context of MAC (Mandatory Access Control)?

A) A form of encryption used to secure data
B) Classification levels assigned to objects and subjects
C) Access tokens distributed to users
D) Temporary permissions assigned to a user
Correct answer: B) Classification levels assigned to objects and subjects

Q8: Which access control model dynamically assigns roles to users based on predefined rules?

A) Attribute-Based Access Control (ABAC)
B) Rule-Based Role-Based Access Control (RB-RBAC)
C) Discretionary Access Control (DAC)
D) Mandatory Access Control (MAC)
Correct answer: B) Rule-Based Role-Based Access Control (RB-RBAC)

Q9: What is the purpose of the principle of least privilege in access control?

A) To grant users the maximum access rights possible
B) To restrict users to only the permissions necessary for their tasks
C) To allow users to change their own access permissions
D) To revoke all user access privileges automatically
Correct answer: B) To restrict users to only the permissions necessary for their tasks

Q10: Which of the following services provides centralized authentication and authorization in a network environment?

A) LDAP
B) RADIUS

C) Kerberos
D) TACACS+
Correct answer: B) RADIUS

Q11: What is the main purpose of Access Control Lists (ACLs)?

A) To track user login times
B) To specify which users or processes are allowed to access specific resources
C) To encrypt data on the network
D) To prevent unauthorized software installations
Correct answer: B) To specify which users or processes are allowed to access specific resources

Q12: Which protocol is commonly used to maintain distributed directory information services over a network?

A) RADIUS
B) LDAP
C) Kerberos
D) SAML
Correct answer: B) LDAP

—----------

Lecture 6 : Security in the Network and Internet

Q1: Which of the following is NOT a typical characteristic of networks?

A) Anonymity
B) Automation
C) Transparency
D) Routing diversity
Correct answer: C) Transparency

Q2: What does TCP/IP stand for?

A) Transmission Control Protocol/Internet Protocol
B) Transfer Communication Protocol/Internet Process
C) Technical Communication Process/Internet Program
D) Transmission Communication Protocol/Internal Process
Correct answer: A) Transmission Control Protocol/Internet Protocol

Q3: Which of the following is a vulnerability specific to networks?

A) Single user
B) Centralized control
C) Shared resources
D) No need for security policies
Correct answer: C) Shared resources

Q4: What is a typical characteristic of a Local Area Network (LAN)?

A) Covers a wide geographic area
B) Shared by multiple organizations
C) Locally controlled and physically protected
D) Exposed to the general public
Correct answer: C) Locally controlled and physically protected

Q5: Which of the following describes a "Man-in-the-Middle" attack?

A) An attacker intercepts communication between two parties and pretends to be one of them.
B) An attacker installs malware on a target system.
C) A legitimate user is blocked from accessing a network resource.
D) Sensitive information is encrypted before being transmitted.
Correct answer: A) An attacker intercepts communication between two parties and pretends to be one of them.

Q6: What is the purpose of a firewall in a network?

A) To enhance network speed
B) To prevent unauthorized access to or from a private network
C) To distribute data between different systems
D) To monitor internet usage
Correct answer: B) To prevent unauthorized access to or from a private network

Q7: Which of the following is NOT a type of firewall?

A) Stateful inspection
B) Application proxy
C) Intrusion Detection System (IDS)
D) Packet filtering gateway
Correct answer: C) Intrusion Detection System (IDS)

Q8: Which of the following is a characteristic of a Denial of Service (DoS) attack?

A) Flooding a server with excessive requests to exhaust its resources
B) Hacking into a server to steal data
C) Encrypting sensitive files on a server
D) Installing malware on multiple systems
Correct answer: A) Flooding a server with excessive requests to exhaust its resources

Q9: What is the primary function of encryption in network security?

A) To increase the speed of data transmission
B) To protect data by converting it into a format that is unreadable without a key
C) To allow easy sharing of sensitive information

D) To prevent data from being backed up
Correct answer: B) To protect data by converting it into a format that is unreadable without a key

Q10: What does a VPN (Virtual Private Network) do?

A) Blocks harmful websites
B) Provides anonymous browsing
C) Establishes a secure connection over a public network
D) Encrypts data at rest
Correct answer: C) Establishes a secure connection over a public network

—----------

bonus

Q1: What is the primary focus of the course CEG4399 - Design of Secure Computer Systems?

A) Software development practices
B) Fundamentals of secure system design and cybersecurity
C) Hardware optimization
D) Cloud infrastructure management
Correct answer: B) Fundamentals of secure system design and cybersecurity

Q2: Which of the following security principles are covered in the first week of the course?

A) Cryptography, PKI, and SSL
B) Confidentiality, Integrity, Availability (CIA)
C) Malware detection, Firewalls, VPNs
D) Software licensing and open-source tools
Correct answer: B) Confidentiality, Integrity, Availability (CIA)

Q3: What is a key goal of secure system design mentioned in the document?

A) Maximizing performance
B) Balancing security with risk
C) Reducing operational costs
D) Improving user interface design
Correct answer: B) Balancing security with risk

Q4: What is the significance of CrowdStrike in the context of this course?

A) It's a case study on software development best practices
B) It represents a real-world example of a major cybersecurity incident
C) It is a tool used for secure coding
D) It's an example of a new encryption standard
Correct answer: B) It represents a real-world example of a major cybersecurity incident

Q5: Which of the following is NOT mentioned as a focus area in the course structure?

A) Web Application Security
B) Mobile and IoT Security
C) Database performance optimization
D) Cloud Security
Correct answer: C) Database performance optimization

Q6: What is the importance of network security according to the course?

A) It prevents software crashes
B) It protects against vulnerabilities in communication protocols
C) It reduces hardware costs
D) It improves website design
Correct answer: B) It protects against vulnerabilities in communication protocols

Q7: Which type of assessment contributes the most to the overall grade in CEG4399?

A) Class activities
B) Midterm exam
C) Assignments
D) Final exam
Correct answer: D) Final exam (30%)

Q8: What is a recommended security practice for web application development, as mentioned in the course outline?

A) Use of deprecated libraries
B) Implementing firewalls and DDoS protection
C) Following OWASP Top 10 guidelines
D) Avoiding encryption for performance reasons
Correct answer: C) Following OWASP Top 10 guidelines

Q9: What is a key takeaway regarding the role of information in modern life according to the document?
A) Information is no longer as important in global transactions
B) Information flows are critical, and computing security is a high priority
C) Modern life can function without computerized systems
D) Data privacy is not a primary concern anymore
Correct answer: B) Information flows are critical, and computing security is a high priority

Q10: Which methodology is introduced in the course to address threats in software development?
A) Waterfall model
B) DevSecOps
C) Agile development
D) SCRUM
Correct answer: B) DevSecOps

Lecture 7 : Program Security

Q1: What is the primary difference between a fault and a failure in program security?

- A) A fault is external, while a failure is internal.
- B) A fault is the cause of a problem, and a failure is the effect.
- C) A failure occurs during development, and a fault occurs during execution.
- D) A fault results in positive outcomes, and a failure leads to errors.

Correct answer: B) A fault is the cause of a problem, and a failure is the effect.

Q2: What is a major drawback of the "penetrate and patch" method in program security?

- A) It introduces new faults while fixing existing ones.
- B) It focuses too much on user interface improvements.
- C) It reduces overall system performance significantly.
- D) It is only applicable to open-source software.

Correct answer: A) It introduces new faults while fixing existing ones.

Q3: How can flaws in secure programs be categorized?

- A) Inherent and inherited
- B) Intentional and inadvertent
- C) Active and passive
- D) Known and unknown

Correct answer: B) Intentional and inadvertent

Q4: What is a buffer overflow?

- A) An error caused by exceeding memory bounds in a program
- B) A security flaw where a file is not closed properly
- C) An error caused by incomplete mediation
- D) A type of encryption failure

Correct answer: A) An error caused by exceeding memory bounds in a program

---

Q5: What is a time-of-check to time-of-use error (TOCTTOU)?

- A) An error caused by modifying a resource after it has been checked but before use
- B) An error caused by incorrect initialization of variables
- C) An error caused by failure to encrypt sensitive data
- D) An error that occurs during system boot-up

Correct answer: A) An error caused by modifying a resource after it has been checked but before use

---

Q6: Which of the following is a characteristic of a resident virus?

- A) It only operates while the host program is running.
- B) It spreads through physical mediums only.
- C) It remains active in memory even after the host program ends.
- D) It requires user intervention for every replication.

Correct answer: C) It remains active in memory even after the host program ends.

Q7: What is a Trojan horse in the context of malicious code?

- A) A program that replicates itself across networks
- B) A piece of malicious software disguised as a legitimate program
- C) A virus that self-replicates indefinitely
- D) A network protocol vulnerability

Correct answer: B) A piece of malicious software disguised as a legitimate program

---

Q8: What distinguishes a worm from a virus?

- A) A worm requires a host program to operate, while a virus is standalone.
- B) A worm spreads via networks, whereas a virus can spread through any medium.
- C) A virus spreads faster than a worm.
- D) A worm causes more damage than a virus.

Correct answer: B) A worm spreads via networks, whereas a virus can spread through any medium.

Q9: What is the purpose of encapsulation in secure software development?

- A) To reduce code execution time
- B) To isolate program components for easier maintenance
- C) To ensure software usability
- D) To limit user interaction with the system

Correct answer: B) To isolate program components for easier maintenance

---

Q10: What does mutual suspicion imply in secure software design?

- A) All system components share a single access level.
- B) Sub-procedures and calling programs do not fully trust each other.
- C) All components must have the same encryption method.
- D) The system does not allow third-party modules.

Correct answer: B) Sub-procedures and calling programs do not fully trust each other.

Q11: Which type of testing evaluates the internal logic and structure of code?

- A) Black-box testing
- B) Regression testing
- C) White-box testing
- D) Penetration testing

Correct answer: C) White-box testing

Q12: Which testing type focuses on evaluating a system's vulnerability to malicious attacks?

- A) Unit testing
- B) Penetration testing
- C) Integration testing
- D) Performance testing

Correct answer: B) Penetration testing

Lecture 8 : Database Security and Inference Control

Q1: What is the primary function of a database?

- A) To store unstructured data
- B) To organize data by specifying relationships among the data
- C) To manage software execution
- D) To replace file systems entirely

Correct answer: B) To organize data by specifying relationships among the data

---

Q2: Which of the following is an advantage of a database over a simple file system?

- A) Minimal redundancy
- B) Decentralized data management
- C) Lack of shared access
- D) Lack of access control

Correct answer: A) Minimal redundancy

Q3: What is the purpose of physical database integrity?

- A) To ensure only authorized users access the database
- B) To make the database immune to physical failures like power outages
- C) To encrypt data at rest
- D) To enable shared access to data

Correct answer: B) To make the database immune to physical failures like power outages

---

Q4: What does auditability in database security ensure?

- A) Consistent data format
- B) The ability to track who accessed or modified the database
- C) Faster database queries
- D) Removal of redundant data

Correct answer: B) The ability to track who accessed or modified the database

---

Q5: What is the role of user authentication in database security?

- A) To speed up data retrieval
- B) To positively identify users for access and auditing purposes
- C) To encrypt database queries
- D) To allow anonymous access to sensitive data

Correct answer: B) To positively identify users for access and auditing purposes

---

Q6: What does the two-phase update process address?

- A) Inconsistent database queries
- B) Failures during data modification
- C) Unauthorized user access
- D) Redundant database fields

Correct answer: B) Failures during data modification

Q7: What are shadow fields used for in database security?

- A) Encrypting sensitive data
- B) Duplicating records to detect inconsistencies
- C) Creating temporary backups
- D) Allowing faster queries

Correct answer: B) Duplicating records to detect inconsistencies

---

Q8: What is the purpose of state constraints in database monitors?

- A) To ensure queries are optimized
- B) To prevent duplication of sensitive data
- C) To describe acceptable conditions of the entire database
- D) To encrypt data during transit

Correct answer: C) To describe acceptable conditions of the entire database

---

Q9: Which of the following factors can make data sensitive?

- A) Inherent sensitivity
- B) Declared sensitivity by a database administrator
- C) Sensitivity in relation to other disclosed data
- D) All of the above

Correct answer: D) All of the above

Q10: What type of sensitive data disclosure involves revealing that a value lies between two boundaries?

- A) Exact data
- B) Probable value
- C) Bounds
- D) Negative result

Correct answer: C) Bounds

Q11: What is a direct attack in the context of database inference?

- A) Using queries to directly deduce sensitive information
- B) Exploiting unencrypted data transfers
- C) Gaining unauthorized physical access to the database
- D) Using brute force to decrypt sensitive data

Correct answer: A) Using queries to directly deduce sensitive information

---

Q12: What is the "n items over k percent" rule used for in database security?

- A) To limit the number of database users
- B) To prevent revealing results dominated by a small group of individuals
- C) To encrypt sensitive database queries
- D) To control database replication rates

Correct answer: B) To prevent revealing results dominated by a small group of individuals

---

Q13: What is the purpose of suppression in database security?

- A) To prevent database backups
- B) To reject or withhold sensitive query results
- C) To speed up database operations
- D) To duplicate sensitive records

Correct answer: B) To reject or withhold sensitive query results

---

Q14: Which of the following is a method of concealing data in response to queries?

- A) Rounding values to a specified precision
- B) Disabling sensitive data encryption
- C) Limiting database user accounts
- D) Allowing only exact query matches

Correct answer: A) Rounding values to a specified precision

Q15: What is the purpose of random data perturbation in database security?

- A) To permanently alter sensitive data
- B) To add small errors to data for increased security
- C) To generate random queries for testing
- D) To reduce database access speed

Correct answer: B) To add small errors to data for increased security

---

Lecture 10 : Cloud deck

Q1: What was the main factor driving increased cloud usage, according to the document?

- A) Advancements in AI
- B) COVID-19 and remote work trends
- C) Cheaper cloud services
- D) Better encryption technologies

Correct answer: B) COVID-19 and remote work trends

Q2: Which of the following is the most commonly reported cloud security threat?

- A) Exfiltration of sensitive data
- B) Misconfiguration of cloud platforms
- C) Insecure APIs
- D) Denial of Service (DoS) attacks

Correct answer: B) Misconfiguration of cloud platforms

Q3: What percentage of cybersecurity professionals expressed concern about cloud security?

- A) 72%
- B) 64%
- C) 96%
- D) 81%

Correct answer: C) 96%

Q4: What is a significant barrier to cloud security adoption mentioned in the document?

- A) Lack of encryption tools
- B) Limited hardware support
- C) Lack of knowledge about cloud security features
- D) Excessive cost of cloud services

Correct answer: C) Lack of knowledge about cloud security features

---

Q5: Which of the following are key advantages of cloud-based security solutions?

- A) Faster deployment, scalability, and real-time threat detection
- B) Hardware independence and lack of regulatory compliance
- C) Exclusive use of public APIs
- D) Reduced need for encryption

Correct answer: A) Faster deployment, scalability, and real-time threat detection

---

Q6: What are common misconfigurations in cloud platforms that lead to breaches?

- A) Excessive encryption
- B) Improper access controls and publicly exposed sensitive data
- C) Lack of collaboration tools
- D) Use of third-party APIs

Correct answer: B) Improper access controls and publicly exposed sensitive data

---

Q7: What is the primary benefit of Identity and Access Management (IAM) in cloud environments?

- A) To store data securely
- B) To encrypt data in transit
- C) To control who has access to cloud resources and their permissions
- D) To eliminate all risks in multi-cloud systems

Correct answer: C) To control who has access to cloud resources and their permissions

---

Q8: Which tool is critical for monitoring and detecting threats in cloud environments?

- A) SIEM (Security Information and Event Management)
- B) Code compilers
- C) Cloud storage databases
- D) Firewalls only

Correct answer: A) SIEM (Security Information and Event Management)

Q9: Why is encryption essential in cloud security?

- A) It ensures faster data transfer
- B) It protects data at rest and in transit from unauthorized access
- C) It replaces the need for backups
- D) It reduces storage costs

Correct answer: B) It protects data at rest and in transit from unauthorized access

---

Q10: What is a key challenge in multi-cloud security?

- A) Limited storage capacity
- B) Lack of internet access
- C) Difficulty in enforcing consistent security policies across providers
- D) Overuse of automation tools

Correct answer: C) Difficulty in enforcing consistent security policies across providers

---

Q11: What is one of the main drivers for adopting cloud-native security solutions?

- A) Improved integration with traditional tools
- B) Scalability and real-time monitoring
- C) Reduced dependency on encryption
- D) Slower but more secure systems

Correct answer: B) Scalability and real-time monitoring

Q12: What is an effective mitigation strategy against cryptojacking in cloud environments?

- A) Manual threat analysis
- B) Real-time threat detection tools and encryption
- C) Limiting multi-cloud strategies
- D) Avoiding use of cloud-native tools

Correct answer: B) Real-time threat detection tools and encryption

---

Lecture : Identity and Access Management

Q1: What is the primary objective of Identity and Access Management (IAM)?

- A) To monitor network traffic
- B) To manage and control user access to systems and resources
- C) To enhance user interface design
- D) To prevent software crashes

Correct answer: B) To manage and control user access to systems and resources

---

Q2: Which of the following is a key component of IAM?

- A) Encryption protocols
- B) Role-based access control (RBAC)
- C) Network optimization
- D) Data storage solutions

Correct answer: B) Role-based access control (RBAC)

Q3: What does Multi-Factor Authentication (MFA) provide in IAM?

- A) A way to encrypt all communications
- B) An extra layer of security by requiring multiple verification methods
- C) A method to manage data backups
- D) A strategy to monitor user activity

Correct answer: B) An extra layer of security by requiring multiple verification methods

---

Q4: What is the primary advantage of using Single Sign-On (SSO) in IAM?

- A) It eliminates the need for user authentication
- B) It allows users to access multiple applications with one set of credentials
- C) It ensures data is encrypted during transmission
- D) It enhances system performance

Correct answer: B) It allows users to access multiple applications with one set of credentials

---

Q5: Which of the following is NOT an IAM feature?

- A) Privileged Access Management (PAM)
- B) Firewall configuration
- C) Identity Federation
- D) User provisioning and de-provisioning

Correct answer: B) Firewall configuration

Q6: What is Identity Federation in IAM?

- A) A process to store user credentials in one location
- B) A method to allow users to access multiple systems across organizations with a single identity
- C) A tool for encrypting user credentials
- D) A feature for blocking unauthorized users

Correct answer: B) A method to allow users to access multiple systems across organizations with a single identity

---

Q7: Which protocol is commonly used in IAM for authentication and authorization?

- A) TCP/IP
- B) SAML (Security Assertion Markup Language)
- C) FTP
- D) SMTP

Correct answer: B) SAML (Security Assertion Markup Language)

Q8: What is the purpose of user provisioning in IAM?

- A) To encrypt user credentials
- B) To create, update, and delete user accounts and permissions
- C) To monitor data transfer rates
- D) To enhance network bandwidth

Correct answer: B) To create, update, and delete user accounts and permissions

---

Q9: Why is auditing important in IAM?

- A) To improve system performance
- B) To identify and track unauthorized access attempts
- C) To optimize user interface design
- D) To reduce data storage requirements

Correct answer: B) To identify and track unauthorized access attempts

---

Q10: What is Privileged Access Management (PAM) focused on in IAM?

- A) Encrypting all data traffic
- B) Securing and monitoring access to critical systems by privileged accounts
- C) Ensuring fast network connectivity
- D) Managing user session logs

Correct answer: B) Securing and monitoring access to critical systems by privileged accounts

---

Q11: Which of the following is a common IAM challenge for organizations?

- A) Lack of encryption protocols
- B) Difficulty in managing user identities across multiple platforms
- C) Poor network bandwidth
- D) Outdated user interface designs

Correct answer: B) Difficulty in managing user identities across multiple platforms

---

Q12: What is the role of access controls in IAM?

- A) To manage user preferences
- B) To define who is allowed to access what resources and under what conditions
- C) To enhance software coding practices
- D) To streamline system updates

Correct answer: B) To define who is allowed to access what resources and under what conditions

---

Bonus : OWASP Top 10 - 2017

Q1: What is the main purpose of the OWASP Top 10 project?

- A) To provide coding standards
- B) To identify the most critical web application security risks
- C) To develop open-source tools
- D) To improve software usability

Correct answer: B) To identify the most critical web application security risks

---

Q2: Which two new issues were added to the OWASP Top 10 - 2017 based on community feedback?

- A) Injection and Sensitive Data Exposure
- B) Insecure Deserialization and Insufficient Logging & Monitoring
- C) Security Misconfiguration and Broken Authentication
- D) Cross-Site Scripting and XML External Entities

Correct answer: B) Insecure Deserialization and Insufficient Logging & Monitoring

---

Q3: What is an injection flaw?

- A) A failure in session management
- B) Sending untrusted data to an interpreter as part of a command or query

- C) The misuse of cryptographic algorithms
- D) Failure to validate input length

Correct answer: B) Sending untrusted data to an interpreter as part of a command or query

---

Q4: Which is NOT a method to prevent injection flaws?

- A) Using parameterized queries
- B) Escaping special characters in queries
- C) Validating user inputs
- D) Using default database configurations

Correct answer: D) Using default database configurations

Q5: Which scenario indicates broken authentication?

- A) Passwords are stored in plain text
- B) The application uses a strong password policy
- C) Multi-factor authentication is enforced
- D) Session IDs are rotated after login

Correct answer: A) Passwords are stored in plain text

Q6: What is one way to prevent broken authentication vulnerabilities?

- A) Use default credentials for all admin accounts
- B) Implement multi-factor authentication
- C) Avoid using hashed passwords
- D) Allow long session expiration times

Correct answer: B) Implement multi-factor authentication

Q7: Which of the following is a common consequence of sensitive data exposure?

- A) Session hijacking
- B) Identity theft
- C) SQL injection
- D) Buffer overflow

Correct answer: B) Identity theft

Q8: What is a recommended practice to protect sensitive data?

- A) Storing sensitive data in clear text
- B) Using strong encryption algorithms
- C) Disabling security headers
- D) Avoiding HTTPS connections

Correct answer: B) Using strong encryption algorithms

Q9: Which of the following is an example of security misconfiguration?

- A) Using default error messages
- B) Properly configuring security headers
- C) Disabling unused features
- D) Using strong encryption protocols

Correct answer: A) Using default error messages

Q10: How can security misconfiguration be mitigated?

- A) Ignoring software updates
- B) Automating configuration review processes
- C) Disabling HTTPS
- D) Allowing directory listing by default

Correct answer: B) Automating configuration review processes

Q11: What is a typical consequence of insufficient logging and monitoring?

- A) Rapid breach detection
- B) Delayed detection of malicious activities
- C) Increased system performance
- D) Reduced number of alerts

Correct answer: B) Delayed detection of malicious activities

Q12: Which practice can improve logging and monitoring?

- A) Disabling all logs to save disk space
- B) Using standardized logging formats and alerting
- C) Ignoring unusual login patterns
- D) Storing logs without any access control

Correct answer: B) Using standardized logging formats and alerting

---

Bonus : CompTIA Security+ Acronyms Cheatsheet

Q1: What does AAA stand for in the context of security?

- A) Advanced Application Analysis
- B) Authentication, Authorization, and Accounting
- C) Automated Access Architecture
- D) Advanced Access Algorithm

Correct answer: B) Authentication, Authorization, and Accounting

---

Q2: What is the purpose of ACL (Access Control List)?

- A) To encrypt sensitive files
- B) To specify access permissions for users and systems
- C) To monitor data usage
- D) To configure firewall settings

Correct answer: B) To specify access permissions for users and systems

---

Q3: What is AES commonly used for?

- A) Intrusion detection
- B) File system organization
- C) Symmetric encryption
- D) Wireless communication

Correct answer: C) Symmetric encryption

Q4: Which protocol is responsible for translating IP addresses to MAC addresses?

- A) ARP (Address Resolution Protocol)
- B) DHCP (Dynamic Host Configuration Protocol)
- C) DNS (Domain Name System)
- D) NAT (Network Address Translation)

Correct answer: A) ARP (Address Resolution Protocol)

Q5: What does ABAC stand for?

- A) Attribute-based Access Control
- B) Algorithm-based Automated Control
- C) Access-based Application Control
- D) Audit-based Authentication Control

Correct answer: A) Attribute-based Access Control

Q6: What is the main use of a DMZ (Demilitarized Zone) in network security?

- A) Encrypting network traffic
- B) Isolating sensitive data from external access
- C) Protecting the internal network by exposing only specific services to the internet
- D) Monitoring data flow between endpoints

Correct answer: C) Protecting the internal network by exposing only specific services to the internet

---

Q7: Which of the following defines the purpose of Multi-Factor Authentication (MFA)?

- A) To enhance password length
- B) To require multiple forms of verification for access
- C) To simplify user login processes
- D) To eliminate the need for passwords

Correct answer: B) To require multiple forms of verification for access

---

Q8: What is a CA (Certificate Authority)?

- A) A system for granting network access
- B) An organization that issues and manages digital certificates
- C) A tool for encrypting sensitive files
- D) A software for malware detection

Correct answer: B) An organization that issues and manages digital certificates

---

Q9: What is an APT (Advanced Persistent Threat)?

- A) A short-term vulnerability exploit
- B) A long-term, targeted attack often by organized groups
- C) A type of phishing attack
- D) A vulnerability in public networks

Correct answer: B) A long-term, targeted attack often by organized groups

---

Q10: What does DDoS stand for?

- A) Distributed Denial of Service
- B) Dual Data Optimization System
- C) Decentralized Data Overlap Service
- D) Data Directory Output Sequence

Correct answer: A) Distributed Denial of Service

Q11: What is the purpose of a DRP (Disaster Recovery Plan)?

- A) To encrypt data during transit
- B) To ensure business continuity in the event of a disaster
- C) To monitor network traffic in real-time
- D) To automate routine system maintenance

Correct answer: B) To ensure business continuity in the event of a disaster

---

Q12: What does SIEM stand for in security systems?

- A) System Information and Execution Monitoring
- B) Secure Information and Encryption Management
- C) Security Information and Event Management
- D) Standard Information Encoding Methodology

Correct answer: C) Security Information and Event Management

—----------

Bonus : Common CompTIA Simulations Type Questions

Q1: What is the purpose of a DMZ (Demilitarized Zone) in a network?

- A) To isolate sensitive data from external access
- B) To expose external-facing services to the internet while protecting internal systems
- C) To increase network performance
- D) To encrypt all internal communications

Correct answer: B) To expose external-facing services to the internet while protecting internal systems

---

Q2: What does the private IP address range `172.30.80.57` indicate?

- A) Loopback
- B) Multicast
- C) Private IP address
- D) APIPA

Correct answer: C) Private IP address

Q3: What is the purpose of port 443 in network security?

- A) SMTP (email sending)
- B) HTTP (unsecured web access)
- C) HTTPS (secured web access)
- D) SSH (secure shell access)

Correct answer: C) HTTPS (secured web access)

Q4: Which factor of authentication is associated with biometric data like fingerprints or retina scans?

- A) Something you know
- B) Something you have
- C) Something you are
- D) Somewhere you are

Correct answer: C) Something you are

Q5: What authentication mechanism is implemented when an employee uses a smart card and a PIN to access a system?

- A) Single-factor authentication
- B) Two-factor authentication
- C) Multi-factor authentication
- D) Password-based authentication

Correct answer: B) Two-factor authentication

Q6: Which encryption type is used with WPA2 for securing wireless networks?

- A) RC4
- B) DES

- C) AES
- D) 3DES

Correct answer: C) AES

Q7: What is the recommended non-overlapping channel selection for 802.11g wireless networks?

- A) Channels 1, 6, 11
- B) Channels 2, 4, 8
- C) Channels 3, 5, 9
- D) Channels 7, 8, 9

Correct answer: A) Channels 1, 6, 11

Q8: What type of attack is described by an email sent to multiple users containing a malicious link to verify credentials?

- A) Spoofing
- B) Phishing
- C) Vishing
- D) Whaling

Correct answer: B) Phishing

Q9: A phone call is made to the CEO of an organization asking for sensitive financial data. What type of attack does this represent?

- A) Social engineering
- B) Vishing
- C) Whaling
- D) Pharming

Correct answer: C) Whaling

Q10: Which protocol should be allowed in a firewall rule to permit secure file transfers?

- A) HTTP
- B) SCP
- C) Telnet
- D) FTP

Correct answer: B) SCP

Q11: What is the correct port number for Remote Desktop Protocol (RDP)?

- A) 22
- B) 3389
- C) 443
- D) 80

Correct answer: B) 3389

Q12: What is the correct order of volatility in incident response?

- A) Network traffic, cache, RAM, disk
- B) Disk, RAM, network traffic, cache
- C) RAM, network traffic, cache, disk
- D) Cache, network traffic, disk, RAM

Correct answer: A) Network traffic, cache, RAM, disk

Q13: What does a honeypot simulate in a network environment?

- A) A legitimate target to attract and analyze attacks
- B) A firewall to block traffic
- C) A database for backup purposes
- D) A proxy server for content filtering

Correct answer: A) A legitimate target to attract and analyze attacks

---

Q14: What access control model restricts access based on a user's role within an organization?

- A) Mandatory Access Control (MAC)
- B) Discretionary Access Control (DAC)
- C) Role-Based Access Control (RBAC)
- D) Attribute-Based Access Control (ABAC)

Correct answer: C) Role-Based Access Control (RBAC)

Q15: In the context of security policies, what does a mantrap provide?

- A) A method to monitor network access
- B) A physical security mechanism to prevent tailgating
- C) A tool for encrypting sensitive data
- D) A software tool to log access attempts

Correct answer: B) A physical security mechanism to prevent tailgating

---

Bonus : CISSP Prep - Chapter 6: Identity and Access Management

Q1: What is Type 3 authentication?

- A) Something you know
- B) Something you have
- C) Something you are
- D) Somewhere you are

Correct answer: C) Something you are

Q2: Which of the following is an example of a dynamic password?

- A) A reusable password
- B) A one-time password
- C) A password that changes at regular intervals
- D) A passphrase

Correct answer: C) A password that changes at regular intervals

---

Q3: What is the purpose of a salt in password security?

- A) To encrypt passwords
- B) To make hashed passwords unique and resistant to rainbow table attacks
- C) To speed up the hashing process
- D) To replace plaintext passwords

Correct answer: B) To make hashed passwords unique and resistant to rainbow table attacks

---

Q4: Which access control model assigns permissions based on a user's job function?

- A) Discretionary Access Control (DAC)

- B) Mandatory Access Control (MAC)
- C) Role-Based Access Control (RBAC)
- D) Rule-Based Access Control

Correct answer: C) Role-Based Access Control (RBAC)

Q5: In which model do users have complete control over their resources?

- A) Mandatory Access Control (MAC)
- B) Role-Based Access Control (RBAC)
- C) Discretionary Access Control (DAC)
- D) Non-Discretionary Access Control

Correct answer: C) Discretionary Access Control (DAC)

Q6: What is the focus of Task-Based Access Control?

- A) Assigning permissions based on job roles
- B) Assigning permissions based on tasks a user must perform
- C) Controlling access based on organizational hierarchy
- D) Applying access rules dynamically

Correct answer: B) Assigning permissions based on tasks a user must perform

---

Q7: What is the False Accept Rate (FAR) in biometrics?

- A) When a legitimate user is denied access
- B) When an unauthorized user is granted access
- C) When the biometric system fails completely
- D) When the system is unable to identify the user

Correct answer: B) When an unauthorized user is granted access

---

Q8: Why are retina scans rarely used in biometric systems?

- A) Low accuracy compared to other methods
- B) Health risks and invasion-of-privacy concerns
- C) They are less secure than fingerprint scans
- D) They are easily fooled by photographs

Correct answer: B) Health risks and invasion-of-privacy concerns

---

Q9: What is a major risk of Single Sign-On (SSO)?

- A) Increased system complexity
- B) Difficulty in implementation
- C) A single compromise can lead to access across multiple systems
- D) Redundancy in access management

Correct answer: C) A single compromise can lead to access across multiple systems

---

Q10: Which protocol is commonly used to support Single Sign-On (SSO) on the internet?

- A) RADIUS
- B) Kerberos
- C) Security Assertion Markup Language (SAML)
- D) LDAP

Correct answer: C) Security Assertion Markup Language (SAML)

Q11: What is Identity as a Service (IDaaS)?

- A) A type of cloud service for integrating identity management and authentication
- B) A security protocol for user authentication
- C) A tool for managing user passwords
- D) A service for monitoring access logs

Correct answer: A) A type of cloud service for integrating identity management and authentication

---

Q12: What is the purpose of an Access Provisioning Lifecycle?

- A) To audit user accounts for compliance
- B) To manage user access rights throughout their association with an organization
- C) To control password complexity
- D) To enforce biometric authentication

Correct answer: B) To manage user access rights throughout their association with an organization

---

Q13: What is a primary advantage of Kerberos over other authentication protocols?

- A) It supports public key encryption
- B) It prevents replay attacks and ensures mutual authentication

- C) It is faster than LDAP
- D) It uses plaintext transmission for simplicity

Correct answer: B) It prevents replay attacks and ensures mutual authentication

---

Q14: What is the primary use of RADIUS in identity management?

- A) To enforce password policies
- B) To provide centralized authentication for remote access
- C) To encrypt user sessions
- D) To manage local device access

Correct answer: B) To provide centralized authentication for remote access