

## Introduction

Fill-in-the-Blank Questions:

1. \_\_\_\_\_ est la pratique consistant à protéger les données, le matériel et les logiciels contre l'accès non autorisé.  
**Réponse:** La sécurité informatique
2. L'objectif principal de la sécurité informatique est de préserver la confidentialité, l'intégrité et \_\_\_\_\_ des ressources du système.  
**Réponse:** La disponibilité
3. Les attaques passives, comme \_\_\_\_\_, consistent à surveiller les transmissions pour obtenir des informations.  
**Réponse:** L'écoute clandestine (eavesdropping)
4. Le modèle de défense en profondeur utilise des mesures préventives, détectives et \_\_\_\_\_ pour protéger les systèmes.  
**Réponse:** Correctives
5. Les menaces comme \_\_\_\_\_ visent à empêcher l'utilisation légitime d'un système en saturant les ressources disponibles.  
**Réponse:** Les attaques par déni de service (DoS)
6. \_\_\_\_\_ est un outil de modélisation des menaces qui classe les risques selon le dommage, la reproductibilité, l'exploitabilité, les utilisateurs touchés et la découvrabilité.  
**Réponse:** DREAD
7. L'architecture de sécurité de l'OSI inclut des mécanismes comme le chiffrement, les pare-feu et \_\_\_\_\_ pour protéger les données en transit.  
**Réponse:** Les contrôles d'accès
8. \_\_\_\_\_ signifie limiter les privilèges des utilisateurs pour réduire les risques d'exploitation.  
**Réponse:** Minimiser les privilèges
9. Une vulnérabilité "Zero-day" est exploitée avant qu'un correctif ou \_\_\_\_\_ ne soit disponible pour la corriger.  
**Réponse:** Un patch
10. \_\_\_\_\_ représente les points d'entrée potentiels pour des attaques, y compris les ports ouverts et les dépendances logicielles.  
**Réponse:** La surface d'attaque

## Review of Cryptography

1. \_\_\_\_\_ cryptography uses a single key for both encryption and decryption.  
**Answer:** Symmetric
2. In public-key cryptography, the key used for encryption is called the \_\_\_\_\_ key.  
**Answer:** Public

3. A hash function is used to ensure \_\_\_\_\_ of data.  
**Answer:** Integrity
4. The RSA algorithm relies on the mathematical difficulty of factoring large \_\_\_\_\_.  
**Answer:** Prime numbers
5. In cryptography, the term \_\_\_\_\_ refers to converting plain text into an unreadable format.  
**Answer:** Encryption
6. \_\_\_\_\_ is the process of verifying the authenticity of a message or document using a digital signature.  
**Answer:** Authentication
7. The \_\_\_\_\_ protocol is widely used to secure communications over the internet, such as in HTTPS.  
**Answer:** TLS (Transport Layer Security)
8. \_\_\_\_\_ cryptography ensures secure communication without the need to exchange secret keys in advance.  
**Answer:** Asymmetric
9. The \_\_\_\_\_ algorithm is an example of a block cipher.  
**Answer:** AES (Advanced Encryption Standard)
10. A \_\_\_\_\_ attack involves an unauthorized party attempting to decrypt a message without a key.  
**Answer:** Brute force

## Access Control and Management-2

Fill-in-the-Blank Questions:

1. \_\_\_\_\_ refers to the process of granting or denying permission to utilize specific resources within a system or environment.  
**Answer:** Access control
2. In access control, \_\_\_\_\_ is the process of verifying the identity by checking the validity of the credentials presented.  
**Answer:** Authentication
3. The \_\_\_\_\_ access control model assigns access permissions based on user roles within an organization.  
**Answer:** Role-Based Access Control (RBAC)
4. A \_\_\_\_\_ is a centralized database on a network that stores crucial information about users, devices, and network resources.  
**Answer:** Directory service
5. The \_\_\_\_\_ principle ensures that users or systems are only granted the minimal levels of access necessary to complete their tasks.  
**Answer:** Least privilege
6. In the \_\_\_\_\_ model, the resource owner decides who can access specific resources and can transfer permissions to others.

**Answer:** Discretionary Access Control (DAC)

7. \_\_\_\_\_ ensures users cannot perform high-privileged operations unless explicitly authorized in Microsoft Windows systems.

**Answer:** User Access Control (UAC)

8. The \_\_\_\_\_ access control model uses attributes like user roles, environmental conditions, and object characteristics to determine access.

**Answer:** Attribute-Based Access Control (ABAC)

9. \_\_\_\_\_ is a security protocol that uses strong encryption methods to authenticate users and protect sensitive data.

**Answer:** Kerberos

10. The \_\_\_\_\_ phase in account auditing ensures a user's access controls and roles are still appropriate and necessary.

**Answer:** Recertification

## **Security-In-The-Software-Development-Life-Cycle\_**

Fill-in-the-Blank Questions:

1. \_\_\_\_\_ vulnerabilities occur when more data is written to a buffer than it can hold, potentially causing crashes or unauthorized code execution.

**Answer:** Buffer overflow

2. The \_\_\_\_\_ phase in the Software Development Lifecycle is responsible for identifying and mitigating vulnerabilities in the code before deployment.

**Answer:** Testing

3. \_\_\_\_\_ refers to the practice of integrating security measures into every phase of the Software Development Lifecycle (SDLC).

**Answer:** Secure software development

4. A \_\_\_\_\_ attack involves inserting malicious SQL code into queries to manipulate the database.

**Answer:** SQL injection

5. In software security, \_\_\_\_\_ code analysis refers to analyzing source code without executing it to identify vulnerabilities.

**Answer:** Static

6. The principle of \_\_\_\_\_ ensures that users and systems have the minimum level of access required to perform their tasks.

**Answer:** Least privilege

7. A \_\_\_\_\_ model in software development involves overlapping steps to ensure flexibility and early risk assessment.

**Answer:** Spiral

8. In secure software practices, \_\_\_\_\_ disclosure involves notifying the vendor of a vulnerability privately and giving them time to patch it before public release.

**Answer:** Responsible

9. The \_\_\_\_\_ maturity level of the Software Capability Maturity Model (CMM) focuses on a controlled and measured process for software development.

**Answer:** Managed

10. In database security, a \_\_\_\_\_ attack combines many low-privilege records to deduce high-privilege data.

**Answer:** Aggregation

## Security-In-The-Network and Internet

Fill-in-the-Blank Questions:

1. \_\_\_\_\_ encryption is applied between two applications to secure data from one end to the other.

**Answer:** End-to-end

2. In network security, a \_\_\_\_\_ attack involves sending excessive requests to a server to overwhelm it and deny service to legitimate users.

**Answer:** Denial of Service (DoS)

3. A \_\_\_\_\_ firewall keeps track of the state of network connections and does not treat each packet in isolation.

**Answer:** Stateful inspection

4. In a \_\_\_\_\_ attack, an attacker intercepts communications between two parties to modify or steal data without their knowledge.

**Answer:** Man-in-the-Middle

5. \_\_\_\_\_ is a security tool that monitors and analyzes network traffic to detect suspicious activities and prevent potential attacks.

**Answer:** Intrusion Detection System (IDS)

6. In a \_\_\_\_\_ network, all devices use the same public IP address but retain unique private IPs, masking internal device addresses.

**Answer:** Network Address Translation (NAT)

7. A \_\_\_\_\_ is a malicious program controlled remotely, often used to carry out Distributed Denial of Service (DDoS) attacks.

**Answer:** Bot

8. The \_\_\_\_\_ model is the framework for network communication with layers such as physical, data link, and application layers.

**Answer:** OSI

9. A \_\_\_\_\_ is a separate network area designed to allow limited access for external users, often used to secure public-facing services.

**Answer:** Demilitarized Zone (DMZ)

10. In email security, \_\_\_\_\_ ensures that the sender cannot deny having sent the message.

**Answer:** Nonrepudiation

## Cissp-Prep-Chapter-6.-Identity-And-Access-Management

Fill-in-the-Blank Questions:

1. \_\_\_\_\_ authentication relies on verifying a user's unique biological characteristics, such as fingerprints or iris patterns.  
**Answer:** Biometric
2. A \_\_\_\_\_ token is synchronized with a central server and changes values based on time or a counter.  
**Answer:** Synchronous dynamic
3. \_\_\_\_\_ is a centralized authentication protocol that uses symmetric encryption to prevent eavesdropping and replay attacks.  
**Answer:** Kerberos
4. In access control models, the \_\_\_\_\_ model assigns permissions based on user roles within an organization.  
**Answer:** Role-Based Access Control (RBAC)
5. The \_\_\_\_\_ model assigns clearance levels to subjects and labels to objects, typically used in high-security environments.  
**Answer:** Mandatory Access Control (MAC)
6. A \_\_\_\_\_ password is valid for only one use and cannot be reused.  
**Answer:** One-time
7. The \_\_\_\_\_ rate in biometric systems measures the probability of incorrectly rejecting an authorized user.  
**Answer:** False Reject
8. \_\_\_\_\_ is a federated identity framework that enables Single Sign-On (SSO) by exchanging authentication information using XML.  
**Answer:** Security Assertion Markup Language (SAML)
9. In the lifecycle of access provisioning, \_\_\_\_\_ occurs when users accumulate permissions from old roles without losing previous access rights.  
**Answer:** Authorization creep
10. \_\_\_\_\_ is a stronger password technique where random values are added before hashing to make rainbow tables less effective.  
**Answer:** Salting

## Cloud deck

Fill-in-the-Blank Questions:

1. \_\_\_\_\_ is the primary concern in cloud security, with many organizations worried about accidental data exposure or loss.  
**Answer:** Data loss/leakage
2. The lack of \_\_\_\_\_ about cloud security features remains a significant barrier to its adoption.  
**Answer:** Knowledge

3. In cloud security, the risk of \_\_\_\_\_ is increasing, with attackers exploiting misconfigurations in cloud platforms.  
**Answer:** Misconfiguration
4. \_\_\_\_\_ encryption protects sensitive data both at rest and during transmission across cloud environments.  
**Answer:** Data
5. Organizations often face challenges with securing \_\_\_\_\_, which are vital for interacting with cloud services.  
**Answer:** APIs
6. \_\_\_\_\_ is a cloud security tool that helps monitor and prevent unauthorized data transfers in the cloud.  
**Answer:** Data Loss Prevention (DLP)
7. Cloud-based security solutions offer \_\_\_\_\_ scalability, enabling organizations to adapt quickly to changes.  
**Answer:** Better
8. The adoption of \_\_\_\_\_ security solutions is driven by faster deployment and better integration with cloud environments.  
**Answer:** Cloud-native
9. In cloud security, \_\_\_\_\_ control mechanisms help restrict access to cloud resources and ensure proper authentication.  
**Answer:** Access
10. \_\_\_\_\_ is essential in cloud security to manage encrypted data and ensure that it remains protected from unauthorized access.  
**Answer:** Key management
11. \_\_\_\_\_ remains the leading cause of cloud security breaches, often resulting from improper access controls or exposed sensitive data.  
**Answer:** Misconfiguration
12. To prevent unauthorized access, organizations should implement \_\_\_\_\_, which adds an additional layer of security to user logins.  
**Answer:** Multi-factor authentication
13. The lack of qualified \_\_\_\_\_ is a major barrier for organizations trying to secure their cloud environments effectively.  
**Answer:** Cloud security specialists
14. In cloud security, \_\_\_\_\_ tools help monitor and prevent unauthorized data transfers, mitigating data exfiltration risks.  
**Answer:** Data Loss Prevention (DLP)
15. \_\_\_\_\_ APIs are a significant threat in cloud environments, as they can be exploited to gain unauthorized access to cloud services.  
**Answer:** Insecure
16. Cloud-native security solutions are designed specifically for cloud environments and offer better \_\_\_\_\_ and scalability than traditional tools.  
**Answer:** Integration
17. To address data privacy and compliance concerns, cloud environments must ensure the use of strong \_\_\_\_\_ algorithms like AES-256.  
**Answer:** Encryption
18. A \_\_\_\_\_ environment introduces unique security challenges as each provider has its own security model.  
**Answer:** Multi-cloud
19. Organizations must continuously update and refine their \_\_\_\_\_ strategies to stay ahead of attackers in the cloud.  
**Answer:** Threat detection
20. Cloud governance frameworks help enforce \_\_\_\_\_ policies and ensure compliance with industry regulations and standards.  
**Answer:** Security