Chapter 1 – Security Principles

Q1. Security that is appropriate to the level of risk and potential harm is known as:

A. Defense in depth
B. Risk management
C. **Adequate security**
D. Risk avoidance

✓ **Correct Answer:** Adequate security
📝 Security controls should match the level of risk and potential damage.

Q2. Which type of control is implemented through policies, procedures, and processes?

A. Technical controls
B. Physical controls
C. **Administrative controls**
D. Detective controls

✓ **Correct Answer:** Administrative controls
📝 Policies, procedures, and approvals are administrative safeguards.

Q3. The ability of systems to simulate human intelligence is called:

A. Automation
B. Machine learning
C. **Artificial Intelligence**
D. Robotics

✓ **Correct Answer:** Artificial Intelligence
📝 AI enables systems to perform tasks that normally require human intelligence.

Q4. Anything of value owned by an organization is referred to as a(n):

A. Resource
B. **Asset**
C. Threat
D. Vulnerability

✓ **Correct Answer:** Asset
📝 Assets include systems, data, property, and intellectual property.

Q5. The process of verifying a user's claimed identity is known as:

A. Authorization
B. Accounting
C. **Authentication**
D. Auditing

✓ **Correct Answer:** Authentication
📝 Authentication confirms who the user is.

Q6. Granting permissions to an authenticated user is called:

A. Authentication
B. **Authorization**
C. Identification
D. Auditing

✅ **Correct Answer:** Authorization
📝 Authorization defines what a user is allowed to do.

Q7. Ensuring information is accessible when needed by authorized users refers to:

A. Confidentiality
B. Integrity
C. **Availability**
D. Authenticity

✅ **Correct Answer:** Availability
📝 Availability ensures systems and data are usable when required.

Q8. The minimum acceptable security configuration is known as:

A. Benchmark
B. Policy
C. **Baseline**
D. Standard

✅ **Correct Answer:** Baseline
📝 A baseline defines the lowest allowed security level.

Q9. Fingerprints, iris scans, and voice recognition are examples of:

A. Tokens
B. Credentials
C. **Biometrics**
D. Certificates

✅ **Correct Answer:** Biometrics
📝 Biometrics use physical or behavioral characteristics.

Q10. Malware that allows attackers to remotely control infected systems is called a:

A. Virus
B. Worm
C. **Bot**
D. Spyware

✅ **Correct Answer:** Bot
📝 Bots enable attackers to control systems remotely.

Q11. Information that requires protection from unauthorized disclosure is called:

A. Public data
B. **Classified or sensitive information**
C. Open data
D. Metadata

✓ **Correct Answer:** Classified or sensitive information
📝 Such data must be protected due to its value or impact.

Q12. Preventing unauthorized disclosure of information refers to:

A. Integrity
B. Availability
C. **Confidentiality**
D. Authenticity

✓ **Correct Answer:** Confidentiality
📝 Confidentiality ensures data is only accessed by authorized users.

Q13. The importance of information to business success is known as:

A. Sensitivity
B. **Criticality**
C. Impact
D. Risk

✓ **Correct Answer:** Criticality
📝 Criticality measures how essential information is to operations.

Q14. Ensuring data is not altered without authorization refers to:

A. Confidentiality
B. Availability
C. **Integrity**
D. Authenticity

✓ **Correct Answer:** Integrity
📝 Integrity protects data accuracy and completeness.

Q15. Converting plaintext into ciphertext is called:

A. Hashing
B. Encoding
C. **Encryption**
D. Obfuscation

✓ **Correct Answer:** Encryption
📝 Encryption protects data confidentiality.

Q16. Which regulation protects personal data of EU citizens?

A. HIPAA
B. PCI-DSS
C. **GDPR**
D. SOX

✓ **Correct Answer:** GDPR
📝 GDPR enforces strict privacy and data protection rules.

Q17. The framework for managing and making organizational decisions is known as:

A. Compliance
B. **Governance**
C. Risk treatment
D. Auditing

✓ **Correct Answer:** Governance
📝 Governance defines roles, policies, and decision-making processes.

Q18. The primary U.S. law protecting healthcare information is:

A. GDPR
B. SOX
C. **HIPAA**
D. GLBA

✓ **Correct Answer:** HIPAA
📝 HIPAA protects patient health information.

Q19. The amount of damage a threat could cause is called:

A. Likelihood
B. Probability
C. **Impact**
D. Risk

✓ **Correct Answer:** Impact
📝 Impact measures potential harm.

Q20. The potential harm resulting from a threat exploiting a vulnerability is known as:

A. Threat
B. Vulnerability
C. **Information security risk**
D. Control

✓ **Correct Answer:** Information security risk
📝 Risk combines likelihood and impact.

Q21. Ensuring data accuracy and consistency for its intended purpose refers to:

A. Confidentiality
B. **Integrity**
C. Availability
D. Authenticity

✓ **Correct Answer:** Integrity
📝 Integrity ensures trustworthy information.

Q22. Which organization develops international standards like ISO/IEC 27001?

A. IETF
B. IEEE
C. **ISO**
D. NIST

✓ **Correct Answer:** ISO
📝 ISO publishes global standards.

Q23. Which organization defines internet protocols such as TCP/IP?

A. IEEE
B. **IETF**
C. ISO
D. NIST

✓ **Correct Answer:** IETF
📝 IETF develops internet standards.

Q24. The chance that a vulnerability will be exploited is known as:

A. Impact
B. **Likelihood**
C. Risk
D. Threat

✓ **Correct Answer:** Likelihood
📝 Likelihood measures probability of occurrence.

Q25. A subjective estimate of threat exploitation probability is called:

A. Impact rating
B. **Likelihood of occurrence**
C. Risk tolerance
D. Probability

✓ **Correct Answer:** Likelihood of occurrence
📝 It reflects expert judgment rather than statistics.

Q26. Using two or more authentication factors is known as:

A. SSO
B. **Multi-factor authentication**
C. Biometric authentication
D. Token authentication

✓ **Correct Answer:** Multi-factor authentication
📝 MFA increases security by combining factors.

Q27. Which U.S. organization publishes SP 800 security standards?

A. ISO
B. IEEE
C. **NIST**
D. IETF

✓ **Correct Answer:** NIST
📝 NIST provides U.S. federal security guidance.

Q28. The inability to deny performing an action is known as:

A. Integrity
B. Authentication
C. **Non-repudiation**
D. Authorization

✅ **Correct Answer:** Non-repudiation
📝 Ensures actions cannot be denied later.

Q29. Information that can identify an individual is called:

A. PHI
B. **PII**
C. PCI data
D. Classified data

✅ **Correct Answer:** PII
📝 PII includes names, SSNs, and biometrics.

Q30. Security controls such as locks, fences, and guards are:

A. Administrative
B. Technical
C. **Physical controls**
D. Detective controls

✅ **Correct Answer:** Physical controls
📝 Physical controls protect facilities and assets.

Q31. An individual's right to control personal information refers to:

A. Confidentiality
B. **Privacy**
C. Integrity
D. Security

✅ **Correct Answer:** Privacy
📝 Privacy focuses on personal data rights.

Q32. The chance that a threat will exploit a vulnerability is called:

A. Risk
B. Impact
C. **Probability**
D. Sensitivity

✅ **Correct Answer:** Probability
📝 Probability measures chance of occurrence.

Q33. Healthcare-related personal data is known as:

A. PII
B. **PHI**

C. PCI
D. Classified data

✓ **Correct Answer:** PHI
📝 PHI is protected under HIPAA.

Q34. Risk analysis using labels such as low, medium, and high is:

A. Quantitative analysis
B. **Qualitative risk analysis**
C. Cost analysis
D. Impact analysis

✓ **Correct Answer:** Qualitative risk analysis
📝 Uses descriptive values instead of numbers.

Q35. Risk analysis using numerical values is known as:

A. Qualitative analysis
B. **Quantitative risk analysis**
C. Baseline analysis
D. Threat analysis

✓ **Correct Answer:** Quantitative risk analysis
📝 Uses statistics and monetary values.

Q36. A possible event that could cause harm is called a:

A. Vulnerability
B. **Risk**
C. Control
D. Asset

✅ **Correct Answer:** Risk
📝 Risk represents potential negative events.

Q37. Accepting risk without additional controls is known as:

A. Risk mitigation
B. Risk transference
C. **Risk acceptance**
D. Risk avoidance

✅ **Correct Answer:** Risk acceptance
📝 The organization chooses to live with the risk.

Q38. Identifying and analyzing organizational risks is called:

A. Risk treatment
B. **Risk assessment**
C. Risk avoidance
D. Risk transfer

✅ **Correct Answer:** Risk assessment
📝 It evaluates threats and vulnerabilities.

Q39. Choosing not to perform a risky activity is known as:

A. Risk acceptance
B. Risk mitigation
C. **Risk avoidance**
D. Risk transfer

✅ **Correct Answer:** Risk avoidance
📝 The risk is eliminated by avoiding the activity.

Q40. The overall process of managing risks is called:

A. Risk assessment
B. **Risk management**
C. Risk treatment
D. Governance

✅ **Correct Answer:** Risk management
📝 It includes identification, assessment, and monitoring.

Q41. A structured approach for managing enterprise risk is:

A. ISO standard
B. **Risk Management Framework**
C. Baseline
D. Control set

✅ **Correct Answer:** Risk Management Framework
📝 RMF provides a systematic risk approach.

Q42. Implementing controls to reduce risk is known as:

A. Risk acceptance
B. Risk transfer
C. **Risk mitigation**
D. Risk avoidance

✓ **Correct Answer:** Risk mitigation
📝 Controls reduce likelihood or impact.

Q43. The amount of risk an organization is willing to accept is called:

A. Risk impact
B. Risk likelihood
C. **Risk tolerance**
D. Risk threshold

✓ **Correct Answer:** Risk tolerance
📝 Defines acceptable risk levels.

Q44. Shifting risk to a third party is known as:

A. Risk acceptance
B. Risk avoidance
C. **Risk transference**
D. Risk mitigation

✅ **Correct Answer:** Risk transference
📝 Insurance is a common example.

Q45. Selecting how to respond to risk is known as:

A. Risk management
B. Risk assessment
C. **Risk treatment**
D. Risk tolerance

✅ **Correct Answer:** Risk treatment
📝 Determines mitigation, acceptance, transfer, or avoidance.

Q46. Safeguards protecting confidentiality, integrity, and availability are called:

A. Threats
B. Vulnerabilities
C. **Security controls**
D. Assets

✅ **Correct Answer:** Security controls
📝 Controls protect systems and information.

Q47. The importance of data protection based on value is known as:

A. Criticality
B. **Sensitivity**

C. Integrity
D. Impact

✓ **Correct Answer:** Sensitivity
📝 Sensitive data requires stronger protection.

Q48. Authentication using only one factor is called:

A. MFA
B. **Single-factor authentication**
C. Biometric authentication
D. Adaptive authentication

✓ **Correct Answer:** Single-factor authentication
📝 Uses only one credential type.

Q49. The condition of an entity at a specific time is called:

A. Status
B. **State**
C. Mode
D. Phase

✓ **Correct Answer:** State
📝 State represents a snapshot in time.

Q50. A system operating correctly without unauthorized changes has:

A. Data integrity
B. Confidentiality
C. **System integrity**
D. Availability

✓ **Correct Answer:** System integrity
📝 System integrity ensures reliable operation.

Q51. Controls implemented via hardware or software are:

A. Administrative
B. Physical
C. **Technical controls**
D. Preventive controls

✓ **Correct Answer:** Technical controls
📝 Firewalls and encryption are technical controls.

Q52. Any potential cause of harm to a system is called a:

A. Vulnerability
B. Risk
C. **Threat**
D. Asset

✓ **Correct Answer:** Threat
📝 Threats exploit vulnerabilities.

Q53. An individual or group that carries out an attack is a:

A. Threat
B. **Threat actor**
C. Vulnerability
D. Asset owner

✓ **Correct Answer:** Threat actor
📝 Threat actors initiate attacks.

Q54. The method used to carry out an attack is known as:

A. Threat source
B. **Threat vector**
C. Vulnerability
D. Exploit

✓ **Correct Answer:** Threat vector
📝 Vectors describe attack paths.

Q55. A physical device used for authentication is called a:

A. Certificate
B. Biometric
C. **Token**
D. Password

✓ **Correct Answer:** Token
📝 Tokens are something you have.

Q56. A weakness that can be exploited is called a:

A. Threat
B. **Vulnerability**
C. Risk
D. Control

✓ **Correct Answer:** Vulnerability
📝 Vulnerabilities enable attacks.

Q57. Which organization develops networking and engineering standards?

A. ISO
B. IETF
C. **IEEE**
D. NIST

✓ **Correct Answer:** IEEE
📝 IEEE defines standards like 802.3 and 802.11.

Chapter 2 – Incident Response, Business Continuity and Disaster Recovery Concepts

---

Q1. Events such as system crashes, malware execution, or web defacement are called:

A. Incidents
B. Events
C. **Adverse events**
D. Breaches

✓ **Correct Answer:** Adverse events
📝 These events cause negative impact to systems or operations.

Q2. Unauthorized access or disclosure of personally identifiable information is known as a:

A. Incident
B. Exploit
C. **Breach**
D. Threat

✓ **Correct Answer:** Breach
📝 A breach involves loss of control over sensitive personal data.

Q3. Ensuring critical business operations continue during disruptions is known as:

A. Disaster recovery
B. Incident response
C. **Business continuity**
D. Risk management

✅ **Correct Answer:** Business continuity
📝 Focuses on maintaining essential functions during disruptions.

Q4. A documented plan for sustaining business operations during disruption is a:

A. DRP
B. BIA
C. **Business Continuity Plan (BCP)**
D. IRP

✅ **Correct Answer:** BCP
📝 BCP outlines how operations continue during and after disruption.

Q5. An analysis identifying system priorities and dependencies is called:

A. Risk assessment
B. **Business Impact Analysis (BIA)**
C. Gap analysis
D. Threat modeling

✅ **Correct Answer:** BIA
📝 BIA determines critical systems and acceptable downtime.

Q6. Restoring IT services after an outage is referred to as:

A. Business continuity
B. **Disaster recovery**

C. Incident handling
D. Risk mitigation

✅ **Correct Answer:** Disaster recovery
📝 DR focuses on restoring IT infrastructure and services.

Q7. A documented plan for recovering systems after a disaster is a:

A. BCP
B. IRP
C. **Disaster Recovery Plan (DRP)**
D. SOP

✅ **Correct Answer:** DRP
📝 DRP defines recovery steps after major disruptions.

Q8. Any observable occurrence in a system or network is called a:

A. Incident
B. **Event**
C. Threat
D. Exploit

✅ **Correct Answer:** Event
📝 Not all events are security incidents.

Q9. An attack that takes advantage of a vulnerability is known as an:

A. Incident
B. Threat
C. **Exploit**
D. Breach

✓ **Correct Answer:** Exploit
📝 Exploits leverage system weaknesses.

Q10. An event that jeopardizes confidentiality, integrity, or availability is a:

A. Event
B. Threat
C. **Incident**
D. Vulnerability

✓ **Correct Answer:** Incident
📝 Incidents require investigation and response.

Q11. Mitigating violations of security policies is known as:

A. Disaster recovery
B. **Incident handling**
C. Risk acceptance
D. Auditing

✓ **Correct Answer:** Incident handling
📝 Includes detection, analysis, and containment.

Q12. Coordinated actions to respond to security incidents are called:

A. Incident handling
B. Business continuity
C. **Incident response**
D. Risk mitigation

✅ **Correct Answer:** Incident response
📝 Focuses on responding and limiting damage.

Q13. A documented plan for detecting and responding to cyberattacks is a:

A. DRP
B. BCP
C. **Incident Response Plan (IRP)**
D. SOP

✅ **Correct Answer:** IRP
📝 IRP provides structured response procedures.

Q14. Unauthorized access attempts to a system are known as:

A. Breaches
B. **Intrusions**
C. Exploits
D. Threats

✅ **Correct Answer:** Intrusion
📝 Intrusions involve unauthorized system access.

Q15. A centralized team monitoring security events is called a:

A. CSIRT
B. NOC
C. **Security Operations Center (SOC)**
D. CERT

✓ **Correct Answer:** SOC
📝 SOC monitors, detects, and responds to incidents.

Q16. A weakness that can be exploited by a threat is a:

A. Threat
B. Incident
C. **Vulnerability**
D. Exploit

✓ **Correct Answer:** Vulnerability
📝 Vulnerabilities enable successful attacks.

Q17. An unknown vulnerability with no existing patch is called a:

A. Threat
B. Exploit
C. **Zero-day vulnerability**
D. Breach

✓ **Correct Answer:** Zero-day vulnerability
📝 Zero-days are exploited before detection or fixes exist.

Chapter 3 – Access Control Concepts

Q1. An independent review of system activities and records is known as:

A. Logging
B. Monitoring
C. **Audit**
D. Assessment

✓ **Correct Answer:** Audit
📝 Audits ensure compliance and control effectiveness.

Q2. Designing spaces to reduce crime using environmental features is called:

A. Physical security
B. **CPTED**
C. Defense in depth
D. Access control

✓ **Correct Answer:** CPTED
📝 CPTED discourages criminal behavior through design.

Q3. Using multiple security layers to protect assets is known as:

A. Segmentation
B. **Defense in depth**
C. Least privilege
D. Hardening

✅ **Correct Answer:** Defense in depth
📝 Multiple layers increase resistance to attacks.

Q4. Access control where owners decide permissions is:

A. MAC
B. RBAC
C. **DAC**
D. ABAC

✅ **Correct Answer:** DAC
📝 Owners control access rights.

Q5. Protecting data by converting it into unreadable form is called:

A. Encoding
B. Hashing
C. **Encryption**
D. Masking

✅ **Correct Answer:** Encryption
📝 Encryption ensures confidentiality.

Q6. Devices that filter network traffic based on rules are:

A. IDS
B. Routers
C. **Firewalls**
D. Proxies

✓ **Correct Answer:** Firewalls
📝 Firewalls enforce network security policies.

Q7. A trusted individual who misuses access is an example of:

A. External attacker
B. **Insider threat**
C. Threat vector
D. Hacker

✓ **Correct Answer:** Insider threat
📝 Insiders already have authorized access.

Q8. Apple's mobile operating system is called:

A. Android
B. macOS
C. **iOS**
D. Unix

✓ **Correct Answer:** iOS
📝 iOS is used on iPhones and iPads.

Q9. Multiple consecutive security controls are known as:

A. Segmentation
B. **Layered defense**
C. Hardening
D. Isolation

✓ **Correct Answer:** Layered defense
📝 Also referred to as defense in depth.

Q10. An open-source operating system is:

A. Windows
B. iOS
C. **Linux**
D. macOS

✓ **Correct Answer:** Linux
📝 Linux source code is publicly available.

Q11. An unusual pattern found in logs is called a:

A. Event
B. Incident

C. **Log anomaly**
D. Alert

✓ **Correct Answer:** Log anomaly
📝 May indicate suspicious activity.

Q12. Recording system and user activities is known as:

A. Monitoring
B. Auditing
C. **Logging**
D. Reporting

✓ **Correct Answer:** Logging
📝 Logs support detection and investigations.

Q13. Systems that control user access to resources are called:

A. Physical access systems
B. **Logical access control systems**
C. Network controls
D. Monitoring systems

✓ **Correct Answer:** Logical access control systems
📝 They enforce authentication and authorization.

Q14. Access control managed strictly by system policy is:

A. DAC
B. RBAC
C. **Mandatory Access Control (MAC)**
D. ABAC

✓ **Correct Answer:** Mandatory Access Control
📝 Users cannot change permissions.

Q15. A security doorway allowing only one person at a time is a:

A. Turnstile
B. **Mantrap**
C. Gate
D. Airlock

✓ **Correct Answer:** Mantrap
📝 Prevents tailgating.

Q16. A passive entity containing information is called a:

A. Subject
B. **Object**
C. Asset
D. Token

✓ **Correct Answer:** Object
📝 Objects store or receive data.

Q17. Security controls such as locks and guards are:

A. Technical controls
B. Administrative controls
C. **Physical access controls**
D. Preventive controls

✓ **Correct Answer:** Physical access controls
📝 They protect physical assets and locations.

Q18. Granting only minimum required permissions follows the:

A. Defense in depth
B. **Principle of least privilege**
C. Separation of duties
D. Zero trust

✓ **Correct Answer:** Principle of least privilege
📝 Limits damage from compromised accounts.

Q19. Accounts with elevated permissions are called:

A. User accounts
B. Service accounts
C. **Privileged accounts**
D. Guest accounts

✓ **Correct Answer:** Privileged accounts
📝 Require strict monitoring and control.

Q20. Malware that locks data until payment is made is:

A. Trojan
B. Worm
C. **Ransomware**
D. Spyware

✅ **Correct Answer:** Ransomware
📝 Extorts victims for system access.

Q21. Access permissions based on job roles use:

A. DAC
B. MAC
C. **RBAC**
D. ABAC

✅ **Correct Answer:** RBAC
📝 Simplifies permission management.

Q22. Instructions allowing or denying access are known as:

A. Policies
B. **Rules**
C. Permissions
D. Controls

✅ **Correct Answer:** Rule
📝 Rules enforce access decisions.

Q23. Ensuring one person cannot complete a task alone is:

A. Least privilege
B. **Segregation of duties**
C. RBAC
D. Auditing

✅ **Correct Answer:** Segregation of duties
📝 Reduces insider threat risk.

Q24. An active entity accessing objects is called a:

A. Object
B. Asset
C. **Subject**
D. User

✅ **Correct Answer:** Subject
📝 Subjects perform actions on objects.

Q25. Security controls implemented via software or hardware are:

A. Administrative
B. Physical

C. **Technical controls**
D. Detective

✅ **Correct Answer:** Technical controls
📝 Examples include firewalls and encryption.

Q26. A one-way barrier allowing single-person entry is a:

A. Mantrap
B. Gate
C. **Turnstile**
D. Fence

✅ **Correct Answer:** Turnstile
📝 Controls physical entry flow.

Q27. An operating system commonly used in development is:

A. Windows
B. Linux
C. **Unix**
D. iOS

✅ **Correct Answer:** Unix
📝 Unix is widely used in enterprise and development environments.

Q28. Managing the lifecycle of user accounts is called:

A. Access control
B. Authentication
C. **User provisioning**
D. Auditing

✓ **Correct Answer:** User provisioning
📝 Includes creating, modifying, and disabling accounts.

Chapter 4 – Network Security

Q1. A set of routines, standards, protocols, and tools for building software applications to access web-based software is called:

A. Protocols
B. Middleware
C. **Application Programming Interface (API)**
D. Framework

✓ **Correct Answer:** Application Programming Interface (API)
📝 APIs allow software to communicate with other software or services.

Q2. The smallest unit of data at OSI Layer 1 is a:

A. Byte
B. Packet
C. **Bit**
D. Frame

✅ **Correct Answer:** Bit
📝 Represents 0 or 1 in digital communication.

Q3. A one-to-many transmission in networking is called:

A. Unicast
B. Multicast
C. **Broadcast**
D. Anycast

✅ **Correct Answer:** Broadcast
📝 Broadcasts send data to all devices in a network segment.

Q4. A unit of digital information consisting of 8 bits is called a:

A. Bit
B. **Byte**
C. Packet
D. Segment

✅ **Correct Answer:** Byte
📝 A byte is the standard data unit for storage and communication.

Q5. On-demand network access to shared computing resources is:

A. SaaS
B. **Cloud Computing**

C. LAN
D. VPN

✅ **Correct Answer:** Cloud Computing
📝 Provides scalable, on-demand resources with minimal management.

Q6. A cloud infrastructure used exclusively by a group of organizations with shared concerns is a:

A. Private Cloud
B. Public Cloud
C. **Community Cloud**
D. Hybrid Cloud

✅ **Correct Answer:** Community Cloud
📝 Shared infrastructure for organizations with similar requirements.

Q7. The process of unpacking or revealing bundled data is:

A. Encryption
B. **De-encapsulation**
C. Hashing
D. Fragmentation

✅ **Correct Answer:** De-encapsulation
📝 Opposite of encapsulation in networking.

Q8. Preventing authorized access or delaying critical operations is a:

A. Firewall
B. Virus
C. **Denial-of-Service (DoS)**
D. Zero trust attack

✅ **Correct Answer:** Denial-of-Service (DoS)
📝 DoS attacks disrupt services temporarily or permanently.

Q9. A service, server, and network protocol acronym for resolving domain names:

A. SMTP
B. DHCP
C. **DNS**
D. FTP

✅ **Correct Answer:** DNS
📝 Translates human-readable domain names to IP addresses.

Q10. Hiding and bundling data and methods during development is:

A. Encryption
B. **Encapsulation**
C. Obfuscation
D. Fragmentation

✅ **Correct Answer:** Encapsulation
📝 Encapsulation protects data and organizes code.

Q11. Converting plaintext into unreadable form is:

A. Hashing
B. **Encryption**
C. Decryption
D. Encoding

✅ **Correct Answer:** Encryption
📝 Encryption ensures confidentiality of data in transit or storage.

Q12. The standard internet protocol for transferring files between hosts is:

A. HTTP
B. SMTP
C. **FTP**
D. SNMP

✅ **Correct Answer:** FTP
📝 FTP is used to upload/download files between systems.

Q13. Fragmenting traffic to prevent reassembly is a:

A. DoS attack
B. Spoofing attack

C. **Fragment attack**
D. Man-in-the-middle attack

✅ **Correct Answer:** Fragment attack
📝 Exploits packet reassembly vulnerabilities.

Q14. The physical parts of a computer are:

A. Software
B. Protocols
C. **Hardware**
D. Firmware

✅ **Correct Answer:** Hardware
📝 Includes CPU, memory, storage devices, and peripherals.

Q15. A combination of public and private cloud storage is called:

A. Public cloud
B. **Hybrid cloud**
C. Private cloud
D. Community cloud

✅ **Correct Answer:** Hybrid cloud
📝 Some data resides in private cloud, some in public cloud.

Q16. Core computing, storage, and network resources offered as an outsourced service is:

A. SaaS
B. PaaS
C. **IaaS**
D. DaaS

✅ **Correct Answer:** IaaS
📝 Infrastructure as a Service allows deployment of virtual servers, storage, and networks.

Q17. Protocol used to determine host availability is:

A. TCP
B. UDP
C. **ICMP**
D. ARP

✅ **Correct Answer:** ICMP
📝 Used by ping and traceroute utilities.

Q18. Protocol for packet-switched data transmission is:

A. FTP
B. **IPv4**
C. SMTP
D. DNS

✅ **Correct Answer:** IPv4
📝 Internet Protocol provides addressing and routing.

Q19. An attacker intercepting and modifying communication is:

A. Phishing
B. Spoofing
C. **Man-in-the-Middle (MITM)**
D. DoS

✅ **Correct Answer:** Man-in-the-Middle
📝 MITM intercepts communication to steal or alter data.

Q20. Breaking LANs into small zones to enforce granular security is:

A. VLAN
B. NAT
C. **Microsegmentation**
D. Zero Trust

✅ **Correct Answer:** Microsegmentation
📝 Enhances security by isolating workloads and traffic.

Q21. Sending packets larger than expected to crash a system is a:

A. Ping sweep
B. Fragment attack

C. **Oversized Packet Attack**
D. MITM attack

✅ **Correct Answer:** Oversized Packet Attack
📝 Exploits buffer limitations on receiving systems.

Q22. Data representation at OSI Layer 3 is called a:

A. Frame
B. Segment
C. **Packet**
D. Byte

✅ **Correct Answer:** Packet
📝 Packets carry Layer 3 addresses and payload.

Q23. The main action of malware is its:

A. Exploit
B. Trojan
C. **Payload**
D. Virus

✅ **Correct Answer:** Payload
📝 Payload is the harmful part of malware.

Q24. Security standard for credit/debit card processors is:

A. HIPAA
B. ISO 27001
C. **PCI DSS**
D. NIST

✅ **Correct Answer:** PCI DSS
📝 Governs payment data security for merchants.

Q25. Middleware environment for building cloud apps is:

A. IaaS
B. **PaaS**
C. SaaS
D. DaaS

✅ **Correct Answer:** PaaS
📝 Platform as a Service simplifies app development and deployment.

Q26. Cloud platform behind corporate firewall is:

A. Public cloud
B. Hybrid cloud
C. **Private cloud**
D. Community cloud

✅ **Correct Answer:** Private cloud
📝 Offers enterprise control and compliance benefits.

Q27. Rules and procedures enabling system communication are:

A. Standards
B. Frameworks
C. **Protocols**
D. Policies

✓ **Correct Answer:** Protocols
📝 Protocols define communication behavior between devices.

Q28. Cloud infrastructure open to general public is:

A. Private cloud
B. Hybrid cloud
C. **Public cloud**
D. Community cloud

✓ **Correct Answer:** Public cloud
📝 Public cloud services are accessible by anyone.

Q29. Standard email sending/receiving protocol is:

A. POP3
B. IMAP
C. **SMTP**
D. FTP

✓ **Correct Answer:** SMTP
📝 Simple Mail Transfer Protocol is used for sending emails.

Q30. Programs and data that are executed or used by hardware are:

A. Firmware
B. **Software**
C. CPU
D. Protocol

✓ **Correct Answer:** Software
📝 Software enables hardware to perform tasks.

Q31. Cloud applications accessed from clients without managing infrastructure is:

A. PaaS
B. IaaS
C. **SaaS**
D. DaaS

✓ **Correct Answer:** SaaS
📝 Software as a Service delivers apps via the cloud.

Q32. Faking the sender address to gain unauthorized access is:

A. MITM
B. Sniffing
C. **Spoofing**
D. Phishing

✅ **Correct Answer:** Spoofing
📝 Spoofing disguises the source to bypass security.

Q33. IETF network model specifying four layers is:

A. OSI model
B. **TCP/IP model**
C. Internet model
D. Layered model

✅ **Correct Answer:** TCP/IP Model
📝 TCP/IP has Link, Internet, Transport, and Application layers.

Q34. Logical group of network devices in the same LAN is a:

A. VPN
B. VLAN
C. Subnet
D. Domain

✅ **Correct Answer:** VLAN
📝 VLANs group devices logically regardless of location.

Q35. Secure communication tunnel over existing networks is:

A. VLAN
B. SSL

C. **VPN**
D. MPLS

✓ **Correct Answer:** VPN
📝 VPN encrypts traffic between endpoints.

Q36. Wireless LAN network is:

A. WAN
B. LAN
C. **WLAN**
D. PAN

✓ **Correct Answer:** WLAN
📝 WLANs use radio instead of wired connections.

Q37. GUI for Nmap Security Scanner is:

A. Zenmap
B. Wireshark
C. **Zenmap**
D. Kali GUI

✓ **Correct Answer:** Zenmap
📝 Provides graphical interface to Nmap scanning tool.

Q38. Security model removing trusted network assumption is:

A. Microsegmentation
B. NAC
C. **Zero Trust**
D. VLAN

✓ **Correct Answer:** Zero Trust
📝 Zero Trust assumes no implicit trust in any network segment.

Chapter 5 – Security Operations

Q1. A computer responsible for hosting applications to user workstations is called:

A. Database Server
B. Web Server
C. **Application Server**
D. Proxy Server

✓ **Correct Answer:** Application Server
📝 Hosts business applications and serves them to client computers.

Q2. An algorithm that uses one key to encrypt and a different key to decrypt data is:

A. Symmetric Encryption
B. **Asymmetric Encryption**

C. Hashing
D. Digital Signature

✅ **Correct Answer:** Asymmetric Encryption
📝 Public key encrypts, private key decrypts.

Q3. A digit representing the sum of correct digits in stored or transmitted data used to detect errors is:

A. Hash
B. **Checksum**
C. Digital Signature
D. Ciphertext

✅ **Correct Answer:** Checksum
📝 Helps detect accidental errors in data transmission.

Q4. The altered form of a plaintext message, unreadable to unauthorized users, is:

A. Ciphertext
B. Plaintext
C. Hash
D. Checksum

✅ **Correct Answer:** Ciphertext
📝 Encrypted data that hides the original message.

Q5. Identifying the degree of harm if data is exposed is:

A. Sensitivity
B. **Classification**
C. Encryption
D. Risk Assessment

✓ **Correct Answer:** Classification
📝 Determines the confidentiality level required.

Q6. A process to ensure only authorized changes are made to a system is:

A. Change Management
B. Patch Management
C. **Configuration Management**
D. Logging

✓ **Correct Answer:** Configuration Management
📝 Prevents unauthorized or unverified system modifications.

Q7. One who studies cryptography techniques to attempt defeating them is called:

A. Cryptographer
B. **Cryptanalyst**
C. Hacker
D. Security Engineer

✅ **Correct Answer:** Cryptanalyst
📝 Focuses on analyzing and breaking cryptographic methods.

Q8. The study or application of methods to secure messages, files, or information is:

A. Encryption
B. **Cryptography**
C. Hashing
D. Security Analysis

✅ **Correct Answer:** Cryptography
📝 Ensures confidentiality, integrity, and authentication.

Q9. System capabilities designed to detect and prevent unauthorized transmission of information are:

A. Firewall
B. IDS
C. IPS
D. **Data Loss Prevention (DLP)**

✅ **Correct Answer:** Data Loss Prevention (DLP)
📝 Prevents sensitive data from leaving the organization.

Q10. The reverse of encryption, converting ciphertext back to plaintext, is:

A. Hashing
B. Encryption
C. **Decryption**
D. Encoding

✓ **Correct Answer:** Decryption
📝 Uses the cryptographic key to recover the original message.

Q11. A technique of erasing data to prevent magnetic remanence recovery is:

A. Overwriting
B. **Degaussing**
C. Shredding
D. Wiping

✓ **Correct Answer:** Degaussing
📝 Demagnetizes storage media to destroy residual data.

Q12. A cryptographic transformation providing origin authentication, integrity, and non-repudiation is:

A. Hash
B. Digital Certificate
C. **Digital Signature**
D. Ciphertext

✓ **Correct Answer:** Digital Signature
📝 Confirms sender identity and data integrity.

Q13. Monitoring outgoing network traffic is called:

A. Ingress Monitoring
B. **Egress Monitoring**
C. Traffic Analysis
D. Packet Sniffing

✅ **Correct Answer:** Egress Monitoring
📝 Helps detect data exfiltration and policy violations.

Q14. Converting plaintext to ciphertext is also called:

A. Encryption
B. Decryption
C. Hashing
D. Encoding

✅ **Correct Answer:** Encryption
📝 Ensures that data cannot be read by unauthorized users.

Q15. Total set of algorithms, processes, and tools providing encryption/decryption is:

A. Encryption Algorithm
B. Key Management System
C. **Encryption System**
D. Cryptography

✅ **Correct Answer:** Encryption System
📝 Includes software, hardware, and procedures for cryptography.

Q16. Applying secure configurations to reduce attack surface is called:

A. Patching
B. **Hardening**
C. Configuration Management
D. Security Governance

✅ **Correct Answer:** Hardening
📝 Reduces vulnerabilities in systems and applications.

Q17. Algorithm computing a numeric fingerprint for a file or message is:

A. Checksum
B. Encryption
C. **Hash Function**
D. Digital Signature

✅ **Correct Answer:** Hash Function
📝 Produces a fixed-size value representing the data.

Q18. Using a mathematical algorithm to produce a numeric representative value is:

A. Encryption
B. **Hashing**
C. Decryption
D. Digital Signature

✓ **Correct Answer:** Hashing
📝 Often used to verify integrity of data.

Q19. The requirements for information sharing between IT systems are:

A. Protocols
B. APIs
C. **Information Sharing**
D. Middleware

✓ **Correct Answer:** Information Sharing
📝 Ensures interoperability across multiple systems.

Q20. Monitoring incoming network traffic is called:

A. Egress Monitoring
B. **Ingress Monitoring**
C. Firewalling
D. Network Sniffing

✓ **Correct Answer:** Ingress Monitoring
📝 Detects threats entering the network.

Q21. A digital signature uniquely identifying data is called:

A. Checksum
B. Hash Function
C. **Message Digest**
D. Fingerprint

✓ **Correct Answer:** Message Digest
📝 Small fixed-size representation of a larger data block.

Q22. The software master control program of a computer is:

A. Application
B. BIOS
C. Firmware
D. **Operating System**

✓ **Correct Answer:** Operating System
📝 Manages hardware and application interactions.

Q23. Software component that modifies files or device settings without version change is:

A. Upgrade
B. Patch
C. **Patch**
D. Hotfix

✅ **Correct Answer:** Patch
📝 Fixes bugs or vulnerabilities in existing software.

Q24. Systematic notification, deployment, and verification of OS and application code revisions is:

A. Change Management
B. **Patch Management**
C. Version Control
D. Configuration Management

✅ **Correct Answer:** Patch Management
📝 Ensures updates are applied safely and effectively.

Q25. Message in its natural readable form is called:

A. Ciphertext
B. **Plaintext**
C. Hash
D. Encoded Text

✅ **Correct Answer:** Plaintext
📝 The unencrypted original message.

Q26. Recorded evidence of activities, used to verify processes, is called:

A. Audit Log
B. **Records**
C. Reports
D. Database

✓ **Correct Answer:** Records
📝 Can be manual or automated, used for verification.

Q27. Practice of retaining records as long as necessary, then destroying them:

A. Record Keeping
B. Backup
C. **Records Retention**
D. Archiving

✓ **Correct Answer:** Records Retention
📝 Ensures compliance and reduces storage risk.

Q28. Residual data left on media after clearing is called:

A. Remanence
B. Residual Data
C. Shadow Data
D. Artifacts

✓ **Correct Answer:** Remanence
📝 Requires secure deletion methods.

Q29. First stage of change management, requesting a change, is:

A. Change Approval
B. Implementation
C. **Request for Change (RFC)**
D. Testing

✅ **Correct Answer:** Request for Change (RFC)
📝 RFC initiates the formal change process.

Q30. The complete policies, roles, and processes used to make security decisions is:

A. Security Management
B. Security Policy
C. **Security Governance**
D. Configuration Management

✅ **Correct Answer:** Security Governance
📝 Framework for managing security decisions and compliance.

Q31. Tactics to trick users via email, phone, or social media are:

A. Phishing
B. Social Engineering
C. Spoofing
D. **Social Engineering**

✅ **Correct Answer:** Social Engineering
📝 Exploits human behavior to gain unauthorized access.

Q32. Algorithm using the same key for both encryption and decryption is:

A. RSA
B. **Symmetric Encryption**
C. AES
D. Hash Function

✅ **Correct Answer:** Symmetric Encryption
📝 Both encryption and decryption use the same secret key.

Q33. Computer that provides WWW services, including OS, hardware, and web content is:

A. Application Server
B. Database Server
C. **Web Server**
D. Proxy Server

✅ **Correct Answer:** Web Server
📝 Hosts websites and serves them to clients over HTTP/HTTPS.

Q34. Phishing attacks targeting high-value individuals for large fund transfers are:

A. Spear Phishing
B. Social Engineering
C. Whaling
D. BEC

✅ **Correct Answer:** Whaling Attack
📝 Targets executives or high-net-worth individuals.

Cloud Computing & Cybersecurity MCQs

Q1. What is the primary purpose of a Cloud Security Group (CSG)?

A. Physical security of data centers
B. Access control for cloud resources
C. Resource optimization
D. Regulatory enforcement

✅ **Correct Answer:** B
📝 Controls inbound and outbound traffic to cloud resources.

Q2. Why is symmetric encryption preferred for large data volumes?

A. Stronger security
B. Faster performance
C. Easier key exchange
D. Public key usage

✅ **Correct Answer:** B
📝 Symmetric algorithms are faster and computationally efficient.

Q3. What is the main purpose of digital signatures?

A. Encrypt data
B. Verify integrity and authenticity
C. Generate keys
D. Control access

✅ **Correct Answer:** B
📝 Digital signatures ensure data has not been altered and verify sender identity.

Q4. Which protocol secures HTTP traffic?

A. IPsec
B. SSH
C. SSL/TLS
D. VPN

✅ **Correct Answer:** C
📝 HTTPS uses TLS to encrypt web communication.

Q5. Which is a key characteristic of IaaS?

A. Limited scalability
B. Pay-as-you-go pricing

C. Fixed software stack
D. No user control

✅ **Correct Answer:** B
📝 IaaS offers flexible resources billed based on usage.

Q6. Why is disaster recovery important in cloud environments?

A. Prevent attacks
B. Ensure service availability
C. Reduce cost
D. Automate deployment

✅ **Correct Answer:** B
📝 DR ensures systems remain available during outages or disasters.

Q7. Which device connects a LAN to a WAN?

A. Firewall
B. Router
C. Switch
D. Hub

✅ **Correct Answer:** B
📝 Routers forward traffic between different networks.

Q8. Which cloud model allows developers to deploy apps without managing servers?

A. IaaS
B. PaaS
C. SaaS
D. FaaS

✅ **Correct Answer:** B
📝 PaaS abstracts infrastructure and runtime management.

Q9. Intercepting traffic between two communicating parties is called?

A. Spoofing
B. Phishing
C. On-path attack
D. Side-channel attack

✅ **Correct Answer:** C
📝 On-path (MITM) attacks allow attackers to eavesdrop or modify traffic.

Q10. Which control authenticates devices before network access?

A. VPN
B. IDS
C. NAC
D. Packet filtering

✅ **Correct Answer:** C
📝 NAC enforces authentication and authorization at network entry.

Q11. Which port does FTP use?

A. 21
B. 22
C. 23
D. 80

✅ **Correct Answer:** A
📝 FTP control channel operates on port 21.

Q12. Which authentication method is most secure for external cloud access?

A. Username & password
B. Biometrics
C. OAuth
D. LDAP

✅ **Correct Answer:** C
📝 OAuth uses tokens and avoids exposing credentials.

Q13. Which port is used by SSH?

A. 22
B. 23

C. 80
D. 443

✅ **Correct Answer:** A
📝 SSH provides encrypted remote access over port 22.

Q14. Why encrypt data in transit?

A. Reduce costs
B. Protect data during transmission
C. Improve performance
D. Automate updates

✅ **Correct Answer:** B
📝 Prevents data interception and eavesdropping.

Q15. Fake emails asking for credentials are examples of?

A. Spoofing
B. Phishing
C. Malware
D. DDoS

✅ **Correct Answer:** B
📝 Phishing tricks users into revealing sensitive information.

Q16. Which protocol securely transfers files over SSH?

A. FTP
B. SFTP
C. TFTP
D. FTPS

✓ **Correct Answer:** B
📝 SFTP encrypts file transfers using SSH.

Q17. Why should BCP plans be tested regularly?

A. Reduce cost
B. Validate effectiveness
C. Increase revenue
D. Avoid disasters

✓ **Correct Answer:** B
📝 Testing identifies gaps and improves preparedness.

Q18. What is a key benefit of CASB?

A. DDoS prevention
B. Cloud traffic visibility
C. Disk encryption
D. Cost optimization

✓ **Correct Answer:** B
📝 CASBs monitor and control cloud data usage.

Q19. What is the goal of a Business Continuity Plan?

A. Stop disasters
B. Continue operations
C. Reduce spending
D. Increase profits

✅ **Correct Answer:** B
📝 BCP ensures business functions continue during disruptions.

Q20. Flooding a server with traffic is known as?

A. Spoofing
B. Virus
C. DDoS
D. Phishing

✅ **Correct Answer:** C
📝 DDoS overwhelms systems to make them unavailable.

Q21. Which cloud model is dedicated to one organization?

A. Public
B. Private
C. Hybrid
D. Community

✅ **Correct Answer:** B
📝 Private clouds provide exclusive infrastructure.

Q22. What is the main goal of CASB solutions?

A. IAM
B. Cloud traffic control
C. Encryption
D. Auto-scaling

✅ **Correct Answer:** B
📝 CASBs enforce security policies across cloud services.

Q23. Which protocol secures Wi-Fi networks?

A. WPA2
B. TLS
C. AES
D. SSL

✅ **Correct Answer:** A
📝 WPA2 encrypts wireless communications.

Q24. How does IPsec prevent replay attacks?

A. Encryption
B. Hashing
C. Sequence numbers
D. Firewalls

✅ **Correct Answer:** C
📝 Sequence numbers detect duplicated packets.

Q25. Which cloud model combines public and private resources?

A. Public
B. Private
C. Hybrid
D. Community

✅ **Correct Answer:** C
📝 Hybrid clouds offer flexibility and scalability.

Q26. Which port is used by Telnet?

A. 21
B. 22
C. 23
D. 80

✅ **Correct Answer:** C
📝 Telnet communicates in plaintext over port 23.

Q27. What is RBAC used for?

A. Prevent DDoS
B. Role-based permissions

C. Monitoring
D. Encryption

✅ **Correct Answer:** B
📝 RBAC restricts access based on job roles.

Q28. Why is network segmentation important?

A. Speed
B. Cost savings
C. Isolation of workloads
D. Automation

✅ **Correct Answer:** C
📝 Segmentation limits lateral movement of attackers.

Q29. Which is a registered port example?

A. HTTP
B. Microsoft SQL Server
C. FTP
D. DNS

✅ **Correct Answer:** B
📝 Registered ports range from 1024–49151.

Q30. Why use a VPN?

A. Improve speed
B. Secure remote access
C. Block malware
D. Manage users

✅ **Correct Answer:** B
📝 VPN encrypts traffic over public networks.

Q31. Which service delivers ready-to-use software?

A. IaaS
B. PaaS
C. SaaS
D. FaaS

✅ **Correct Answer:** C
📝 SaaS provides complete applications over the internet.

Q32. VPN tunnel instability usually relates to which OSI layer?

A. Application
B. Transport
C. Network
D. Physical

✅ **Correct Answer:** C
📝 VPNs primarily operate at the network layer.

Q33. Which hash algorithm is vulnerable to collisions?

A. AES
B. RSA
C. MD5
D. SHA-256

✓ **Correct Answer:** C
📝 MD5 is cryptographically broken.

Q34. What is the purpose of DDoS mitigation services?

A. Authentication
B. Traffic analysis
C. Block malicious traffic
D. Load balancing

✓ **Correct Answer:** C
📝 Protects services from traffic floods.

Q35. Which device is considered an endpoint?

A. Firewall
B. Router
C. Laptop
D. Switch

✓ **Correct Answer:** C
📝 Endpoints are user-operated devices.

Q36. Which protocol secures data in transit?

A. AES
B. RSA
C. TLS
D. MD5

✓ **Correct Answer:** C
📝 TLS encrypts communication between systems.

Q37. What is an IPv4 address size?

A. 128-bit
B. 64-bit
C. 32-bit
D. 16-bit

✓ **Correct Answer:** C
📝 IPv4 uses 32-bit addressing.

Q38. MITM attacks target which activity?

A. Password storage
B. Data interception
C. Malware injection
D. Disk access

✅ **Correct Answer:** B
📝 MITM intercepts communication between parties.

Q39. Which malware demands payment to decrypt files?

A. Virus
B. Worm
C. Trojan
D. Ransomware

✅ **Correct Answer:** D
📝 Ransomware encrypts files for extortion.

Q40. Which control secures data in transit?

A. RBAC
B. IDS
C. TLS
D. Encryption at rest

✅ **Correct Answer:** C
📝 TLS protects data during transmission.

Q41. Which BCP component identifies critical functions?

A. Risk assessment
B. BIA

C. Plan testing
D. Recovery plan

✅ **Correct Answer:** B
📝 BIA analyzes business impact of disruptions.

Q42. Main goal of disaster recovery in cloud?

A. Prevent attacks
B. Maintain availability
C. Reduce costs
D. Improve automation

✅ **Correct Answer:** B
📝 DR restores services after failures.

Q43. Why use digital certificates in PKI?

A. Encrypt files
B. Authenticate identities
C. Store passwords
D. Generate keys

✅ **Correct Answer:** B
📝 Certificates verify entity identities.

Q44. Intercepting traffic at ARP level affects which OSI layer?

A. Physical
B. Data Link
C. Network
D. Application

✓ **Correct Answer:** B
📝 ARP operates at Layer 2.

Q45. How do organizations verify cloud providers' security?

A. IDS
B. Encryption
C. Security certifications
D. Firewalls

✓ **Correct Answer:** C
📝 Certifications show compliance with standards.

Q46. Which protocol is primarily used to securely access and manage remote servers over an encrypted connection?

A. Telnet
B. FTP
C. **SSH**
D. HTTP

✅ **Correct Answer:** SSH
📝 SSH provides encrypted remote login and command execution.

Q47. Which security control helps ensure data confidentiality and integrity during transmission over public networks?

A. RBAC
B. IDS
C. **Transport Layer Security (TLS)**
D. DLP

✅ **Correct Answer:** TLS
📝 TLS encrypts data in transit and prevents eavesdropping and tampering.

Q48. Which attack attempts to overwhelm a switch by filling its MAC address table with fake addresses?

A. ARP spoofing
B. **MAC flooding**
C. DNS poisoning
D. VLAN hopping

✅ **Correct Answer:** MAC flooding
📝 This forces the switch to behave like a hub, enabling sniffing attacks.

Q49. Which cloud security principle ensures users have only the minimum access necessary to perform their job?

A. Defense in depth
B. Zero trust
C. **Principle of least privilege**
D. Separation of duties

✅ **Correct Answer:** Principle of least privilege
📝 Reduces attack surface by limiting unnecessary permissions.

Q50. Which AWS service is commonly used to protect applications from web-based attacks such as SQL injection and XSS?

A. AWS Shield
B. AWS Inspector
C. **AWS WAF**
D. AWS GuardDuty

✅ **Correct Answer:** AWS WAF
📝 AWS WAF filters malicious HTTP/S traffic at the application layer.

Q51. Which encryption algorithm is commonly used to protect data in transit in cloud environments?

A. AES
B. DES
C. RSA
D. MD5

✅ **Correct Answer:** A
📝 AES is widely used within TLS to encrypt data during transmission.

Q52. Which is a characteristic of a public cloud deployment model?

A. Dedicated infrastructure
B. Limited scalability
C. Shared infrastructure
D. Full hardware control

✅ **Correct Answer:** C
📝 Public clouds share infrastructure among multiple customers.

Q53. At which TCP/IP layer do stateful firewalls mainly operate?

A. Layer 1
B. Layer 2
C. Layer 3
D. Layer 4

✅ **Correct Answer:** D
📝 Firewalls commonly inspect ports and sessions at the transport layer.

Q54. Why is salt used when hashing passwords?

A. Improve usability
B. Increase entropy

C. Reduce security
D. Speed hashing

✓ **Correct Answer:** B
📝 Salting prevents rainbow table and precomputed hash attacks.

Q55. Which control prevents unauthorized access to cloud databases?

A. RBAC
B. NIDS
C. DDoS mitigation
D. SIEM

✓ **Correct Answer:** A
📝 RBAC ensures users access only permitted data.

Q56. Which protocol uses port 53?

A. DNS
B. SMTP
C. HTTP
D. HTTPS

✓ **Correct Answer:** A
📝 DNS resolves domain names to IP addresses.

Q57. Which OSI layer is targeted by a ping flood attack?

A. Layer 3
B. Layer 4
C. Layer 5
D. Layer 6

✅ **Correct Answer:** A
📝 Ping floods abuse ICMP, which operates at the network layer.

Q58. What is the impact of an IPsec replay attack?

A. Unauthorized access
B. Communication disruption
C. Traffic manipulation
D. All of the above

✅ **Correct Answer:** D
📝 Replay attacks can disrupt sessions and bypass protections.

Q59. Which control protects data in transit?

A. Encryption at rest
B. NIDS
C. TLS
D. RBAC

✅ **Correct Answer:** C
📝 TLS encrypts data exchanged between clients and servers.

Q60. Why implement MFA in cloud environments?

A. Prevent unauthorized access
B. Improve performance
C. Automate deployment
D. Monitor users

✅ **Correct Answer:** A
📝 MFA adds extra verification beyond passwords.

Q61. Which cloud model is exclusive to one organization?

A. Hybrid
B. Public
C. Private
D. Community

✅ **Correct Answer:** C
📝 Private clouds offer dedicated resources.

Q62. What is the purpose of network segmentation?

A. Block all access
B. Increase speed
C. Improve security and performance
D. Monitor compliance

✅ **Correct Answer:** C
📝 Segmentation limits attack spread and improves control.

Q63. Which algorithm is commonly used for encrypting data at rest?

A. AES
B. RSA
C. DES
D. MD5

✅ **Correct Answer:** A
📝 AES is industry-standard for storage encryption.

Q64. Malware disguised as legitimate software is called?

A. Worm
B. Virus
C. Trojan
D. Ransomware

✅ **Correct Answer:** C
📝 Trojans rely on user deception to install malware.

Q65. Network issues caused by faulty cabling affect which OSI layer?

A. Application
B. Transport
C. Network
D. Physical

✅ **Correct Answer:** D
📝 Cables and connectors belong to the physical layer.

Q66. What is the goal of Data Loss Prevention (DLP)?

A. Block logins
B. Control data movement
C. Optimize resources
D. Automate deployments

✅ **Correct Answer:** B
📝 DLP prevents sensitive data leakage.

Q67. A DDoS flood mainly targets which OSI layer?

A. Physical
B. Data Link
C. Network
D. Transport

✅ **Correct Answer:** C
📝 DDoS attacks overwhelm network-layer resources.

Q68. Which port is used by SMTP?

A. 25
B. 80

C. 443
D. 22

✅ **Correct Answer:** A
📝 SMTP handles email delivery.

Q69. Registered ports are typically used for?

A. Vendor applications
B. Core protocols
C. Web servers
D. In-house apps

✅ **Correct Answer:** A
📝 Registered ports (1024–49151) serve vendor services.

Q70. Which model allows app deployment without managing infrastructure?

A. IaaS
B. PaaS
C. SaaS
D. FaaS

✅ **Correct Answer:** B
📝 PaaS abstracts infrastructure management.

Q71. Port scanning targets which OSI layer?

A. Layer 1
B. Layer 2
C. Layer 3
D. Layer 4

✓ **Correct Answer:** D
📝 Port scanning probes transport-layer services.

Q72. Unable to access a specific website indicates which OSI layer?

A. Application
B. Transport
C. Network
D. Data Link

✓ **Correct Answer:** A
📝 Web access issues often relate to application-layer services.

Q73. What is the primary purpose of CASB?

A. Manage vendors
B. Optimize usage
C. Monitor cloud traffic
D. Encrypt databases

✓ **Correct Answer:** C
📝 CASBs enforce security between users and cloud apps.

Q74. Which cloud model provides exclusive resources?

A. Public
B. Private
C. Hybrid
D. Community

✓ **Correct Answer:** B
📝 Private cloud infrastructure is not shared.

Q75. What does a CSPM tool do?

A. Enforce cloud security compliance
B. Reduce costs
C. Encrypt data
D. Deploy software

✓ **Correct Answer:** A
📝 CSPM detects misconfigurations and compliance gaps.

Q76. Which control protects data at rest?

A. RBAC
B. Encryption
C. IDS
D. MFA

✓ **Correct Answer:** B
📝 Encryption secures stored data.

Q77. Key advantage of CASB solutions?

A. DDoS protection
B. Cloud visibility
C. Storage encryption
D. Cost optimization

✓ **Correct Answer:** B
📝 CASBs provide visibility and policy enforcement.

Q78. Primary goal of a Disaster Recovery Plan?

A. Prevent disasters
B. Ensure service continuity
C. Reduce costs
D. Increase profit

✓ **Correct Answer:** B
📝 DR focuses on recovery after failures.

Q79. Which cloud model uses dedicated infrastructure?

A. Public
B. Private
C. Hybrid
D. Community

✅ **Correct Answer:** B
📝 Private clouds isolate infrastructure per organization.

Q80. Which protocol uses port 80?

A. HTTP
B. FTP
C. SSH
D. Telnet

✅ **Correct Answer:** A
📝 HTTP handles unencrypted web traffic.

Q81. Purpose of a Virtual Private Cloud (VPC)?

A. Dedicated physical servers
B. Network isolation
C. VM optimization
D. Access enforcement

✅ **Correct Answer:** B
📝 VPC logically isolates cloud networks.

Q82. Purpose of DDoS mitigation services?

A. Access control
B. Traffic analysis

C. Block malicious traffic
D. Resource optimization

✅ **Correct Answer:** C
📝 Protects availability of services.

Q83. Which control detects security incidents?

A. MFA
B. IDS
C. RBAC
D. Encryption

✅ **Correct Answer:** B
📝 IDS monitors for suspicious activity.

Q84. Goal of cloud disaster recovery planning?

A. Prevent access
B. Ensure availability
C. Reduce costs
D. Automate deployment

✅ **Correct Answer:** B
📝 DR ensures uptime during disasters.

Q85. Unable to access a website indicates which layer?

A. Application
B. Transport
C. Network
D. Data Link

✅ **Correct Answer:** A
📝 Web services operate at Layer 7.

Q86. MITM attacks commonly target which OSI layer?

A. Layer 2
B. Layer 3
C. Layer 4
D. Layer 7

✅ **Correct Answer:** B
📝 MITM often manipulates IP routing or ARP.

Q87. Main advantage of CASB?

A. DDoS prevention
B. Traffic monitoring
C. Database encryption
D. Cost reduction

✅ **Correct Answer:** B
📝 CASBs provide centralized cloud security control.

Q88. Which model provides virtualized computing resources?

A. IaaS
B. SaaS
C. PaaS
D. FaaS

✅ **Correct Answer:** A
📝 IaaS delivers VMs, storage, and networking.

Q89. Purpose of RBAC in cloud environments?

A. Stop DDoS
B. Enforce compliance
C. Monitor behavior
D. Restrict access by role

✅ **Correct Answer:** D
📝 RBAC enforces least privilege.

Q90. Why use encryption at rest?

A. Prevent login attacks
B. Protect data in transit
C. Improve performance
D. Protect stored data

✅ **Correct Answer:** D
📝 Prevents unauthorized access to stored data.

Q91. Which BCP phase identifies risks?

A. Risk assessment
B. BIA
C. Testing
D. Implementation

✓ **Correct Answer:** A
📝 Identifies threats impacting operations.

Q92. Secure authentication for external cloud access?

A. Username/password
B. Biometrics
C. OAuth
D. LDAP

✓ **Correct Answer:** C
📝 OAuth provides token-based authentication.

Q93. Why use network segmentation?

A. Increase bandwidth
B. Increase latency
C. Isolate workloads
D. Automate networks

✅ **Correct Answer:** C
📝 Limits attack surface and lateral movement.

Q94. Which model abstracts infrastructure for developers?

A. IaaS
B. PaaS
C. SaaS
D. FaaS

✅ **Correct Answer:** B
📝 PaaS simplifies application deployment.

Q95. Purpose of cloud security groups?

A. Physical security
B. Access control
C. Resource allocation
D. Compliance enforcement

✅ **Correct Answer:** B
📝 Security groups act as virtual firewalls.

Q96. Malware that encrypts files for ransom?

A. Ransomware
B. Worm

C. Trojan
D. Virus

✅ **Correct Answer:** A
📝 Ransomware extorts victims for decryption.

Q97. Main benefit of CASB?

A. DDoS defense
B. Cloud traffic control
C. Encryption
D. Cost optimization

✅ **Correct Answer:** B
📝 CASBs protect data usage in cloud apps.

Q98. Why use a nonce in cryptography?

A. Add randomness
B. Strengthen keys
C. Prevent replay attacks
D. Authenticate users

✅ **Correct Answer:** C
📝 Nonces ensure messages are unique.

Q99. DNS spoofing mainly affects which OSI layer?

A. Physical
B. Data Link
C. Network
D. Application

✓ **Correct Answer:** D
📝 DNS manipulation impacts application-level services.

Q100. Intercepting communication between two parties is called?

A. On-path attack
B. Spoofing
C. Phishing
D. Side-channel

✓ **Correct Answer:** A
📝 On-path attacks enable traffic interception.

Q101. Which security control monitors, collects, and analyzes logs to identify suspicious user activity in cloud environments?

A. IDS
B. MFA
C. RBAC
D. **SIEM**

✓ **Answer:** D
📝 SIEM aggregates logs and events to detect threats and anomalies.

Q102. What is the primary purpose of Role-Based Access Control (RBAC) in cloud environments?

A. Prevent DDoS attacks
B. Enforce compliance
C. Monitor activity
D. **Restrict access based on user roles**

✓ **Answer:** D
📝 RBAC enforces least privilege by assigning permissions based on roles.

Q103. What is the range of dynamic (private) TCP/UDP ports?

A. 0–1023
B. 1024–49151
C. **49152–65535**
D. None of the above

✓ **Answer:** C
📝 Dynamic ports are used for temporary client-side connections.

Q104. Which control best prevents buffer overflow attacks?

A. IDS
B. Firewalls
C. Antivirus
D. **Input validation**

✅ **Answer:** D
📝 Input validation prevents malicious data from exceeding memory limits.

Q105. A MAC flooding attack targets which OSI layer?

A. **Layer 2**
B. Layer 3
C. Layer 4
D. Layer 7

✅ **Answer:** A
📝 MAC flooding overwhelms switch CAM tables at Layer 2.

Q106. Why is Multi-Factor Authentication (MFA) implemented in cloud environments?

A. Optimize performance
B. **Prevent unauthorized access**
C. Automate deployment
D. Monitor users

✅ **Answer:** B
📝 MFA adds additional verification beyond passwords.

Q107. What is the main purpose of an Incident Response Plan (IRP)?

A. Improve productivity
B. Prevent all incidents
C. Allocate maintenance resources
D. **Provide procedures for handling security incidents**

✓ **Answer:** D
📝 IRP defines structured steps for detection, response, and recovery.

Q108. What is the primary function of a Cloud Security Group (CSG)?

A. Physical security
B. **Network access control**
C. Resource optimization
D. Compliance enforcement

✓ **Answer:** B
📝 Security groups act as virtual firewalls.

Q109. What is the primary goal of RBAC?

A. DDoS protection
B. Compliance enforcement
C. Activity monitoring
D. **Role-based access restriction**

✓ **Answer:** D
📝 RBAC limits access according to job responsibilities.

Q110. Which attack floods systems with traffic to cause service disruption?

A. **DoS / DDoS**
B. Spoofing
C. Phishing
D. Virus

✓ **Answer:** A
📝 DDoS attacks exhaust system resources.

Q111. Why are DDoS mitigation services used in cloud environments?

A. Prevent unauthorized access
B. Monitor traffic
C. **Block malicious traffic**
D. Optimize performance

✓ **Answer:** C
📝 These services absorb and filter attack traffic.

Q112. Malware disguised as legitimate software that tricks users is called?

A. Worm
B. Virus
C. **Trojan**
D. Ransomware

✓ **Answer:** C
📝 Trojans rely on social engineering rather than self-propagation.

Q113. Which cloud model combines public and private infrastructure?

A. Public
B. Private
C. **Hybrid**
D. Community

✓ **Answer:** C
📝 Hybrid clouds balance scalability and control.

Q114. A key characteristic of public cloud deployment is:

A. Dedicated infrastructure
B. Limited scalability
C. **Shared infrastructure**
D. Full hardware control

✓ **Answer:** C
📝 Resources are shared across multiple tenants.

Q115. Which control best protects against stolen credentials?

A. IDS
B. **MFA**
C. Encryption at rest
D. Segmentation

✓ **Answer:** B
📝 MFA blocks access even if passwords are compromised.

Q116. A DDoS attack primarily targets which OSI layer?

A. Physical
B. Data Link
C. **Network**
D. Transport

✓ **Answer:** C
📝 Network-layer floods overwhelm routing capacity.

Q117. What is the main objective of a CASB?

A. Vendor management
B. Cost optimization
C. **Control cloud data traffic**
D. Database encryption

✓ **Answer:** C
📝 CASBs enforce security policies between users and cloud apps.

Q118. A SYN flood attack targets which OSI layer?

A. **Layer 4**
B. Layer 5

C. Layer 6
D. Layer 7

✓ **Answer:** A
📝 SYN floods exploit TCP handshake mechanisms.

Q119. Best protection against compromised credentials is:

A. IDS
B. **MFA**
C. Encryption at rest
D. Segmentation

✓ **Answer:** B
📝 MFA prevents unauthorized login even with valid passwords.

Q120. Which encryption algorithm is commonly used for data in transit?

A. **AES**
B. RSA
C. DES
D. MD5

✓ **Answer:** A
📝 AES is used within TLS sessions.

Q121. VPN disconnect issues are most often related to which OSI layer?

A. Application
B. **Transport**
C. Network
D. Physical

✓ **Answer:** B
📝 VPN tunnels depend on TCP/UDP stability.

Q122. Which cloud model delivers complete software applications?

A. PaaS
B. IaaS
C. **SaaS**
D. FaaS

✓ **Answer:** C
📝 SaaS requires minimal customer management.

Q123. Which authentication method enables secure third-party cloud access?

A. Username/password
B. Biometrics
C. **OAuth**
D. LDAP

✓ **Answer:** C
📝 OAuth uses tokens instead of sharing credentials.

Q124. Network cabling issues affect which OSI layer?

A. Application
B. Transport
C. Network
D. **Physical**

✓ **Answer:** D
📝 Physical layer handles cables and signals.

Q125. What is an IPv4 address?

A. 128-bit address
B. **32-bit logical address**
C. Private-only address
D. Documentation address

✓ **Answer:** B
📝 IPv4 uses 32-bit addressing.

Q126. Which control detects suspicious activity in real time?

A. **IDS**
B. MFA
C. RBAC
D. Encryption

✓ **Answer:** A
📝 IDS monitors traffic for attack patterns.

Q127. Which control prevents unauthorized database access?

A. **RBAC**
B. NIDS
C. DDoS mitigation
D. SIEM

✅ **Answer:** A
📝 RBAC limits database permissions.

Q128. CASB solutions primarily:

A. Manage vendors
B. Optimize costs
C. **Control cloud data flow**
D. Encrypt databases

✅ **Answer:** C
📝 CASBs provide visibility and policy enforcement.

Q129. Which cloud model uses dedicated infrastructure?

A. Public
B. **Private**
C. Hybrid
D. Community

✅ **Answer:** B
📝 Private clouds are exclusive to one organization.

Q130. What is the well-known port range?

A. **0–1023**
B. 1024–49151
C. 49152–65535
D. None

✅ **Answer:** A
📝 Reserved for standard services like HTTP, FTP.

Q131. What is the primary function of a firewall?

A. Performance tuning
B. **Traffic filtering**
C. Encryption
D. Physical security

✅ **Answer:** B
📝 Firewalls enforce security rules on traffic.

Q132. A private cloud characteristic is:

A. Shared infrastructure
B. Limited scalability

C. **Dedicated infrastructure**
D. No customization

✅ **Answer:** C
📝 Private clouds offer greater control.

Q133. Best encryption for data at rest is:

A. **AES**
B. RSA
C. DES
D. MD5

✅ **Answer:** A
📝 AES is fast and secure for storage encryption.

Q134. An IP address is:

A. Physical address
B. Interface identifier
C. Vendor identifier
D. **Logical network address**

✅ **Answer:** D
📝 IP addresses identify devices logically.

Q135. What differentiates a switch from a hub?

A. Hub is smarter
B. Switch is outdated
C. VLAN creation
D. **Switch forwards traffic intelligently**

✅ **Answer:** D
📝 Switches use MAC tables to forward traffic.

Q136. Which device controls traffic within a LAN?

A. **Switch**
B. Firewall
C. Hub
D. Router

✅ **Answer:** A
📝 Switches manage internal network traffic.

Q137. Which protocols secure email communication?

A. SMTPS
B. IMAPS
C. POP3S
D. **All of the above**

✅ **Answer:** D
📝 These protocols encrypt email data.

Q138. Which IRP phase limits damage during an incident?

A. Preparation
B. Detection
C. **Response and mitigation**
D. Recovery

✓ **Answer:** C
📝 Focuses on containment and damage control.

Q139. Buffer overflow attacks target which OSI layer?

A. Layer 5
B. Layer 6
C. **Layer 7**
D. Layer 8

✓ **Answer:** C
📝 Application logic is exploited.

Q140. The cloud shared responsibility model defines:

A. Encryption ownership
B. **Provider vs customer security roles**
C. Hardware ownership
D. Compliance rules

✓ **Answer:** B
📝 Security duties are divided.

Q141. Why is network segmentation used?

A. Increase bandwidth
B. Increase latency
C. **Isolate workloads**
D. Automate provisioning

✓ **Answer:** C
📝 Limits lateral movement of attackers.

Q142. Subnetting improves performance by:

A. **Reducing congestion**
B. Increasing bandwidth
C. Improving security only
D. Simplifying management

✓ **Answer:** A
📝 Smaller broadcast domains reduce traffic.

Q143. Which model delivers complete applications?

A. IaaS
B. PaaS
C. **SaaS**
D. FaaS

✓ **Answer:** C

Q144. HTTPS uses which port?

A. 80
B. **443**
C. 446
D. 22

✓ **Answer:** B

Q145. Which security control is used to prevent unauthorized access to sensitive data in cloud databases?

A. Network Intrusion Detection System (NIDS)
B. Distributed Denial of Service (DDoS) mitigation
C. Security Information and Event Management (SIEM)
D. **Role-Based Access Control (RBAC)**

✓ **Correct Answer:** Role-Based Access Control (RBAC)
📝 RBAC ensures users can access only the data permitted by their assigned roles.

Q146. What security measure helps prevent unauthorized access through stolen or compromised credentials?

A. Network segmentation
B. Data encryption at rest
C. Intrusion Detection System (IDS)
D. **Multi-Factor Authentication (MFA)**

✅ **Correct Answer:** Multi-Factor Authentication (MFA)
📝 MFA adds an extra verification layer beyond username and password.

Q147. What is the primary purpose of implementing network encryption in a cloud environment?

A. To automate deployments
B. To optimize resource usage
C. **To protect data during transmission**
D. To restrict user permissions

✅ **Correct Answer:** To protect data during transmission
📝 Encryption prevents eavesdropping and data tampering in transit.

Q148. What is the primary purpose of Role-Based Access Control (RBAC)?

A. To monitor user activity
B. To enforce compliance
C. To block network attacks
D. **To restrict access based on user roles**

✅ **Correct Answer:** To restrict access based on user roles
📝 RBAC limits permissions to job responsibilities, reducing security risks.

Q149. A hacker performs a man-in-the-middle attack and injects malicious packets between two systems. Which OSI layer is primarily targeted?

A. Physical
B. **Transport**
C. Data Link
D. Application

✓ **Correct Answer:** Transport
📝 MITM attacks often exploit session handling at the transport layer.

Q150. Which security control is used to protect data at rest in cloud storage?

A. TLS
B. IDS
C. MFA
D. **Data Encryption**

✓ **Correct Answer:** Data Encryption
📝 Encryption ensures stored data remains unreadable without proper keys.

Q151. What is an IPSec replay attack?

A. Packet modification attack
B. Network flooding attack
C. Passive traffic sniffing
D. **Injection of captured packets into an active session**

✓ **Correct Answer:** Injection of captured packets into an active session
📝 Replay attacks reuse valid packets to bypass security controls.

Q152. What is the primary goal of Intrusion Detection and Prevention Systems (IDPS)?

A. Improve network performance
B. Enforce compliance
C. **Detect and respond to malicious activities**
D. Prevent physical access

✅ **Correct Answer:** Detect and respond to malicious activities
📝 IDPS identifies attacks and can actively block them.

Q153. Network congestion caused by improper router configuration affects which OSI layer?

A. Application
B. Transport
C. **Network**
D. Data Link

✅ **Correct Answer:** Network
📝 Routing and packet forwarding are functions of the network layer.

Q154. Which cloud service model provides virtualized computing resources over the internet?

A. SaaS
B. PaaS
C. FaaS
D. **Infrastructure as a Service (IaaS)**

✅ **Correct Answer:** Infrastructure as a Service (IaaS)
📝 IaaS delivers virtual machines, storage, and networking resources.

Q155. What is the primary goal of Data Loss Prevention (DLP) in cloud environments?

A. Prevent unauthorized logins
B. Optimize performance
C. Automate deployments
D. **Monitor and control data movement**

✅ **Correct Answer:** Monitor and control data movement
📝 DLP prevents sensitive data from being leaked or misused.

Q156. What is the main advantage of a rainbow table attack over brute-force attacks?

A. Requires less memory
B. Slower but stealthier
C. **Faster password cracking using precomputed hashes**
D. Less likely to succeed

✅ **Correct Answer:** Faster password cracking using precomputed hashes
📝 Rainbow tables trade storage space for speed.

Q157. Improper router configuration causing congestion impacts which OSI layer?

A. Application
B. Transport
C. **Network**
D. Physical

✓ **Correct Answer:** Network
📝 Routers operate at Layer 3 and manage traffic flow.

Q158. A malicious email attachment installs malware after being opened. Which OSI layer is targeted?

A. Physical
B. Network
C. Transport
D. **Application**

✓ **Correct Answer:** Application
📝 Malware execution occurs at the application layer.

Q159. What is the purpose of encryption at rest in cloud storage?

A. Improve performance
B. Automate backups
C. Prevent data transmission attacks
D. **Protect stored data from unauthorized access**

✓ **Correct Answer:** Protect stored data from unauthorized access
📝 Encryption secures data even if storage media is compromised.

Q160. Which security control monitors and analyzes logs and user activity across cloud systems?

A. IDS
B. MFA
C. RBAC
D. **SIEM**

✓ **Correct Answer:** SIEM
📝 SIEM provides centralized log analysis and threat detection.

Q161. What is the primary goal of Data Loss Prevention (DLP)?

A. Stop DDoS attacks
B. Control access permissions
C. **Prevent sensitive data leakage**
D. Encrypt cloud storage

✓ **Correct Answer:** Prevent sensitive data leakage
📝 DLP enforces policies to protect confidential information.

Q162. Which security control helps prevent credential-based attacks?

A. IDS
B. Encryption
C. Network segmentation
D. **Multi-Factor Authentication (MFA)**

✅ **Correct Answer:** Multi-Factor Authentication (MFA)
📝 MFA blocks attackers even if passwords are compromised.

Q163. Which cloud service model requires the least customer management effort?

A. IaaS
B. PaaS
C. FaaS
D. **Software as a Service (SaaS)**

✅ **Correct Answer:** Software as a Service (SaaS)
📝 SaaS providers manage infrastructure, platform, and application.

Q164. What is the main advantage of a One-Time Pad (OTP) encryption scheme?

A. Small key size
B. Fast computation
C. Easy implementation
D. **Perfect secrecy**

✅ **Correct Answer:** Perfect secrecy
📝 OTP is theoretically unbreakable when used correctly.

Q165. What is a key benefit of containerization in cloud environments?

A. Lower bandwidth usage
B. Better hardware security
C. **Simplified application deployment**
D. Reduced storage costs

✅ **Correct Answer:** Simplified application deployment
📝 Containers package apps with dependencies for portability.

Q166. Which encryption algorithm is commonly used to protect data in transit?

A. MD5
B. DES
C. RSA
D. **AES**

✅ **Correct Answer:** AES
📝 AES is used within TLS to encrypt transmitted data.

Q167. What is a major risk of assigning static administrative privileges to database users?

A. Higher cost
B. Limited access
C. Forgotten privileges
D. **Security depends entirely on login credentials**

✅ **Correct Answer:** Security depends entirely on login credentials
📝 Static privileges increase damage if credentials are compromised.

Charlie