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.

---

168. A cyberattacker changes the website of a pharmacy so it displays incorrect information about COVID testing. This is an example of what kind of compromise?

A. Confidentiality
B. Integrity
C. Availability
D. Nonrepudiation

ANS: B. Changing data without proper authorization is a compromise of integrity.

---

169. The function of a computer system that verifies the identity of a user is called _____.

A. Authentication
B. Authorization
C. Authenticity
D. Availability

ANS: A. Authentication is the function of verifying a user's identity.

---

170. Jane received an electronic message from Fred that was digitally signed proving it came from him. However, Fred said he never sent it. This is an example of what message integrity characteristic?

A. Nonreputation
B. Nonrefutability

C. Nonrepudiation
D. Authenticity

ANS: C. Nonrepudiation technologies guarantee that a sender of a message cannot later deny sending the message.

---

171. Which of the following elements do not apply to privacy?

A. Confidentiality
B. Integrity
C. Availability
D. None of the above

ANS: D. All of the items listed apply to privacy.

---

172. Information assurance refers to the _____ of information security.

A. Quality
B. Confidentiality
C. Ethics
D. Measurement

ANS: D. Information assurance is the measurement of the security controls an organization has put into place.

---

173. What is the first thing a cyberattacker would want to do to launch an attack against an organization?

A. Learn about the organization's vulnerabilities
B. Learn about the organization's business, including domain names, corporate information, facilities, names of employees, etc.
C. Deploy malware
D. Steal data

ANS: B. Learning about the organization's business details provides the basic information a cyberattacker needs to plan an attack.

---

174. An earthquake is an example of a _____?

A. Threat agent
B. Threat
C. Vulnerability
D. Risk

ANS: B. An earthquake is a natural disaster that may occur and could cause harm; therefore, it is a threat.

---

175. Which of the following statements is most correct?

A. Security should be done the same way regardless of the situation
B. Security should be tailored based on the situation
C. It's always best to mitigate risks rather than transfer them
D. Risk avoidance trumps security controls every time

ANS: B. Security is never absolute; it is tailored based on the organization's risk tolerance.

176. You are asked to perform a risk assessment of an information system for the purpose of recommending the most appropriate security controls. You have a short amount of time to do this. You know how each asset is used and its importance to the business but have no financial information. Which method is most appropriate?

A. Qualitative
B. Threat modeling
C. Quantitative
D. Delphi

ANS: A. Without financial data, a quantitative assessment is not possible; qualitative analysis based on asset importance is appropriate.

---

177. You are asked to implement a risk treatment in which your IT department removes a server considered too risky due to many vulnerabilities. Which type of risk treatment is this?

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

ANS: B. Risk avoidance involves removing the risky system entirely to avoid the risk.

---

178. A security engineer is reviewing a datacenter that lacks security cameras. What type of control does this represent?

A. Administrative
B. Technical

C. Physical
D. Logical

ANS: C. Security cameras are a physical security control.

---

179. Which statement is true regarding types of security controls?

A. Physical controls are also referred to as logical controls
B. Logical controls are also referred to as managerial controls
C. Physical controls are also referred to as managerial controls
D. Administrative controls are also referred to as soft controls

ANS: D. Administrative controls are also referred to as soft controls or managerial controls.

---

180. A document providing step-by-step instructions to perform a vulnerability scan is an example of:

A. Policy
B. Procedure
C. Guideline
D. Law

ANS: B. Step-by-step instructions are a procedure; policies provide high-level directives.

---

181. An information security policy is an example of which type of control?

A. Administrative
B. Technical

C. Logical
D. Physical

ANS: A. Policies are administrative controls providing directives to personnel.

---

182. Sarah discovers Kyle running a crypto-mining program on a company server. How should she respond?

A. Ask Kyle to stop
B. Ask Kyle to share the profits
C. Mind her own business
D. Escalate to senior management

ANS: D. Escalate to senior leadership according to policy; this is the ethical response.

---

183. Jane sets up access for a new employee only to the manufacturing area, not parts storage. Which principle is she applying?

A. Principle of authentication
B. Two-person rule
C. Need to know
D. Least privilege

ANS: D. Least privilege restricts access to only what is required for the job.

---

184. Which statement best describes the relationship between subjects, objects, and rules?

A. A subject grants access to an object based on rules
B. An object is granted access to a subject based on rules
C. A subject is granted access to an object based on rules
D. An object is granted access to a subject based on credentials

ANS: C. A subject is granted access to an object based on rules.

---

185. Credentials are composed of which elements?

A. Username and password
B. Authorization and accountability
C. Something you know and something you have
D. Subjects and objects

ANS: A. Identification (username) and authentication (password) are typically used together as credentials.

---

186. Joe has to log in to many systems daily and has too many passwords to remember. What is the best way for Joe to manage his passwords?

A. Write passwords on paper
B. Store passwords in a text file
C. Use the same password everywhere
D. Use a password manager or vault

ANS: D. Using a password manager securely stores and encrypts passwords, reducing risk and making management easier.

187. Debby has accumulated access to systems she doesn't need over time. This is an example of:

A. Privilege modification
B. Access management
C. Privileged access management
D. Privilege creep

ANS: D. Privilege creep occurs when users gain excessive access beyond what is necessary.

---

188. The identity and access management lifecycle consists of:

A. Provisioning, review, revocation
B. Setup, review, auditing
C. Creation, monitoring, termination
D. Identification, authentication, authorization

ANS: A. IAM lifecycle includes provisioning access, periodic review, and revocation when access is no longer needed.

---

189. Which access control model leverages roles to provision access to multiple users with similar needs?

A. DAC
B. MAC
C. RBAC
D. None of the above

ANS: C. RBAC assigns access based on roles, grouping users with similar responsibilities.

---

190. To prevent a car from driving into a building, which security measure is most effective?

A. Biometrics
B. RBAC
C. Badge system
D. Bollards

ANS: D. Bollards physically block vehicles and protect entrances.

---

191. A datacenter door should allow safe exit during a fire with a power loss. Which configuration is correct?

A. Always remain locked
B. Fail-secure
C. Fail-open
D. Automatically lock with no power

ANS: C. Fail-open ensures people can safely exit during emergencies.

---

192. Two doors requiring the first to close before unlocking the second is an example of:

A. Bollard
B. Mantrap
C. Fence
D. Biometric

ANS: B. A mantrap is a physical access control mechanism using sequential doors.

---

193. Which access control model allows the resource creator to assign permissions to others?

A. DAC
B. MAC
C. RBAC
D. None of the above

ANS: A. DAC allows the owner/creator of a resource to control access.

---

194. Which of the following is referred to as a physical address in networking?

A. IPv4 address
B. IPv6 address
C. MAC address
D. Loopback address

ANS: C. MAC addresses are hardware-based physical addresses for devices.

---

195. How many layers are in the OSI model?

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

ANS: B. OSI model has 7 layers: Application, Presentation, Session, Transport, Network, Data Link, Physical.

---

196. A computer providing content or services to other computers is called:

A. Client
B. Server
C. Endpoint
D. Router

ANS: B. A server delivers content or services to clients.

---

197. Name of the 7th layer of the OSI model?

A. Application
B. Session
C. Presentation
D. Network

ANS: A. The Application Layer is Layer 7 of the OSI model.

---

198. Which attacks are most likely carried out by a botnet?

A. Advanced persistent threat attack
B. DDoS attack
C. Trojan horse attack
D. Backdoor attack

ANS: B. Botnets are typically used for coordinated attacks like DDoS.

---

199. Difference between phishing and spear phishing:

A. Phishing is to a specific person; spear phishing is to a whole company
B. Phishing is to random recipients; spear phishing targets specific recipients
C. Phishing is to an entire company; spear phishing targets specific person
D. Spear phishing is random; phishing targets specific

ANS: B. Phishing is wide, random; spear phishing targets specific individuals or groups.

---

200. Which statement about worms is false?

A. Can replicate itself
B. Type of malware
C. Type of botnet
D. Does not require host program

ANS: C. Worms are malware, self-replicating, and do not require a host, but they are **not** botnets.

---

201. A rainbow table attack:

A. True
B. False

ANS: A. True. Rainbow tables precompute password hashes to bypass brute-force attacks.

---

202. Primary difference between IDS and IPS:

A. They are the same
B. IDS detects; IPS prevents
C. IDS detects; IPS monitors performance
D. IDS detects; IPS detects and takes action

ANS: D. IDS detects malicious activity; IPS detects and actively prevents it.

---

203. Joe, a cybercriminal, wants to see if a server has unpatched vulnerabilities. What does he do?

A. Launch smurf attack
B. Run vulnerability scan
C. Send phishing email
D. Send spear phishing email

ANS: B. A vulnerability scan identifies unpatched systems.

---

204. Attack method entering SQL commands into a vulnerable web page:

A. Buffer overflow
B. SQL injection
C. HTTP response splitting
D. Backdoor

ANS: B. SQL injection executes unauthorized SQL commands via user input fields.

---

205. Weakest link in cybersecurity is usually:

A. Passwords
B. Backdoors
C. Laws
D. People

ANS: D. Humans are widely recognized as the weakest link.

---

206. Hacker uses phishing to steal credentials and exfiltrate data. This is an example of:

A. Denial of service
B. Advanced persistent threat
C. Extortion
D. Data exfiltration

ANS: D. Unauthorized transfer of data is data exfiltration.

---

207. Cybercriminal installs malware over weeks, expanding across systems. Term for this activity:

A. DoS attack
B. Advanced persistent threat (APT)
C. Extortion attack
D. Website defacement

ANS: B. APTs involve long-term, targeted attacks, often stealthy and multi-stage.

---

208. Mary wants to hide a database server IP with a firewall. Which type?

A. Proxy
B. Packet filter
C. Stateful/dynamic
D. Database filter

ANS: A. Proxy firewalls hide internal IPs by acting as an intermediary.

---

209. Antivirus vendors use _____ to stay updated on threats:

A. Google
B. National Vulnerability Database
C. Threat intelligence
D. NSA

ANS: C. Threat intelligence informs vendors of latest malware and threats.

---

210. Responsibility of a third-party cloud provider always:

A. Data security
B. Physical security of datacenter
C. Identity and access management
D. Endpoint protection

ANS: B. Cloud providers always handle physical security of their facilities.

211. Cloud service allows building and deploying custom apps on a framework. Model?

A. IaaS
B. PaaS
C. SaaS
D. On-premises

ANS: B. Platform as a Service provides frameworks to develop and deploy apps.

---

212. Cloud provider hosts infrastructure; customer manages OS and apps. Service model?

A. IaaS
B. PaaS
C. SaaS
D. On-premises

ANS: A. IaaS gives virtualized infrastructure; customer manages OS, tools, apps.

---

213. Organization builds a cloud in its datacenter for exclusive use by employees. Deployment model?

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

ANS: B. Private cloud is dedicated to a single organization.

---

214. Organization uses private cloud but also AWS for peak loads. Deployment model?

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

ANS: D. Hybrid cloud mixes private and public cloud resources.

---

215. Organization uses Gmail for email. Cloud service model?

A. SaaS
B. PaaS
C. IaaS
D. On-premises

ANS: A. SaaS provides hosted applications like Gmail.

---

216. Alice sends Bob a message encrypted with a private key; Bob decrypts with the same key. Encryption type?

A. Asymmetric
B. Symmetric
C. Hashing
D. None

ANS: B. Symmetric encryption uses a single shared key for encryption and decryption.

---

217. Not a secure method of data deletion:

A. Empty recycle bin
B. Physical destruction
C. Zeroization
D. Overwriting

ANS: A. Simply emptying the recycle bin does not securely remove data.

---

218. Which can create message digests?

A. Symmetric encryption algorithms
B. Asymmetric encryption algorithms
C. Hash functions
D. All of the above

ANS: C. Hash functions generate fixed-length digests for data integrity verification.

---

219. Automated monitoring of logs is best done with:

A. Regular manual review
B. Centralized log server
C. SIEM
D. Firewall

ANS: C. SIEM centralizes log collection and automates alerting for suspicious activity.

220. Encryption with two keys, one for encryption and another for decryption, is called:

A. Asymmetric
B. Symmetric
C. Hashing
D. None

ANS: A. Asymmetric encryption uses a public and a private key.

---

221. Endpoints show vulnerabilities in scans. Most likely root cause?

A. APT attack
B. Missing antimalware
C. Missing security patches
D. Brute force

ANS: C. Lack of latest security patches is the main cause of endpoint vulnerabilities.

---

222. A firewall no longer matches DISA recommended settings. Likely reason?

A. DISA settings were wrong
B. Configuration management not followed
C. Privilege creep
D. Data integrity

ANS: B. Someone likely changed settings without following CM procedures.

223. Mary is unsure if she can use a company laptop for Facebook. Which policy to check?

A. AUP
B. BYOD
C. Data handling policy
D. None

ANS: A. Acceptable Use Policy (AUP) provides guidance on permitted device usage.

---

224. Policy guiding VPN access from a home computer:

A. AUP
B. BYOD
C. Data handling
D. None

ANS: B. BYOD policies govern connecting personal devices securely to corporate networks.

---

225. Poster reminding employees to use a password vault is an example of:

A. Security awareness
B. Security training
C. Security policy
D. Security testing

ANS: A. Awareness uses reminders and communications to reinforce security practices.

226. Best reason to provide social engineering training:

A. Show how to perform attacks
B. Teach reporting violations
C. Teach what to look out for
D. None

ANS: C. Training helps employees recognize and defend against social engineering attacks.

---

227. During which phase of incident response is the plan developed?

A. Preparation
B. Containment, eradication, recovery
C. Detection and analysis
D. Post-incident activity

ANS: A. Incident response plans are developed during the preparation phase.

---

228. Lessons-learned assessment occurs in which phase?

A. Detection and analysis
B. Containment, eradication, recovery
C. Preparation
D. Post-incident activity

ANS: D. Post-incident activity involves lessons learned for process improvement.

---

229. Reviewing logs to determine if an incident occurred is in which phase?

A. Containment, eradication, recovery
B. Detection and analysis
C. Preparation
D. Post-incident activity

ANS: B. Log analysis happens in detection and analysis phase.

---

230. Recovering a system from backup occurs in which phase?

A. Preparation
B. Detection and analysis
C. Post-incident activity
D. Containment, eradication, and recovery

ANS: D. Recovery is part of containment, eradication, and recovery.

---

231. Phase after detection and analysis in incident response:

A. Containment, eradication, recovery
B. Preparation
C. Post-incident activity
D. Detection is last

ANS: A. Detection/analysis → Containment, eradication, recovery → Post-incident activity.

---

232. To determine which business functions should be restored after an incident, Carol should:

A. Conduct risk assessment
B. Interview stakeholders
C. Calculate MTD
D. Conduct business impact analysis

ANS: D. BIA identifies critical functions and restoration priorities.

---

233. Most likely reason a business continuity program might fail:

A. Failure to test plan/procedures
B. Failure to document activation procedures
C. Failure to address most likely threats
D. All of the above

ANS: D. All these failures can cause BC program to fail.

---

234. Alice wants a datacenter up in a few days but without full equipment installed. Best choice:

A. Hot site
B. Warm site
C. Cold site
D. Tertiary site

ANS: B. Warm site has infrastructure ready but not fully equipped with computing resources.

---

235. Best example of a hot site:

A. Facility with infrastructure but no computing equipment
B. Facility with infrastructure and fully configured computing equipment
C. Facility with infrastructure and installed but not configured equipment
D. Facility with equipment installed but not powered

ANS: B. Hot site is fully equipped and configured for immediate operations.

---

236. Best example of a cold site:

A. Facility with infrastructure but no computing equipment
B. Facility with infrastructure and fully configured computing equipment
C. Facility with infrastructure and installed but not configured equipment
D. Facility with equipment installed but not powered

ANS: A. Cold site has only infrastructure; computing equipment must be brought in.

ISC2 CC Practice Questions (1-20)

1. Which concept describes an information security strategy that integrates people, technology, and operations in order to establish security controls across multiple layers of the organization?

- **Options:** (A) Least Privilege, (B) Defense in Depth, (C) Access Control, (D) Risk Management.
- **Answer: (B) Defense in Depth** [01:01]
- **Explanation:** Defense in Depth is a layered security approach that provides redundancy in case one security control fails. It integrates various measures across physical, technical, and administrative layers [03:31].

2. Which of the following is NOT an ethical canon of the ISC2?

- **Options:** (A) Advance and protect the profession, (B) Protect the society, the common good, necessary public trust and confidence, (C) Act honorably, honestly, justly, responsibly, and legally, (D) Provide active and qualified service to principals.
- **Answer:** *(Note: The video lists the four canons and asks to identify the one that is NOT. Based on standard ISC2 canons, all listed A, B, and C are correct canons. Option D is usually phrased as "Provide diligent and competent service to principals")* [03:43].

3. Which of the following is an example of a "Technical" control?

- **Answer: Firewalls** (found in later context [10:54]).
- **Explanation:** Technical controls (or logical controls) use technology to protect systems, such as encryption, firewalls, and antivirus software [04:37:53].

4. Which type of intrusion detection system is most effective at detecting an intrusion into a network?

- **Options:** (A) Routers, (B) HIDS, (C) Firewalls, (D) NIDS.
- **Answer: (D) NIDS (Network-based Intrusion Detection System)** [10:54]
- **Explanation:** NIDS monitors traffic across the entire network, whereas HIDS (Host-based) only monitors activity on a specific individual host [11:53].

5. Which access control is more effective at protecting a door against unauthorized physical access?

- **Options:** (A) Fences, (B) Turnstyles, (C) Barriers, (D) Locks.
- **Answer: (D) Locks** [12:44]
- **Explanation:** Locks are specifically designed to secure doors directly to prevent unauthorized physical entry [12:44].

6. Which of the following is a detection control that detects an intrusion (specifically smoke/fire)?

- **Options:** (A) Turnstyles, (B) Smoke detectors, (C) Bollards, (D) Firewalls.
- **Answer: (B) Smoke detectors** [13:53]

- **Explanation:** Smoke sensors are detection controls because they identify the presence of a threat (smoke/fire) and trigger an alert [14:04].

7. Which type of attack has the primary objective of controlling the system from the outside?

- **Options:** (A) Backdoors, (B) Rootkits, (C) Cross-site scripting, (D) Trojans.
- **Answer: (A) Backdoors** [15:12]
- **Explanation:** A backdoor allows an attacker to bypass normal authentication to gain remote access and control over a system [15:21].

8. What is the foundational principle in disaster recovery and business continuity planning?

- **Answer: Prioritizing human safety** [25:55]
- **Explanation:** In any emergency or disaster scenario, the safety of people always comes before the preservation of data or equipment [26:06].

9. The process that ensures system changes do not adversely impact business operations is known as:

- **Options:** (A) Change management, (B) Vulnerability management, (C) Configuration management, (D) Inventory management.
- **Answer: (A) Change management** [26:28]
- **Explanation:** Change management is the formal process of requesting, reviewing, and approving changes to ensure they don't cause unintended disruptions [26:28].

10. Which access control model specifies access based on a user's role within an organization?

- **Options:** (A) RBAC, (B) MAC, (C) DAC, (D) ABAC.
- **Answer: (A) RBAC (Role-Based Access Control)** [28:35]
- **Explanation:** RBAC assigns permissions to roles rather than individuals, making it easier to manage access in large organizations [28:47].

11. Which of the following is NOT an example of a physical control?

- **Options:** (A) Firewalls, (B) Biometric access control, (C) Remote control electronic locks, (D) Security cameras.
- **Answer: (A) Firewalls** [29:26]
- **Explanation:** Firewalls are logical (technical) controls used to manage network traffic, whereas the others are physical measures to protect a facility [04:37:53].

11. Which concept describes the process of granting users only the minimum level of access necessary to perform their jobs?

- **Options:** (A) Least Privilege, (B) Defense in Depth, (C) Separation of Duties, (D) Need to Know.
- **Answer: (A) Least Privilege**
- **Explanation:** Least privilege ensures that users have no more access than required for their specific tasks, reducing the risk of unauthorized access or damage.

12. Which security principle divides a task into multiple steps that must be performed by different individuals?

- **Options:** (A) Defense in Depth, (B) Least Privilege, (C) Separation of Duties, (D) Job Rotation.
- **Answer: (C) Separation of Duties**
- **Explanation:** This prevents a single person from having total control over a critical process, thereby reducing the likelihood of fraud or error.

13. Which type of control is a policy or a procedure?

- **Options:** (A) Technical, (B) Physical, (C) Administrative, (D) Logical.
- **Answer: (C) Administrative**
- **Explanation:** Administrative controls consist of management-oriented actions like policies, training, and background checks.

14. Which of the following is a "preventive" control?

- **Options:** (A) Audit logs, (B) Motion sensors, (C) Security guards, (D) Firewalls.
- **Answer: (D) Firewalls**
- **Explanation:** Firewalls act as a preventive measure by blocking unauthorized traffic before it enters the network.

15. What is the main goal of Business Continuity Planning (BCP)?

- **Answer: To ensure the business remains operational during and after a disaster.** [25:55]
- **Explanation:** BCP focuses on maintaining critical functions even when standard operations are disrupted.

16. The process that ensures system changes do not adversely impact business operations is known as:

- **Answer: (A) Change management** [26:28]
- **Explanation:** It involves formal approval and testing before implementing any modifications to systems.

17. Which access control model uses "tags" or "labels" to determine access?

- **Options:** (A) DAC, (B) MAC, (C) RBAC, (D) ABAC.
- **Answer: (B) MAC (Mandatory Access Control)**
- **Explanation:** MAC relies on sensitivity labels (e.g., Top Secret) assigned to objects and clearances assigned to users.

18. Which access control model specifies access to resources based on a user's role?

- **Answer: (A) RBAC (Role-Based Access Control)** [28:35]
- **Explanation:** Permissions are tied to roles, making it easy to assign access to groups of employees [28:47].

19. Which of the following is NOT an example of a physical control?

- **Options:** (A) Firewalls, (B) Biometric locks, (C) Fences, (D) Security cameras.

- **Answer: (A) Firewalls** [29:26]
- **Explanation:** Firewalls are logical/technical controls, while others physically protect the premises [04:37:53].

20. What is "phishing"?

- **Answer: A social engineering attack used to trick users into disclosing sensitive information.** [34:52]
- **Explanation:** It typically involves fraudulent emails appearing to come from a reputable source.

21. Which type of malware records every keystroke made on a computer?

- **Answer: Keylogger**
- **Explanation:** Keyloggers are used to capture passwords, credit card numbers, and other sensitive typed data.

22. Which attack denies legitimate users access to a system by overwhelming it with traffic?

- **Answer: DoS (Denial of Service) or DDoS (Distributed Denial of Service)**
- **Explanation:** These attacks flood a target with traffic to exhaust its resources and make it unavailable.

23. Which type of attack embeds a malicious payload inside a reputable software?

- **Answer: (A) Trojan Horse** [35:17]
- **Explanation:** A Trojan appears to be useful or legitimate software but performs hidden malicious actions [35:30].

24. What is "Ransomware"?

- **Answer: Malware that encrypts files and demands payment for the decryption key.**
- **Explanation:** It holds data "hostage" until the victim pays the attacker.

25. Which term describes a vulnerability that is unknown to the vendor?

- **Answer: Zero-day vulnerability**
- **Explanation:** This refers to a flaw that is exploited before the developer has a chance to create a patch.

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

- **Answer: To provide a structured approach for handling security incidents.**
- **Explanation:** It outlines the steps to take to detect, contain, and recover from a breach.

27. What does CIA stand for in cybersecurity?

- **Answer: Confidentiality, Integrity, and Availability**
- **Explanation:** These are the three core principles of information security.

28. Which principle ensures that data has not been altered by unauthorized parties?

- **Answer: Integrity**
- **Explanation:** Integrity means the data is accurate and trustworthy.

29. Which principle ensures that information is accessible to authorized users when needed?

- **Answer: Availability**
- **Explanation:** This ensures systems are up and running and data is reachable.

30. Which principle ensures that sensitive information is only accessible to those with authorized access?

- **Answer: Confidentiality**
- **Explanation:** Confidentiality protects data from being seen by unauthorized individuals.

31. What is "Multifactor Authentication" (MFA)?

- **Answer: Using two or more different types of credentials to verify identity.**

- **Explanation:** Common factors include something you know (password), something you have (token), or something you are (biometrics).

32. What is "Social Engineering"?

- **Answer: Manipulating people into performing actions or divulging confidential information.**
- **Explanation:** It relies on human psychology rather than technical hacking techniques.

33. What is a "DMZ" (Demilitarized Zone)?

- **Answer: A subnetwork that sits between an internal private network and an external public network (like the Internet).**
- **Explanation:** It hosts public-facing services (like web servers) to protect the internal network.

34. What is "Encryption"?

- **Answer: Converting data into a coded format (ciphertext) that cannot be read without a key.**
- **Explanation:** This is a key technical control for protecting data confidentiality.

35. What is "Decryption"?

- **Answer: The process of converting ciphertext back into its original readable format (plaintext).**
- **Explanation:** It requires the correct cryptographic key.

36. What is "Hashing"?

- **Answer: A mathematical process that converts data into a fixed-length string of characters.**
- **Explanation:** It is primarily used to verify the integrity of data; even a small change in input results in a completely different hash.

37. What is a "Digital Signature"?

- **Answer: A cryptographic technique used to validate the authenticity and integrity of a message or document.**
- **Explanation:** It ensures the sender is who they claim to be and that the message wasn't changed.

38. What is a "Vulnerability"?

- **Answer: A weakness in a system or network that could be exploited by a threat.**
- **Explanation:** Vulnerabilities can exist in software, hardware, or human processes.

39. What is a "Threat"?

- **Answer: Anything that has the potential to cause harm to a system or organization.**
- **Explanation:** Threats can be human-made (hackers) or natural (floods).

40. What is "Risk"?

- **Answer: The likelihood of a threat exploiting a vulnerability and the resulting impact.**
- **Explanation:** Risk = Threat × Vulnerability × Impact.

41. What is "Risk Mitigation"?

- **Answer: Taking steps to reduce the likelihood or impact of a risk.**
- **Explanation:** Examples include installing antivirus software or creating backups.

42. What is "Risk Acceptance"?

- **Answer: Deciding to take on a risk because the cost of mitigation outweighs the potential loss.**
- **Explanation:** This is often done for very low-impact risks.

43. What is "Risk Avoidance"?

- **Answer: Eliminating a risk by not engaging in the activity that causes it.**
- **Explanation:** For example, not using a certain risky software application.

44. What is "Risk Transfer"?

- **Answer: Shifting the impact of a risk to another party.**
- **Explanation:** Purchasing cyber insurance is a common way to transfer financial risk.

45. What is a "Security Audit"?

- **Answer: A formal assessment of an organization's security controls to ensure they are effective.**
- **Explanation:** Audits verify compliance with policies and standards.

46. What is "Patch Management"?

- **Answer: The process of applying updates to software to fix security vulnerabilities.**
- **Explanation:** Keeping systems patched is critical to preventing exploitation.

47. What is an "Intrusion Detection System" (IDS)?

- **Answer: A device or software that monitors a network or system for malicious activity.**
- **Explanation:** It sends alerts when suspicious behavior is detected.

48. What is an "Intrusion Prevention System" (IPS)?

- **Answer: An IDS that also has the capability to block or stop the detected malicious activity.**
- **Explanation:** IPS is an active control, while IDS is a passive monitoring tool.

49. What is a "VPN" (Virtual Private Network)?

- **Answer: A secure, encrypted tunnel that allows users to access a private network over a public network.**

- **Explanation:** VPNs protect data privacy and security during transmission.

50. What is "BYOD" (Bring Your Own Device)?

- **Answer: A policy that allows employees to use their personal devices for work purposes.**
- **Explanation:** It creates security challenges because the organization has less control over personal hardware.

51. What is "Tailgating"?

- **Answer: A physical security breach where an unauthorized person follows an authorized person through a secure door.**
- **Explanation:** It relies on the authorized person's politeness to keep the door open.

52. What is "Piggybacking"?

- **Answer: Similar to tailgating, but with the knowledge and consent of the authorized person.**
- **Explanation:** Both are methods to bypass physical access controls.

53. What is a "Firewall"?

- **Answer: A security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.**
- **Explanation:** It acts as a barrier between a trusted network and an untrusted network.

54. What is "Malware"?

- **Answer: Short for malicious software; it is any software specifically designed to disrupt, damage, or gain unauthorized access to a computer system.**
- **Explanation:** Common types include viruses, worms, Trojans, and spyware.

55. What is a "Virus"?

- **Answer: A type of malware that attaches itself to a legitimate program and spreads when that program is executed.**
- **Explanation:** Viruses require human action (like running a file) to spread.

56. What is a "Worm"?

- **Answer: A type of malware that can self-replicate and spread across networks without human intervention.**
- **Explanation:** Worms often exploit vulnerabilities in network protocols.

57. What is "Spyware"?

- **Answer: Malware that secretly gathers information about a person or organization and sends it to another entity.**
- **Explanation:** It often tracks browsing habits or captures sensitive data like passwords.

58. What is "Adware"?

- **Answer: Software that automatically displays or downloads advertising material when a user is online.**
- **Explanation:** While often just annoying, some adware can be malicious or invasive.

59. What is "Botnet"?

- **Answer: A network of infected computers (bots) controlled by a single attacker to perform tasks like DDoS attacks.**
- **Explanation:** Each computer in the botnet is often called a "zombie."

60. What is "SQL Injection"?

- **Answer: An attack that inserts malicious SQL code into a web form or database query to gain unauthorized access to data.**
- **Explanation:** It exploits vulnerabilities in how an application interacts with its database.

61. What is "Cross-Site Scripting" (XSS)?

- **Answer: An attack that injects malicious scripts into trusted websites, which are then executed in the victim's browser.**
- **Explanation:** It is often used to steal session cookies or personal information.

62. What is "Zero-Day Attack"?

- **Answer: An attack that takes advantage of a software vulnerability that has no available patch or fix.**
- **Explanation:** The "zero-day" refers to the fact that the developer has had zero days to fix the problem.

63. What is a "Buffer Overflow"?

- **Answer: An anomaly where a program, while writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory.**
- **Explanation:** Attackers can use this to execute malicious code or crash a system.

64. What is "Network Address Translation" (NAT)?

- **Answer: A method of remapping one IP address space into another by modifying network address information in the IP header of packets.**
- **Explanation:** It allows multiple devices on a private network to share a single public IP address.

65. What is "Port Scanning"?

- **Answer: A technique used to identify open ports and services available on a network host.**
- **Explanation:** While used for network management, it is also a common reconnaissance step for attackers.

66. What is "Packet Sniffing"?

- **Answer: The process of capturing and inspecting data packets as they travel across a network.**

- **Explanation:** Tools like Wireshark are used for this purpose [36:58].

67. What is "Wireshark"?

- **Answer: A popular network protocol analyzer used for packet sniffing and network troubleshooting.** [36:58]
- **Explanation:** It captures real-time traffic and allows for deep inspection of network communication [37:08].

68. What is "Encryption at Rest"?

- **Answer: The practice of encrypting data while it is stored on a physical medium (like a hard drive or cloud storage).**
- **Explanation:** It protects data even if the storage device is stolen.

69. What is "Encryption in Transit"?

- **Answer: The practice of encrypting data while it is being sent over a network.**
- **Explanation:** Protocols like HTTPS and TLS provide encryption in transit.

70. What is "Public Key Infrastructure" (PKI)?

- **Answer: A system of digital certificates and CA (Certificate Authorities) that verify and authenticate the validity of each party involved in an electronic transaction.**
- **Explanation:** It uses asymmetric encryption (public and private keys).

71. What is a "Public Key"?

- **Answer: A cryptographic key that can be shared with anyone; it is used to encrypt data.**
- **Explanation:** In asymmetric encryption, data encrypted with a public key can only be decrypted with the corresponding private key.

72. What is a "Private Key"?

- **Answer: A cryptographic key that must be kept secret by its owner; it is used to decrypt data.**
- **Explanation:** The security of asymmetric encryption depends on the private key remaining confidential.

73. What is "Symmetric Encryption"?

- **Answer: A type of encryption where the same key is used for both encryption and decryption.**
- **Explanation:** It is faster than asymmetric encryption but requires a secure way to share the key.

74. What is "Asymmetric Encryption"?

- **Answer: A type of encryption that uses a pair of keys: a public key for encryption and a private key for decryption.**
- **Explanation:** Also known as public-key cryptography.

75. What is "Data Loss Prevention" (DLP)?

- **Answer: A strategy and set of tools used to ensure that sensitive data is not lost, misused, or accessed by unauthorized users.**
- **Explanation:** DLP systems monitor data moving in, out, and within the network.

76. What is a "Security Policy"?

- **Answer: A formal document that outlines the rules, requirements, and procedures for protecting an organization's assets.**
- **Explanation:** Policies provide the high-level framework for security.

77. What is "Acceptable Use Policy" (AUP)?

- **Answer: A set of rules applied by the owner or manager of a network that restrict the ways in which the network or system may be used.**

- **Explanation:** It usually defines what is considered "proper" use of company equipment and internet.

78. What is "Change Control"?

- **Answer: A formal process used to ensure that changes to a product or system are introduced in a controlled and coordinated manner.**
- **Explanation:** It minimizes the risk of disruptions during updates.

79. What is "Asset Management"?

- **Answer: The process of identifying, tracking, and managing an organization's hardware and software assets.**
- **Explanation:** You cannot protect what you don't know you have.

80. What is a "Security Guard"?

- **Answer: A physical security control that provides a human presence to monitor and protect an area.** [04:37:15]
- **Explanation:** Guards can respond to incidents, verify IDs, and deter intruders [04:37:44].

81. What is "Biometrics"?

- **Answer: Security measures that use unique biological characteristics (like fingerprints or iris scans) to verify identity.**
- **Explanation:** Biometrics represent "something you are."

82. What is "Principle of Need to Know"?

- **Answer: A security principle where a user is given access only to the specific information required to perform their job.**
- **Explanation:** It is more specific than least privilege, focusing on the data itself.

83. What is "Mandatory Access Control" (MAC)?

- **Answer: An access control model where the system (not the owner) determines access based on security labels.**
- **Explanation:** It is commonly used in highly secure military environments.

84. What is "Discretionary Access Control" (DAC)?

- **Answer: An access control model where the owner of the object has the power to grant or deny access.**
- **Explanation:** It is the most common model used in personal computer systems.

85. What is "Attribute-Based Access Control" (ABAC)?

- **Answer: An access control model that uses attributes (of users, resources, and environment) to make access decisions.**
- **Explanation:** It is highly flexible and granular.

86. What is "HIDS"?

- **Answer: Host-based Intrusion Detection System; it monitors activity on a single computer.** [11:53]
- **Explanation:** It analyzes logs and system files for signs of a breach.

87. What is "NIDS"?

- **Answer: Network-based Intrusion Detection System; it monitors traffic for an entire network.** [10:54]
- **Explanation:** It is placed at strategic points to see all traffic entering or leaving the network.

88. What is "Cloud Computing"?

- **Answer: The delivery of computing services (servers, storage, databases, etc.) over the Internet.**
- **Explanation:** It offers scalability and cost-efficiency.

89. What is "SaaS" (Software as a Service)?

- **Answer: A cloud model where applications are provided over the internet (e.g., Gmail, Office 365).**
- **Explanation:** The user doesn't manage the underlying infrastructure or application platform.

90. What is "PaaS" (Platform as a Service)?

- **Answer: A cloud model that provides a platform allowing customers to develop, run, and manage applications.**
- **Explanation:** The customer manages the apps, while the provider manages the servers and OS.

91. What is "IaaS" (Infrastructure as a Service)?

- **Answer: A cloud model that provides basic computing infrastructure (servers, storage, networking) over the internet.**
- **Explanation:** The customer manages the OS, middleware, and applications.

92. What is a "Public Cloud"?

- **Answer: A cloud environment where services are offered over the public internet and shared across multiple organizations.**
- **Explanation:** Examples include AWS, Microsoft Azure, and Google Cloud.

93. What is a "Private Cloud"?

- **Answer: A cloud environment used exclusively by a single organization.**
- **Explanation:** It provides more control and security but is more expensive to maintain.

94. What is a "Hybrid Cloud"?

- **Answer: A combination of public and private clouds, allowing data and applications to be shared between them.** [07:01]

- **Explanation:** It allows organizations to keep sensitive data on-premises while using the public cloud for other tasks [07:18].

95. What is "Security Governance"?

- **Answer: The framework that guides how security is managed and directed within an organization.**
- **Explanation:** It ensures security goals align with business objectives.

96. What is "Risk Assessment"?

- **Answer: The process of identifying and evaluating risks to an organization's assets.**
- **Explanation:** It is a critical step in risk management.

97. What is "Security Awareness Training"?

- **Answer: A program designed to educate employees about security threats and their responsibilities in protecting the organization.**
- **Explanation:** It helps reduce the risk of human-based attacks like phishing.

98. What is a "Logic Bomb"?

- **Answer: A string of malicious code that is inserted into a system and triggered by a specific event or time.**
- **Explanation:** For example, a code that deletes files on a specific date.

99. What is "Social Engineering: Baiting"?

- **Answer: An attack where the attacker leaves an infected physical device (like a USB drive) in a public place, hoping someone will plug it in.**
- **Explanation:** It exploits human curiosity.

100. What is "Social Engineering: Pretexting"?

- **Answer: Creating a fabricated scenario (pretext) to trick a victim into providing information.**
- **Explanation:** The attacker might pretend to be from tech support or HR.

101. What is "Spear Phishing"?

- **Answer: A targeted phishing attack aimed at a specific individual, group, or organization.**
- **Explanation:** It is more personalized and convincing than standard broad-based phishing.

102. What is "Whaling"?

- **Answer: A form of spear phishing that targets high-profile individuals, such as CEOs or CFOs.**
- **Explanation:** These targets have access to highly sensitive information and high-value financial assets.

103. What is "Vishing"?

- **Answer: Phishing that takes place over the phone (Voice Phishing).**
- **Explanation:** The attacker uses voice communication to trick victims into revealing sensitive data.

104. What is "Smishing"?

- **Answer: Phishing that takes place via SMS (text messages).**
- **Explanation:** Victims receive a text with a malicious link or a request for information.

105. What is a "Honey Pot"?

- **Answer: A decoy system designed to lure in attackers and monitor their activities.**
- **Explanation:** It helps security teams learn about attack methods without risking real production systems.

106. What is "Zero Trust Architecture"?

- **Answer: A security model that requires strict identity verification for every person and device trying to access resources on a private network, regardless of whether they are sitting inside or outside of the network perimeter.**
- **Explanation:** Its core motto is "never trust, always verify."

107. What is "Multi-Tenancy"?

- **Answer: An architecture in which a single instance of a software application serves multiple customers (tenants).**
- **Explanation:** This is a core concept in cloud computing.

108. What is "Shadow IT"?

- **Answer: The use of IT systems, software, or devices within an organization without explicit departmental approval.**
- **Explanation:** It creates security risks because the IT department is unaware of these assets and cannot protect them.

109. What is "Endpoint Security"?

- **Answer: An approach to protecting a computer network that is remotely bridged to client devices (endpoints like laptops, tablets, smartphones).**
- **Explanation:** It focuses on securing the points where devices connect to the network.

110. What is "Forensics" in cybersecurity?

- **Answer: The process of collecting, analyzing, and preserving digital evidence related to a security incident or crime.**
- **Explanation:** It is used to understand how a breach happened and who was responsible.

111. What is "Chain of Custody"?

- **Answer: The documented history of who had possession of a piece of evidence from the time it was collected until it is presented in court.**
- **Explanation:** It is essential for ensuring that evidence remains admissible and untampered.

112. What is "Business Impact Analysis" (BIA)?

- **Answer: A process to identify and evaluate the potential effects (financial and operational) of an interruption to critical business operations.** [04:39:20]
- **Explanation:** BIA helps prioritize which systems and processes need to be recovered first after a disaster [04:39:28].

113. What is "RTO" (Recovery Time Objective)?

- **Answer: The maximum amount of time a system or process can be down before causing significant damage to the business.**
- **Explanation:** It defines the "target time" for recovery.

114. What is "RPO" (Recovery Point Objective)?

- **Answer: The maximum amount of data loss (measured in time) an organization can tolerate.**
- **Explanation:** For example, an RPO of 1 hour means you must be able to restore data to a point no more than 1 hour ago.

115. What is "Sanitization" of media?

- **Answer: The process of permanently and irreversibly removing data from storage media so that it cannot be recovered.**
- **Explanation:** Methods include degaussing, physical destruction, or secure overwriting.

116. What is "Degaussing"?

- **Answer: A method of sanitization that uses a strong magnetic field to erase data from magnetic media (like hard drives or tapes).**

- **Explanation:** It renders the media unusable in many cases.

117. What is "Cold Site"?

- **Answer: A backup facility that has the necessary space and power but no computer equipment or data.**
- **Explanation:** It is the cheapest backup site option but takes the longest to get operational.

118. What is "Warm Site"?

- **Answer: A backup facility that is equipped with hardware and communication links but does not have a current copy of the data.**
- **Explanation:** It is a middle-ground option in terms of cost and recovery speed.

119. What is "Hot Site"?

- **Answer: A fully operational backup facility that has all the necessary hardware and a near real-time copy of the data.**
- **Explanation:** It is the most expensive option but allows for the fastest recovery (often within minutes).

120. What is "Separation of Privilege"?

- **Answer: A security design principle that requires multiple conditions to be met before access to a sensitive resource is granted.**
- **Explanation:** It is similar to separation of duties but focuses on technical permissions.

121. What is "Least Functionality"?

- **Answer: The practice of configuring systems to provide only the essential functions and services required for their intended purpose.**
- **Explanation:** Disabling unnecessary services reduces the attack surface.

122. What is "Hardening"?

- **Answer: The process of securing a system by reducing its surface of vulnerability.**
- **Explanation:** This includes removing unnecessary software, closing unused ports, and applying security patches.

123. What is "Ingress Filtering"?

- **Answer: A technique used to ensure that incoming packets are actually from the networks from which they claim to originate.**
- **Explanation:** It helps prevent IP spoofing attacks.

124. What is "Egress Filtering"?

- **Answer: A technique used to monitor and restrict outgoing traffic from a network.**
- **Explanation:** It helps prevent malware from communicating with its Command & Control (C2) server or prevents data exfiltration.

125. What is "IP Spoofing"?

- **Answer: A technique where an attacker sends packets with a forged source IP address to impersonate another system.**
- **Explanation:** It is often used in DDoS attacks or to bypass network filters.

126. What is "MAC Spoofing"?

- **Answer: A technique where an attacker changes the Media Access Control (MAC) address of their network interface to impersonate another device.**
- **Explanation:** It is used to bypass MAC-based access controls on a network.

127. What is "ARP Spoofing" (or ARP Poisoning)?

- **Answer: An attack where the attacker sends forged Address Resolution Protocol (ARP) messages onto a local network to link their MAC address with the IP address of a legitimate server.**
- **Explanation:** This allows the attacker to intercept, modify, or stop traffic intended for the legitimate server.

128. What is "DNS Poisoning" (or DNS Cache Poisoning)?

- **Answer: An attack that inserts false information into a DNS resolver's cache, causing it to return an incorrect IP address for a domain name.**
- **Explanation:** Users are redirected to malicious websites without their knowledge.

129. What is "Session Hijacking"?

- **Answer: An attack where the attacker takes over an active computer session by stealing or predicting the session ID.**
- **Explanation:** Once hijacked, the attacker can act as the legitimate user.

130. What is "Man-in-the-Middle" (MitM) Attack?

- **Answer: An attack where the attacker secretly relays and possibly alters communication between two parties who believe they are communicating directly.**
- **Explanation:** The attacker intercepts the traffic, which may include sensitive data like credentials.

131. What is "Bluejacking"?

- **Answer: Sending unsolicited messages to Bluetooth-enabled devices.**
- **Explanation:** While mostly annoying, it is a form of unauthorized communication.

132. What is "Bluesnarfing"?

- **Answer: The unauthorized access of information from a wireless device through a Bluetooth connection.**
- **Explanation:** It is more serious than bluejacking as it involves data theft.

133. What is "War Driving"?

- **Answer: The act of searching for Wi-Fi wireless networks by a person in a moving vehicle, using a computer or smartphone.**
- **Explanation:** It is often done to find insecure networks to exploit.

134. What is "Evil Twin"?

- **Answer: A fraudulent Wi-Fi access point that appears to be a legitimate one offered on the premises.**
- **Explanation:** Users connect to the "twin," and the attacker intercepts their traffic.

135. What is "WPA3" (Wi-Fi Protected Access 3)?

- **Answer: The latest security protocol for Wi-Fi networks, providing stronger encryption and protection against password-guessing attacks.**
- **Explanation:** It replaces WPA2 as the industry standard.

136. What is "SSID" (Service Set Identifier)?

- **Answer: The name of a Wi-Fi network.**
- **Explanation:** While SSID broadcasting can be disabled, it is not a strong security measure.

137. What is "Containerization"?

- **Answer: A lightweight form of virtualization that allows an application and its dependencies to be packaged and run consistently across different environments.**
- **Explanation:** Popular tools include Docker and Kubernetes.

138. What is "Serverless Computing"?

- **Answer: A cloud model where the provider dynamically manages the allocation of machine resources, and the user only pays for the actual execution of code.**
- **Explanation:** The developer doesn't need to manage the underlying servers.

139. What is "API" (Application Programming Interface) Security?

- **Answer: The practice of protecting APIs from attacks and unauthorized access.**
- **Explanation:** APIs are often targets for data breaches and must be secured with authentication and rate limiting.

140. What is "CI/CD" (Continuous Integration / Continuous Deployment)?

- **Answer: A set of practices and tools used to automate the stages of software development and delivery.**
- **Explanation:** Security should be integrated into the CI/CD pipeline (DevSecOps).

141. What is "DevSecOps"?

- **Answer: An approach to software development that integrates security practices throughout the entire development life cycle (from planning to deployment).**
- **Explanation:** It ensures security is not an afterthought.

142. What is "Privacy by Design"?

- **Answer: An approach to systems engineering which takes privacy into account throughout the whole engineering process.**
- **Explanation:** It is a core requirement of regulations like GDPR.

143. What is "GDPR" (General Data Protection Regulation)?

- **Answer: A comprehensive data privacy regulation in the European Union (EU) that gives individuals control over their personal data.**
- **Explanation:** It has significant legal and financial impacts for global organizations.

144. What is "PII" (Personally Identifiable Information)?

- **Answer: Any information that can be used to identify a specific individual (e.g., name, SSN, address).**
- **Explanation:** Protecting PII is a primary goal of many security programs and regulations.

145. What is "PHI" (Protected Health Information)?

- **Answer: Individually identifiable health information that is protected by laws like HIPAA.**

- **Explanation:** It includes medical records and payment information for healthcare.

146. What is "PCI DSS" (Payment Card Industry Data Security Standard)?

- **Answer: A set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment.**
- **Explanation:** Compliance is mandatory for businesses handling credit card data.

147. What is "SLA" (Service Level Agreement)?

- **Answer: A formal contract between a service provider and a customer that defines the expected level of service, including uptime and response times.**
- **Explanation:** It often includes penalties for failing to meet the agreed-upon standards.

148. What is "Supply Chain Risk Management"?

- **Answer: The process of identifying and managing risks associated with external vendors and partners.**
- **Explanation:** A vulnerability in a vendor's system can compromise the organization's security.

149. What is "Security Operations Center" (SOC)?

- **Answer: A centralized unit that deals with security issues on an organizational and technical level.**
- **Explanation:** SOC teams monitor, detect, and respond to security incidents.

150. What is "SIEM" (Security Information and Event Management)?

- **Answer: A technology that provides real-time analysis of security alerts generated by applications and network hardware.**
- **Explanation:** It aggregates logs from multiple sources to provide a unified view of the organization's security posture.

151. What is the primary purpose of a "Vulnerability Scanner"?

- **Answer:** To automatically identify known security weaknesses in a system or network.
- **Explanation:** It compares system configurations against a database of known vulnerabilities.

152. What is "Penetration Testing" (Ethical Hacking)?

- **Answer:** An authorized simulated cyberattack on a computer system, performed to evaluate its security.
- **Explanation:** Unlike a scan, a pen test attempts to exploit vulnerabilities to see how much damage could be done.

153. What is "Red Teaming"?

- **Answer:** An advanced security assessment where a team acts as adversaries to test an organization's detection and response capabilities.
- **Explanation:** It is often unannounced to the internal security team (Blue Team) to ensure a realistic test.

154. What is "Blue Teaming"?

- **Answer:** The internal security team responsible for defending the organization's assets and responding to incidents.

155. What is "Purple Teaming"?

- **Answer:** A collaborative approach where Red and Blue teams work together to share insights and improve security posture.

156. What is "Security Orchestration, Automation, and Response" (SOAR)?

- **Answer:** Technology that allows organizations to collect data about security threats and respond to low-level security events without human assistance.

157. What is "Digital Rights Management" (DRM)?

- **Answer:** Tools or technological protection measures used to control the use of proprietary hardware and copyrighted works.

158. What is "Steganography"?

- **Answer:** The practice of hiding a secret message within a non-secret file (like an image or audio file).

159. What is "Cryptanalysis"?

- **Answer:** The study of analyzing information systems in order to find hidden aspects of the systems (essentially "breaking" codes).

160. What is "Non-Repudiation"?

- **Answer:** A legal/technical concept that ensures a person cannot deny the authenticity of their signature or the sending of a message.
- **Explanation:** This is achieved through digital signatures and hashing.

161. What is "E-Discovery"?

- **Answer:** The process of identifying, collecting, and producing electronically stored information (ESI) in response to a request for production in a lawsuit or investigation.

162. What is the "Principle of Least Astonishment"?

- **Answer:** A design principle stating that a system should behave in a way that users expect it to behave.

163. What is "Fuzzing"?

- **Answer:** An automated software testing technique that involves providing invalid, unexpected, or random data as inputs to a computer program.

164. What is "Rooting" or "Jailbreaking"?

- **Answer:** Removing software restrictions imposed by the device manufacturer, often on mobile operating systems.
- **Explanation:** While it grants more control, it significantly lowers the device's security.

165. What is "Mobile Device Management" (MDM)?

- **Answer:** Software that allows IT administrators to control, secure, and enforce policies on smartphones and tablets.

166. What is "Geofencing"?

- **Answer:** Using GPS or RFID technology to create a virtual geographic boundary, enabling software to trigger a response when a device enters or leaves a particular area.

167. What is "Remote Wipe"?

- **Answer:** A security feature that allows a device owner or administrator to command a device to delete all its data remotely.

168. What is "Context-Aware Authentication"?

- **Answer:** A method of verifying identity based on supplemental information like location, time of day, and device health.

169. What is "Single Sign-On" (SSO)?

- **Answer:** An authentication scheme that allows a user to log in with a single ID to any of several related, yet independent, software systems.

170. What is "Federated Identity Management" (FIdM)?

- **Answer:** An arrangement that can be made between two or more trust domains to allow users to use the same identification data to access applications in all domains.

171. What is "OAuth"?

- **Answer:** An open standard for access delegation, commonly used as a way for internet users to grant websites access to their information on other websites without giving them passwords.

172. What is "SAML" (Security Assertion Markup Language)?

- **Answer:** An XML-based standard for exchanging authentication and authorization data between parties (Identity Provider and Service Provider).

173. What is a "Logic Gate" in the context of physical security?

- **Answer:** A physical barrier that controls the flow of people or vehicles.

174. What is "Mantrapping"?

- **Answer:** A physical security access control system comprising a small space with two sets of interlocking doors, such that the first set of doors must close before the second set can open.

175. What is "CCTV" (Closed-Circuit Television)?

- **Answer:** The use of video cameras to transmit a signal to a specific place on a limited set of monitors.

176. What is "Tempering" (as per STRIDE)?

- **Answer:** The unauthorized modification of data or system components.

177. What is "Information Disclosure" (as per STRIDE)?

- **Answer:** Providing information to individuals who are not authorized to have access to it.

178. What is "Repudiation" (as per STRIDE)?

- **Answer:** The ability of a user to deny performing an action without there being a way to prove otherwise.

179. What is "Elevation of Privilege"?

- **Answer:** When a user gains more permissions than they are supposed to have.

180. What is "Secure Boot"?

- **Answer:** A security standard developed by members of the PC industry to help make sure that a device boots using only software that is trusted by the Original Equipment Manufacturer (OEM).

181. What is "TPM" (Trusted Platform Module)?

- **Answer:** A dedicated microcontroller designed to secure hardware through integrated cryptographic keys.

182. What is "Data Sovereignty"?

- **Answer:** The concept that data is subject to the laws and governance structures within the nation it is collected.

183. What is "Data Portability"?

- **Answer:** The right of a data subject to receive personal data concerning them in a structured, commonly used, and machine-readable format.

184. What is "Right to be Forgotten" (Right to Erasure)?

- **Answer:** The right of an individual to request that an organization delete their personal data under certain conditions.

185. What is "Clickjacking"?

- **Answer:** A malicious technique of tricking a user into clicking on something different from what the user perceives.

186. What is "Typosquatting" (URL Hijacking)?

- **Answer:** A form of cybersquatting that relies on mistakes such as typographical errors made by Internet users when inputting a website address.

187. What is "Domain Fronting"?

- **Answer:** A technique that circumvents censorship by hiding the true destination of a communication behind a different domain.

188. What is "Side-Channel Attack"?

- **Answer:** An attack based on information gained from the implementation of a computer system, rather than weaknesses in the implemented algorithm itself (e.g., power consumption, electromagnetic leaks).

189. What is "Air Gapping"?

- **Answer:** A network security measure employed on one or more computers to ensure that a secure computer network is physically isolated from unsecured networks, such as the public Internet.

190. What is "Data Obfuscation"?

- **Answer:** The practice of making data unintelligible or difficult for a human to understand, often used to protect PII.

191. What is "Tokenization"?

- **Answer:** The process of replacing sensitive data with a non-sensitive equivalent, called a token, that has no extrinsic or exploitable meaning or value.

192. What is "Anonymization"?

- **Answer:** The process of either removing personally identifiable information from data sets, so that the people whom the data describe remain anonymous.

193. What is "Pseudo-anonymization"?

- **Answer:** A data management and de-identification procedure by which personally identifiable information is replaced by one or more artificial identifiers, or pseudonyms.

194. What is a "Policy" vs. a "Standard"?

- **Answer:** A policy is a high-level statement of intent, while a standard is a mandatory, specific requirement for hardware or software.

195. What is a "Guideline"?

- **Answer:** Recommended actions and operational guides to users, IT staff, operations staff, and others when a specific standard does not apply (Non-mandatory).

196. What is a "Procedure"?

- **Answer:** Detailed step-by-step instructions on how to achieve a certain goal.

197. Which of the following is an example of a physical security control?

- **Options:** (A) Firewall, (B) Encryption, (C) Security Guard, (D) Antivirus.
- **Answer: (C) Security Guard**
- **Explanation:** Security guards provide a direct human presence to protect physical access.

198. Which phase of the Disaster Recovery Plan involves the restoration of normal operations?

- **Options:** (A) Response, (B) Recovery, (C) Mitigation, (D) BIA.
- **Answer: (B) Recovery**

- **Explanation:** During the recovery phase, systems and services are brought back online and business resumes.

199. Which of the following is a primary component of an Incident Response Plan?

- **Options:** (A) Risk assessment, (B) Communication procedures, (C) Security policy development, (D) Physical security measures.
- **Answer: (B) Communication procedures**
- **Explanation:** Ensures clear coordination with internal and external parties during a breach.

200. Which of the following is a key activity in security operations to maintain the integrity of systems?

- **Options:** (A) Implementing access control, (B) Performing regular backups, (C) Conducting security audits, (D) Monitoring network traffic.
- **Answer: (C) Conducting security audits**
- **Explanation:** Audits identify vulnerabilities and verify that systems are functioning as intended without being tampered with.

Part 1: Questions 1 - 15

1. Most Effective Physical Control for a Data Center

- **Question:** What is the most effective physical control to prevent unauthorized access to a data center?
- **Answer: Man Trap control configured with biometrics.** [01:01]
- **Explanation:** A Man Trap (double-door system) prevents tailgating/piggybacking, and biometrics ensure strong individual accountability.

2. Protecting Brand Name and Goodwill

- **Question:** Which legal protection is used to protect a company's brand name and logo?
- **Answer: Trademark.** [04:15]
- **Explanation:** Trademarks protect names, brands, and logos. Patents protect ideas/innovations, and Copyrights protect expressions of ideas (like code or music). [06:52]

3. Healthcare Regulation in the US

- **Question:** A US healthcare company collects patient data; which primary regulation must it follow?
- **Answer: HIPAA (Health Insurance Portability and Accountability Act).** [07:06]
- **Explanation:** HIPAA is a federal law designed specifically to protect sensitive patient health information in the US. [08:00]

4. Accountability in the Cloud

- **Question:** If a company moves payment services to the cloud, who remains accountable for PCI DSS accreditation?
- **Answer: The Cloud Customer.** [10:05]
- **Explanation:** Even if operations are transferred to a provider, the customer is ultimately accountable to regulators and auditors for compliance. [10:56]

5. Critical Requirement for Cloud Migration

- **Question:** What is the most critical requirement to review before migrating data to a cloud environment?
- **Answer: Laws and regulations that apply to both the customer and the provider.** [11:52]
- **Explanation:** You must understand the legal obligations imposed on both parties, especially regarding regional data residency. [12:53]

6. Monitoring for Malicious Activity

- **Question:** Which solution monitors an environment for malicious activity and reports it to an administrator?

- **Answer: IDS (Intrusion Detection System).** [13:15]
- **Explanation:** An IDS passively logs and reports activity. An IPS (Prevention System) would actively block it. [14:05]

7. Ideal Firewall Location

- **Question:** Where is the most strategic location to place a network firewall?
- **Answer: Between the organization's router and the internet.** [18:09]
- **Explanation:** This provides the first level of inspection to filter out major attack patterns before they hit the internal network. [17:35]

8. Documenting Service Expectations

- **Question:** Which document best describes an organization's service quality expectations from a vendor?
- **Answer: SLA (Service Level Agreement).** [18:47]
- **Explanation:** An SLA is a variable part of a contract used to enforce specific performance duties and resolve disputes. [20:27]

9. Network-Based Port Security

- **Question:** Which control prevents malicious traffic on unauthorized ports at the network level?
- **Answer: ACL (Access Control List).** [22:32]
- **Explanation:** ACLs (often on routers or firewalls) define rules to permit or deny traffic based on source/destination IP and port. [21:47]

10. Disaster Recovery (DR) Plan Definition

- **Question:** What is the true statement about a Disaster Recovery plan?
- **Answer: A written plan for recovering information systems at an alternate facility.** [23:45]
- **Explanation:** While BCP (Business Continuity) sustains business processes, DR focuses specifically on restoring IT systems. [24:13]

11. Non-Mandatory Security Documents

- **Question:** Which document contains elements that are *not* mandatory?
- **Answer: Guidelines.** [25:35]
- **Explanation:** Policies and Standards are mandatory; Procedures are step-by-step requirements. Guidelines are recommendations. [25:21]

12. Properties NOT Provided by Digital Signatures

- **Question:** Which security property is NOT provided by a digital signature?
- **Answer: Confidentiality.** [28:39]
- **Explanation:** Digital signatures provide Integrity, Non-repudiation, and Authentication, but they do not encrypt the message for privacy. [29:05]

13. Ransomware Identification

- **Question:** An attack confirms data is encrypted and demands a fee for access. What type of attack is this?
- **Answer: Ransomware.** [30:43]
- **Explanation:** The key characteristics are unauthorized encryption and a demand for payment (ransom). [31:15]

14. Measuring Training Effectiveness

- **Question:** What is the best metric to measure the effectiveness of security awareness training?
- **Answer: Increase in incident reports.** [33:36]
- **Explanation:** An increase in reporting shows that employees are now aware enough to recognize and flag suspicious activity. [33:07]

15. Primary Objective of Awareness Training

- **Question:** What is the main goal of security awareness training?
- **Answer: To notify employees of their information security responsibilities.** [34:01]

- **Explanation:** It aims to modify human behavior, as humans are often the "weakest link" in security. [34:52]

Part 2: Questions 16 - 30

16. Communicating Data Handling Practices

- **Question:** Which document effectively addresses concerns by communicating how an organization handles personal data?
- **Answer: Developing a comprehensive Privacy Policy.**
- **Explanation:** A privacy policy outlines the collection, use, and storage practices for personal data, such as location data.

17. Policy for Network Misuse

- **Question:** Which policy addresses infections caused by unauthorized file sharing on a campus network?
- **Answer: Acceptable Use Policy (AUP).**
- **Explanation:** The AUP outlines what is considered acceptable and unacceptable behavior (do's and don'ts) when using organization resources.

18. Achieving Uniformity Across Desktops

- **Question:** Which function is most useful for ensuring hundreds of desktops have the same antivirus and scanning settings?
- **Answer: Configuration Management.**
- **Explanation:** Configuration management defines standard settings (baselines) and ensures uniformity, making it easier to patch and audit systems.

19. Targeted Attack on Executives

- **Question:** A CEO receives a fake email from the "Legal Department" asking for a wire transfer. What type of attack is this?

- **Answer: Whaling.**
- **Explanation:** Whaling is a specific form of spear-fishing that targets high-ranking "big fish" like CEOs or Senior Management.

20. OSI Model: Data to Packets

- **Question:** At which OSI layer is data encapsulated into "packets"?
- **Answer: Layer 3 (Network Layer).**
- **Explanation:** Data at Layer 4 are Segments; at Layer 3 they are Packets; and at Layer 2 they are Frames.

21. OSI Model: Error-Free Exchange

- **Question:** Which layer ensures that information is exchanged error-free between nodes?
- **Answer: Layer 2 (Data Link Layer).**
- **Explanation:** Layer 2 uses a Frame Check Sequence (FCS) or CRC to verify the integrity of the frame and ensure it is error-free.

22. OSI Model: Flow Control and Error Detection

- **Question:** Which layer handles data transfer between applications, including flow control and error correction?
- **Answer: Layer 4 (Transport Layer).**
- **Explanation:** The Transport Layer manages end-to-end communication and uses sequencing to maintain flow control and ensure data reaches the application correctly.

23. OSI Model: Encryption and Encoding

- **Question:** Which layer ensures information is encrypted and encoded?
- **Answer: Layer 6 (Presentation Layer).**
- **Explanation:** The Presentation Layer is responsible for translating, encrypting, and formatting data so the application layer can understand it.

24. Port Categories (Port 1123)

- **Question:** Which category does port number 1123 belong to?
- **Answer: Registered Ports.**
- **Explanation:** Well-known ports are 0–1023. Registered ports are 1024–49151. Dynamic/Ephemeral ports are 49152–65535.

25. Layer for DNS, SMTP, and HTTP

- **Question:** At which OSI layer do DNS, SMTP, and HTTP operate?
- **Answer: Layer 7 (Application Layer).**
- **Explanation:** These protocols interact directly with software applications to initiate network services.

26. Purpose of Port 53

- **Question:** What is the primary purpose of Port 53?
- **Answer: DNS resolution (translating names to IP addresses).**
- **Explanation:** DNS uses Port 53 to help the computer find the correct IP address for a typed URL.

27. Preventing DNS Poisoning

- **Question:** Which measure is most effective in preventing users from being redirected to fake sites (DNS Poisoning)?
- **Answer: DNSSEC (DNS Security Extensions).**
- **Explanation:** DNSSEC provides integrity and authenticity to DNS records by digitally signing them.

28. Secure Remote Management

- **Question:** Which protocol is best for securely configuring and troubleshooting network devices remotely?
- **Answer: SSH (Secure Shell).**
- **Explanation:** SSH is the secure alternative to Telnet; it uses Port 22 and provides encryption for remote management.

29. Preventing Man-in-the-Middle on the Web

- **Question:** Which protocol secures data transmission over the internet to prevent eavesdropping and hijacking?
- **Answer: SSL/TLS.**
- **Explanation:** SSL/TLS creates a secure, encrypted channel (HTTPS) for data exchange over the web.

30. Mitigating Hash Cracking (Salting)

- **Question:** Which technique prevents attackers from using pre-computed hash tables (Rainbow Tables) to crack passwords?
- **Answer: Salting the password before hashing.**
- **Explanation:** Salting adds unique, random data to each password so that identical passwords produce different, unique hashes.

31. Purpose of ICMP

- **Question:** Which protocol is primarily used by the "Ping" utility?
- **Answer: ICMP (Internet Control Message Protocol).**
- **Explanation:** Ping uses ICMP Echo Request and Echo Reply messages to test connectivity.

Part 1: Security Principles and Concepts

1. Defense in Depth

- **Question:** Which strategy integrates people, technology, and operations to establish security controls across multiple layers?

- **Answer: Option B: Defense in depth.** [01:47]
- **Explanation:** This approach ensures that if one layer (e.g., physical security) is compromised, additional layers (e.g., network or application security) continue to provide protection. [03:23]

2. ISC2 Ethical Canons

- **Question:** Which of the following is NOT an ethical canon of ISC2?
- **Answer: Option D: Provide active and qualified service to the principles.** [04:31]
- **Explanation:** The correct phrasing is "provide **diligent and competent** service to principles." [05:52]

3. Hybrid Cloud Model

- **Question:** What is the model where a company has resources both on-premise and in the cloud?
- **Answer: Option A: Hybrid Cloud.** [06:18]
- **Explanation:** It is a combination of two or more cloud models (e.g., public and private) or on-premise infrastructure with a cloud provider. [07:18]

4. Identifying Public IP Addresses

- **Question:** Which of the following is a public IP address?
- **Answer: Option A: 13.16.123.1.** [08:20]
- **Explanation:** The other options (starting with 192.168, 172.16, and 10.) are reserved private IP ranges and are not routable over the internet. [09:04]

5. Intrusion Detection Systems (NIDS vs. HIDS)

- **Question:** Which device is most effective in detecting an intrusion into a *network*?
- **Answer: Option D: nids (Network Intrusion Detection System).** [11:06]
- **Explanation:** While HIDS monitors individual hosts, NIDS monitors traffic across the entire network to identify abnormal behavior. [11:44]

6. Physical Security: Protecting Doors

- **Question:** Which access control is most effective at protecting a door against unauthorized access?
- **Answer: Option D: Locks.** [12:53]
- **Explanation:** Locks are specifically designed to provide a direct control mechanism for doors, unlike fences or barriers which secure the perimeter. [13:02]

7. Detection Controls

- **Question:** Which of the following is a detection control?
- **Answer: Option B: Smoke detectors.** [14:08]
- **Explanation:** Smoke sensors identify the presence of a threat (fire) and trigger an alert, which is the definition of a detection control. [14:17]

8. Remote System Control (Backdoors)

- **Question:** Which type of attack aims to control a system from the outside?
- **Answer: Option A: Backdoors.** [15:23]
- **Explanation:** A backdoor allows an attacker to bypass normal authentication and re-enter a system remotely. [15:39]

9. OSI Model: Layer 3 Protocols

- **Question:** Which of the following is NOT a protocol of OSI Layer 3?
- **Answer: Option A: SNMP.** [17:03]
- **Explanation:** SNMP (Simple Network Management Protocol) operates at the Application Layer (Layer 7). ICMP and IP operate at Layer 3. [17:26]

10. Risk Management: Insurance

- **Question:** When a company hires an insurance company to mitigate risk, which technique is being applied?
- **Answer: Option B: Risk transfer.** [18:12]
- **Explanation:** Risk transfer shifts the financial responsibility for a risk to a third party. [18:34]

Part 2: Access Control and Network Security

11. SMTP Layer

- **Question:** At which OSI layer does SMTP operate?
- **Answer: Option A: Layer 7.** [19:33]
- **Explanation:** SMTP is an application-level protocol for email transfer. Bonus: It uses TCP Port 25. [20:04]

12. Proving Identity

- **Question:** What is the process of verifying or proving a user's identification?
- **Answer: Option C: Authentication.** [20:40]
- **Explanation:** Authentication ensures that an entity is who they claim to be, distinct from authorization (granting permissions). [21:06]

13. Preventing Tailgating

- **Question:** Which physical control is most effective against tailgating?
- **Answer: Option D: Turnstiles.** [22:05]
- **Explanation:** Turnstiles are designed to allow only one person to pass at a time after authentication. [23:10]

14. Logging and Monitoring

- **Question:** Logging and monitoring systems are essential for what?
- **Answer: Option C: Identifying inefficient systems, detecting compromises, and providing usage records.** [24:10]
- **Explanation:** They help with operational efficiency, threat detection, and audit compliance. [24:40]

15. Primary Objective in Disaster

- **Question:** In the event of a disaster, what is the primary objective?
- **Answer: Option A: Guarantee the safety of people.** [25:46]
- **Explanation:** Human safety always takes precedence over data or system continuity in disaster recovery planning. [26:04]

16. Change Management

- **Question:** Which process ensures that system changes do not adversely impact operations?
- **Answer: Option A: Change management.** [26:40]
- **Explanation:** This involves assessing and documenting changes to maintain stability. [26:50]

17. Data Life Cycle: Final Phase

- **Question:** What is the last phase in the data security cycle?
- **Answer: Option D: Destruction.** [27:46]
- **Explanation:** Once data has served its purpose, it must be securely destroyed to prevent recovery. [27:55]

18. Role-Based Access Control (RBAC)

- **Question:** Which model specifies access based on the subject's role?
- **Answer: Option A: RBAC.** [28:45]
- **Explanation:** Permissions are assigned to roles rather than individuals, simplifying management. [29:04]

19. Physical vs. Logical Controls

- **Question:** Which of the following is NOT a physical control?
- **Answer: Option A: Firewalls.** [29:58]
- **Explanation:** Firewalls are technical/logical network controls, not physical barriers. [30:07]

20. Rootkits

- **Question:** Which attack effectively maintains remote access and control by hiding from detection?
- **Answer: Option D: Rootkits.** [30:56]
- **Explanation:** Rootkits embed deep in the OS to hide their presence and provide persistent access. [31:05]

Part 3: Vulnerabilities and Incident Response

21. Zero Day Definition

- **Question:** What does "zero day" mean in incident terminology?
- **Answer: Option B: A previously unknown system vulnerability.** [31:55]
- **Explanation:** It refers to a flaw exploited before the vendor has a chance to create a patch. [32:17]

22. Non-Compliant Devices

- **Question:** What should be done with a device that doesn't comply with the security baseline?
- **Answer: Option B: Disabled or isolated into a quarantine area.** [33:04]
- **Explanation:** Isolation prevents the device from introducing risks to the rest of the network. [33:45]

23. Denial of Service (DoS)

- **Question:** Which attack primarily aims to make a resource inaccessible?
- **Answer: Option A: Denial of service.** [34:33]
- **Explanation:** DoS attacks overwhelm systems with traffic to disrupt normal service. [34:51]

24. Trojan Horses

- **Question:** Which attack embeds a malicious payload inside trusted software?

- **Answer: Option A: Trojans.** [35:52]
- **Explanation:** Trojans disguise themselves as legitimate programs to gain unauthorized access. [36:02]

25. Network Sniffing Tools

- **Question:** Which tool is commonly used to sniff network traffic?
- **Answer: Option C: Wireshark.** [37:05]
- **Explanation:** Wireshark captures and inspects network packets in real-time. [37:15]

26. Side Channel Attacks

- **Question:** Which of these is NOT an attack against an IP network?
- **Answer: Option A: Side channel attack.** [38:13]
- **Explanation:** Side channel attacks exploit physical factors like power consumption or timing rather than the network itself. [38:26]

27. Procedures

- **Question:** Where are the detailed steps to complete tasks documented?
- **Answer: Option D: Procedures.** [39:08]
- **Explanation:** Procedures provide the step-by-step instructions needed to implement high-level policies. [39:21]

28. Router Function

- **Question:** Which device connects a LAN to the internet?
- **Answer: Option C: Router.** [40:44]
- **Explanation:** Routers direct data packets between different networks. [41:01]

29. SIEM Meaning

- **Question:** What does SIEM stand for?
- **Answer: Option B/D: Security Information and Event Manager.** [42:20]

- **Explanation:** SIEM systems collect and analyze security data from various sources to detect threats. [42:42]

30. Security Safeguard

- **Question:** A security safeguard is the same as a...?
- **Answer: Option C: Security control.** [43:25]
- **Explanation:** These terms are synonymous and refer to mechanisms implemented to mitigate risk. [43:37]

Part 4: Technical Controls and Regulations

31. Attribute-Based Access Control (ABAC)

- **Question:** Which model grants access based on complex rules and attributes?
- **Answer: Option B: ABAC.** [44:21]
- **Explanation:** ABAC uses attributes (location, time, role) to provide granular and dynamic control. [45:06]

32. HTTPS Port

- **Question:** Which port is used for secure web communication (HTTPS)?
- **Answer: Option D: 443.** [46:17]
- **Explanation:** Port 443 uses SSL/TLS to encrypt traffic, while Port 80 is for unencrypted HTTP. [46:54]

33. Business Impact Analysis (BIA)

- **Question:** What is the primary objective of a BIA?
- **Answer: Option B: Identifying and prioritizing critical business processes.** [47:51]
- **Explanation:** BIA is the first step in business continuity planning. [48:13]

34. Storage Controls

- **Question:** Which of the following is NOT a standard type of security control?
- **Answer: Option D: Storage control.** [49:37]
- **Explanation:** Recognized types include common, hybrid, and system-specific controls. [49:49]

35. Security Awareness Activities

- **Question:** Which is NOT a primary learning activity for security awareness?
- **Answer: Option D: Tutorial.** [50:52]
- **Explanation:** The three standard pillars are Awareness, Training, and Education. [51:05]

36. Impact Definition

- **Question:** The magnitude of harm from a security incident is known as...?
- **Answer: Option C: Impact.** [52:12]
- **Explanation:** Impact measures the severity of consequences if a threat exploits a vulnerability. [52:23]

37. Risk Reduction

- **Question:** Implementing security controls is a form of...?
- **Answer: Option A: Risk reduction.** [53:23]
- **Explanation:** Controls lessen the likelihood or impact of a threat, which is reduction (or mitigation). [53:34]

38. Cross-Site Scripting (XSS)

- **Question:** Which attack takes advantage of poor input validation on websites?
- **Answer: Option B: Cross-site scripting.** [54:37]
- **Explanation:** XSS involves injecting malicious scripts into pages viewed by other users. [54:48]

39. Administrative Controls

- **Question:** Which is an example of an administrative security control?

- **Answer: Option B: Acceptable use policies (AUP).** [55:49]
- **Explanation:** Administrative controls are management-based, like policies and procedures. [56:02]

40. Rollback Procedures

- **Question:** In change management, which component undoes a failed change?
- **Answer: Option C: Rollback.** [56:57]
- **Explanation:** Rollback procedures define how to revert a system to its previous stable state. [57:08]

Part 5: Cryptography and Network Infrastructure

41. Digital Signatures

- **Question:** Which property is NOT guaranteed by digital signatures?
- **Answer: Option B: Confidentiality.** [58:01]
- **Explanation:** Digital signatures provide authentication, integrity, and non-repudiation, but *encryption* is needed for confidentiality. [58:14]

42. SIEM Purpose

- **Question:** Which device has the primary objective of analyzing security events?
- **Answer: Option D: SIEM.** [59:12]
- **Explanation:** SIEM systems correlate data from multiple sources for threat detection. [59:31]

43. System Hardening

- **Question:** What is an effective way of hardening a system?
- **Answer: Option A: Patch the system.** [01:00:13]
- **Explanation:** Patching addresses known vulnerabilities and is a core part of system hardening. [01:00:26]

44. Symmetric Keys

- **Question:** Which key type can both encrypt and decrypt the same message?
- **Answer: Option D: A symmetric key.** [01:01:21]
- **Explanation:** Symmetric encryption uses one shared key for both operations. [01:01:58]

45. GDPR

- **Question:** Which regulation addresses data privacy in Europe?
- **Answer: Option D: GDPR.** [01:02:40]
- **Explanation:** GDPR (General Data Protection Regulation) is the primary EU privacy framework. [01:02:54]

46. Firewall Packet Inspection

- **Question:** Which device inspects packet headers to allow or deny traffic?
- **Answer: Option B: Firewalls.** [01:04:25]
- **Explanation:** Firewalls act as a barrier based on predefined security rules. [01:04:53]

47. DMZ (Demilitarized Zone)

- **Question:** Where should a web server accepting external requests be placed?
- **Answer: Option B: DMZ.** [01:06:00]
- **Explanation:** A DMZ isolates publicly accessible services from the internal network. [01:06:12]

48. Data Labels

- **Question:** How many data labels are considered good practice?
- **Answer: Option A: 2 to 3.** [01:07:11]
- **Explanation:** Keeping labels simple (e.g., Public, Internal, Confidential) ensures they are applied accurately. [01:07:21]

49. Security Awareness: Visual Aids

- **Question:** Security posters are primarily used for...?
- **Answer: Option A: Security awareness.** [01:08:08]
- **Explanation:** Posters promote a security-conscious culture. [01:08:21]

50. Privileged Accounts

- **Question:** Which user is LEAST likely to have a privileged account?
- **Answer: Option D: External worker.** [01:09:17]
- **Explanation:** Privileged access is usually reserved for internal staff like administrators and help desk support. [01:09:27]

Part 1: Business Continuity and Risk Management

51. Predetermined Instructions After a Disaster

- **Question:** The predetermined set of instructions or procedures to sustain business operations after a disaster is known as:
- **Answer: Option D: Business continuity plan (BCP).** [01:34]
- **Explanation:** BCP is the umbrella plan for maintaining or quickly resuming operations. [01:41]

52. System Security Configuration Management

- **Question:** Which of the following is NOT an element of system security configuration management?
- **Answer: Option D: Audit logs.** [02:49]
- **Explanation:** Core elements include inventory, baselines, and updates. Audit logs are for monitoring and detection, not configuration. [02:55]

53. Incident Response Plan Steps

- **Question:** What are the components/steps of an incident response plan?
- **Answer: Option D: Preparation, detection and analysis, containment, eradication and recovery, and post-incident activity.** [04:36]

54. Two-Factor Authentication (2FA) Example

- **Question:** Which of the following is an example of 2FA?
- **Answer: Option D: One-time password (OTP).** [06:12]
- **Explanation:** In context, an OTP serves as the second factor (something you have) alongside a password (something you know). [07:55]

55. Cryptographic Hash Features

- **Question:** Which of the following is NOT a feature of a cryptographic hash function?
- **Answer: Option A: Reversible.** [08:35]
- **Explanation:** Hashing is a "one-way" function and cannot be reversed to find the original data. [09:09]

56. TCP Three-Way Handshake

- **Question:** What are the three packets used in the TCP connection handshake?
- **Answer: Option B: SYN, SYN-ACK, and ACK.** [10:39]

57. Returning to Normal After an Earthquake

- **Question:** Which document contains procedures to return business to normal operation after a disaster?
- **Answer: Option D: Disaster recovery plan (DRP).** [12:49]
- **Explanation:** DRP focuses specifically on the restoration of IT systems and infrastructure. [13:05]

58. Consequence of a DoS Attack

- **Question:** What is the consequence of a denial-of-service (DoS) attack?
- **Answer: Option A: Exhaustion of device resources.** [13:46]
- **Explanation:** Attackers overwhelm the CPU, memory, or bandwidth so legitimate users can't access it. [14:16]

59. Six Phases of Data Handling (ISC2)

- **Question:** What is the correct order for the six phases of data handling?
- **Answer: Option B: Create, Store, Use, Share, Archive, Destroy.** [15:17]

60. Incident Response Team Composition

- **Question:** Who is least likely to be part of a core incident response team?
- **Answer: Option B: Human Resources (HR).** [17:08]
- **Explanation:** HR involvement is situational (e.g., employee misconduct) rather than essential for every technical incident. [17:20]

Part 2: Tools, Policies, and Cloud Models

61. Password Cracking Tools

- **Question:** Which tool is commonly used to crack passwords?
- **Answer: Option C: John the Ripper.** [18:12]

62. Personal Device Policy

- **Question:** Which policy explains if personal tablets are allowed in the office?
- **Answer: Option A: BYOD (Bring Your Own Device).** [19:26]

63. Shared Resources in Cloud

- **Question:** In which model do companies share resources and infrastructure?
- **Answer: Option D: Community Cloud.** [20:44]
- **Explanation:** Shared by organizations with similar requirements (e.g., compliance). [21:01]

64. DRP Primary Objective

- **Question:** What is the primary objective of a Disaster Recovery Plan?

- **Answer: Option A: Restore company operation to the last known reliable state.** [22:33]

65. Entity Exploiting Vulnerabilities

- **Question:** An entity that acts to exploit a target organization's system is a:
- **Answer: Option A: Threat actor.** [23:51]
- **Explanation:** The transcript notes Option B (Threat Vector) was highlighted, but the definition provided describes a **Threat Actor**. [24:00]

66. Patch Management Best Practice

- **Question:** What is a best practice of patch management?
- **Answer: Option B: Test patches before applying them.** [25:07]

67. Controlling Network Access

- **Question:** Which tool is specifically used to control access to a network?
- **Answer: Option D: NAC (Network Access Control).** [26:33]

68. Change Management Components

- **Question:** Which of these is NOT a change management component?
- **Answer: Option D: Governance.** [28:03]
- **Explanation:** RFC, Approval, and Rollback are specific components; Governance is overall management. [28:09]

69. Social Engineering Techniques

- **Question:** Which of the following is NOT a social engineering technique?
- **Answer: Option C: Double dealing.** [29:14]

70. Reliable Connection Protocol

- **Question:** Which protocol should be used for a reliable connection with no time constraints?
- **Answer: Option A: TCP.** [30:29]

Part 3: Access Control and Security Models

71. System Weakness

- **Question:** An exploitable weakness or flaw in a system is a:
- **Answer: Option C: Vulnerability.** [32:40]

72. Least Customer Responsibility in Cloud

- **Question:** In which model does the customer have the least responsibility?
- **Answer: Option D: SaaS (Software as a Service).** [33:59]

73. Risk Management Definition

- **Question:** Risk management is:
- **Answer: Option D: The identification, evaluation, and prioritization of risks.** [36:00]

74. Non-Mandatory Documents

- **Question:** Which document contains elements that are NOT mandatory?
- **Answer: Option B: Guidelines.** [37:08]
- **Explanation:** Policies, procedures, and regulations are mandatory. [37:22]

75. Prioritizing Incident Response

- **Question:** In which phase are incident responses prioritized?
- **Answer: Option B: Detection and Analysis.** [38:16]

76. Necessary Permissions Only

- **Question:** Which principle states a user should only have necessary permissions?
- **Answer: Option C: Least privilege.** [39:47]

77. Bell-LaPadula Model

- **Question:** The Bell-LaPadula model is a form of:
- **Answer: Option C: MAC (Mandatory Access Control).** [41:24]
- **Explanation:** It focuses on confidentiality using labels like "Top Secret." [41:34]

78. Risk Priority

- **Question:** Highest priority is given to a risk where:
- **Answer: Option A: Frequency is low, but expected impact is high.** [43:15]

79. PII Property

- **Question:** Which area is most connected to PII (Personally Identifiable Information)?
- **Answer: Option D: Confidentiality.** [44:58]

80. Attacking Executives

- **Question:** Malicious emails targeting company executives are:
- **Answer: Option B: Whaling.** [46:26]

Part 4: Regulations and Technical Controls

81. Financial Penalties

- **Question:** Governments impose financial penalties for breaking a:
- **Answer: Option A: Regulation.** [48:03]

82. Fraudulent Message Attacks

- **Question:** Tricking a user via fraudulent messages is:
- **Answer: Option A: Fishing (Phishing).** [49:15]

83. Delegating Permissions

- **Question:** In which model can the creator delegate permissions?
- **Answer: Option D: DAC (Discretionary Access Control).** [51:04]

84. Encrypting for Ransom

- **Question:** Which attack encrypts data and demands payment?
- **Answer: Option A: Ransomware.** [52:33]

85. Access to Fundamental Resources

- **Question:** Which cloud model gives access to fundamental computing resources?
- **Answer: Option D: IaaS (Infrastructure as a Service).** [54:28]

86. OSI Model Layers

- **Question:** How many layers does the OSI model have?
- **Answer: Option A: 7.** [56:05]

87. Fraud Detection Principle

- **Question:** Which principle aims primarily at fraud detection?
- **Answer: Option D: Separation of duties.** [58:10]

88. Reliable Handshake Protocol

- **Question:** Which protocol uses a three-way handshake?
- **Answer: Option A: TCP.** [59:54]

89. Technical Security Control Example

- **Question:** Which of the following is a technical security control?
- **Answer: Option A: Access Control List (ACL).** [01:01:05]

90. Power Consumption Observation

- **Question:** Gaining info by observing a device's power consumption is:
- **Answer: Option A: Side channel attack.** [01:02:11]

Part 5: Security Standards and Final Questions

91. PHI Property

- **Question:** What is the most distinctive property of PHI (Protected Health Information)?
- **Answer: Option B: Confidentiality.** [01:04:03]

92. BCP Testing Method

- **Question:** What is the most efficient way to test a BCP?
- **Answer: Option A: Simulations.** [01:04:51]

93. Authorized Access Only

- **Question:** Which concept guarantees info is accessible only to authorized users?
- **Answer: Option A: Confidentiality.** [01:05:35]

94. Primary Objective in Disaster

- **Question:** What is the primary objective in the event of a disaster?
- **Answer: Option C: Guarantee the safety of people.** [01:06:20]

95. Reporting Policy Violations

- **Question:** To whom should a professional report company policy violations?

- **Answer: Option B: Company management.** [01:07:12]

96. Department Least Involved in DRP

- **Question:** Which department is not regularly involved in Hands-on DRP?
- **Answer: Option A: Executives.** [01:08:33]

97. SLA Contents

- **Question:** Which is included in an SLA (Service Level Agreement)?
- **Answer: Option B: Instructions on data ownership and destruction.** [01:09:05]

98. MAC vs. DAC Difference

- **Question:** What is the most important difference between MAC and DAC?
- **Answer: Option C: In MAC, admins assign permissions; in DAC, object owners decide.** [01:10:01]

99. Role-Based Access

- **Question:** Requiring a specific role to access resources is:
- **Answer: Option C: RBAC (Role-Based Access Control).** [01:11:02]

100. Vital Systems Running During Disruption

- **Question:** Which document ensures vital systems keep running during disruption?
- **Answer: Option D: Business continuity plan (BCP).** [01:12:04]

Domain 1: Security Principles

1. Access Control Strategy

- **Question:** Everlast Cyber is starting a new project involving sensitive data. What security measures should be put in place to ensure only authorized individuals have access?
- **Answer: Option B: Principle of least privilege.** [02:44]
- **Explanation:** This ensures individuals are granted only the minimum levels of access or permissions needed to perform their job functions. [01:48]

2. Ethical Canons (ISC2)

- **Question:** Which of the following is NOT an ethical canon of the ISC2?
- **Answer: Option D: Provide active and qualified service to principal.** [21:18]
- **Explanation:** The actual canon is to "provide **diligent and competent** service to principles." [21:43]

3. Safety in Disaster

- **Question:** What role does a business continuity team serve?
- **Answer: Option D: All of the above (Develop, maintain, implement, test, and evaluate).** [27:15]

4. Data Confidentiality

- **Question:** Everlast Cyber aims to guarantee that an internet-transmitted message remains unreadable even if intercepted. What approach should they employ?
- **Answer: Option B: Encryption.** [40:30]
- **Explanation:** Encryption converts data into a coded format that is unreadable without the appropriate decryption key. [39:55]

Domain 2: Business Continuity, Disaster Recovery, and Incident Response

5. Corrective Controls

- **Question:** Which of these represents a corrective control within incident response?
- **Answer: Option B: Incident response plan.** [26:35]
- **Explanation:** Corrective controls are designed to fix or mitigate damage after a security incident has occurred. [25:46]

6. Identifying System Occurrences

- **Question:** Which of the following best describes or characterizes an unusual occurrence noticed by a cybersecurity expert within the system or network?
- **Answer: Option A: Events.** [37:41]
- **Explanation:** An event refers to any observable occurrence; unusual events are often the first sign that something may be wrong. [36:48]

Domain 3: Access Control Concepts

7. Multi-Layered Defense

- **Question:** Which concept describes an information security strategy that integrates people, technology, and operation across multiple layers?
- **Answer: Option B: Defense in depth.** [12:33]
- **Explanation:** The idea is that if one layer of defense fails, other layers will still provide protection. [11:57]

8. Physical Security: Unauthorized Entry

- **Question:** When an outsider follows an employee into a building without providing a badge, what kind of attack is this called?
- **Answer: Option A: Piggybacking.** [16:07]
- **Explanation:** Also known as tailgating, this involves following an authorized individual closely to gain entry. [16:17]

9. Password/Credential Theft

- **Question:** What is the term used to describe the act of spying on someone's computer screen to gain unauthorized access to sensitive information?
- **Answer: Option B: Shoulder surfing.** [18:21]

10. Authentication Tokens

- **Question:** Anna uses a software-based token that changes its code every minute. What type of token is this?
- **Answer: Option B: Synchronous token.** [39:06]
- **Explanation:** It generates a code at fixed intervals and stays in sync with a server-side clock. [38:24]

Domain 4: Network Security

11. IP Version Usage

- **Question:** What is the most widely used IP version?
- **Answer: Option A: IP version 4.** [10:53]
- **Explanation:** IPv4 uses 32-bit addresses and remains the most common despite the emergence of IPv6. [10:04]

12. Network Mapping

- **Question:** Which method is commonly used to map live hosts in the network?
- **Answer: Option A: Ping sweep.** [22:57]
- **Explanation:** This involves sending ICMP echo requests to a range of IP addresses to see which ones are active. [22:14]

13. Secure Remote Access

- **Question:** Which protocol is used to securely access a remote computer over an unsecured network?
- **Answer: Option D: SSH (Secure Shell).** [31:52]

- **Explanation:** SSH encrypts all data transmitted between the client and the server. [31:54]

14. Firewall Function

- **Question:** Which of the following best describes the purpose of a firewall in a network?
- **Answer: Option C: To filter incoming and outgoing network traffic based on rules.** [29:11]

Domain 5: Security Operations

15. Malware: Keylogging

- **Question:** Which type of malware is specifically designed to collect information by logging keystrokes?
- **Answer: Option C: Keylogger.** [03:59]

16. Phishing Signs

- **Question:** Which of the following is a common sign of a phishing email?
- **Answer: Option B: A sense of urgency or threat of account suspension.** [06:12]

17. Trojan Horse Function

- **Question:** What is the primary function of a Trojan horse?
- **Answer: Option B: To disguise itself as legitimate software while performing malicious actions.** [09:39]

18. Regulation Objectives

- **Question:** What is the main objective of security regulations and laws?
- **Answer: Option D: To regulate the collection and use of personal information.** [14:43]

19. Denial of Service (DoS)

- **Question:** What type of attack involves overwhelming a system with traffic to make it unavailable to users?
- **Answer: Option C: Denial of service.** [17:41]

20. Phishing Primary Goal

- **Question:** What is the primary goal of a phishing attack?
- **Answer: Option C: To steal sensitive information such as passwords and credit card numbers.** [20:44]

21. Sophisticated Long-Term Threats

- **Question:** Which refers to threats with unusually high operational and technical sophistication spanning months or even years?
- **Answer: Option C: Advanced persistent threats (APT).** [24:09]

22. Malware: Self-Replication

- **Question:** Which malware type can replicate itself without user intervention and spread across networks?
- **Answer: Option C: Worm.** [33:12]

23. Law Categories

- **Question:** What category of law is applied when a company faces fines for failing to adhere to a government regulation?
- **Answer: Option B: Administrative law.** [35:12]
- **Explanation:** Administrative law governs the actions of government agencies and the regulations they create. [34:27]

24. Mandatory vs. Non-Mandatory Documents

- **Question:** Which of the following documents contains elements that are not mandatory?

- **Answer: Option A: Guideline.** [36:14]
- **Explanation:** Policies, regulations, and procedures are mandatory; guidelines are recommended advice. [35:38]

25. Phishing Methods

- **Question:** Which of the following is a typical method used in phishing attacks?
- **Answer: Option A: Sending an email with a fake link that looks like a legitimate website.** [30:41]

Questions 1 - 25: Foundational Principles & Risk Management

1. Unauthorized Access to Data

- **Question:** A company stores sensitive customer data on its servers. Which element of the CIA Triad would be most affected if this data were accessed by unauthorized personnel?
- **Answer: A. Confidentiality** [00:46]
- **Explanation:** Confidentiality ensures data is protected from unauthorized access.

2. Suspicious Email Attachments

- **Question:** You receive an email from an unknown source containing a suspicious attachment. What is the best immediate course of action?
- **Answer: B. Delete the email without opening it** [01:32]
- **Explanation:** Deleting minimizes the risk of executing malware.

3. Modifying Records

- **Question:** An attacker modifies financial records on a company's database. Which aspect of the CIA Triad is violated?
- **Answer: B. Integrity** [02:00]
- **Explanation:** Integrity ensures that data remains unaltered and accurate.

4. Risk Transference

- **Question:** Which risk management strategy involves shifting the financial impact of a risk to a third party, such as through insurance?
- **Answer: B. Risk transference** [02:35]

5. Password Change Policies

- **Question:** An organization enforces mandatory password changes every 90 days. What type of security control does this represent?
- **Answer: C. Administrative control** [03:10]
- **Explanation:** Administrative controls involve policies, procedures, and guidelines.

6. Halting a Project

- **Question:** A CEO decides to halt a risky project to prevent any potential loss. Which risk treatment strategy is this?
- **Answer: D. Risk avoidance** [03:38]

7. Purpose of Encryption

- **Question:** What is the primary purpose of encryption in cybersecurity?
- **Answer: A. To ensure data confidentiality** [04:10]

8. Badge Readers

- **Question:** A badge reader at the entrance of a restricted area is an example of which type of security control?
- **Answer: A. Physical control** [04:42]

9. Accidental Data Leaks

- **Question:** An employee accidentally sends sensitive customer information to an external recipient. Which type of threat actor does this represent?
- **Answer: A. Insider human error** [05:14]

10. Least Privilege

- **Question:** Which of the following best describes the principle of least privilege?
- **Answer: A. Users are granted only the access necessary for their job** [05:47]

11. MFA and the CIA Triad

- **Question:** A company implements multi-factor authentication (MFA). What aspect of the CIA Triad does this enhance?
- **Answer: A. Confidentiality** [06:23]

12. Acceptable Use Policy (AUP)

- **Question:** A company requires all employees to sign an AUP. What type of governance element is this?
- **Answer: C. Policy** [06:58]

13. Flooding Servers (DoS)

- **Question:** An attacker floods a company's server with excessive requests, causing it to crash. Which aspect of the CIA Triad is impacted?
- **Answer: C. Availability** [07:35]

14. Firewall Function

- **Question:** What is the purpose of a firewall in a corporate network?
- **Answer: A. To prevent unauthorized access to the network** [08:01]

15. Risk Assessment Process

- **Question:** A team evaluates potential risks to their new software development project. What process are they performing?
- **Answer: B. Risk assessment** [08:40]

16. Government Issued Rules

- **Question:** Which governance element is mandatory and issued by a government body, often carrying financial penalties?
- **Answer: D. Regulation** [09:15]

17. Ransomware Attackers

- **Question:** A hacker gains access to a network and installs ransomware. Which type of threat actor does this represent?
- **Answer: C. Cyber criminal** [09:41]

18. Off-site Backups

- **Question:** Storing backups at an off-site location supports which aspect of the CIA Triad?
- **Answer: C. Availability** [10:13]

19. Software Updates

- **Question:** An IT department regularly updates software to fix vulnerabilities. Which risk treatment strategy is this?
- **Answer: C. Risk reduction** [10:47]

20. Restricting Software Installations

- **Question:** Preventing employees from installing unapproved software through system policies is which type of control?
- **Answer: C. Technical control** [11:21]

21. Biometric Scanners

- **Question:** A data center uses biometric scanners to verify identity. What type of security control is this?
- **Answer: A. Physical control** [11:57]

22. Immediate Action for Compromise

- **Question:** A user discovers unknown processes running in the background. What is the best immediate action?
- **Answer: B. Disconnect the computer from the network** [12:31]

23. Living with Risk

- **Question:** Which risk treatment strategy involves deciding to live with a potential risk without taking action?
- **Answer: C. Risk acceptance** [13:01]

24. Man-in-the-Middle (MitM)

- **Question:** An attacker intercepts unencrypted communication between two parties. What is this attack called?
- **Answer: A. Man in the middle** [13:43]

25. Purpose of SIEM

- **Question:** An organization uses a SIEM system to monitor activity. Which aspect of security does this primarily support?
- **Answer: D. Accountability** [14:13]

Questions 26 - 50: Security Controls & Operations

26. Incorrect Records

- **Question:** An HR database contains several incorrect employee records. Which aspect of the CIA Triad has been compromised?
- **Answer: B. Integrity** [14:48]

27. Access Control Mechanisms

- **Question:** What is the primary role of Access Control mechanisms?
- **Answer: B. To ensure only authorized users can access resources** [15:23]

28. Data Loss Prevention (DLP)

- **Question:** Using DLP tools to block sensitive information from leaving the network is an example of what?
- **Answer: B. Technical control** [15:58]

29. Preventing Exploits of Outdated Servers

- **Question:** What could have prevented an attack on an outdated web server?
- **Answer: B. Regular patch management** [16:31]

30. Passwords + Physical Tokens

- **Question:** What type of authentication uses a password and a physical token?
- **Answer: B. Multi-factor authentication (MFA)** [17:06]

31. Analyst Response to Unusual Logins

- **Question:** An analyst detects unusual login attempts for a single user account. What is the next step?
- **Answer: A. Disable the account temporarily** [17:43]

32. 24/7 Record Access

- **Question:** Ensuring patient records are accessible 24/7 addresses which aspect?
- **Answer: C. Availability** [18:24]

33. Security Cameras

- **Question:** What type of security control are cameras at a data center?
- **Answer: B. Physical control** [18:58]

34. Vulnerability Assessment Purpose

- **Question:** What is the main purpose of a vulnerability assessment?
- **Answer: A. To identify and document security weaknesses** [19:23]

35. Fraudulent Trusted Emails

- **Question:** An attacker sends emails pretending to be a trusted contact. What type of attack is this?
- **Answer: A. Phishing** [19:55]

36. Cost-Benefit Risk Strategy

- **Question:** A manager accepts a minor risk rather than investing in expensive mitigation. What strategy is this?
- **Answer: D. Risk acceptance** [20:38]

37. Auto-Locking Workstations

- **Question:** A workstation set to lock after 5 minutes of inactivity is which type of control?
- **Answer: A. Technical control** [21:07]

38. Reporting Incidents

- **Question:** Requiring employees to report suspected incidents immediately is which type of control?
- **Answer: B. Administrative control** [21:40]

39. Privilege Escalation

- **Question:** An attacker gains access and increases their privileges to an administrator level. What is this called?
- **Answer: A. Privilege escalation** [22:15]

40. Encrypting Laptop Data

- **Question:** Encryption to secure data on company laptops is which type of control?
- **Answer: B. Technical control** [22:48]

41. Personal Device Policy

- **Question:** Which policy regulates the use of personal devices on the corporate network?
- **Answer: B. BYOD policy** [23:21]

42. Proactive Backup Measures

- **Question:** Daily backups and off-site storage represent which risk treatment?
- **Answer: D. Risk mitigation** [24:02]

43. Password Encryption

- **Question:** Encrypting passwords before storing them in a database addresses which principle?
- **Answer: A. Confidentiality** [24:34]

44. Credential Stuffing

- **Question:** Attackers use stolen username/password combinations to gain unauthorized access. What is this called?
- **Answer: C. Credential stuffing** [25:03]

45. Firewall Control Type

- **Question:** What type of security control is a firewall?
- **Answer: C. Technical control** [25:36]

46. BCP Objective

- **Question:** What is the primary objective of a Business Continuity Plan (BCP)?
- **Answer: B. To ensure critical operations can continue during a disruption** [26:08]

47. Preventing Unpatched Exploits

- **Question:** What could have prevented an attacker from using an unpatched software vulnerability?
- **Answer: C. Regular software updates** [26:48]

48. Database Modification Integrity

- **Question:** Ensuring only authenticated/authorized users can modify a database ensures what?
- **Answer: B. Integrity** [27:23]

49. 90-Day Reset Policy

- **Question:** Resetting passwords every 90 days is which type of control?
- **Answer: B. Administrative control** [28:00]

50. Excessive Traffic Attack

- **Question:** Flooding a server to make it unavailable is what type of attack?
- **Answer: C. Denial of service (DoS)** [28:25]

Questions 51 - 75: Access Control & Network Defense

51. Role-Based Access Control (RBAC)

- **Question:** What is the key benefit of RBAC?
- **Answer: C. Provides access based on job responsibilities** [29:06]

52. Reviewing Audit Logs

- **Question:** What type of security control is daily log review?
- **Answer: A. Detective control** [29:48]

53. Data Classification

- **Question:** What is the purpose of data classification?
- **Answer: B. To identify and label data based on its sensitivity** [30:12]

54. Keystroke Malware

- **Question:** Malware that records keystrokes is called a...?
- **Answer: B. Keylogger** [30:53]

55. VPN Principle

- **Question:** Using a VPN to encrypt communication supports which principle?
- **Answer: A. Confidentiality** [31:26]

56. Risk Transference (Insurance)

- **Question:** Transferring financial impact to an insurer is called...?
- **Answer: B. Risk transference** [31:54]

57. SQL Command Injection

- **Question:** Injecting malicious SQL commands into a web app is called...?
- **Answer: B. SQL injection** [32:25]

58. Network Segmentation

- **Question:** Separating a network into multiple segments to limit malware spread is called...?
- **Answer: B. Network segmentation** [32:59]

59. Security Awareness Training

- **Question:** Training employees on recognizing phishing is which type of control?
- **Answer: C. Administrative control** [33:34]

60. Minimum Necessary Access

- **Question:** Which principle ensures users have only the minimum access needed?
- **Answer: B. Principle of least privilege** [34:08]

61. CCTV Cameras

- **Question:** CCTV cameras are what type of control?
- **Answer: A. Physical control** [34:38]

62. Deceptive Phishing Emails

- **Question:** Posing as a trusted entity to trick users is called...?
- **Answer: A. Phishing** [35:11]

63. Financial Approvals

- **Question:** Requiring multiple individuals to approve transactions supports what?
- **Answer: B. Separation of duties** [35:45]

64. Encryption Purpose

- **Question:** What is the primary purpose of encryption?
- **Answer: B. Preventing unauthorized access** [36:18]

65. Biometric Principle

- **Question:** Biometric authentication (fingerprints) is based on what factor?
- **Answer: C. Something you are** [36:44]

66. DNS Poisoning

- **Question:** Redirecting users to a fraudulent site by compromising a DNS server is called...?
- **Answer: A. DNS poisoning** [37:17]

67. Intrusion Detection System (IDS)

- **Question:** What type of security control is an IDS?
- **Answer: C. Detective control** [37:51]

68. Cloud Backup Strategy

- **Question:** Cloud-based backups represent which risk treatment?
- **Answer: C. Risk mitigation** [38:25]

69. Website Restrictions Policy

- **Question:** Restricting certain websites during work hours is usually found in which policy?
- **Answer: A. Acceptable use policy** [39:00]

70. MFA Advantage

- **Question:** What is the key advantage of an MFA system?
- **Answer: A. It reduces the risk of unauthorized access** [39:32]

71. Cross-Site Scripting (XSS)

- **Question:** Executing malicious scripts in another user's browser is called...?
- **Answer: B. Cross-site scripting** [40:15]

72. Recovery Time Objective (RTO)

- **Question:** The target time for system restoration after an outage is called...?
- **Answer: A. Recovery time objective** [40:50]

73. Strong Password Policy Type

- **Question:** Mandating strong passwords is which type of control?
- **Answer: A. Preventive control** [41:23]

74. RBAC Definition

- **Question:** Granting permissions based on job roles is which model?
- **Answer: B. Role-based Access Control (RBAC)** [41:56]

75. Wireless Encryption (WPA3)

- **Question:** What could prevent password guessing on a wireless network?
- **Answer: B. Using WPA3 encryption** [42:33]

Questions 76 - 100: Vulnerabilities & Professional Ethics

76. Man-in-the-Middle (MitM)

- **Question:** Intercepting and altering communications without knowledge is...?
- **Answer: C. Man in the middle** [43:10]

77. Mandatory Vacation Policy

- **Question:** Mandatory vacations for financial employees primarily address what?
- **Answer: B. Fraud detection** [43:42]

78. Penetration Testing Goal

- **Question:** What is the primary goal of penetration testing?
- **Answer: B. To identify and exploit vulnerabilities** [44:21]

79. Backup Generators

- **Question:** Maintaining power during outages supports which principle?
- **Answer: B. Availability** [44:54]

80. Buffer Overflow Cause

- **Question:** What is the primary cause of buffer overflow vulnerabilities?
- **Answer: B. Poor input validation** [45:21]

81. Restricting Shared Folders

- **Question:** Restricting folder access by department follows which principle?
- **Answer: A. Least privilege** [46:06]

82. Testing Backups

- **Question:** Testing restoration processes is which type of control?
- **Answer: C. Corrective control** [46:37]

83. Sharing Passwords Risk

- **Question:** What is the primary risk of users sharing passwords?
- **Answer: C. Lack of accountability** [47:09]

84. Geo-fencing

- **Question:** Restricting network connection based on location is a form of...?
- **Answer: D. Access control** [47:52]

85. Monitoring Failed Logins

- **Question:** Monitoring failed login attempts is which type of control?
- **Answer: B. Detective control** [48:26]

86. CIA and Encryption

- **Question:** Encrypting a customer database addresses which CIA element?
- **Answer: A. Confidentiality** [48:50]

87. Business Email Compromise (BEC)

- **Question:** Gaining access to an email account to send fraudulent payment requests is called...?
- **Answer: B. Business email compromise** [49:14]

88. Encrypted USB Strategy

- **Question:** Requiring encrypted USB drives for sensitive data is which strategy?
- **Answer: C. Risk mitigation** [50:00]

89. Shoulder Surfing

- **Question:** Observing a user entering a password from a distance is called...?
- **Answer: A. Shoulder surfing** [50:33]

90. ISC2 Code of Ethics

- **Question:** Which is a requirement of the ISC2 Code of Ethics?
- **Answer: B. Protecting the common good** [51:05]

91. Database Compromise Response

- **Question:** What is the best immediate response to a database exploit?
- **Answer: B. Disconnecting the affected system from the network** [51:36]

92. Dual Control

- **Question:** Requiring two employees to access a vault simultaneously is...?
- **Answer: C. Dual control** [52:17]

93. Firewall Blocking Type

- **Question:** Blocking traffic by IP and Port is which type of control?
- **Answer: B. Technical control** [52:43]

94. Low Likelihood, High Impact Strategy

- **Question:** How should you approach a risk with low likelihood but high impact?
- **Answer: C. Transfer the risk** [53:17]

95. Business Impact Analysis (BIA)

- **Question:** What is the purpose of a BIA?
- **Answer: A. To identify critical business functions** [54:02]

96. Credential Reuse Prevention

- **Question:** What policy prevents credentials from being stolen due to password reuse?
- **Answer: C. Unique password policy** [54:32]

97. Vulnerability Definition

- **Question:** Which of the following describes a vulnerability?
- **Answer: A. A flaw in the system that can be exploited** [55:06]

98. Identifying Phishing Links

- **Question:** Best way to avoid falling victim to a malicious disguised link?
- **Answer: B. Hover over the link to check its URL** [55:40]

99. Data Masking Purpose

- **Question:** What is the main purpose of data masking?
- **Answer: A. To hide sensitive information from unauthorized users** [56:14]

100. AUP Primary Reason

- **Question:** Primary reason for requiring employees to sign an AUP?
- **Answer: A. To ensure employees understand security expectations** [56:54]

Questions 1 - 25

1. Change Management Components

- **Question:** Which is not a component of change management?
- **Answer: Option A: Governance.** [01:00]
- **Explanation:** RFC (Request for Change), Rollback, and Approval are standard components; Governance is the overarching management framework.

2. Physical Control Example

- **Question:** Which of the following is an example of a physical control?
- **Answer: Option A: CCTV.** [01:40]
- **Explanation:** Physical controls are tangible measures like cameras, fences, or locks.

3. Disaster Recovery Priority

- **Question:** In the event of a disaster, which of the following is the most important priority?
- **Answer: Option C: Safety of people.** [02:20]
- **Explanation:** Human life is always the first priority in any disaster recovery situation.

4. Remote Management Protocol

- **Question:** Which protocol is used for remote management of network devices?

- **Answer: Option C: SNMP (Simple Network Management Protocol).** [03:00]

5. Business Impact Analysis (BIA) Goal

- **Question:** What is the primary goal of a BIA?
- **Answer: Option A: To identify and prioritize critical business functions.** [03:40]

6. Security Procedures

- **Question:** What is the primary purpose of security procedures?
- **Answer: Option B: To outline the step-by-step instructions for implementing security controls.** [06:20]

7. ABAC Definition

- **Question:** What is Attribute-Based Access Control (ABAC)?
- **Answer: Option A: A control that uses attributes of users, objects, and the environment to make decisions.** [07:29]

8. European Privacy Regulation

- **Question:** Which of the following is an EU regulation for data protection and privacy?
- **Answer: Option C: General Data Protection Regulation (GDPR).** [08:42]
- **Explanation:** FISMA, SOX, and HIPAA are United States federal laws.

9. DRP Challenges

- **Question:** What are some challenges in developing a Disaster Recovery Plan (DRP)?
- **Answer: Option B: Ensuring that all critical business processes are identified.** [10:09]

10. App Hosting Cloud Model

- **Question:** Which cloud service model is tailored for hosting and deploying consumer-facing applications?

- **Answer: Option D: PaaS (Platform as a Service).** [10:39]

11. Security Awareness Objective

- **Question:** What is the primary objective of security awareness training?
- **Answer: Option A: To influence user behavior and foster a security-conscious culture.** [11:20]

12. Risk Avoidance

- **Question:** When an organization decides not to engage in a risky activity, which risk strategy is applied?
- **Answer: Option D: Risk avoidance.** [12:00]

13. Non-Repudiation

- **Question:** Which security concept ensures that an individual cannot deny an action?
- **Answer: Option B: Non-repudiation.** [12:40]

14. Confidentiality Requirement Exception

- **Question:** Which of the following is *not* a requirement for maintaining confidentiality?
- **Answer: Option B: Data backup.** [15:25]
- **Explanation:** Data backup is for availability, while access control and authentication are for confidentiality.

15. Learning Activity Exception

- **Question:** Which of the following is not a common type of learning activity?
- **Answer: Option D: Tutorial.** [16:10]
- **Explanation:** ISC2 standard learning categories are Awareness, Training, and Education.

16. OSI Layer 2 Device

- **Question:** Which device operates at Layer 2 (Data Link) of the OSI model?

- **Answer: Option B: Switch.** [17:00]

17. Data Life Cycle: Initial Phase

- **Question:** What is the first stage in the data life cycle?
- **Answer: Option A: Creation.** [17:40]

18. Vulnerability Definition

- **Question:** What is a vulnerability in information security?
- **Answer: Option B: A weakness or flaw that could be exploited.** [18:20]

19. Integrity Definition

- **Question:** Which of the following best describes data integrity?
- **Answer: Option C: Ensuring that data is accurate and unchanged during transit or storage.** [19:00]

20. Social Engineering: Phishing

- **Question:** Which social engineering attack uses fraudulent emails to steal information?
- **Answer: Option A: Phishing.** [19:40]

21. Logical Access Control

- **Question:** Which of the following is a logical access control?
- **Answer: Option D: Passwords.** [20:20]

22. SIEM Function

- **Question:** What is the primary function of a SIEM system?
- **Answer: Option B: Real-time monitoring and analysis of security events.** [21:00]

23. Principle of Least Privilege

- **Question:** What does the principle of least privilege require?
- **Answer: Option A: Providing users with the minimum level of access required for their job.** [21:40]

24. Incident Response Steps

- **Question:** What is the correct order of the incident response lifecycle?
- **Answer: Option B: Preparation, Detection, Containment, Eradication, Recovery, Post-Incident.** [22:20]

25. Security Policy Purpose

- **Question:** What is the main purpose of a security policy?
- **Answer: Option A: To define the organization's high-level security goals and requirements.** [23:00]

Questions 26 - 50

26. Symmetric Encryption

- **Question:** Symmetric encryption uses:
- **Answer: Option A: One key for both encryption and decryption.** [24:00]

27. Asymmetric Encryption

- **Question:** Asymmetric encryption uses:
- **Answer: Option B: A public key to encrypt and a private key to decrypt.** [24:40]

28. Risk Acceptance

- **Question:** When a company chooses to accept a risk because the cost of mitigation is too high, it is:
- **Answer: Option C: Risk acceptance.** [25:20]

29. Role-Based Access Control (RBAC)

- **Question:** RBAC assigns permissions based on:
- **Answer: Option B: The user's job function or role.** [26:00]

30. Data Destruction

- **Question:** Which data destruction method is most secure for magnetic hard drives?
- **Answer: Option C: Degaussing.** [26:40]

31. Asset Inventory

- **Question:** What is the primary purpose of asset inventory?
- **Answer: Option A: To identify and track all organizational assets.** [27:20]

32. Threat Definition

- **Question:** What is a threat in the context of security?
- **Answer: Option B: Any potential cause of an unwanted incident.** [28:00]

33. Mandatory Access Control (MAC)

- **Question:** In a MAC model, access is determined by:
- **Answer: Option A: Security labels and clearances.** [28:40]

34. Firewall Type

- **Question:** A stateful firewall keeps track of:
- **Answer: Option B: The state of active network connections.** [29:20]

35. Patch Management

- **Question:** What is the goal of patch management?
- **Answer: Option C: To keep software and systems updated and secure.** [30:00]

36. Zero-Day Vulnerability

- **Question:** A zero-day vulnerability is one that:
- **Answer: Option D: Is unknown to the vendor and has no patch.** [30:40]

37. Administrative Control Example

- **Question:** Which of the following is an administrative control?
- **Answer: Option A: Security policy.** [31:20]

38. Detective Control Example

- **Question:** Which of the following is a detective control?
- **Answer: Option B: Intrusion Detection System (IDS).** [32:00]

39. Preventive Control Example

- **Question:** Which of the following is a preventive control?
- **Answer: Option C: Firewall.** [32:40]

40. Risk Mitigation

- **Question:** Implementing security controls to reduce risk is known as:
- **Answer: Option B: Risk mitigation.** [33:20]

41. Discretionary Access Control (DAC)

- **Question:** In a DAC model, access is granted by:
- **Answer: Option B: The owner of the resource.** [34:00]

42. Denial of Service (DoS)

- **Question:** A DoS attack aims to:
- **Answer: Option C: Disrupt system availability.** [34:40]

43. Identity Management

- **Question:** What is the primary goal of identity management?
- **Answer: Option A: To ensure that users are who they claim to be.** [35:20]

44. Digital Signature

- **Question:** A digital signature provides:
- **Answer: Option D: Integrity and non-repudiation.** [36:00]

45. Public Key Infrastructure (PKI)

- **Question:** PKI is used to manage:
- **Answer: Option B: Digital certificates and public-private keys.** [36:40]

46. Business Continuity Plan (BCP)

- **Question:** The primary focus of a BCP is:
- **Answer: Option A: Maintaining critical business operations during a disruption.** [37:20]

47. Social Engineering: Pretexting

- **Question:** Pretexting involves:
- **Answer: Option B: Creating a fabricated scenario to obtain information.** [38:00]

48. Asset Classification

- **Question:** Asset classification is based on:
- **Answer: Option B: The sensitivity or value of the asset.** [38:40]

49. Network Segmentation

- **Question:** Network segmentation helps to:
- **Answer: Option C: Limit the spread of attacks within a network.** [39:20]

50. Encryption at Rest

- **Question:** Encryption at rest protects data that is:
- **Answer: Option A: Stored on a physical device or medium.** [40:00]

Questions 51 - 75: Data Security & Incident Response

51. Data Classification Levels

- **Question:** Which data classification level is usually reserved for information that, if disclosed, could cause exceptional damage to national security?
- **Answer: Top Secret.**
- **Explanation:** In government classification, "Top Secret" is the highest level of sensitivity.

52. Hashing and Integrity

- **Question:** What is the primary purpose of using a cryptographic hash function?
- **Answer: To verify data integrity.**
- **Explanation:** A hash creates a unique fingerprint of data; if the data changes, the hash changes.

53. Incident Containment

- **Question:** What is the main goal of the containment phase in incident response?
- **Answer: To limit the scope and magnitude of an incident.**
- **Explanation:** Containment prevents the threat from spreading further through the network.

54. Social Engineering: Tailgating

- **Question:** An attacker following an authorized person into a secure building without their knowledge is called:

- **Answer: Tailgating (or Piggybacking).**

55. Qualitative Risk Analysis

- **Question:** Qualitative risk analysis is based on:
- **Answer: Subjective judgment and experience.**
- **Explanation:** Unlike quantitative analysis (money-based), qualitative uses scales like "Low, Medium, High."

56. Intrusion Prevention System (IPS)

- **Question:** What is the difference between an IDS and an IPS?
- **Answer: An IPS can actively block or prevent a detected threat.**

57. Multi-Factor Authentication (MFA)

- **Question:** Which of the following is a "something you have" factor in MFA?
- **Answer: A hardware token or smartphone app.**

58. Security Awareness: Quid Pro Quo

- **Question:** A social engineering attack where an attacker offers a service in exchange for information is:
- **Answer: Quid Pro Quo.**

59. Disaster Recovery Site: Hot Site

- **Question:** Which DR site is fully equipped and can be operational within hours?
- **Answer: Hot Site.**

60. Least Privilege vs. Need to Know

- **Question:** Which principle specifically refers to the necessity of accessing specific information to perform a task?
- **Answer: Need to Know.**

61. Network Ports: HTTPS

- **Question:** Which port does HTTPS typically use?
- **Answer: Port 443.**

62. Vulnerability Scanning

- **Question:** What is the primary purpose of a vulnerability scanner?
- **Answer: To identify known security flaws in a system.**

63. Brute Force Attack

- **Question:** An attack that tries every possible combination of characters to guess a password is:
- **Answer: Brute Force.**

64. Data Lifecycle: Archiving

- **Question:** In the data lifecycle, archiving occurs when data is:
- **Answer: No longer needed for active use but must be kept for legal or historical reasons.**

65. Physical Security: Mantrap

- **Question:** A physical security control consisting of two interlocking doors to prevent tailgating is a:
- **Answer: Mantrap.**

66. Incident Response: Eradication

- **Question:** The phase where the root cause of the incident is removed from the environment is:
- **Answer: Eradication.**

67. Security Control: Deterrent

- **Question:** A "Warning: Security Cameras in Use" sign is what type of control?
- **Answer: Deterrent.**

68. Cryptography: Steganography

- **Question:** The practice of hiding a secret message inside a non-secret file (like an image) is:
- **Answer: Steganography.**

69. Cloud Security Responsibility

- **Question:** In a SaaS model, who is primarily responsible for the security of the underlying infrastructure?
- **Answer: The Cloud Service Provider (CSP).**

70. Recovery Point Objective (RPO)

- **Question:** RPO defines:
- **Answer: The maximum amount of data loss an organization can tolerate.**

71. Social Engineering: Vishing

- **Question:** Phishing conducted over a voice call is known as:
- **Answer: Vishing.**

72. Principle of Accountability

- **Question:** Which mechanism ensures that an individual's actions can be traced back to them?
- **Answer: Audit Logs.**

73. OSI Model: Layer 3

- **Question:** Which layer of the OSI model handles routing and IP addressing?
- **Answer: Layer 3 (Network Layer).**

74. Malware: Ransomware

- **Question:** Malware that encrypts a victim's files and demands payment is:
- **Answer: Ransomware.**

75. Access Control: Biometrics

- **Question:** Which biometric factor measures physical patterns of the eye?
- **Answer: Iris or Retina scan.**

Questions 76 - 100: Governance & Network Defense

76. Security Standards: ISO/IEC 27001

- **Question:** What is the focus of ISO/IEC 27001?
- **Answer: Information Security Management Systems (ISMS).**

77. Network Defense: Honeypot

- **Question:** A decoy system designed to lure and trap attackers is a:
- **Answer: Honeypot.**

78. Data Privacy: PII

- **Question:** What does PII stand for?
- **Answer: Personally Identifiable Information.**

79. Risk Management: Mitigation

- **Question:** Installing an antivirus is an example of which risk response?
- **Answer: Mitigation (Reduction).**

80. Access Control: Smart Cards

- **Question:** A smart card is an example of which authentication factor?
- **Answer: Something you have.**

81. Incident Response: Post-Incident Activity

- **Question:** The "Lessons Learned" meeting occurs in which phase?
- **Answer: Post-Incident Activity.**

82. Network Security: VPN

- **Question:** A VPN provides a secure tunnel over an insecure network using:
- **Answer: Encryption and Tunneling Protocols.**

83. Security Policy: Password Complexity

- **Question:** A rule requiring a mix of uppercase, lowercase, numbers, and symbols is:
- **Answer: Password Complexity.**

84. Physical Security: Bollards

- **Question:** Short, sturdy posts used to prevent vehicles from crashing into a building are:
- **Answer: Bollards.**

85. Information Security: The CIA Triad

- **Question:** Which element of CIA is concerned with systems being accessible when needed?
- **Answer: Availability.**

86. Malware: Trojan Horse

- **Question:** A malicious program that disguises itself as a useful application is a:
- **Answer: Trojan Horse.**

87. Governance: Due Care

- **Question:** The legal term for doing what a reasonable person would do in a given situation is:
- **Answer: Due Care.**

88. Access Control: False Acceptance Rate (FAR)

- **Question:** In biometrics, when an unauthorized person is incorrectly granted access, it is a:
- **Answer: False Acceptance (Type II Error).**

89. Network Security: DMZ

- **Question:** A sub-network that contains an organization's external-facing services is a:
- **Answer: DMZ (Demilitarized Zone).**

90. Cryptography: Non-repudiation

- **Question:** Which cryptographic tool provides non-repudiation?
- **Answer: Digital Signatures.**

91. Security Operations: Asset Management

- **Question:** You cannot protect what you don't know you have. This refers to:
- **Answer: Asset Inventory/Management.**

92. Social Engineering: Dumpster Diving

- **Question:** Searching through trash to find sensitive information is:
- **Answer: Dumpster Diving.**

93. Risk Management: Quantitative Analysis

- **Question:** Which formula is used to calculate the Annualized Loss Expectancy (ALE)?
- **Answer: SLE x ARO = ALE.**

94. Security Controls: Logical Control

- **Question:** An Access Control List (ACL) on a router is what type of control?
- **Answer: Logical (Technical) Control.**

95. Business Continuity: MTD

- **Question:** What does MTD stand for in BCP?
- **Answer: Maximum Tolerable Downtime.**

96. Network Protocols: DNS

- **Question:** DNS translates:
- **Answer: Domain names to IP addresses.**

97. Data Security: Data in Motion

- **Question:** Data being transmitted over a network is referred to as:
- **Answer: Data in Motion (or Transit).**

98. Access Control: Single Sign-On (SSO)

- **Question:** SSO allows a user to:
- **Answer: Log in once and access multiple related systems.**

99. Malware: Spyware

- **Question:** Software that secretly monitors a user's activity and reports it back to an attacker is:
- **Answer: Spyware.**

100. Professional Ethics: ISC2 Code of Ethics

- **Question:** What is the first canon of the ISC2 Code of Ethics?

- **Answer: Protect society, the common good, necessary public trust and confidence, and the infrastructure.**

Questions 101 - 125: Network Security & Access Control

101. Network Layer (OSI) Protocol

- **Question:** Which of the following is a Layer 3 protocol used for routing and addressing?
- **Answer: IP (Internet Protocol).**
- **Explanation:** IP is the fundamental protocol of the Network Layer (Layer 3) that handles addressing and routing of packets.

102. Physical Access Control: Fence Height

- **Question:** To deter a determined intruder, what is the minimum recommended height for a security fence?
- **Answer: 8 feet (with top guard like barbed wire).**

103. Security Control: Compensating

- **Question:** What type of control is used when a primary security control cannot be implemented or is not sufficient?
- **Answer: Compensating Control.**
- **Explanation:** It "compensates" for the lack of a primary control (e.g., using logs because a real-time firewall rule isn't possible).

104. Data Center Hazard: Fire Suppression

- **Question:** Which fire suppression system is most safe for electronic equipment in a data center?
- **Answer: Clean Agent Systems (e.g., FM-200 or CO2).**
- **Explanation:** These do not leave residue or liquid that could damage electronics.

105. Network Security: 802.1X

- **Question:** What does the 802.1X standard provide?
- **Answer: Port-based Network Access Control.**
- **Explanation:** It ensures that a device is authenticated before it can access network resources.

106. Authentication: Bio-Signatures

- **Question:** Which biometric factor is considered a "behavioral" characteristic?
- **Answer: Keystroke dynamics or Signature dynamics.**

107. Incident Response: Detection & Analysis

- **Question:** Which phase of incident response involves identifying that an incident has occurred and determining its severity?
- **Answer: Detection and Analysis.**

108. Cryptography: Salt

- **Question:** In password hashing, what is "Salt"?
- **Answer: Random data added to a password before hashing to prevent rainbow table attacks.**

109. Network Ports: DNS

- **Question:** DNS typically uses which port for standard queries?
- **Answer: Port 53 (UDP).**

110. Cloud Security: Shared Responsibility

- **Question:** In the Shared Responsibility Model, who is responsible for securing data "in the cloud"?
- **Answer: The Customer.**

111. Asset Disposal: Incineration

- **Question:** Incineration is a method used for:
- **Answer: Physical destruction of paper or media.**

112. Security Architecture: Zero Trust

- **Question:** What is the core principle of Zero Trust architecture?
- **Answer: Never trust, always verify.**

113. Network Security: IDS vs. IPS

- **Question:** Which system sends an alert but does *not* drop the malicious traffic?
- **Answer: IDS (Intrusion Detection System).**

114. Data Lifecycle: Use

- **Question:** The phase where data is viewed, processed, or otherwise used in an application is:
- **Answer: Use.**

115. Access Control: Separation of Duties

- **Question:** Why is Separation of Duties important?
- **Answer: To prevent fraud by requiring more than one person to complete a critical task.**

116. Social Engineering: Influence Tactics

- **Question:** An attacker pretending to be a CEO to demand an urgent wire transfer is using which tactic?
- **Answer: Authority and Urgency.**

117. Cryptography: Key Management

- **Question:** What is the most challenging part of using symmetric encryption at scale?
- **Answer: Secure key distribution.**

118. Physical Security: Lighting

- **Question:** Lighting is considered which type of security control?
- **Answer: Deterrent and Detective.**

119. Business Continuity: BIA Impact

- **Question:** Which metric from a BIA describes the maximum time a business process can be down before the organization is critically damaged?
- **Answer: Maximum Tolerable Downtime (MTD).**

120. Network Security: VLANs

- **Question:** VLANs are used to:
- **Answer: Logically segment a network at the Data Link Layer (Layer 2).**

121. Malware: Virus vs. Worm

- **Question:** What is the main difference between a virus and a worm?
- **Answer: A virus requires a host file or user action to spread; a worm spreads automatically.**

122. Risk Management: Residual Risk

- **Question:** What is residual risk?
- **Answer: The risk that remains after security controls have been applied.**

123. Identity Management: Provisioning

- **Question:** The process of creating, maintaining, and deactivating user accounts is:
- **Answer: User Provisioning.**

124. Security Standards: PCI DSS

- **Question:** PCI DSS applies to any organization that:
- **Answer: Processes, stores, or transmits credit card data.**

125. OSI Model: Layer 1

- **Question:** Which layer is responsible for the transmission of raw bits over a physical medium?
- **Answer: Layer 1 (Physical Layer).**

Questions 126 - 150: Final Review & Exam Practice

126. Data Masking

- **Question:** Replacing sensitive data with functional but fake data is called:
- **Answer: Data Masking (or Obfuscation).** [02:32:07] (Referenced in similar contexts).

127. Administrative Control: Background Checks

- **Question:** Performing background checks on new hires is an example of:
- **Answer: Administrative (Preventive) Control.**

128. Network Security: Firewall Placement

- **Question:** A firewall placed between the internal network and the internet is a:
- **Answer: Perimeter Firewall.**

129. Incident Response: Preparation

- **Question:** Which phase involves creating the incident response team and training them?
- **Answer: Preparation.**

130. Security Concept: Least Privilege

- **Question:** Granting a user "Read Only" access to a file because they don't need to edit it is an example of:
- **Answer: Least Privilege.**

131. Access Control: Multi-Factor (MFA)

- **Question:** Using a password and a fingerprint scan is:
- **Answer: Something you know + Something you are.**

132. Disaster Recovery: Cold Site

- **Question:** A site with power and cooling but no pre-installed hardware is a:
- **Answer: Cold Site.**

133. Cryptography: Digital Certificates

- **Question:** Who issues digital certificates?
- **Answer: Certificate Authority (CA).**

134. Risk Response: Sharing

- **Question:** Risk transference is also known as risk:
- **Answer: Sharing.**

135. Network Protocols: ARP

- **Question:** ARP resolves:
- **Answer: IP addresses to MAC addresses.**

136. Security Operations: Patching

- **Question:** What type of control is patching a vulnerability?
- **Answer: Corrective Control.** [02:31:46]

137. Information Security: Accountability

- **Question:** Accountability is achieved through:
- **Answer: Identification, Authentication, and Auditing.**

138. Data Sensitivity: PHI

- **Question:** What does PHI stand for?
- **Answer: Protected Health Information.**

139. Network Security: Proxy Server

- **Question:** A server that acts as an intermediary for requests from clients seeking resources from other servers is a:
- **Answer: Proxy Server.**

140. Physical Security: Guard

- **Question:** A security guard is which type of control?
- **Answer: Physical (Preventive/Detective).**

141. Malware: Logic Bomb

- **Question:** Code that lies dormant until a specific condition (like a date) is met is a:
- **Answer: Logic Bomb.**

142. Risk Management: Threat x Vulnerability

- **Question:** Risk is often calculated as:
- **Answer: Threat x Vulnerability.**

143. Access Control: Implicit Deny

- **Question:** The principle that if access is not explicitly granted, it is denied, is called:
- **Answer: Implicit Deny.**

144. Governance: Policies vs. Procedures

- **Question:** Which one is high-level and mandatory?
- **Answer: Policy.**

145. Data Security: Data at Rest

- **Question:** Hard drive encryption protects:
- **Answer: Data at Rest.**

146. Social Engineering: Baiting

- **Question:** Leaving a malware-infected USB drive in a parking lot is an example of:
- **Answer: Baiting.**

147. Security Control Type: Patching

- **Question:** Patching software vulnerabilities is a:
- **Answer: Corrective Control.** [02:31:46]

148. Data Integrity Significance

- **Question:** What is the significance of Data Integrity?
- **Answer: Ensuring data is accurate and unchanged.** [02:32:27]

149. Man-in-the-Middle (MitM) Function

- **Question:** What is the primary function of the attacker in a MitM attack?
- **Answer: Intercepts and possibly alters communication between two parties.** [02:33:27]

150. Risk Assessment Report Goal

- **Question:** What does a risk assessment report aim to achieve?

- **Answer: To communicate the results of the risk assessment to stakeholders.** [02:34:57]

Part 1: Questions 1 - 50

1. Discretionary Access Control (DAC) Permissions

- **Question:** What are the tasks that can solely be executed by the subject within a discretionary Access Control policy scenario?
- **Answer: Option B: Changing security attributes** [00:48]
- **Explanation:** In DAC, the subject (owner) has the discretion to modify permissions and security attributes for other users.

2. Goal of a Rootkit

- **Question:** What is the main goal achieved by installing a rootkit on a computer system?
- **Answer: Option D: To conceal logs and other system events** [03:16]
- **Explanation:** Rootkits are designed to hide their presence and malicious activities to evade detection.

3. Emergency Access Locks

- **Question:** What kind of lock is best for a door where firefighters and ambulance crews need to get in quickly?
- **Answer: Option B: Smart Lock** [05:29]
- **Explanation:** Smart locks allow for keyless entry and remote unlocking, which is crucial during time-sensitive emergencies.

4. Detecting Malicious Traffic

- **Question:** What is the main tool utilized for detecting potential malicious activities on a network through traffic analysis?
- **Answer: Option B: Intrusion Detection System (IDS)** [08:05]
- **Explanation:** An IDS monitors network traffic and generates alerts for suspicious patterns.

5. Least Privilege Implementation

- **Question:** Which principle aligns with the concept of restricting user access to only what is required to fulfill their job responsibilities?
- **Answer: Need-to-know principle** [16:21]
- **Explanation:** Users should only have access to information necessary for their specific roles.

6. Reducing Attack Surface

- **Question:** Which process is most effective at reducing the attack surface of IT infrastructure?
- **Answer: Configuration Management** [25:48]
- **Explanation:** Consistent and secure configuration minimizes vulnerabilities that attackers could exploit.

7. Adding System Elements

- **Question:** When adding new elements to a system, what is the focus regarding sensitive information?
- **Answer:** Ensuring appropriate security measures are in place for the new data. [32:45]
- **Explanation:** Sanitization is usually for removal/replacement, while additions require new protection measures.

8. Malware Independence

- **Question:** Which type of malware has the ability to self-replicate and spread autonomously?
- **Answer: Worm** [44:38]
- **Explanation:** Unlike viruses or Trojans, worms do not require a host file or user interaction to reproduce.

9. Unauthorized Alteration Protection

- **Question:** Which security principle focuses on protecting data from unauthorized alteration or destruction?
- **Answer: Integrity** [50:03]
- **Explanation:** Integrity ensures that information remains accurate and hasn't been tampered with.

10. ISC2 Code of Ethics - 4th Canon

- **Question:** What is the fourth canon of the ISC2 Code of Ethics?
- **Answer: Option A: Advance and protect the profession** [51:26]
- **Explanation:** This canon requires professionals to share knowledge and promote ethical behavior within the industry.

11. Verifying Employee Privileges

- **Question:** What process should a company use to verify that an employee with multiple roles (HR, Payroll, etc.) has the correct privileges?
- **Answer: Option D: Account Review** [01:07:09]
- **Explanation:** Regular reviews ensure permissions remain aligned with current responsibilities and minimize "privilege creep."

12. Behavioral-Based Detection

- **Question:** How does behavioral-based detection operate in an IDS?
- **Answer:** By detecting deviations from an established baseline of normal activity. [09:01:35]

- **Explanation:** It triggers alerts when unusual patterns occur that differ from typical network behavior.

13. Username/Password Vulnerabilities

- **Question:** What vulnerabilities exist in a system relying solely on usernames and passwords?
- **Answer: Option D: All of these** (Users forgetting, sharing, or passwords being stolen) [09:03:35]

14. Data Handling Policy Exceptions

- **Question:** Which of the following does *not* qualify as a direct data handling policy example?
- **Answer: Option B: Acceptable Use Policy (AUP)** [09:04:45]
- **Explanation:** While an AUP influences behavior, it focuses on the use of resources rather than the specific mechanics of data handling like anonymization or transfer.

15. Security Control: Deterrent

- **Question:** Which of the following is designed to discourage a potential attacker from even attempting an intrusion?
- **Answer: Warning Signs.**
- **Explanation:** Deterrent controls like signs or fences aim to make the effort seem too high for the attacker.

16. The CIA Triad: Availability

- **Question:** Ensuring that systems and data are accessible when needed by authorized users refers to:
- **Answer: Availability.**

17. Physical Security: Lighting

- **Question:** What is the primary security purpose of outdoor lighting?
- **Answer: To increase the chance of detection.**

18. Access Control: Biometrics

- **Question:** Which biometric factor is the most difficult to forge?
- **Answer: Retina Scan.**

19. Social Engineering: Baiting

- **Question:** Leaving a malware-infected USB drive in a public place is an example of:
- **Answer: Baiting.**

20. Risk Management: Transference

- **Question:** Purchasing cyber insurance is an example of which risk strategy?
- **Answer: Risk Transference.**

21. Network Security: Firewalls

- **Question:** A firewall that filters traffic based on the application or service is called:
- **Answer: Application-level Gateway (Proxy).**

22. Data Handling: Disposal

- **Question:** What is the most secure way to dispose of sensitive paper documents?
- **Answer: Cross-cut shredding or Incineration.**

23. Identity Management: Identification

- **Question:** Presenting a username to a system is an act of:
- **Answer: Identification.**

24. OSI Model: Layer 3

- **Question:** At which layer of the OSI model does a router primarily operate?
- **Answer: Layer 3 (Network Layer).**

25. Disaster Recovery: RTO

- **Question:** What does RTO stand for?
- **Answer: Recovery Time Objective.**

26. Security Governance: Policies

- **Question:** Which document provides a high-level statement of management's intent?
- **Answer: Security Policy.**

27. Malware: Logic Bomb

- **Question:** Malicious code that executes when a specific date or event occurs is a:
- **Answer: Logic Bomb.**

28. Network Security: VPN

- **Question:** What does a VPN provide for remote workers?
- **Answer: Confidentiality and Integrity over public networks.**

29. Access Control: MAC

- **Question:** Which access control model is the most restrictive and used in high-security military environments?
- **Answer: Mandatory Access Control (MAC).**

30. Incident Response: Preparation

- **Question:** Training an Incident Response Team (IRT) is part of which phase?
- **Answer: Preparation.**

31. Physical Security: Mantrap

- **Question:** A small room with two doors to prevent unauthorized entry is a:
- **Answer: Mantrap.**

32. Data Lifecycle: Archiving

- **Question:** Moving data that is no longer in active use to long-term storage is:
- **Answer: Archiving.**

33. Cryptography: Hashing

- **Question:** Which of the following provides data integrity?
- **Answer: Hashing.**

34. Social Engineering: Pretexting

- **Question:** An attacker creating a fake scenario to gain trust is:
- **Answer: Pretexting.**

35. Risk Assessment: Quantitative

- **Question:** Which risk analysis method uses dollar values and percentages?
- **Answer: Quantitative Risk Analysis.**

36. Network Protocols: SSH

- **Question:** Which protocol is a secure replacement for Telnet?
- **Answer: SSH (Secure Shell).**

37. Administrative Control: Separation of Duties

- **Question:** Ensuring one person cannot complete a sensitive transaction alone is:
- **Answer: Separation of Duties.**

38. The CIA Triad: Confidentiality

- **Question:** Using encryption to protect data from being read by unauthorized people ensures:
- **Answer: Confidentiality.**

39. Physical Security: Perimeter

- **Question:** Fences and gates are examples of:
- **Answer: Perimeter Security.**

40. Business Continuity: BIA

- **Question:** The process of identifying critical business functions is called:
- **Answer: Business Impact Analysis.**

41. Network Security: DMZ

- **Question:** Where should a public-facing web server be placed?
- **Answer: DMZ (Demilitarized Zone).**

42. Asset Management: Inventory

- **Question:** The first step in protecting assets is:
- **Answer: Creating an Asset Inventory.**

43. Malware: Ransomware

- **Question:** Malware that locks files until a fee is paid is:
- **Answer: Ransomware.**

44. Access Control: RBAC

- **Question:** Granting access based on an employee's job title is:
- **Answer: Role-Based Access Control.**

45. Security Awareness: Training

- **Question:** What is the best way to prevent social engineering attacks?
- **Answer: Security Awareness Training.**

46. Data Integrity: Checksums

- **Question:** A value used to verify that a file has not been altered is a:
- **Answer: Checksum.**

47. Professional Ethics: Public Trust

- **Question:** Which ISC2 canon emphasizes protecting the common good?
- **Answer: Canon 1.**

48. Disaster Recovery: Cold Site

- **Question:** Which DR site is the least expensive but takes the longest to set up?
- **Answer: Cold Site.**

49. Network Ports: HTTP

- **Question:** Which port does standard HTTP use?
- **Answer: Port 80.**

50. Incident Response: Lessons Learned

- **Question:** Which phase occurs after the incident is fully resolved?
- **Answer: Post-Incident Activity (Lessons Learned).**

51. ISC2 Code of Ethics - 1st Canon

- **Question:** Which canon of the ISC2 Code of Ethics requires protecting society and the common good?
- **Answer: Canon 1.** [51:12]

52. Physical Security: Bollards

- **Question:** What are short, sturdy vertical posts used to prevent vehicles from ramming into a building?
- **Answer: Bollards.**

53. Access Control: Multi-Factor Authentication (MFA)

- **Question:** Using a password and a smart card represents which two factors?
- **Answer: Something you know and Something you have.**

54. Data Security: Masking

- **Question:** Replacing sensitive data with a non-sensitive version that looks like the original is:
- **Answer: Data Masking.**

55. Information Security: Non-Repudiation

- **Question:** Which concept ensures that a sender cannot later deny sending a message?
- **Answer: Non-repudiation.**

56. Network Security: Patch Management

- **Question:** What is the primary reason for applying patches to a system?
- **Answer: To fix security vulnerabilities.**

57. Physical Security: CCTV

- **Question:** CCTV cameras are primarily which type of security control?
- **Answer: Detective Control.**

58. Cloud Security: IaaS Responsibility

- **Question:** In Infrastructure as a Service (IaaS), who is responsible for securing the guest operating system?
- **Answer: The Customer.**

59. Disaster Recovery: Warm Site

- **Question:** A disaster recovery site that has network connectivity and some hardware but requires restoration of data is a:
- **Answer: Warm Site.**

60. The CIA Triad: Integrity

- **Question:** Digital signatures are used to ensure which part of the CIA triad?
- **Answer: Integrity.**

61. Social Engineering: Vishing

- **Question:** Phishing attacks conducted over a telephone call are known as:
- **Answer: Vishing.**

62. Administrative Control: Job Rotation

- **Question:** Which policy helps detect fraudulent activity by having employees move to different roles?
- **Answer: Job Rotation.**

63. Network Security: DMZ

- **Question:** What is the primary purpose of a DMZ (Demilitarized Zone)?
- **Answer: To separate internal network resources from external-facing services.**

64. Data Handling: PII Definition

- **Question:** What does PII stand for in data privacy?
- **Answer: Personally Identifiable Information.**

65. Access Control: Biometric Accuracy

- **Question:** Which biometric metric measures the rate at which authorized users are denied access?
- **Answer: False Rejection Rate (FRR).**

66. Risk Management: Avoidance

- **Question:** Deciding not to proceed with a project because the risk is too high is:
- **Answer: Risk Avoidance.**

67. Incident Response: Containment

- **Question:** Disconnecting a compromised server from the network is an example of:
- **Answer: Containment.**

68. Network Security: Port 443

- **Question:** Which service typically uses TCP port 443?
- **Answer: HTTPS.**

69. Asset Management: Lifecycle

- **Question:** What is the final phase of the asset lifecycle?
- **Answer: Disposal.**

70. Security Governance: Standards

- **Question:** Which document provides specific, mandatory rules for security?
- **Answer: Standards.**

71. Malware: Trojan Horse

- **Question:** A malicious program disguised as a legitimate game or utility is a:
- **Answer: Trojan Horse.**

72. Physical Security: Biometric Door Lock

- **Question:** A fingerprint scanner on a door is an example of:
- **Answer: Physical and Technical control.**

73. The CIA Triad: Data in Motion

- **Question:** TLS/SSL encryption is primarily used to protect:
- **Answer: Data in Motion.**

74. Administrative Control: Mandatory Vacations

- **Question:** Forcing employees to take time off to help uncover potential fraud is:
- **Answer: Mandatory Vacations.**

75. Network Security: IDS Placement

- **Question:** Where is a Host-based IDS (HIDS) installed?
- **Answer: On a specific server or workstation.**

76. Business Continuity: MTD

- **Question:** What defines the absolute maximum time a business can survive without a specific process?
- **Answer: Maximum Tolerable Downtime (MTD).**

77. Access Control: Implicit Deny

- **Question:** "If access is not specifically allowed, it is blocked" refers to:
- **Answer: Implicit Deny.**

78. Social Engineering: Shoulder Surfing

- **Question:** Watching someone enter their PIN at an ATM is:
- **Answer: Shoulder Surfing.**

79. Risk Management: Mitigation

- **Question:** Installing a firewall to reduce the likelihood of an attack is:
- **Answer: Risk Mitigation.**

80. Cryptography: Symmetric Key

- **Question:** In symmetric encryption, how many keys are used for encryption and decryption?
- **Answer: One shared key.**

81. Network Security: SSID

- **Question:** The name of a wireless network is called the:
- **Answer: SSID (Service Set Identifier).**

82. Data Handling: Labeling

- **Question:** What is the first step in a data classification program?
- **Answer: Identifying the data owners.**

83. Physical Security: Two-Person Integrity

- **Question:** Requiring two people to be present when accessing a vault is:
- **Answer: Two-Person Integrity.**

84. Identity Management: Authorization

- **Question:** Determining what a user can do after they log in is:
- **Answer: Authorization.**

85. Professional Ethics: Legality

- **Question:** Which ISC2 canon requires professionals to act honorably and legally?
- **Answer: Canon 2.** [51:12]

86. Disaster Recovery: Recovery Point Objective (RPO)

- **Question:** Which metric focuses on how much data loss is acceptable?
- **Answer: RPO.**

87. Network Security: MAC Filtering

- **Question:** Restricting network access based on hardware addresses is:
- **Answer: MAC Filtering.**

88. Incident Response: Eradication

- **Question:** Removing a virus from a file system is part of:
- **Answer: Eradication.**

89. The CIA Triad: Hashing

- **Question:** Which of the following does NOT provide confidentiality?
- **Answer: Hashing.** (It provides integrity).

90. Administrative Control: Background Checks

- **Question:** Checking a new hire's criminal record is:
- **Answer: Administrative (Preventive) control.**

91. Physical Security: Motion Sensors

- **Question:** A sensor that triggers an alarm when someone enters a dark room is:
- **Answer: Detective control.**

92. Cloud Security: SaaS Responsibility

- **Question:** Who is responsible for application security in Software as a Service (SaaS)?
- **Answer: The Provider.**

93. Access Control: Single Sign-On (SSO)

- **Question:** Logged into one system to gain access to multiple related systems is:
- **Answer: SSO.**

94. Risk Management: Qualitative

- **Question:** Assessing risk as "High," "Medium," or "Low" is:
- **Answer: Qualitative Assessment.**

95. Network Security: ARP Spoofing

- **Question:** An attack where the MAC address is linked to the IP of another host is:
- **Answer: ARP Spoofing.**

96. Data Handling: Sanitization

- **Question:** Permanently removing data from a hard drive so it cannot be recovered is:
- **Answer: Sanitization.** [32:57]

97. Physical Security: Turnstiles

- **Question:** Which physical device helps prevent tailgating?
- **Answer: Turnstiles.**

98. Cryptography: Public Key

- **Question:** In asymmetric encryption, which key is used to encrypt a message for a specific recipient?
- **Answer: The recipient's public key.**

99. Administrative Control: Separation of Duties

- **Question:** Why should a developer not have access to the production environment?
- **Answer: To maintain Separation of Duties.**

100. Security Operations: Logs

- **Question:** What is the most important source of information during a forensic investigation?
- **Answer: System and Audit Logs.** [09:05:36]

101. Network Protocols: ICMP

- **Question:** Which protocol is used by the ping command to test network connectivity?
- **Answer: ICMP (Internet Control Message Protocol).**

102. Access Control: Role-Based (RBAC)

- **Question:** In RBAC, permissions are assigned to:
- **Answer: Roles, not individual users.**

103. Security Concept: Due Diligence

- **Question:** The ongoing research and monitoring to maintain a security posture is known as:
- **Answer: Due Diligence.**

104. Data Handling: Encryption at Rest

- **Question:** BitLocker and FileVault are examples of:
- **Answer: Encryption at Rest.**

105. Physical Security: Motion Detectors

- **Question:** Which type of sensor detects changes in infrared light levels?
- **Answer: Passive Infrared (PIR) Sensor.**

106. Network Security: SQL Injection

- **Question:** An attack where malicious code is inserted into a web form to manipulate a database is:
- **Answer: SQL Injection.**

107. Incident Response: Recovery

- **Question:** Bringing affected systems back into production after an incident is:
- **Answer: Recovery.**

108. The CIA Triad: Digital Signatures

- **Question:** Digital signatures provide both:
- **Answer: Integrity and Non-repudiation.**

109. Social Engineering: Scareware

- **Question:** A popup that falsely claims your computer is infected with 50 viruses to trick you into buying software is:
- **Answer: Scareware.**

110. Administrative Control: Data Retention Policy

- **Question:** A policy that defines how long data must be kept for legal reasons is:
- **Answer: Data Retention Policy.**

111. Physical Security: Badge Reader

- **Question:** A device that reads a proximity card to unlock a door is a:
- **Answer: Physical Access Control System (PACS).**

112. Cloud Security: PaaS Responsibility

- **Question:** In Platform as a Service (PaaS), who is responsible for the security of the application code?
- **Answer: The Customer.**

113. Network Security: Honeypot

- **Question:** A decoy system designed to distract and study attackers is a:

- **Answer: Honeypot.**

114. Access Control: Privilege Creep

- **Question:** When a user accumulates more permissions than they need over time as they change jobs, it is called:
- **Answer: Privilege Creep.** [01:06:45]

115. Information Security: Least Privilege

- **Question:** Giving a user "Read Only" access when they don't need "Write" access is:
- **Answer: Least Privilege.** [16:21]

116. Network Protocols: DNS

- **Question:** Which protocol translates domain names like google.com into IP addresses?
- **Answer: DNS (Domain Name System).**

117. Risk Management: Quantitative Calculation

- **Question:** In risk assessment, SLE x ARO equals:
- **Answer: ALE (Annualized Loss Expectancy).**

118. Physical Security: Faraday Cage

- **Question:** An enclosure used to block electromagnetic fields is a:
- **Answer: Faraday Cage.**

119. Data Security: Steganography

- **Question:** The process of hiding a secret message inside an image file is:
- **Answer: Steganography.**

120. Administrative Control: Acceptable Use Policy

- **Question:** Which policy tells employees what they can and cannot do on company computers?
- **Answer: Acceptable Use Policy (AUP).** [09:04:45]

121. Malware: Adware

- **Question:** Software that automatically displays or downloads advertising material is:
- **Answer: Adware.**

122. Network Security: 2FA

- **Question:** Using a password and a code sent to your phone is:
- **Answer: Two-Factor Authentication.**

123. Access Control: Mandatory (MAC)

- **Question:** In which model are users assigned "clearance" levels?
- **Answer: MAC (Mandatory Access Control).**

124. Security Operations: SIEM

- **Question:** A tool that collects and analyzes log data from across the network is:
- **Answer: SIEM (Security Information and Event Management).**

125. OSI Model: Layer 2

- **Question:** At which layer do network switches and MAC addresses operate?
- **Answer: Layer 2 (Data Link Layer).**

126. Professional Ethics: Mentoring

- **Question:** Mentoring others in the field falls under which ISC2 canon?
- **Answer: Advance and protect the profession.** [51:26]

127. Physical Security: Biometric Error

- **Question:** A "Type 1 Error" in biometrics occurs when:
- **Answer: An authorized user is falsely rejected.**

128. Disaster Recovery: Hot Site

- **Question:** Which DR site is ready for immediate switchover?
- **Answer: Hot Site.**

129. Risk Management: Acceptance

- **Question:** Choosing to do nothing because the cost of a countermeasure is higher than the asset value is:
- **Answer: Risk Acceptance.**

130. Network Protocols: DHCP

- **Question:** Which protocol automatically assigns IP addresses to devices on a network?
- **Answer: DHCP.**

131. Access Control: DAC Owner

- **Question:** In Discretionary Access Control, who decides who has access to a file?
- **Answer: The Data Owner.** [00:48]

132. Information Security: Availability

- **Question:** A Denial of Service (DoS) attack is an attack on:
- **Answer: Availability.**

133. Physical Security: Mantraps

- **Question:** What is the main purpose of a mantrap?
- **Answer: To prevent tailgating.**

134. Data Handling: Labeling

- **Question:** Marking a document as "Confidential" or "Public" is called:
- **Answer: Data Labeling.**

135. Network Security: WPA3

- **Question:** What is the most secure current standard for Wi-Fi encryption?
- **Answer: WPA3.**

136. Incident Response: Eradication

- **Question:** Rebuilding a system from a clean backup is part of:
- **Answer: Eradication.**

137. Cloud Security: Shared Responsibility

- **Question:** Who is responsible for physical security in a Public Cloud?
- **Answer: The Cloud Service Provider.**

138. Risk Management: Asset Value

- **Question:** What is the first step in a Quantitative Risk Assessment?
- **Answer: Identify and value assets.**

139. Physical Security: Pressure Sensors

- **Question:** A sensor placed under a rug to detect an intruder is a:
- **Answer: Physical Detective Control.**

140. Administrative Control: Exit Interview

- **Question:** Ensuring an employee returns their badge and laptop when they leave is part of:
- **Answer: The Termination Process.**

141. Malware: Spyware

- **Question:** Software that secretly records your keystrokes is:
- **Answer: Spyware (Keylogger).**

142. Network Security: VLANs

- **Question:** Using a switch to create separate logical networks is:
- **Answer: VLAN (Virtual Local Area Network) Tagging.**

143. Access Control: Biometric FRR

- **Question:** FRR stands for:
- **Answer: False Rejection Rate.**

144. Data Security: PII Examples

- **Question:** Which of the following is considered PII?
- **Answer: Social Security Number.**

145. Information Security: Accountability

- **Question:** Being able to prove which user performed an action is:
- **Answer: Accountability.**

146. Social Engineering: Urgency

- **Question:** "Your account will be deleted in 10 minutes unless you click here" uses which tactic?
- **Answer: Urgency.**

147. Risk Management: Residual Risk

- **Question:** The risk that remains after all controls are implemented is:
- **Answer: Residual Risk.**

148. Network Protocols: TCP vs UDP

- **Question:** Which protocol is "connection-oriented"?
- **Answer: TCP.**

149. Physical Security: Bollards

- **Question:** Which device stops a truck from driving through a front door?
- **Answer: Bollards.**

150. Disaster Recovery: BCP vs DRP

- **Question:** Which plan focuses on keeping business operations running *during* a disaster?
- **Answer: Business Continuity Plan (BCP).**

151. Network Defense: Deep Packet Inspection (DPI)

- **Question:** What is the primary difference between a traditional firewall and one using DPI?
- **Answer:** DPI examines the data part (payload) of the packet, not just the header.

152. Access Control: Federation

- **Question:** What allows a user to use a single set of credentials to access applications across different organizations?
- **Answer: Identity Federation.**

153. Security Operations: Vulnerability Assessment

- **Question:** A systematic review of security weaknesses in an information system is a:
- **Answer: Vulnerability Assessment.**

154. Data Security: Data at Rest

- **Question:** Which of the following is the best protection for data stored on a lost laptop?
- **Answer: Full Disk Encryption (FDE).**

155. Physical Security: Infrared Sensors

- **Question:** A sensor that detects a break in a beam of light is a:
- **Answer: Active Infrared Sensor.**

156. Network Security: Evil Twin

- **Question:** A fraudulent Wi-Fi access point that appears to be legitimate is called:
- **Answer: An Evil Twin.**

157. Incident Response: Chain of Custody

- **Question:** To ensure evidence is admissible in court, what must be maintained?
- **Answer: Chain of Custody.**

158. The CIA Triad: Checksums

- **Question:** When downloading a file, the provider gives a SHA-256 string. This helps you verify:
- **Answer: Integrity.**

159. Social Engineering: Spear Phishing

- **Question:** A phishing attack specifically targeted at a high-level executive is:
- **Answer: Whaling.**

160. Administrative Control: Onboarding

- **Question:** Signing an NDA (Non-Disclosure Agreement) typically happens during:
- **Answer: Onboarding.**

161. Network Protocols: Port 22

- **Question:** Which protocol uses Port 22 for secure command-line access?
- **Answer: SSH.**

162. Cloud Security: Multi-Tenancy

- **Question:** The cloud characteristic where multiple customers share the same physical hardware is:
- **Answer: Multi-tenancy.**

163. Access Control: Smart Cards

- **Question:** A smart card contains a microchip. This is an example of:
- **Answer: Something you have.**

164. Risk Management: Inherent Risk

- **Question:** The risk level before any security measures or "treatments" are applied is:
- **Answer: Inherent Risk.**

165. Information Security: Non-Repudiation

- **Question:** Which technology uses a private key to "sign" a message to prove its origin?
- **Answer: Digital Signature.**

166. OSI Model: Layer 4

- **Question:** Which layer is responsible for end-to-end communication and error recovery?
- **Answer: Layer 4 (Transport Layer).**


7 Layers
OSI M

Opens in a new window
Shutterstock

167. Network Security: Zero-Day

- **Question:** An exploit that attacks a flaw for which no patch yet exists is a:
- **Answer: Zero-Day Exploit.**

168. Physical Security: Guard Dogs

- **Question:** Guard dogs are considered which type of security control?
- **Answer: Physical (Deterrent and Detective).**

169. Data Handling: Data Owner vs. Custodian

- **Question:** Who is responsible for the technical environment and daily backups of data?
- **Answer: The Data Custodian.**

170. Governance: Guidelines

- **Question:** Which document provides "best practices" or suggestions that are NOT mandatory?
- **Answer: Guidelines.**

171. Malware: Rootkits

- **Question:** Which malware modifies the operating system kernel to hide its existence?
- **Answer: Rootkit.**

172. Network Protocols: SMTP

- **Question:** Which protocol is used primarily for sending emails?
- **Answer: SMTP (Simple Mail Transfer Protocol).**

173. Access Control: False Acceptance

- **Question:** In biometrics, what is a "Type 2 Error"?
- **Answer: False Acceptance (an intruder is let in).**

174. Disaster Recovery: RPO Calculation

- **Question:** If you back up your data every 24 hours, your RPO is:
- **Answer: 24 Hours.**

175. Security Operations: Penetration Testing

- **Question:** An authorized simulated attack to find and exploit weaknesses is:
- **Answer: Penetration Testing.**

176. The CIA Triad: UPS

- **Question:** An Uninterruptible Power Supply (UPS) supports which goal?
- **Answer: Availability.**

177. Social Engineering: Consensus

- **Question:** "All your coworkers have already upgraded their software; you should too" uses:
- **Answer: Consensus (or Social Proof).**

178. Risk Management: Transference

- **Question:** Hiring a third-party managed security service (MSSP) to handle security is:
- **Answer: Risk Transference (Sharing).**

179. Cryptography: Key Escrow

- **Question:** Storing a copy of an encryption key with a trusted third party is:
- **Answer: Key Escrow.**

180. Network Security: Air Gap

- **Question:** A computer that is physically isolated from all other networks is:
- **Answer: Air-gapped.**

181. Identity Management: Identification

- **Question:** An ID badge is a form of:
- **Answer: Identification.**

182. Physical Security: Locks

- **Question:** A "cipher lock" requires:
- **Answer: A code entered on a keypad.**

183. Access Control: Discretionary (DAC)

- **Question:** Which model is most common in home operating systems like Windows or macOS?
- **Answer: DAC.**

184. Information Security: Principle of Least Privilege

- **Question:** A user should have the minimum access necessary for their job. This is:
- **Answer: Least Privilege.**

185. Network Protocols: Port 80 vs 443

- **Question:** Why is Port 443 preferred over Port 80?
- **Answer: It provides encryption (HTTPS).**

186. Data Handling: Shredding

- **Question:** Why is cross-cut shredding better than strip-cut shredding?
- **Answer: It makes it much harder to reconstruct the document.**

187. Incident Response: Forensic Image

- **Question:** What is a "bit-stream" copy of a hard drive used in investigations?
- **Answer: A Forensic Image.**

188. Security Governance: COBIT

- **Question:** COBIT is a framework primarily used for:
- **Answer: IT Governance and Management.**

189. Malware: Worms

- **Question:** Which malware caused the "Morris" incident by spreading across the internet?
- **Answer: A Worm.**

190. Physical Security: Motion Sensors

- **Question:** A microwave sensor is an example of:
- **Answer: An Active Motion Sensor.**

191. The CIA Triad: Integrity

- **Question:** If a file size changes unexpectedly, which CIA principle has been violated?
- **Answer: Integrity.**

192. Risk Management: Qualitative vs Quantitative

- **Question:** Which method is faster but more subjective?
- **Answer: Qualitative.**

193. Administrative Control: Separation of Duties

- **Question:** "The person who requests a check cannot be the person who signs the check." This is:
- **Answer: Separation of Duties.**

194. Network Security: Firewalls

- **Question:** A "Stateless" firewall filters based on:
- **Answer: Individual packets (Source/Destination IP and Port).**

195. Access Control: Bio-Signatures

- **Question:** Measuring the speed and pressure of a person's handwriting is:
- **Answer: Behavioral Biometrics.**

196. Data Security: Data in Use

- **Question:** Data currently being processed in RAM is:
- **Answer: Data in Use.**

197. Identity Management: Authentication

- **Question:** Verification of a user's claimed identity is:
- **Answer: Authentication.**

198. Disaster Recovery: Cold Site

- **Question:** A site that is just an empty shell with power is:
- **Answer: A Cold Site.**

199. Professional Ethics: Society

- **Question:** "Protect society, the common good, and the infrastructure" is:
- **Answer: The 1st Canon of ISC2.**

200. Incident Response: Detection

- **Question:** Which IR phase involves monitoring logs for suspicious behavior?
- **Answer: Detection and Analysis.**

201. Access Control: Role-Based (RBAC) Logic

- **Question:** In RBAC, what is the relationship between users and permissions?
- **Answer:** Users are assigned to roles, and roles are granted permissions.
- **Explanation:** This simplifies management; when a person's job changes, you simply change their role.

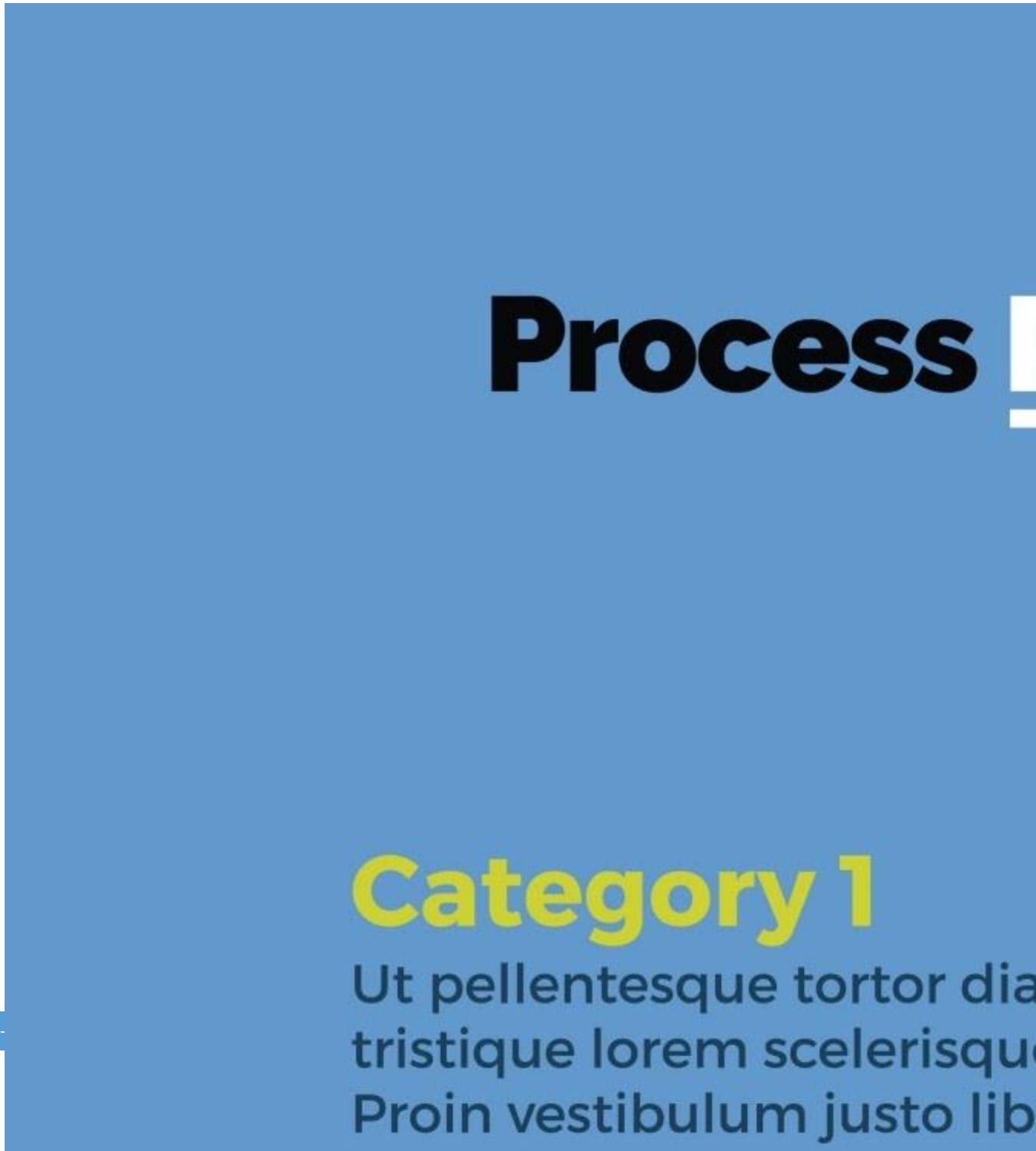
202. The CIA Triad: Impact of Encryption

- **Question:** While encryption provides confidentiality, what is a potential negative impact on availability?
- **Answer:** If the encryption key is lost, the data becomes unavailable.

203. Network Security: Defense in Depth

- **Question:** What is the primary goal of a "Defense in Depth" strategy?
- **Answer:** To provide multiple layers of security so that if one fails, others are in place.

charlie


Process
Category 1
Ut pellentesque tortor dia
tristique lorem scelerisqu
Proin vestibulum justo lib

Opens in a new window
Shutterstock

204. Physical Security: Tailgating vs. Piggybacking

- **Question:** What is the difference between tailgating and piggybacking?
- **Answer:** Tailgating is following without consent; piggybacking is following with the authorized person's consent.

205. Risk Management: Annualized Rate of Occurrence (ARO)

- **Question:** If a fire is expected to happen once every 10 years, what is the ARO?
- **Answer: 0.1** (1 divided by 10).

206. Network Protocols: IPsec

- **Question:** Which protocol suite provides security for IP communications by authenticating and encrypting each IP packet?
- **Answer: IPsec.**

207. Identity Management: Provisioning

- **Question:** The process of removing access rights when an employee leaves is:
- **Answer: De-provisioning.**

208. Data Handling: Data Sanitization (Purging)

- **Question:** Which method of data removal ensures that data cannot be recovered even with laboratory tools?
- **Answer: Purging (or Degaussing for magnetic media).**

209. Access Control: ABAC

- **Question:** Attribute-Based Access Control (ABAC) makes decisions based on:
- **Answer:** User, resource, and environmental attributes (like time or location).

210. Information Security: Accountability

- **Question:** What is the prerequisite for accountability?
- **Answer: Identification and Authentication.** (You cannot hold someone accountable if you don't know who they are).

211. Network Security: Intrusion Prevention System (IPS)

- **Question:** Where should an IPS generally be placed?
- **Answer: In-line** with network traffic (so it can actively block packets).

212. Physical Security: Class C Fire Extinguisher

- **Question:** Which fire extinguisher is used for electrical fires?
- **Answer: Class C.**

213. Cloud Security: Community Cloud

- **Question:** A cloud infrastructure shared by several organizations with similar concerns (e.g., security or compliance) is a:
- **Answer: Community Cloud.**

214. Administrative Control: Background Checks

- **Question:** Background checks should be performed for:
- **Answer:** All employees, including contractors and third-party vendors.

215. Malware: Keyloggers

- **Question:** A keylogger is a specific type of:
- **Answer: Spyware.**

216. Risk Management: Risk Appetite

- **Question:** The amount of risk an organization is willing to accept in pursuit of its objectives is:
- **Answer: Risk Appetite.**

217. Network Protocols: TELNET

- **Question:** Why is TELNET considered insecure?
- **Answer:** It sends all data, including passwords, in **cleartext**.

218. Access Control: Biometric Crossover Error Rate (CER)

- **Question:** What does a lower CER indicate for a biometric system?
- **Answer: Higher accuracy.** (CER is the point where False Rejection and False Acceptance rates meet).

219. Data Security: Tokenization

- **Question:** Replacing sensitive data with a randomly generated unique identifier (token) that has no exploitable value is:
- **Answer: Tokenization.**

220. Incident Response: Preparation Phase

- **Question:** Establishing a "Jump Bag" with forensic tools is part of:
- **Answer: Preparation.**

221. The CIA Triad: Accountability

- **Question:** Which process involves reviewing logs to see what a user did?
- **Answer: Auditing.**

222. Social Engineering: Influence Tactic - Scarcity

- **Question:** "Only 2 spots left for this exclusive offer!" is an example of:
- **Answer: Scarcity.**

223. Network Security: WPA2-AES

- **Question:** WPA2 uses which encryption algorithm by default?
- **Answer: AES (Advanced Encryption Standard).**

224. Physical Security: Perimeter Fencing

- **Question:** A 3-to-4 foot fence is generally used for:
- **Answer: Discriminating between property lines** (not high security).

225. Disaster Recovery: MTBF

- **Question:** What does Mean Time Between Failures (MTBF) measure?
- **Answer:** The average time a system is expected to work before failing.

226. Information Security: Least Privilege

- **Question:** Which principle is violated if an intern has the same access as the IT Manager?
- **Answer: Least Privilege.**

227. Access Control: Smart Card vs. Proximity Card

- **Question:** Which card typically contains an embedded chip for processing?
- **Answer: Smart Card.**

228. Network Protocols: SSH Port

- **Question:** SSH operates on which default port?
- **Answer: 22.**

229. Risk Management: Vulnerability

- **Question:** An unpatched operating system is an example of a:
- **Answer: Vulnerability.**

230. Data Handling: PII (Personally Identifiable Information)

- **Question:** Which of the following is NOT typically considered PII?
- **Answer: Business office address.** (Names, SSNs, and home addresses are PII).

231. Administrative Control: Separation of Duties

- **Question:** Separating the roles of "System Administrator" and "Security Auditor" is:
- **Answer: Separation of Duties.**

232. Network Security: Switch vs. Hub

- **Question:** Which device is more secure because it sends traffic only to the intended recipient's port?
- **Answer: Switch.**

233. Physical Security: Motion Detectors

- **Question:** A motion detector that emits ultrasonic waves and listens for reflections is:
- **Answer: Active Sensor.**

234. Identity Management: Authentication Factors

- **Question:** A PIN is which type of factor?
- **Answer: Something you know.**

235. Cryptography: Non-repudiation

- **Question:** If Bob sends an encrypted email to Alice, what ensures Bob cannot deny sending it?
- **Answer: Bob's Digital Signature.**

236. Professional Ethics: ISC2 Canon 3

- **Question:** Which canon focuses on "providing diligent and competent service to principals"?
- **Answer: Canon 3.**

237. Disaster Recovery: Cold Site

- **Question:** Which of the following is the biggest disadvantage of a cold site?
- **Answer: Recovery time** (it takes a long time to set up).

238. Risk Management: Threats

- **Question:** An earthquake is an example of a:
- **Answer: Natural Threat.**

239. Network Security: OSI Layer 2 Attack

- **Question:** ARP poisoning is an attack at which layer?
- **Answer: Layer 2 (Data Link).**

240. Data Handling: Data Disposal

- **Question:** What is the primary concern when disposing of a hard drive?
- **Answer: Data remanence** (leftover data that can be recovered).

241. Information Security: Availability

- **Question:** High Availability (HA) clusters support which CIA goal?
- **Answer: Availability.**

242. Access Control: Two-Factor (2FA)

- **Question:** Is "Password" and "Security Question" a valid 2FA?
- **Answer: No** (both are "Something you know").

243. Physical Security: Mantraps

- **Question:** A mantrap helps prevent which physical security breach?
- **Answer: Tailgating.**

244. Incident Response: Eradication

- **Question:** Identifying and removing the root cause of an incident happens in:
- **Answer: Eradication.**

245. Social Engineering: Phishing

- **Question:** Sending a broad email to 10,000 people to steal logins is:
- **Answer: Phishing.**

246. Cloud Security: Hybrid Cloud

- **Question:** A company using an on-premise data center and AWS for "burst" capacity is using:
- **Answer: Hybrid Cloud.**

247. Risk Management: Quantitative vs. Qualitative

- **Question:** Which assessment uses a "Risk Matrix"?
- **Answer: Qualitative.**

248. Network Security: DMZ

- **Question:** A web server that needs to be accessed by the public should be in:
- **Answer: The DMZ.**

249. Administrative Control: NDA

- **Question:** What is the legal purpose of a Non-Disclosure Agreement (NDA)?
- **Answer:** To protect the confidentiality of sensitive information.

250. Security Governance: Guidelines

- **Question:** Are guidelines mandatory?
- **Answer: No** (they are recommendations).

251. Administrative Control: Mandatory Vacations

- **Question:** How long should a mandatory vacation be to be effective for fraud detection?
- **Answer: At least one to two weeks.**
- **Explanation:** This ensures enough time for any hidden cycles or fraudulent processes to fail or be noticed by the person covering the role.

252. Network Security: Broadcast Storms

- **Question:** Which device is used to break up broadcast domains to prevent network congestion?
- **Answer: Router.**

253. Incident Response: Order of Volatility

- **Question:** During evidence collection, which of the following should be collected first?
- **Answer: CPU Cache and RAM.**
- **Explanation:** These are the most volatile; once the power is lost, this data disappears.

254. Access Control: Biometric Enrollment

- **Question:** The process of initially scanning a user's biometric data to create a template is:
- **Answer: Enrollment.**

255. Security Principles: Need to Know

- **Question:** Which principle ensures a user has access to specific information, even if they have the general clearance for it?
- **Answer: Need to Know.**

256. Risk Management: SLE Calculation

- **Question:** If an asset is worth $10,000 and the Exposure Factor (EF) is 25%, what is the SLE?
- **Answer: $2,500.** ($10,000 \times 0.25$).

257. Physical Security: Lighting Types

- **Question:** Which type of lighting is used to create a "glare" effect to blind potential intruders?
- **Answer: Fresnel Lights.**

258. Data Handling: Data Processor

- **Question:** Under GDPR, an entity that processes personal data on behalf of a data controller is a:
- **Answer: Data Processor.**

259. Network Protocols: SNMP

- **Question:** Which protocol is used to monitor and manage network devices like routers and switches?
- **Answer: SNMP (Simple Network Management Protocol).**

260. The CIA Triad: Version Control

- **Question:** Using version control (like Git) for source code primarily supports which goal?
- **Answer: Integrity.** (Ensures changes are tracked and can be rolled back).

261. Social Engineering: Influence Tactic - Liking

- **Question:** An attacker finding common interests with a victim to build trust uses:
- **Answer: Liking.**

262. Administrative Control: Separation of Duties

- **Question:** Why should the person who creates a user account not be the one who audits the logs?
- **Answer: To prevent the concealment of unauthorized actions.**

263. Network Security: Stateful Inspection

- **Question:** A firewall that tracks the "handshake" of a connection is using:
- **Answer: Stateful Inspection.**

264. Physical Security: Fail-Safe vs. Fail-Secure

- **Question:** In the event of a fire, an electric door lock should be:
- **Answer: Fail-Safe.** (Unlocks automatically so people can escape).

265. Identity Management: Federation (SAML)

- **Question:** Which XML-based framework is commonly used for exchanging authentication and authorization data?
- **Answer: SAML (Security Assertion Markup Language).**

266. Risk Management: Transferring Risk

- **Question:** Adding a "Hold Harmless" clause to a contract with a vendor is an example of:
- **Answer: Risk Transference.**

267. Information Security: Due Care

- **Question:** Implementing the security controls that any "reasonable person" would implement is:
- **Answer: Due Care.**

268. Data Security: Masking vs. Anonymization

- **Question:** Which process permanently removes the link between data and the individual so it can never be re-identified?
- **Answer: Anonymization.**

269. Network Security: MAC Address

- **Question:** A MAC address is how many bits long?
- **Answer: 48 bits.**

270. Incident Response: Post-Incident Activity

- **Question:** What is the primary goal of the "Lessons Learned" meeting?
- **Answer: To improve future response capabilities.**

271. Access Control: Constrained User Interface

- **Question:** An ATM that only allows you to select "Withdraw" or "Balance" is an example of:
- **Answer: A Constrained User Interface.**

272. Physical Security: Motion Detector - Ultrasonic

- **Question:** An ultrasonic detector works by sensing changes in:
- **Answer: Sound waves/frequency.**

273. Cloud Security: Managed Service Provider (MSP)

- **Question:** A company that manages a customer's IT infrastructure remotely is an:
- **Answer: MSP.**

274. Professional Ethics: Society and Public Trust

- **Question:** If a security professional discovers a major vulnerability in public infrastructure, their first priority (per ISC2) is:
- **Answer: Public safety and the common good.**

275. Disaster Recovery: BIA Metric (RTO)

- **Question:** The amount of time it takes to restore a system after a failure is the:
- **Answer: Recovery Time Objective (RTO).**

276. Malware: Fileless Malware

- **Question:** Malware that resides only in RAM and uses legitimate system tools (like PowerShell) is:
- **Answer: Fileless Malware.**

277. Network Protocols: SSH Security

- **Question:** SSH uses which type of cryptography for the initial key exchange?
- **Answer: Asymmetric (Public Key) Cryptography.**

278. Access Control: Smart Card (Type of factor)

- **Question:** A certificate stored on a USB token is:
- **Answer: Something you have.**

279. Risk Management: Threat Assessment

- **Question:** Identifying potential "Bad Actors" is part of:
- **Answer: Threat Modeling/Assessment.**

280. Data Handling: Data Sovereignty

- **Question:** The concept that data is subject to the laws of the country in which it is physically located is:
- **Answer: Data Sovereignty.**

281. Administrative Control: Least Privilege

- **Question:** When an employee is promoted, their old permissions should be:

- **Answer: Revoked immediately.**

282. Network Security: SIEM - Correlation

- **Question:** What SIEM function connects multiple separate events to identify a single attack?
- **Answer: Correlation.**

283. Physical Security: CCD vs. CMOS

- **Question:** These terms refer to the sensors used in:
- **Answer: CCTV Cameras.**

284. Identity Management: Identification

- **Question:** Why should usernames be unique?
- **Answer: To ensure accountability.**

285. Information Security: The CIA Triad - Availability

- **Question:** RAID 1 (Mirroring) supports which goal?
- **Answer: Availability.**

286. Social Engineering: Watering Hole Attack

- **Question:** An attacker compromising a website frequently visited by employees of a target company is:
- **Answer: A Watering Hole attack.**

287. Risk Management: Inherent vs. Residual Risk

- **Question:** Inherent Risk minus the impact of Controls equals:
- **Answer: Residual Risk.**

288. Network Security: Defense in Depth (Example)

- **Question:** Using a firewall, an IDS, and antivirus on the same network is:
- **Answer: Layered Security (Defense in Depth).**

289. Access Control: Single Sign-On (Disadvantage)

- **Question:** What is the primary security risk of SSO?
- **Answer: Single Point of Failure** (if the account is compromised, all systems are accessible).

290. Data Handling: Clearing vs. Purging

- **Question:** Which one allows the media to be reused within the same organization?
- **Answer: Clearing.**

291. Physical Security: Perimeter Security - Bollards

- **Question:** Bollards are specifically designed to stop:
- **Answer: Vehicle-borne attacks.**

292. Incident Response: Containment (Isolation)

- **Question:** Putting a suspect's laptop in a "Faraday Bag" is a form of:
- **Answer: Isolation/Containment.**

293. Social Engineering: Influence Tactic - Social Proof

- **Question:** This tactic is also known as:
- **Answer: Consensus.**

294. Risk Management: Qualitative Risk Matrix

- **Question:** A 5x5 grid used to map Likelihood and Impact is:
- **Answer: A Risk Matrix.**

295. Network Security: Port 23

- **Question:** Why should Port 23 be closed on all production servers?
- **Answer: It is used by Telnet, which is unencrypted.**

296. Identity Management: Biometric FRR

- **Question:** A "Type 1 Error" is also called:
- **Answer: False Rejection Rate.**

297. Data Handling: PII (Protected Health Information)

- **Question:** HIPAA specifically protects which type of data?
- **Answer: PHI.**

298. Information Security: Non-Repudiation

- **Question:** Proof of origin and proof of delivery are components of:
- **Answer: Non-repudiation.**

299. Administrative Control: Security Policy

- **Question:** Who should sign the organization's high-level security policy?
- **Answer: Senior Management (e.g., CEO or CISO).**

300. Security Operations: Change Management

- **Question:** What is the primary goal of Change Management?
- **Answer: To ensure that changes do not cause unintended outages or security gaps.**

301. Network Security: Defense in Depth (Philosophy)

- **Question:** Which principle suggests that security should not rely on a single defensive mechanism?
- **Answer: Layered Security.**

302. Wireless Security: SSID Hiding

- **Question:** Does hiding the SSID provide strong security for a wireless network?
- **Answer: No, it is security by obscurity.** (Attackers can still find the network using sniffers).

303. Incident Response: Analysis Phase

- **Question:** Determining the "scope" of an incident (which systems are affected) happens in which phase?
- **Answer: Detection and Analysis.**

304. Access Control: Context-Aware Access

- **Question:** Access based on the time of day, the device being used, and the user's location is called:
- **Answer: Context-Aware Access Control.**

305. Data Security: Data in Transit (Encryption)

- **Question:** Which protocol is the modern standard for encrypting web traffic?
- **Answer: TLS (Transport Layer Security).**
- **Explanation:** SSL is considered deprecated and insecure; TLS 1.2 or 1.3 should be used.

306. Risk Management: Annualized Loss Expectancy (ALE)

- **Question:** If the SLE is $5,000 and the ARO is 2 (twice a year), what is the ALE?
- **Answer: $10,000.** ($5,000 \times 2$).

307. Physical Security: Fire Classes

- **Question:** A fire involving common combustibles like wood or paper is:
- **Answer: Class A.**

308. Network Protocols: FTP vs. SFTP

- **Question:** Why is SFTP preferred over FTP?
- **Answer: SFTP encrypts both data and credentials.** (FTP sends them in cleartext).

309. Administrative Control: Separation of Duties (Example)

- **Question:** Why is it a risk for a system administrator to also be the security auditor?
- **Answer: They could modify logs to hide their own unauthorized actions.**

310. Information Security: The CIA Triad - Confidentiality

- **Question:** "Shoulder surfing" is a direct threat to:
- **Answer: Confidentiality.**

311. Access Control: Federated Identity (Roles)

- **Question:** In a federated environment, the entity that provides the "vouch" for a user's identity is the:
- **Answer: Identity Provider (IdP).**

312. Physical Security: Gate Sensors

- **Question:** A sensor that triggers when a circuit is broken by a door opening is a:
- **Answer: Electromagnetic Switch (Contact Sensor).**

313. Disaster Recovery: Data Restoration

- **Question:** In what order should systems be restored after a disaster?
- **Answer: Mission-critical systems first.**

314. Network Security: Network Address Translation (NAT)

- **Question:** What is a secondary security benefit of using NAT?
- **Answer: It hides internal IP addresses from the external network.**

315. Malware: Logic Bombs (Detection)

- **Question:** What is the best way to detect a logic bomb before it "explodes"?
- **Answer: Code review and integrity checking.**

316. Identity Management: Biometric System (Throughput)

- **Question:** The rate at which a biometric system can process users is called:
- **Answer: Throughput Rate.**

317. Risk Management: Countermeasures

- **Question:** A safeguard or countermeasure is implemented to reduce:
- **Answer: Risk.**

318. Data Handling: Media Destruction

- **Question:** "Degaussing" is effective for which type of media?
- **Answer: Magnetic media (Hard drives, Tapes).**

319. Network Protocols: SSH Port

- **Question:** SSH (Secure Shell) uses which port by default?
- **Answer: 22.**

320. Information Security: Least Privilege (Application)

- **Question:** An application should only have the permissions it needs to run. This is called:
- **Answer: Principle of Least Privilege.**

321. Administrative Control: Security Awareness

- **Question:** What is the primary goal of security awareness training?
- **Answer: To change user behavior and reduce human risk.**

322. Physical Security: Biometrics (FAR vs FRR)

- **Question:** Which error rate is more dangerous from a security perspective?
- **Answer: False Acceptance Rate (FAR).** (It lets the "bad guy" in).

323. Network Security: Intrusion Detection System (Signature-based)

- **Question:** An IDS that looks for a specific string of bytes known to be in a virus is using:
- **Answer: Signature-based detection.**

324. Access Control: Attribute-Based Access Control (ABAC)

- **Question:** In ABAC, the "environment" attribute could include:
- **Answer: Current time or the IP address of the user.**

325. OSI Model: Layer 7

- **Question:** At which layer do HTTP, FTP, and SMTP operate?
- **Answer: Layer 7 (Application Layer).**

326. Social Engineering: Pretexting

- **Question:** An attacker calling an employee and pretending to be from the IT help desk is:
- **Answer: Pretexting.**

327. Risk Management: Transference (Insurance)

- **Question:** Does cyber insurance remove the risk?
- **Answer: No, it transfers the financial impact of the risk.**

328. Incident Response: Preparation (Documentation)

- **Question:** Which document defines the steps to be taken during an incident?
- **Answer: Incident Response Plan (IRP).**

329. Physical Security: Perimeter Security (Infrared)

- **Question:** A "photoelectric" sensor uses:
- **Answer: A light beam.**

330. Identity Management: Multi-Factor Authentication (MFA)

- **Question:** A "push notification" to a mobile app is which factor?
- **Answer: Something you have.**

331. Data Handling: Data Custodian

- **Question:** Who is responsible for implementing the security controls defined by the Data Owner?
- **Answer: The Data Custodian.**

332. Network Security: Switch (VLANs)

- **Question:** VLANs are used to segment a network at which OSI layer?
- **Answer: Layer 2.**

333. Information Security: Accountability (Logging)

- **Question:** Audit logs should be protected from:
- **Answer: Unauthorized modification or deletion.**

334. Professional Ethics: Competence

- **Question:** "Provide diligent and competent service to principals" is part of:
- **Answer: ISC2 Canon 3.**

335. Disaster Recovery: Recovery Point Objective (RPO)

- **Question:** RPO describes the maximum allowable:
- **Answer: Data loss.**

336. Malware: Ransomware (Prevention)

- **Question:** What is the single most effective defense against the impact of ransomware?
- **Answer: Offline/Immutable Backups.**

337. Network Protocols: IPv4 vs IPv6

- **Question:** Which version of IP was developed to address the shortage of addresses?
- **Answer: IPv6.**

338. Access Control: Discretionary Access Control (DAC)

- **Question:** In DAC, who has the "discretion" to grant access?
- **Answer: The owner of the object.**

339. Risk Management: Residual Risk

- **Question:** Can residual risk ever be zero?
- **Answer: No.** (There is always some level of risk remaining).

340. Data Handling: Privacy (GDPR)

- **Question:** Under GDPR, the "Right to be Forgotten" is formally known as:
- **Answer: Right to Erasure.**

341. Administrative Control: Mandatory Vacations

- **Question:** Why does a mandatory vacation require someone else to perform the employee's duties?
- **Answer: To ensure any irregularities are discovered by the replacement.**

342. Physical Security: Mantrap (Interlocks)

- **Question:** If the first door of a mantrap is open, the second door must be:
- **Answer: Locked.**

343. Incident Response: Containment (Purpose)

- **Question:** What is the primary purpose of the containment phase?
- **Answer: To prevent the damage from spreading.**

344. Social Engineering: Authority

- **Question:** "I'm the CEO's assistant, and he needs this password now" uses:
- **Answer: Authority and Urgency.**

345. Cloud Security: Cloud Security Alliance (CSA)

- **Question:** The tool used to assess cloud providers' security controls is the:
- **Answer: CAIQ (Consensus Assessments Initiative Questionnaire).**

346. Network Security: Firewall (Rules)

- **Question:** Firewalls use an "Implicit Deny" rule at the:
- **Answer: End of the rule set.**

347. Access Control: Biometric (Enrollment Error)

- **Question:** If a user's fingerprint is too faint to be recorded, it is a:
- **Answer: Failure to Enroll (FTE).**

348. Information Security: Non-Repudiation (Hashing)

- **Question:** Does hashing alone provide non-repudiation?
- **Answer: No.** (It only provides integrity).

349. Risk Management: Threat x Vulnerability

- **Question:** Threat multiplied by Vulnerability equals:
- **Answer: Risk.**

350. Disaster Recovery: Business Impact Analysis (BIA)

- **Question:** The BIA is a part of which larger plan?
- **Answer: Business Continuity Plan (BCP).**

351. Network Security: Port Scanning

- **Question:** What is the primary purpose of a port scan?
- **Answer:** To identify open ports and services running on a host.

352. The CIA Triad: Destruction

- **Question:** A successful ransomware attack that encrypts all company backups primarily impacts:
- **Answer: Availability.**

353. Access Control: Separation of Duties (Logic)

- **Question:** Which control prevents a single person from having enough power to defraud an organization?
- **Answer: Separation of Duties.**

354. Incident Response: Chain of Custody (Start)

- **Question:** When does the "Chain of Custody" begin?
- **Answer: At the moment the evidence is first collected.**

355. Network Security: Honeynet

- **Question:** A network consisting of multiple honeypots is called a:
- **Answer: Honeynet.**

356. Physical Security: Lighting (Detective)

- **Question:** How does lighting act as a "detective" control?

- **Answer:** By allowing security guards or cameras to see an intruder.

357. Risk Management: Exposure Factor (EF)

- **Question:** If a flood would destroy 50% of a warehouse's value, the EF is:
- **Answer: 0.5 (or 50%).**

358. Data Handling: Data Minimization

- **Question:** The practice of only collecting the personal data that is strictly necessary is:
- **Answer: Data Minimization.**

359. Network Protocols: HTTPS (Handshake)

- **Question:** During an HTTPS handshake, what does the server send to the client to prove its identity?
- **Answer: A Digital Certificate.**

360. Administrative Control: Background Checks (Re-screening)

- **Question:** When should background checks be repeated?
- **Answer: Periodically or when an employee is promoted to a sensitive role.**

361. Access Control: Discretionary (DAC) (Inheritance)

- **Question:** In DAC, if a user creates a folder, they are the owner and "inherit" full control. This is known as:
- **Answer: Ownership-based access.**

362. Information Security: Defense in Depth (Technical layer)

- **Question:** Which of the following is a "Technical" layer in defense in depth?
- **Answer: An Intrusion Prevention System (IPS).**

363. Physical Security: Bollards (Purpose)

- **Question:** What is the primary reason for installing "K-rated" bollards?
- **Answer: To stop high-speed vehicle impacts.**

364. Disaster Recovery: MTTR

- **Question:** What does "Mean Time to Repair" (MTTR) measure?
- **Answer:** The average time it takes to fix a failed system.

365. Identity Management: Identification (Unique IDs)

- **Question:** Why should "Shared Accounts" (like `admin` or `guest`) be avoided?
- **Answer: They prevent accountability.**

366. Risk Management: Quantitative (Formula)

- **Question:** $Asset Value \times Exposure Factor =$?
- **Answer: SLE (Single Loss Expectancy).**

367. Network Security: Wireless (WPA3 Advantage)

- **Question:** What is a major security improvement in WPA3 over WPA2?
- **Answer: Protection against offline dictionary attacks.**

368. Data Handling: PII (Exclusion)

- **Question:** Is a person's public social media handle (e.g., @user123) always considered sensitive PII?
- **Answer: No, it is generally considered public information unless linked to private data.**

369. Information Security: Non-Repudiation (Third Party)

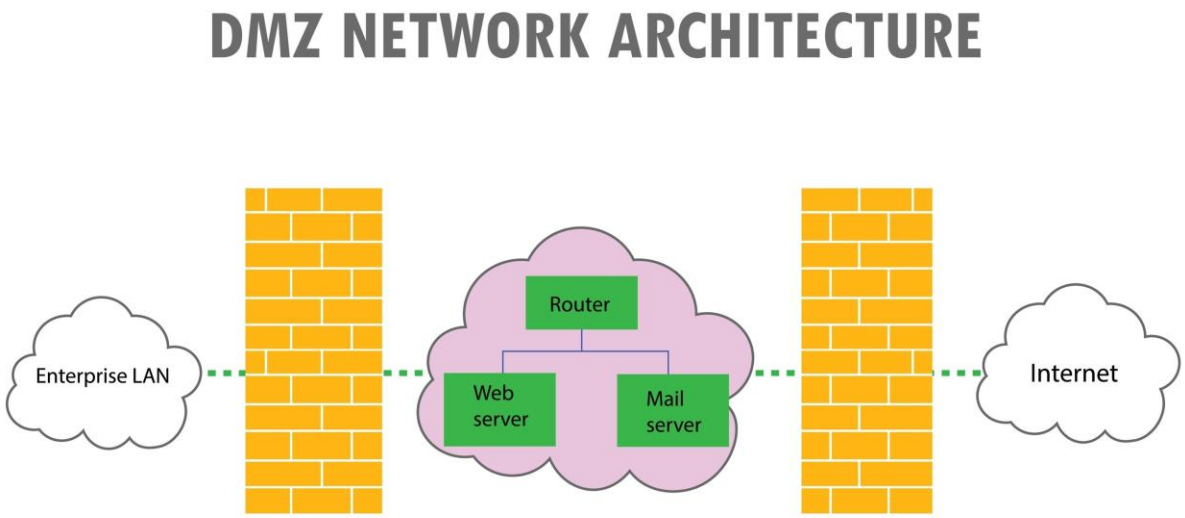
- **Question:** What can a CA (Certificate Authority) provide to support non-repudiation?
- **Answer: Verification of the public key's owner.**

370. Administrative Control: Policies (Hierarchy)

- **Question:** Which is at the top of the security documentation hierarchy?
- **Answer: Policy.**

371. Network Security: DMZ (Traffic Flow)

- **Question:** Traffic from the internet should be allowed into the DMZ but never:
- **Answer: Directly into the internal private network.**



Opens in a new window
Shutterstock

372. Malware: Spyware (Keyloggers)

- **Question:** What is the best defense against hardware-based keyloggers?

- **Answer: Physical inspections of computer ports.**

373. Access Control: Mandatory (MAC) (Labels)

- **Question:** In MAC, what is the label attached to a piece of data called?
- **Answer: Sensitivity Label.**

374. The CIA Triad: Availability (Redundancy)

- **Question:** Using two different internet service providers (ISPs) for a data center is:
- **Answer: ISP Redundancy.**

375. Incident Response: Post-Incident (Retention)

- **Question:** How long should incident evidence be kept?
- **Answer: According to the organization's retention policy or legal requirements.**

376. Social Engineering: Influence Tactic (Commitment)

- **Question:** An attacker getting a victim to agree to a small, easy request before asking for a big one uses:
- **Answer: Commitment (or Foot-in-the-door).**

377. Risk Management: Acceptance (Criteria)

- **Question:** Risk acceptance is only appropriate if:
- **Answer: The cost of mitigation exceeds the potential loss.**

378. Physical Security: Sensors (Vibration)

- **Question:** Which sensor is best for detecting someone trying to cut through a metal fence?
- **Answer: Vibration Sensor.**

379. Network Protocols: TCP (Three-way Handshake)

- **Question:** What are the three steps of the TCP handshake?
- **Answer: SYN, SYN-ACK, ACK.**

380. Information Security: Least Privilege (User)

- **Question:** Granting an employee "Full Admin" rights because it's "easier" is a violation of:
- **Answer: Least Privilege.**

381. Administrative Control: Awareness (Metrics)

- **Question:** How do you measure the effectiveness of a phishing awareness program?
- **Answer: By the "Click Rate" on simulated phishing emails.**

382. Cloud Security: Shared Responsibility (PaaS)

- **Question:** In PaaS, the provider is responsible for the:
- **Answer: Operating System and Runtime.**

383. Access Control: Smart Cards (Contactless)

- **Question:** A "Prox Card" that you wave near a reader uses:
- **Answer: RFID (Radio Frequency Identification).**

384. Disaster Recovery: BCP (Testing)

- **Question:** A "Tabletop Exercise" is a type of:
- **Answer: BCP/DRP Test.**

385. Professional Ethics: Canon 4 (Mentor)

- **Question:** Helping a junior colleague study for a security certification follows:
- **Answer: Canon 4 (Advance and protect the profession).**

386. Network Security: Firewall (Egress filtering)

- **Question:** Filtering traffic *leaving* the network is called:
- **Answer: Egress Filtering.**

387. Data Handling: Sanitization (Overwriting)

- **Question:** Overwriting a hard drive with zeros is a form of:
- **Answer: Clearing.**

388. Information Security: Integrity (Controls)

- **Question:** Which of the following is an integrity control?
- **Answer: File Hashing.**

389. Risk Management: Threat (Insider)

- **Question:** A disgruntled employee stealing data is a:
- **Answer: Malicious Insider Threat.**

390. Physical Security: Locks (Master Key)

- **Question:** A key that opens all locks in a building is a:
- **Answer: Master Key.** (Presents a high security risk if lost).

391. The CIA Triad: Confidentiality (Snooping)

- **Question:** Encryption protects data confidentiality by making it:
- **Answer: Unreadable to unauthorized parties.**

392. Access Control: SSO (Standard)

- **Question:** OAuth 2.0 is primarily used for:
- **Answer: Authorization** (allowing one app to access data in another).

393. Incident Response: Containment (System State)

- **Question:** Should you always turn off a computer as soon as you find malware?
- **Answer: No, you might lose evidence in RAM.**

394. Social Engineering: Influence Tactic (Trust)

- **Question:** An attacker spending weeks building a friendship with a target is:
- **Answer: Liking and Trust-building.**

395. Risk Management: Vulnerability (Scanning)

- **Question:** A "Credentialed Scan" provides:
- **Answer: More detail than a non-credentialed scan.**

396. Network Security: VPN (Split Tunneling)

- **Question:** When only some traffic goes through the VPN and some goes directly to the internet, it is:
- **Answer: Split Tunneling.**

397. Identity Management: Biometrics (Template)

- **Question:** What is stored in the database for biometric comparison?
- **Answer: A mathematical template (not the actual image).**

398. Data Handling: Data Life Cycle (Creation)

- **Question:** At which stage of the data life cycle should classification occur?
- **Answer: Creation (or Collection).**

399. Professional Ethics: Canon 2 (Legal)

- **Question:** Following all local privacy laws is a requirement of:
- **Answer: Canon 2 (Act honorably, honestly, justly, responsibly, and legally).**

400. Final Review: Security Mindset

- **Question:** What is the ultimate goal of an information security program?
- **Answer: To manage risk to an acceptable level for the organization.**