Security + 701

Section one : General Security Concepts

1. **Which of the following is considered a technical security control?**
   a) Firewall
   b) Security policy
   c) Security awareness training
   d) CCTV surveillance
   Answer: A firewall
2. **Which of the following best describes a managerial security control?**
   a) Encryption algorithms
   b) Security policies and risk assessments
   c) Intrusion detection systems
   d) Badge readers
   Answer: Security policies and risk assessments
3. **Which security category focuses on day-to-day procedures and processes to maintain security?**
   a) Managerial
   b) Operational
   c) Technical
   d) Physical
   Answer: Operational
4. **Which of the following security categories involves measures such as fences, security guards, and locks?**
   a) Operational
   b) Technical
   c) Physical
   d) Managerial
   Answer: Physical
5. **Which type of control is designed to stop a security incident before it happens?**
   a) Detective
   b) Corrective
   c) Preventative
   d) Compensating
   Answer: Preventative
6. **Which type of security control is designed to discourage an attacker from attempting malicious actions?**
   a) Detective
   b) Deterrent
   c) Corrective

d) Directive

Answer: Deterrent

7. **Which security control type is used to identify and record security incidents?**
   a) Preventative
   b) Detective
   c) Compensating
   d) Directive
   Answer: Detective
8. **Which type of control is implemented to restore a system or process after an incident?**
   a) Corrective
   b) Deterrent
   c) Preventative
   d) Detective
   Answer: Corrective
9. **Which control type is used as an alternative when the primary security control is not feasible?**
   a) Detective
   b) Compensating
   c) Preventative
   d) Corrective
   Answer: Compensating
10. **Which control type provides guidance on security requirements and procedures?**
    a) Directive
    b) Compensating
    c) Preventative
    d) Deterrent
    Answer: Directive
11. **Which principle of the CIA Triad ensures that information is only accessible to authorized users?**
    a) Availability
    b) Confidentiality
    c) Integrity
    d) Non-repudiation
    Answer: Confidentiality
12. **Which security principle ensures that a user cannot deny taking an action, such as sending an email or making a transaction?**
    a) Non-repudiation
    b) Integrity
    c) Authentication
    d) Authorization
    Answer: Non-repudiation

13. **Which of the following is a key function of authentication in the AAA model?**
    a) Enforcing access policies
    b) Tracking user activity
    c) Encrypting stored data
    d) Verifying a user's identity
    Answer: Verifying a user's identity
14. **Which method is commonly used to authenticate systems rather than users?**
    a) Biometric authentication
    b) Digital certificates
    c) Multifactor authentication
    d) Security questions
    Answer: Digital certificates
15. **Which authorization model grants access based on predefined roles assigned to users?**
    a) Mandatory Access Control
    b) Discretionary Access Control
    c) Role-based Access Control
    d) Rule-based Access Control
    Answer: Role-based Access Control
16. **What is the primary purpose of Gap analysis in cyber security?**
    a) To evaluate and compare current security posture against desired security standards
    b) To encrypt sensitive data in transit
    c) To monitor network traffic for anomalies
    d) To detect and prevent unauthorized access attempts
    Answer: To evaluate and compare current security posture against desired security standards
17. **Which principle of Zero Trust focuses on verifying user identities dynamically based on risk factors?**
    a) Policy-driven Access Control
    b) Threat scope reduction
    c) Adaptive Identity
    d) Policy administrator
    Answer: Adaptive Identity
18. **In Zero Trust architecture, what does threat scope reduction aim to achieve?**
    a) Minimizing the attack surface by restricting lateral movement within the network
    b) Enforcing least privilege access control policies
    c) Implementing multifactor authentication for all users
    d) Auditing user access logs for anomalies
    Answer: Minimizing the attack surface by restricting lateral movement within the network
19. **Which Zero Trust concept ensures access decisions are enforced based on predefined security policies?**
    a) Threat scope reduction
    b) Adaptive Identity

c) Zero Trust control plane
d) Policy-driven Access Control
Answer: Policy-driven Access Control

20. **In the Zero Trust model, what is the role of the policy administrator?**
a) To define and enforce security policies based on contextual data
b) To monitor all network traffic for threats
c) To authenticate users before granting access to resources
d) To encrypt all network communication
Answer: To define and enforce security policies based on contextual data

21. **In a Zero Trust architecture, what is the role of the policy engine in the data plane?**
a) To enforce access controls at network endpoints
b) To monitor network traffic for anomalies
c) To encrypt data in transit
d) To authenticate and authorize access requests based on security policies
Answer: To authenticate and authorize access requests based on security policies

22. **Which term refers to a security zone that assumes all users and devices are potentially untrusted?**
a) Policy enforcement point
b) Implicit trust zones
c) Policy engine
d) Data plane
Answer: Implicit trust zones

23. **In the data plane of Zero Trust architecture, what is a subject system?**
a) An entity such as a user or device requesting access to a resource
b) A tool used to enforce access policies
c) A mechanism for analyzing security events
d) A database that stores access control rules
Answer: An entity such as a user or device requesting access to a resource

24. **What component in Zero Trust architecture is responsible for enforcing security decisions at the resource level?**
a) Policy engine
b) Data plane
c) Policy enforcement point
d) Implicit trust zone
Answer: Policy enforcement point

25. **Which physical security measure is designed to prevent vehicle-based attacks on buildings and pedestrian areas?**
a) Bollards
b) Access control
c) Vestibule
d) Fencing
Answer: Bollards

26. **Which type of sensor detects heat signatures for security monitoring?**
    a) Microwave sensor
    b) Infrared sensor
    c) Pressure sensor
    d) Ultrasonic sensor
    Answer: Infrared sensor
27. **Which security measure is commonly used to detect unauthorized access attempts in high security areas?**
    a) Microwave sensors
    b) Pressure sensors
    c) Infrared cameras
    d) Video surveillance
    Answer: Pressure sensors
28. **Which type of deception technology is designed to attract attackers by simulating a vulnerable system?**
    a) Honey file
    b) Honey net
    c) Honey pot
    d) Honey token
    Answer: Honey pot
29. **Which deception tool consists of a network of decoy systems to detect unauthorized access attempts?**
    a) Honey file
    b) Honey pot
    c) Honey net
    d) Honey token
    Answer: Honey net
30. **What is the purpose of a honey token in cyber security?**
    a) To mimic a vulnerable system and attract attackers
    b) To serve as a fake credential or data entry to detect unauthorized access
    c) To create a network of decoy systems
    d) To encrypt stored files and prevent unauthorized modifications
    Answer: To serve as a fake credential or data entry to detect unauthorized access
31. **Which business process ensures that security-related changes receive proper authorization before implementation?**
    a) Approval process
    b) Standard operating procedure
    c) Maintenance window
    d) Impact analysis
    Answer: Approval process
32. **In security operations, which concept refers to the individual or entity responsible for a system or data asset?**
    a) Impact analysis

b) Ownership
c) Approval process
d) Backout plan
Answer: Ownership

33. **Which term refers to individuals or groups who have an interest in security decisions and outcomes?**
a) Backout plan
b) Stakeholders
c) Standard operating procedure
d) Approval process
Answer: Stakeholders

34. **Which process is used to evaluate potential security risks and their effects on business operations?**
a) Impact analysis
b) Test results
c) Ownership
d) Maintenance window
Answer: Impact analysis

35. **Why are test results important in security operations?**
a) They define security roles and responsibilities
b) They determine the required level of stakeholder involvement
c) They schedule maintenance windows for system updates
d) They provide evidence of system vulnerabilities and effectiveness of security measures
Answer: They provide evidence of system vulnerabilities and effectiveness of security measures

36. **What is the purpose of a backout plan in security operations?**
a) To provide a documented procedure for reverting changes if an issue occurs
b) To determine the impact of a security incident
c) To manage stakeholder expectations during security updates
d) To define who has ownership over a security process
Answer: To provide a documented procedure for reverting changes if an issue occurs

37. **Which business process involves scheduling security updates and changes to minimize operational disruption?**
a) Impact analysis
b) Standard operating procedure
c) Maintenance window
d) Test results
Answer: Maintenance window

38. **Which document provides step-by-step guidance on performing security-related tasks consistently?**
a) Standard operating procedure
b) Stakeholder agreement

c) Impact analysis report
d) Approval process documentation
Answer: Standard operating procedure

39. **Which security measure controls which applications, websites, or services can be accessed on a network?**
a) Legacy applications
b) Service restart
c) Allow lists or deny lists
d) Dependencies
Answer: Allow lists or deny lists

40. **What is the primary purpose of restricting certain activities on a corporate network?**
a) To improve employee productivity
b) To enhance security by preventing unauthorized or harmful actions
c) To reduce software licensing costs
d) To enforce compliance with software update schedules
Answer: To enhance security by preventing unauthorized or harmful actions

41. **Which of the following is a potential security risk when using legacy applications?**
a) They often lack support for modern security updates and patches
b) They require additional server capacity
c) They do not support multiple user authentication methods
d) They automatically update without administrator approval
Answer: They often lack support for modern security updates and patches

42. **What is a key technical implication of downtime in an enterprise environment?**
a) Reduced network latency
b) Increased risk of service disruptions and security vulnerabilities
c) Enhanced system performance
d) Automatic failover to legacy applications
Answer: Increased risk of service disruptions and security vulnerabilities

43. **Why is it important to restart a service after applying security patches?**
a) To finalize the installation and ensure the updates take effect
b) To reset user access permissions
c) To automatically update firewall rules
d) To remove inactive user accounts
Answer: To finalize the installation and ensure the updates take effect

44. **Which of the following is a reason to update network diagrams regularly?**
a) To improve the performance of outdated software
b) To comply with software licensing agreements
c) To reflect changes in the infrastructure and ensure accurate security planning
d) To optimize database indexing
Answer: To reflect changes in the infrastructure and ensure accurate security planning

45. **Why is it necessary to update security policies and procedures?**
a) To improve application performance

b) To automate the patch management process

c) To ensure they reflect new threats, technologies, and compliance requirements

d) To enhance encryption algorithms

Answer: To ensure they reflect new threats, technologies, and compliance requirements

46. **What is the primary benefit of using version control in security documentation?**

a) It tracks changes over time and allows rollback to previous versions if needed

b) It automatically enforces user authentication policies

c) It provides real-time network monitoring capabilities

d) It restricts users from modifying security configurations

Answer: It tracks changes over time and allows rollback to previous versions if needed

47. **Which component of cybersecurity provides a framework for managing digital certificates and encryption keys?**

a) Key escrow

b) Encryption

c) Private key

d) Public key infrastructure

Answer: Public key infrastructure

48. **What is the function of a public key in asymmetric encryption?**

a) Encrypts data that can only be decrypted by the corresponding private key

b) Decrypts data encrypted with the same public key

c) Manages the storage of encryption keys

d) Ensures data remains unchanged during transmission

Answer: Encrypts data that can only be decrypted by the corresponding private key

49. **Which of the following is a characteristic of a private key in asymmetric encryption?**

a) It is shared publicly to allow data encryption

b) It can be used to verify digital signatures only

c) It is kept secret and used to decrypt messages encrypted with the public key

d) It is stored in a key escrow for public access

Answer: It is kept secret and used to decrypt messages encrypted with the public key

50. **What is the purpose of key escrow in encryption?**

a) To generate encryption keys for data encryption

b) To store encryption keys securely for retrieval by authorized parties

c) To distribute public keys among users

d) To prevent unauthorized encryption of sensitive data

Answer: To store encryption keys securely for retrieval by authorized parties

51. **What is the primary function of encryption in cybersecurity?**

a) To convert data into an unreadable format to protect confidentiality

b) To restrict access to files on a system

c) To create digital signatures for authentication

d) To detect unauthorized modifications to data

Answer: To convert data into an unreadable format to protect confidentiality

52. **Which term refers to the scope at which encryption is applied to a system or storage device?**
    a) Partition
    b) Key escrow
    c) Public key infrastructure
    d) Level
    Answer: Level
53. **Which type of encryption ensures that an entire hard drive's data is protected?**
    a) Full disk encryption
    b) File encryption
    c) Partition encryption
    d) Public key encryption
    Answer: Full disk encryption
54. **What type of encryption protects a specific section of a storage device instead of the entire disk?**
    a) Full disk encryption
    b) Public key encryption
    c) Partition encryption
    d) Key escrow encryption
    Answer: Partition encryption
55. **Which type of encryption protects individual documents without encrypting the entire system?**
    a) File encryption
    b) Full disk encryption
    c) Partition encryption
    d) Key escrow encryption
    Answer: File encryption
56. **Which encryption method is used to secure an entire storage unit, such as a disk or logical volume?**
    a) Database encryption
    b) Volume encryption
    c) Record encryption
    d) Symmetric encryption
    Answer: Volume encryption
57. **Which security measure ensures that sensitive data stored in a database remains encrypted?**
    a) Record encryption
    b) Transport encryption
    c) Key exchange
    d) Database encryption
    Answer: Database encryption
58. **Which type of encryption protects individual entries within a database?**
    a) Volume encryption

b) Key exchange encryption
c) Record encryption
d) Symmetric encryption
Answer: Record encryption

59. **Which type of encryption secures data as it moves across a network?**
a) Transport encryption
b) Database encryption
c) Volume encryption
d) Asymmetric encryption
Answer: Transport encryption

60. **Which encryption type uses a pair of keys, one for encryption and one for decryption?**
a) Symmetric encryption
b) Volume encryption
c) Asymmetric encryption
d) Record encryption
Answer: Asymmetric encryption

61. **Which encryption method uses the same key for both encryption and decryption?**
a) Symmetric encryption
b) Asymmetric encryption
c) Key exchange encryption
d) Transport encryption
Answer: Symmetric encryption

62. **What is the purpose of key exchange in encryption?**
a) To generate random encryption keys
b) To store encryption keys in a database
c) To encrypt sensitive data using a shared key
d) To securely share encryption keys between parties
Answer: To securely share encryption keys between parties

63. **Which component of encryption defines the mathematical process used to encrypt and decrypt data?**
a) Encryption algorithm
b) Key exchange
c) Symmetric key
d) Asymmetric key
Answer: Encryption algorithm

64. **What factor in encryption determines the strength of a cryptographic key?**
a) Algorithm type
b) Encryption mode
c) Key length
d) Transport protocol
Answer: Key length

65. **Which security feature is a dedicated chip that provides cryptographic functions such as key storage and secure boot?**
    a) Trusted platform module
    b) Hardware security module
    c) Key management system
    d) Secure enclave
    Answer: Trusted platform module
66. **Which device is specifically designed to manage and protect cryptographic keys in high-security environments?**
    a) Trusted platform module
    b) Secure enclave
    c) Hardware security module
    d) Key exchange protocol
    Answer: Hardware security module
67. **What is the main purpose of a Key Management System (KMS) in cryptographic security?**
    a) To securely generate, store, distribute, and retire encryption keys
    b) To encrypt data at rest and in transit
    c) To store cryptographic keys in a hardware security module
    d) To ensure hardware-based authentication
    Answer: To securely generate, store, distribute, and retire encryption keys
68. **Which security feature creates an isolated execution environment within a processor to protect sensitive data?**
    a) Hardware security module
    b) Key management system
    c) Trusted platform module
    d) Secure enclave
    Answer: Secure enclave
69. **Which technique involves deliberately making source code difficult to read and understand to enhance security?**
    a) Steganography
    b) Obfuscation
    c) Tokenization
    d) Encryption
    Answer: Obfuscation
70. **Which data-hiding technique involves embedding hidden information within an image or audio file?**
    a) Obfuscation
    b) Tokenization
    c) Steganography
    d) Hashing
    Answer: Steganography

71. **Which security method replaces sensitive data with a non-sensitive equivalent, reducing the risk of exposure?**
    a) Tokenization
    b) Steganography
    c) Obfuscation
    d) Encryption
    Answer: Tokenization
72. **Which security technique replaces sensitive data with altered values to protect personal information?**
    a) Hashing
    b) Salting
    c) Encryption
    d) Data masking
    Answer: Data masking
73. **Which process converts data into a fixed-length irreversible string to ensure data integrity?**
    a) Hashing
    b) Salting
    c) Digital signatures
    d) Encryption
    Answer: Hashing
74. **Which technique adds random data to passwords before hashing to protect against rainbow table attacks?**
    a) Key stretching
    b) Hashing
    c) Salting
    d) Data masking
    Answer: Salting
75. **Which cryptographic method provides authentication, integrity, and non-repudiation for digital messages?**
    a) Hashing
    b) Salting
    c) Data masking
    d) Digital signatures
    Answer: Digital signatures
76. **Which cryptographic technique strengthens weak passwords by repeatedly hashing them?**
    a) Key stretching
    b) Salting
    c) Data masking
    d) Digital signatures
    Answer: Key stretching

77. **Which technology maintains a decentralized tamper-resistant ledger for transactions?**
    a) Digital signatures
    b) Certificate authorities
    c) Blockchain
    d) Key stretching
    Answer: Blockchain
78. **What is an open public ledger used for in blockchain technology?**
    a) Storing encryption keys securely
    b) Measuring digital signatures
    c) Encrypting passage passwords for secure authentication
    d) Recording transactions in a transparent and immutable manner
    Answer: Recording transactions in a transparent and immutable manner
79. **What is the function of digital certificates in cybersecurity?**
    a) To encrypt passwords before transmission
    b) To provide secure key stretching
    c) To verify the authenticity of websites, users, or devices
    d) To replace data with masked values for security
    Answer: To verify the authenticity of websites, users, or devices
80. **Which entity is responsible for issuing and managing digital certificates?**
    a) Certificate authority
    b) Blockchain network
    c) Hashing algorithm
    d) Digital signature provider
    Answer: Certificate authority
81. **What is the purpose of a Certificate Revocation List (CRL)?**
    a) To verify the validity of a certificate in real time
    b) To list certificates that have been revoked by the issuing certificate authority
    c) To store public keys for encrypting data
    d) To store passwords for authentication
    Answer: To list certificates that have been revoked by the issuing certificate authority
82. **Which protocol is used to check the status of a digital certificate in real time?**
    a) CRL
    b) FTP
    c) SMTP
    d) OCSP
    Answer: OCSP
83. **What is a self-signed certificate?**
    a) A certificate that is issued by a trusted certificate authority
    b) A certificate that is not trusted by default in most systems
    c) A certificate generated and signed by the certificate owner rather than an external authority
    d) A certificate used for encryption purposes only

Answer: A certificate generated and signed by the certificate owner rather than an external authority

84. **Which of the following is true about third-party certificates?**
    a) They are always free and open source
    b) They are issued by trusted certificate authorities
    c) They are never valid for commercial use
    d) They require manual installation on the client machine
    Answer: They are issued by trusted certificate authorities
85. **What is the root of trust in a Public Key Infrastructure (PKI)?**
    a) The private key of a server
    b) The certificate authority that signs all certificates
    c) The initial certificate that verifies the entire chain of trust
    d) The method of hashing certificates
    Answer: The initial certificate that verifies the entire chain of trust
86. **What is the purpose of generating a Certificate Signing Request (CSR)?**
    a) To create a private key
    b) To request a certificate from a certificate authority
    c) To verify the authenticity of a website
    d) To revoke an existing certificate
    Answer: To request a certificate from a certificate authority
87. **What is a wildcard certificate used for?**
    a) To secure multiple subdomains under a single domain
    b) To encrypt email messages only
    c) To secure a single subdomain under a domain
    d) To authenticate users on a network
    Answer: To secure multiple subdomains under a single domain

Section two : Threats, Vulnerabilities, Mitigations

1. **Which of the following threat actors is typically backed by a government and engages in cyber espionage or cyber warfare?**
    a) Nation state
    b) Unskilled attacker
    c) Hacktivist
    d) Insider threat
    Answer: Nation state
2. **Which term describes an attacker who lacks advanced technical skills and primarily uses pre-existing tools and scripts?**
    a) Nation state
    b) Unskilled attacker
    c) Hacktivist
    d) Organized crime
    Answer: Unskilled attacker

3. **What type of threat actor is motivated by political or ideological beliefs and uses cyber attacks to promote their cause?**
   a) Nation state
   b) Unskilled attacker
   c) Hacktivist
   d) Insider threat
   Answer: Hacktivist
4. **Which type of threat actor has legitimate access to an organization's systems but poses a security risk due to malicious intent or negligence?**
   a) Nation state
   b) Unskilled attacker
   c) Hacktivist
   d) Insider threat
   Answer: Insider threat
5. **Which type of threat actor is typically motivated by financial gain and operates in structured groups with significant resources?**
   a) Nation state
   b) Organized crime
   c) Hacktivist
   d) Insider threat
   Answer: Organized crime
6. **What term describes IT systems or applications that are deployed within an organization without formal approval, often increasing security risks?**
   a) Shadow IT
   b) Insider threat
   c) Organized crime
   d) Hacktivist
   Answer: Shadow IT
7. **Which of the following best differentiates an internal threat actor from an external one?**
   a) Internal threat actors have authorized access to the organization's systems
   b) External threat actors use advanced techniques
   c) Internal threat actors are always motivated by financial gain
   d) External threat actors lack access to systems
   Answer: Internal threat actors have authorized access to the organization's systems
8. **How does resource availability impact the effectiveness of a threat actor?**
   a) More resources allow for more sophisticated attacks and longer campaigns
   b) Fewer resources lead to more targeted attacks
   c) Resource availability does not impact attack effectiveness
   d) More resources reduce attack sophistication
   Answer: More resources allow for more sophisticated attacks and longer campaigns
9. **Which characteristic is often associated with highly sophisticated threat actors?**
   a) They use advanced techniques and custom-developed tools

b) They rely on pre-existing tools and scripts
c) They lack technical skills
d) They avoid targeted attacks
Answer: They use advanced techniques and custom-developed tools

10. **Which term describes the act of stealing sensitive information and transmitting it outside an organization without authorization?**
a) Data exfiltration
b) Espionage
c) Service disruption
d) Blackmail
Answer: Data exfiltration

11. **Which motivation drives cyber criminals or state-sponsored actors to gather confidential business or government information for strategic advantage?**
a) Espionage
b) Financial gain
c) Service disruption
d) Philosophical beliefs
Answer: Espionage

12. **A distributed denial-of-service attack designed to overload a network and make a service unavailable is an example of what type of motivation?**
a) Espionage
b) Service disruption
c) Financial gain
d) Blackmail
Answer: Service disruption

13. **Which type of cyber attack motivation involves threatening to release sensitive information unless a ransom or demand is met?**
a) Espionage
b) Service disruption
c) Blackmail
d) Financial gain
Answer: Blackmail

14. **Ransomware attacks where attackers demand payment in exchange for restoring access to encrypted data are primarily motivated by what?**
a) Espionage
b) Service disruption
c) Blackmail
d) Financial gain
Answer: Financial gain

15. **Hactivists often conduct cyber attacks to promote or oppose certain ideologies. What is their primary motivation?**
a) Financial gain
b) Philosophical or political beliefs

c) Service disruption
d) Revenge
Answer: Philosophical or political beliefs

16. **Which of the following describes ethical hackers who conduct security assessments to identify vulnerabilities before malicious attackers exploit them?**
a) Ethical hacking
b) Hacktivist
c) Insider threat
d) Organized crime
Answer: Ethical hacking

17. **A disgruntled employee launches an attack on their former employer's network to cause damage. What is the primary motivation?**
a) Financial gain
b) Revenge
c) Philosophical beliefs
d) Service disruption
Answer: Revenge

18. **Some cyber criminals engage in attacks with no clear financial or ideological motive, simply aiming to create disorder. What is this motivation called?**
a) Financial gain
b) Revenge
c) Disruption or chaos
d) Espionage
Answer: Disruption or chaos

19. **Cyber attacks that target critical infrastructure, communication networks, or government systems during geopolitical conflicts are typically motivated by what?**
a) Financial gain
b) War
c) Revenge
d) Philosophical beliefs
Answer: War

20. **Which type of attack is commonly delivered via phishing emails to trick users into revealing sensitive information?**
a) Email-based social engineering
b) File-based attacks
c) Image-based attacks
d) Vishing
Answer: Email-based social engineering

21. **What is a common security risk associated with SMS-based phishing or smishing attacks?**
a) Tricking users into clicking malicious links or revealing credentials
b) Overloading network traffic
c) Encrypting user data

d) Modifying system files

Answer: Tricking users into clicking malicious links or revealing credentials

22. **Which messaging platform is often targeted by attackers using fake profiles or malicious links to compromise users?**
    a) Email
    b) Instant messaging
    c) Voice calls
    d) Social media
    Answer: Instant messaging
23. **Steganography is a technique commonly used in which type of cyber attack?**
    a) File-based attacks
    b) Image-based attacks
    c) Vishing
    d) Smishing
    Answer: Image-based attacks
24. **Which attack vector involves disguising malware within seemingly harmless documents such as PDFs or Word files?**
    a) File-based attacks
    b) Image-based attacks
    c) Email-based social engineering
    d) Vishing
    Answer: File-based attacks
25. **Caller ID spoofing is often used in which type of attack?**
    a) Smishing
    b) Voice call-based phishing or vishing
    c) File-based attacks
    d) Image-based attacks
    Answer: Voice call-based phishing or vishing
26. **What is a major security risk associated with using removable storage devices?**
    a) They can spread malware or facilitate data exfiltration
    b) They overload network traffic
    c) They encrypt system files
    d) They block user access
    Answer: They can spread malware or facilitate data exfiltration
27. **Which of the following describes a key security concern with agentless security solutions?**
    a) They rely on external network scanning and may miss endpoint threats
    b) They require excessive system resources
    c) They block legitimate user access
    d) They encrypt network traffic
    Answer: They rely on external network scanning and may miss endpoint threats
28. **What is a primary security risk of using unsupported systems and applications?**
    a) They no longer receive security patches, making them vulnerable to exploits

b) They require excessive bandwidth
c) They block user authentication
d) They encrypt sensitive data
Answer: They no longer receive security patches, making them vulnerable to exploits

29. **Which type of attack commonly uses phishing emails to trick recipients into clicking malicious links or downloading malware?**
a) Email-based phishing
b) Smishing
c) Vishing
d) File-based attacks
Answer: Email-based phishing

30. **Which term describes a phishing attack that is conducted via text messages?**
a) Email-based phishing
b) Smishing
c) Vishing
d) File-based attacks
Answer: Smishing

31. **Attackers may use instant messaging platforms to distribute malware by doing which of the following?**
a) Sending short, malicious links to users
b) Encrypting user messages
c) Overloading the platform with traffic
d) Blocking user access
Answer: Sending short, malicious links to users

32. **What type of cyber attack involves hiding malicious code within an image file?**
a) File-based attack
b) Image-based steganography
c) Smishing
d) Vishing
Answer: Image-based steganography

33. **Which method is commonly used to deliver malware via seemingly harmless documents such as PDFs and Microsoft Office files?**
a) File-based attack
b) Image-based attack
c) Smishing
d) Vishing
Answer: File-based attack

34. **A social engineering attack where an attacker uses caller ID spoofing to impersonate a trusted entity is known as what?**
a) Smishing
b) Vishing
c) File-based attack

d) Image-based attack

Answer: Vishing

35. **Why are removable storage devices often a security risk in organizations?**
    a) They can introduce malware or be used for data exfiltration
    b) They overload network bandwidth
    c) They encrypt sensitive data
    d) They block user authentication
    Answer: They can introduce malware or be used for data exfiltration
36. **What is a key security concern when using an agentless security solution?**
    a) It relies on external scanning and may miss endpoint-specific threats
    b) It requires excessive system resources
    c) It blocks legitimate user access
    d) It encrypts network traffic
    Answer: It relies on external scanning and may miss endpoint-specific threats
37. **What is a major security risk of using unsupported systems and applications?**
    a) They no longer receive security patches, making them vulnerable to exploits
    b) They require excessive bandwidth
    c) They block user authentication
    d) They encrypt sensitive data
    Answer: They no longer receive security patches, making them vulnerable to exploits
38. **Which of the following is a common security risk associated with unsecured wireless networks?**
    a) They allow unauthorized users to intercept and access network traffic
    b) They overload system resources
    c) They block legitimate user access
    d) They encrypt sensitive data
    Answer: They allow unauthorized users to intercept and access network traffic
39. **What is a primary security risk associated with unsecure wired networks?**
    a) Attackers can physically connect to the network and intercept traffic
    b) They overload network bandwidth
    c) They block user authentication
    d) They encrypt sensitive data
    Answer: Attackers can physically connect to the network and intercept traffic
40. **Which type of attack exploits unsecure Bluetooth connections to eavesdrop or manipulate communications?**
    a) Blue snarfing
    b) Smishing
    c) Vishing
    d) File-based attack
    Answer: Blue snarfing
41. **Why are open service ports considered a security risk?**
    a) They can be exploited by attackers to gain unauthorized access to a system
    b) They overload network bandwidth

c) They block user authentication
d) They encrypt sensitive data
Answer: They can be exploited by attackers to gain unauthorized access to a system

42. **Why should default credentials be changed immediately after installing a new device or system?**
a) Default usernames and passwords are widely known and can be exploited by attackers
b) They overload system resources
c) They block legitimate user access
d) They encrypt sensitive data
Answer: Default usernames and passwords are widely known and can be exploited by attackers

43. **Which of the following is a primary risk associated with third-party managed service providers?**
a) They can introduce security vulnerabilities through weak security controls
b) They overload network bandwidth
c) They block user authentication
d) They encrypt sensitive data
Answer: They can introduce security vulnerabilities through weak security controls

44. **Which of the following best describes a security risk posed by vendors in the supply chain?**
a) Vendors may have weak security controls that expose organizations to attacks
b) They overload network bandwidth
c) They block user authentication
d) They encrypt sensitive data
Answer: Vendors may have weak security controls that expose organizations to attacks

45. **Why is supply chain security critical in cybersecurity risk management?**
a) Suppliers can introduce vulnerabilities that affect an organization's security posture
b) They overload network bandwidth
c) They block user authentication
d) They encrypt sensitive data
Answer: Suppliers can introduce vulnerabilities that affect an organization's security posture

46. **Which type of social engineering attack involves sending fraudulent emails that appear to come from a trusted source to trick users into revealing sensitive information?**
a) Phishing
b) Vishing
c) Smishing
d) Pretexting
Answer: Phishing

47. **What type of social engineering attack involves using voice calls to manipulate individuals into divulging confidential information?**

a) Phishing
b) Vishing
c) Smishing
d) Pretexting
Answer: Vishing

48. **A cyber criminal sends a fake text message claiming to be from a bank, urging the recipient to verify their account details. What type of attack is this?**
a) Phishing
b) Vishing
c) Smishing
d) Pretexting
Answer: Smishing

49. **Which of the following describes the intentional spread of false information to manipulate public perception?**
a) Misinformation or disinformation
b) Phishing
c) Vishing
d) Smishing
Answer: Misinformation or disinformation

50. **Which attack involves an individual pretending to be someone else to gain unauthorized access to systems or information?**
a) Impersonation
b) Phishing
c) Vishing
d) Smishing
Answer: Impersonation

51. **A CEO receives an email that appears to be from their CFO instructing them to transfer money to an unfamiliar account. What type of attack is this?**
a) Business email compromise
b) Phishing
c) Vishing
d) Smishing
Answer: Business email compromise

52. **Which social engineering technique involves an attacker creating a fabricated scenario to convince a victim to reveal information?**
a) Pretexting
b) Phishing
c) Vishing
d) Smishing
Answer: Pretexting

53. **An attacker compromises a website frequently visited by a target audience to spread malware. What type of attack is this?**
a) Watering hole attack

b) Phishing
c) Vishing
d) Smishing
Answer: Watering hole attack

54. **Cyber criminals create a fake website that looks identical to a well-known brand to steal user credentials. What type of attack is this?**
a) Brand impersonation
b) Phishing
c) Vishing
d) Smishing
Answer: Brand impersonation

55. **An attacker registers a domain name similar to a legitimate website, hoping users will mistype the URL and enter sensitive information. What is this attack called?**
a) Typosquatting
b) Phishing
c) Vishing
d) Smishing
Answer: Typosquatting

56. **What type of security vulnerability occurs when an application improperly handles user input, leading to unintended actions or code execution?**
a) Application vulnerability
b) Memory injection
c) Buffer overflow
d) Race condition
Answer: Application vulnerability

57. **Which attack technique involves injecting malicious code into a process's memory to execute unauthorized commands?**
a) Memory injection
b) Application vulnerability
c) Buffer overflow
d) Race condition
Answer: Memory injection

58. **A program fails to properly allocate memory, allowing an attacker to overwrite adjacent memory locations. What type of attack is this?**
a) Buffer overflow
b) Application vulnerability
c) Memory injection
d) Race condition
Answer: Buffer overflow

59. **Which type of attack occurs when multiple processes attempt to execute a task simultaneously, causing unpredictable behavior?**
a) Race condition
b) Application vulnerability

c) Memory injection
d) Buffer overflow
Answer: Race condition

60. **Which attack exploits the time gap between checking a resource's state and using it, allowing an attacker to modify it?**
a) Time of check (TOC) attack
b) Application vulnerability
c) Memory injection
d) Buffer overflow
Answer: Time of check (TOC) attack

61. **An attacker modifies a file between its initial verification and execution, leading to unauthorized actions. What type of attack is this?**
a) Time of use (TOU) attack
b) Application vulnerability
c) Memory injection
d) Buffer overflow
Answer: Time of use (TOU) attack

62. **A user installs a software update that contains hidden malware. What type of attack is this?**
a) Malicious update
b) Application vulnerability
c) Memory injection
d) Buffer overflow
Answer: Malicious update

63. **Which type of vulnerability primarily targets operating system processes and security mechanisms?**
a) Operating system-based attack
b) Application vulnerability
c) Memory injection
d) Buffer overflow
Answer: Operating system-based attack

64. **What type of security vulnerability commonly exploits weaknesses in web applications to perform unauthorized actions?**
a) Web-based attack
b) Application vulnerability
c) Memory injection
d) Buffer overflow
Answer: Web-based attack

65. **Which attack technique involves injecting malicious SQL statements into a database query to manipulate or extract data?**
a) SQL injection
b) Cross-site scripting
c) Memory injection

d) Buffer overflow

Answer: SQL injection

66. **Which web security vulnerability allows attackers to inject scripts into web pages viewed by other users?**

a) Cross-site scripting

b) SQL injection

c) Memory injection

d) Buffer overflow

Answer: Cross-site scripting

67. **Which of the following is a security risk associated with outdated firmware?**

a) It no longer receives security updates, making it vulnerable to exploits

b) It overloads system resources

c) It blocks user authentication

d) It encrypts sensitive data

Answer: It no longer receives security updates, making it vulnerable to exploits

68. **What is a major security concern with end-of-life hardware?**

a) It no longer receives security patches, increasing vulnerability to attacks

b) It overloads system resources

c) It blocks user authentication

d) It encrypts sensitive data

Answer: It no longer receives security patches, increasing vulnerability to attacks

69. **Legacy systems often pose a security risk because they...**

a) May not support modern security updates and encryption standards

b) Overload system resources

c) Block user authentication

d) Encrypt sensitive data

Answer: May not support modern security updates and encryption standards

70. **What is the primary security risk of a virtual machine escape attack?**

a) An attacker gains access to the host system from within a virtual machine

b) It overloads system resources

c) It blocks user authentication

d) It encrypts sensitive data

Answer: An attacker gains access to the host system from within a virtual machine

71. **Why is resource reuse a security concern in virtualization?**

a) Residual data from previous virtual machines can be accessed by new instances

b) It overloads system resources

c) It blocks user authentication

d) It encrypts sensitive data

Answer: Residual data from previous virtual machines can be accessed by new instances

72. **Which security concern is unique to cloud environments?**

a) Shared infrastructure can lead to data leakage between tenants

b) It overloads system resources

c) It blocks user authentication
d) It encrypts sensitive data
Answer: Shared infrastructure can lead to data leakage between tenants

73. **What is a primary risk when relying on third-party service providers?**
a) A security breach in the provider system can impact client data
b) It overloads system resources
c) It blocks user authentication
d) It encrypts sensitive data
Answer: A security breach in the provider system can impact client data

74. **What is a common security risk associated with hardware providers in the supply chain?**
a) Hardware components may be compromised before deployment
b) They overload system resources
c) They block user authentication
d) They encrypt sensitive data
Answer: Hardware components may be compromised before deployment

75. **Why is software supply chain security critical?**
a) Compromised software updates can introduce malware into systems
b) They overload system resources
c) They block user authentication
d) They encrypt sensitive data
Answer: Compromised software updates can introduce malware into systems

76. **Which of the following best describes a cryptographic security risk?**
a) Weak encryption algorithms can be cracked by attackers
b) Overloading system resources
c) Blocking user authentication
d) Encrypting sensitive data
Answer: Weak encryption algorithms can be cracked by attackers

77. **Which security risk arises when a system, application, or network is not configured properly, potentially exposing vulnerabilities?**
a) Misconfiguration
b) Overloading system resources
c) Blocking user authentication
d) Encrypting sensitive data
Answer: Misconfiguration

78. **What is the security risk of sideloading applications on a mobile device?**
a) The app may bypass security controls and introduce malware
b) It overloads system resources
c) It blocks user authentication
d) It encrypts sensitive data
Answer: The app may bypass security controls and introduce malware

79. **Which term describes the process of removing manufacturer restrictions on a mobile device, potentially exposing it to security risks?**

a) Jailbreaking
b) Sideloading
c) Misconfiguration
d) Encryption
Answer: Jailbreaking

80. **What type of attack exploits a previously unknown software vulnerability before a fix is available?**
a) Zero-day attack
b) Phishing
c) Vishing
d) Smishing
Answer: Zero-day attack

81. **What type of malware encrypts a victim's files and demands payments to restore access?**
a) Ransomware
b) Trojan
c) Worm
d) Spyware
Answer: Ransomware

82. **Which type of malware disguises itself as a legitimate program but secretly executes malicious activities?**
a) Ransomware
b) Trojan
c) Worm
d) Spyware
Answer: Trojan

83. **Which type of malware is self-replicating and spreads without human intervention?**
a) Ransomware
b) Trojan
c) Worm
d) Spyware
Answer: Worm

84. **Which type of malware is designed to secretly monitor a user's activity and collect personal information?**
a) Ransomware
b) Trojan
c) Worm
d) Spyware
Answer: Spyware

85. **What is a common characteristic of bloatware?**
a) It consists of unnecessary pre-installed software that slows down a device
b) It encrypts sensitive data

c) It blocks user authentication
d) It spreads without human intervention
Answer: It consists of unnecessary pre-installed software that slows down a device

86. **Which type of malware attaches itself to a legitimate file and requires user execution to spread?**
a) Virus
b) Trojan
c) Worm
d) Spyware
Answer: Virus

87. **What type of malware records user keystrokes to steal sensitive information?**
a) Keylogger
b) Trojan
c) Worm
d) Spyware
Answer: Keylogger

88. **What type of malware is designed to execute a malicious function when a specific condition is met?**
a) Logic bomb
b) Trojan
c) Worm
d) Spyware
Answer: Logic bomb

89. **What type of malware is designed to hide its presence by modifying operating system components?**
a) Rootkit
b) Trojan
c) Worm
d) Spyware
Answer: Rootkit

90. **Which type of attack systematically attempts multiple password combinations to gain unauthorized access?**
a) Brute-force attack
b) Phishing
c) Vishing
d) Smishing
Answer: Brute-force attack

91. **Which attack involves copying data from an RFID tag without authorization?**
a) RFID cloning
b) Phishing
c) Vishing
d) Smishing
Answer: RFID cloning

92. **Which physical security risk is associated with extreme heat, cold, or humidity affecting IT infrastructure?**
    a) Environmental attack
    b) Phishing
    c) Vishing
    d) Smishing
    Answer: Environmental attack
93. **Which type of network attack overwhelms a target system with excessive traffic to cause service disruption?**
    a) Distributed Denial of Service (DoS)
    b) Phishing
    c) Vishing
    d) Smishing
    Answer: Distributed Denial of Service (DoS)
94. **Which attack amplifies the amount of traffic sent to a target by leveraging misconfigured third-party servers?**
    a) Amplified attack
    b) Phishing
    c) Vishing
    d) Smishing
    Answer: Amplified attack
95. **A cyber criminal sends a request to multiple open servers, which then respond by sending large amounts of traffic to the victim. What type of attack is this?**
    a) Reflected attack
    b) Phishing
    c) Vishing
    d) Smishing
    Answer: Reflected attack
96. **Which type of attack manipulates DNS records to redirect users to malicious websites?**
    a) DNS attack
    b) Phishing
    c) Vishing
    d) Smishing
    Answer: DNS attack
97. **Which network attack targets weaknesses in wireless security protocols to gain unauthorized access?**
    a) Wireless attack
    b) Phishing
    c) Vishing
    d) Smishing
    Answer: Wireless attack

98. **Which type of attack involves intercepting communication between two parties to steal or modify data?**
    a) On-path attack
    b) Phishing
    c) Vishing
    d) Smishing
    Answer: On-path attack
99. **Which technique involves capturing and reusing authentication data to gain unauthorized access to a system?**
    a) Credential replay attack
    b) Phishing
    c) Vishing
    d) Smishing
    Answer: Credential replay attack
100. **Which type of network attack involves injecting harmful code into a system to compromise security?**
    a) Malicious code attack
    b) Phishing
    c) Vishing
    d) Smishing
    Answer: Malicious code attack
101. **Which type of application attack involves inserting malicious code into an application's input fields to manipulate its execution?**
    a) Injection attack
    b) Buffer overflow
    c) Replay attack
    d) Privilege escalation
    Answer: Injection attack
102. **What type of attack occurs when an application writes more data to a memory buffer than it was designed to hold, potentially allowing arbitrary code execution?**
    a) Buffer overflow
    b) Injection attack
    c) Replay attack
    d) Privilege escalation
    Answer: Buffer overflow
103. **Which attack captures and retransmits valid authentication data to gain unauthorized access to a system?**
    a) Replay attack
    b) Injection attack
    c) Buffer overflow
    d) Privilege escalation
    Answer: Replay attack

104. **Which type of attack occurs when an attacker gains unauthorized access to higher-level privileges in a system or application?**
    a) Privilege escalation
    b) Injection attack
    c) Buffer overflow
    d) Replay attack
    Answer: Privilege escalation
105. **Which application attack tricks a system into performing an action by forging requests from a trusted user?**
    a) Forgery attack
    b) Injection attack
    c) Buffer overflow
    d) Replay attack
    Answer: Forgery attack
106. **What type of attack exploits improper input validation to gain unauthorized access to restricted directories on a web server?**
    a) Directory traversal
    b) Injection attack
    c) Buffer overflow
    d) Replay attack
    Answer: Directory traversal
107. **Which cryptographic attack forces a system to use a weaker encryption protocol, making it easier to compromise?**
    a) Downgrade attack
    b) Collision attack
    c) Birthday attack
    d) Brute-force attack
    Answer: Downgrade attack
108. **Which cryptographic attack occurs when two different inputs produce the same hash value, compromising the integrity of the system?**
    a) Collision attack
    b) Downgrade attack
    c) Birthday attack
    d) Brute-force attack
    Answer: Collision attack
109. **Which cryptographic attack takes advantage of the probability that two different inputs will produce the same hash value?**
    a) Birthday attack
    b) Collision attack
    c) Downgrade attack
    d) Brute-force attack
    Answer: Birthday attack

110. **Which password attack attempts to gain access by testing a few commonly used passwords across many accounts?**
    a) Spraying attack
    b) Brute-force attack
    c) Replay attack
    d) Credential replay attack
    Answer: Spraying attack
111. **Which password attack systematically tries all possible combinations until the correct one is found?**
    a) Brute-force attack
    b) Spraying attack
    c) Replay attack
    d) Credential replay attack
    Answer: Brute-force attack
112. **Which indicator of a password attack involves multiple failed login attempts, resulting in the automatic disabling of an account?**
    a) Account lockout
    b) Concurrent session usage
    c) Impossible travel
    d) Blocked content
    Answer: Account lockout
113. **Which indicator suggests that an account is being accessed from multiple locations at the same time?**
    a) Concurrent session usage
    b) Account lockout
    c) Impossible travel
    d) Blocked content
    Answer: Concurrent session usage
114. **What security indicator prevents users from accessing certain web pages or online services due to security policies?**
    a) Blocked content
    b) Account lockout
    c) Concurrent session usage
    d) Impossible travel
    Answer: Blocked content
115. **Which security alert indicates that a login attempt was made from an unusually distant location in a short period of time?**
    a) Impossible travel
    b) Account lockout
    c) Concurrent session usage
    d) Blocked content
    Answer: Impossible travel

116. **Which of the following indicates an attack that excessively uses CPU, memory, or bandwidth to degrade system performance?**
    a) Resource consumption
    b) Account lockout
    c) Concurrent session usage
    d) Impossible travel
    Answer: Resource consumption
117. **Which security concern involves a user or system being unable to access files, networks, or applications due to an attack?**
    a) Resource inaccessibility
    b) Account lockout
    c) Concurrent session usage
    d) Impossible travel
    Answer: Resource inaccessibility
118. **Which of the following is a sign of potential malicious activity when logs appear outside their normal timeframe?**
    a) Out-of-cycle logging
    b) Account lockout
    c) Concurrent session usage
    d) Impossible travel
    Answer: Out-of-cycle logging
119. **What is a common source for security analysts to find known indicators of compromise (IoCs)?**
    a) Published or documented indicators
    b) Account lockout
    c) Concurrent session usage
    d) Impossible travel
    Answer: Published or documented indicators
120. **Which security issue occurs when logs that should exist for forensic analysis are missing?**
    a) Missing logs
    b) Account lockout
    c) Concurrent session usage
    d) Impossible travel
    Answer: Missing logs
121. **Which security practice involves dividing a network into smaller, isolated sections to reduce attack surfaces?**
    a) Segmentation
    b) Encryption
    c) Patching
    d) Monitoring
    Answer: Segmentation

122. **Which security mechanism defines rules that determine which users or devices can access specific resources?**
    a) Access control list
    b) Encryption
    c) Patching
    d) Monitoring
    Answer: Access control list
123. **Which security feature specifies what actions users can perform on a system or file?**
    a) Permissions
    b) Encryption
    c) Patching
    d) Monitoring
    Answer: Permissions
124. **Which security measure restricts software execution to a predefined list of approved applications?**
    a) Application allow list
    b) Encryption
    c) Patching
    d) Monitoring
    Answer: Application allow list
125. **Which security concept involves running applications or systems in a contained environment to prevent threats from spreading?**
    a) Isolation
    b) Encryption
    c) Patching
    d) Monitoring
    Answer: Isolation
126. **What security practice involves applying updates to software and systems to fix vulnerabilities?**
    a) Patching
    b) Encryption
    c) Isolation
    d) Monitoring
    Answer: Patching
127. **Which security technique ensures that data is encoded so only authorized parties can access it?**
    a) Encryption
    b) Patching
    c) Isolation
    d) Monitoring
    Answer: Encryption

128. **What security practice involves continuously observing network traffic and system activity to detect threats?**
    a) Monitoring
    b) Patching
    c) Encryption
    d) Isolation
    Answer: Monitoring
129. **Which principle ensures that users and applications only have the minimum level of access required to perform their tasks?**
    a) Least privilege
    b) Patching
    c) Encryption
    d) Monitoring
    Answer: Least privilege
130. **Which security control ensures that system configurations comply with established security policies and standards?**
    a) Configuration enforcement
    b) Patching
    c) Encryption
    d) Monitoring
    Answer: Configuration enforcement
131. **What is the process of securely removing outdated systems and hardware to prevent unauthorized access to sensitive data?**
    a) Decommissioning
    b) Patching
    c) Encryption
    d) Monitoring
    Answer: Decommissioning
132. **Which security practice involves strengthening a system by disabling unnecessary services, removing default accounts, and applying security updates?**
    a) Hardening techniques
    b) Patching
    c) Encryption
    d) Monitoring
    Answer: Hardening techniques
133. **Which security technique ensures that data is encoded so that only authorized users can access and read it?**
    a) Encryption
    b) Patching
    c) Isolation
    d) Monitoring
    Answer: Encryption

134. **What is the primary purpose of installing endpoint protection on a device?**
    a) To detect and prevent malware, unauthorized access, and other security threats
    b) To overload system resources
    c) To block user authentication
    d) To encrypt sensitive data
    Answer: To detect and prevent malware, unauthorized access, and other security threats
135. **Which security solution is designed to monitor and filter incoming and outgoing traffic on an individual computer?**
    a) Host-based firewall
    b) Patching
    c) Encryption
    d) Monitoring
    Answer: Host-based firewall
136. **Which security control actively monitors and prevents malicious activities on an endpoint?**
    a) Host-based Intrusion Prevention System (HIPS)
    b) Patching
    c) Encryption
    d) Monitoring
    Answer: Host-based Intrusion Prevention System (HIPS)
137. **Why is it important to disable unnecessary ports and protocols on a system?**
    a) To reduce the attack surface by limiting potential entry points for attackers
    b) To overload system resources
    c) To block user authentication
    d) To encrypt sensitive data
    Answer: To reduce the attack surface by limiting potential entry points for attackers
138. **Why should default passwords on devices and applications be changed immediately after installation?**
    a) Default credentials are widely known and could be exploited by attackers
    b) To overload system resources
    c) To block user authentication
    d) To encrypt sensitive data
    Answer: Default credentials are widely known and could be exploited by attackers
139. **What is the security benefit of removing unnecessary software from a system?**
    a) It reduces the attack surface by eliminating potential vulnerabilities
    b) To overload system resources
    c) To block user authentication
    d) To encrypt sensitive data
    Answer: It reduces the attack surface by eliminating potential vulnerabilities

Section three : Security Architecture

1. **Which of the following is a security concern when using cloud computing?**
   a) Data exposure due to shared infrastructure and multi-tenancy
   b) Overloading system resources
   c) Blocking user authentication
   d) Encrypting sensitive data
   Answer: Data exposure due to shared infrastructure and multi-tenancy
2. **What is the purpose of a responsibility matrix in cloud security?**
   a) To define security and operational responsibilities between cloud providers and customers
   b) To encrypt data in transit
   c) To monitor network traffic
   d) To block unauthorized access
   Answer: To define security and operational responsibilities between cloud providers and customers
3. **Which security concern is unique to hybrid cloud environments?**
   a) Ensuring secure data transfer between on-premises and cloud resources
   b) Overloading system resources
   c) Blocking user authentication
   d) Encrypting sensitive data
   Answer: Ensuring secure data transfer between on-premises and cloud resources
4. **What is a primary security risk associated with third-party vendors in an organization's infrastructure?**
   a) Vendors may have weak security practices that expose the organization to attacks
   b) Overloading system resources
   c) Blocking user authentication
   d) Encrypting sensitive data
   Answer: Vendors may have weak security practices that expose the organization to attacks
5. **Which security advantage does Infrastructure as Code (IaC) provide?**
   a) IaC enforces consistent security configurations across deployments
   b) It overloads system resources
   c) It blocks user authentication
   d) It encrypts sensitive data
   Answer: IaC enforces consistent security configurations across deployments
6. **Which security challenge is associated with serverless computing?**
   a) Lack of control over the underlying infrastructure and runtime environment
   b) Overloading system resources
   c) Blocking user authentication
   d) Encrypting sensitive data
   Answer: Lack of control over the underlying infrastructure and runtime environment
7. **What is a key security consideration when using microservices architecture?**
   a) Securing API communication between services to prevent unauthorized access
   b) Overloading system resources

c) Blocking user authentication
d) Encrypting sensitive data
Answer: Securing API communication between services to prevent unauthorized access

8. **Which of the following best describes a security concern with network infrastructure?**
a) Unauthorized access to critical network devices can lead to data breaches
b) Overloading system resources
c) Blocking user authentication
d) Encrypting sensitive data
Answer: Unauthorized access to critical network devices can lead to data breaches

9. **What is the primary security benefit of physically isolating a system from external networks?**
a) It reduces the risk of remote cyber attacks and data breaches
b) It overloads system resources
c) It blocks user authentication
d) It encrypts sensitive data
Answer: It reduces the risk of remote cyber attacks and data breaches

10. **Which security measure involves completely disconnecting a system from external networks to prevent cyber threats?**
a) Air-gapped
b) Segmentation
c) Encryption
d) Monitoring
Answer: Air-gapped

11. **Logical segmentation in a network is primarily used to do which of the following?**
a) Restrict access between different departments or user groups
b) Overload system resources
c) Block user authentication
d) Encrypt sensitive data
Answer: Restrict access between different departments or user groups

12. **How does Software-Defined Networking (SDN) improve network security?**
a) It centralizes network control, making security policies easier to manage
b) It overloads system resources
c) It blocks user authentication
d) It encrypts sensitive data
Answer: It centralizes network control, making security policies easier to manage

13. **Which of the following is a key security consideration for on-premises infrastructure?**
a) Organizations are fully responsible for securing their hardware and data
b) Overloading system resources
c) Blocking user authentication
d) Encrypting sensitive data
Answer: Organizations are fully responsible for securing their hardware and data

14. **Which statement best describes a security benefit of centralized network management over decentralized management?**
    a) Centralized management allows for uniform security policies and easier monitoring
    b) It overloads system resources
    c) It blocks user authentication
    d) It encrypts sensitive data
    Answer: Centralized management allows for uniform security policies and easier monitoring
15. **Which security advantage does containerization provide?**
    a) It isolates applications to limit the impact of security breaches
    b) It overloads system resources
    c) It blocks user authentication
    d) It encrypts sensitive data
    Answer: It isolates applications to limit the impact of security breaches
16. **Which security risk is commonly associated with virtualization?**
    a) Virtual machine escape where an attacker gains access to the host system
    b) Overloading system resources
    c) Blocking user authentication
    d) Encrypting sensitive data
    Answer: Virtual machine escape where an attacker gains access to the host system
17. **Which security challenge is associated with IoT or Internet of Things devices?**
    a) Many IoT devices lack strong security controls, making them vulnerable to attacks
    b) Overloading system resources
    c) Blocking user authentication
    d) Encrypting sensitive data
    Answer: Many IoT devices lack strong security controls, making them vulnerable to attacks
18. **Which of the following describes a key security concern with Industrial Control Systems (ICS)?**
    a) ICS systems were often designed without built-in security, making them vulnerable to cyber threats
    b) Overloading system resources
    c) Blocking user authentication
    d) Encrypting sensitive data
    Answer: ICS systems were often designed without built-in security, making them vulnerable to cyber threats
19. **Supervisory Control and Data Acquisition (SCADA) systems are commonly targeted by cyber threats because...?**
    a) They control critical infrastructure and are often using outdated security protocols
    b) They overload system resources
    c) They block user authentication
    d) They encrypt sensitive data

Answer: They control critical infrastructure and are often using outdated security protocols

20. **Which of the following is a security risk associated with Real-Time Operating Systems (RTOS)?**
    a) They often prioritize performance over security, making them vulnerable to attacks
    b) They overload system resources
    c) They block user authentication
    d) They encrypt sensitive data
    Answer: They often prioritize performance over security, making them vulnerable to attacks
21. **Why are embedded systems considered a security risk?**
    a) They often have limited security controls and cannot be easily updated
    b) They overload system resources
    c) They block user authentication
    d) They encrypt sensitive data
    Answer: They often have limited security controls and cannot be easily updated
22. **What is the primary goal of high availability in IT security?**
    a) Ensuring continuous system uptime and minimizing downtime due to failures or attacks
    b) Overloading system resources
    c) Blocking user authentication
    d) Encrypting sensitive data
    Answer: Ensuring continuous system uptime and minimizing downtime due to failures or attacks
23. **Which of the following is a key security consideration when implementing new technologies in an organization?**
    a) Ensuring proper risk assessment and compliance with security policies
    b) Overloading system resources
    c) Blocking user authentication
    d) Encrypting sensitive data
    Answer: Ensuring proper risk assessment and compliance with security policies
24. **Which term describes an organization's ability to keep systems operational and accessible during disruptions?**
    a) Availability
    b) Confidentiality
    c) Integrity
    d) Non-repudiation
    Answer: Availability
25. **What is a primary goal of resilience in cybersecurity?**
    a) To ensure systems can recover quickly from disruptions or cyber attacks
    b) Overloading system resources
    c) Blocking user authentication

d) Encrypting sensitive data

Answer: To ensure systems can recover quickly from disruptions or cyber attacks

26. **Why is cost an important factor when implementing cybersecurity solutions?**
    a) Organizations must balance security needs with budget constraints
    b) Overloading system resources
    c) Blocking user authentication
    d) Encrypting sensitive data
    Answer: Organizations must balance security needs with budget constraints
27. **Which factor is critical in evaluating the responsiveness of a cybersecurity solution?**
    a) The ability to detect and mitigate threats in real time
    b) Overloading system resources
    c) Blocking user authentication
    d) Encrypting sensitive data
    Answer: The ability to detect and mitigate threats in real time
28. **What does scalability refer to in cybersecurity architecture?**
    a) The ability to expand security measures as the organization grows
    b) Overloading system resources
    c) Blocking user authentication
    d) Encrypting sensitive data
    Answer: The ability to expand security measures as the organization grows
29. **Why is ease of deployment an important consideration when implementing security solutions?**
    a) Security solutions should be easy to configure and integrate without disrupting business operations
    b) Overloading system resources
    c) Blocking user authentication
    d) Encrypting sensitive data
    Answer: Security solutions should be easy to configure and integrate without disrupting business operations
30. **What is an example of risk transference in cybersecurity?**
    a) Purchasing cybersecurity insurance to cover potential data breaches
    b) Overloading system resources
    c) Blocking user authentication
    d) Encrypting sensitive data
    Answer: Purchasing cybersecurity insurance to cover potential data breaches
31. **Which factor is crucial for ensuring ease of recovery after a cybersecurity incident?**
    a) Maintaining regular backups and a tested disaster recovery plan
    b) Overloading system resources
    c) Blocking user authentication
    d) Encrypting sensitive data
    Answer: Maintaining regular backups and a tested disaster recovery plan

32. **Why is patch availability important in cybersecurity?**
    a) It ensures that known vulnerabilities are fixed before attackers can exploit them
    b) Overloading system resources
    c) Blocking user authentication
    d) Encrypting sensitive data
    Answer: It ensures that known vulnerabilities are fixed before attackers can exploit them
33. **What is a major security risk of an inability to patch a system?**
    a) The system remains vulnerable to known exploits and attacks
    b) Overloading system resources
    c) Blocking user authentication
    d) Encrypting sensitive data
    Answer: The system remains vulnerable to known exploits and attacks
34. **Why is power availability a critical consideration for IT security?**
    a) Power failures can lead to downtime, data corruption, and security vulnerabilities
    b) Overloading system resources
    c) Blocking user authentication
    d) Encrypting sensitive data
    Answer: Power failures can lead to downtime, data corruption, and security vulnerabilities
35. **What is a security concern related to compute resources in an organization?**
    a) Insufficient compute power can hinder security tools like encryption and monitoring
    b) Overloading system resources
    c) Blocking user authentication
    d) Encrypting sensitive data
    Answer: Insufficient compute power can hinder security tools like encryption and monitoring
36. **Why is proper device placement important in network security?**
    a) To ensure critical security devices are positioned for maximum protection
    b) Overloading system resources
    c) Blocking user authentication
    d) Encrypting sensitive data
    Answer: To ensure critical security devices are positioned for maximum protection
37. **What is the purpose of security zones in network architecture?**
    a) To segment the network into different trust levels for better security control
    b) Overloading system resources
    c) Blocking user authentication
    d) Encrypting sensitive data
    Answer: To segment the network into different trust levels for better security control
38. **Which of the following best describes an attack surface?**
    a) The total number of vulnerabilities and entry points that can be exploited
    b) Overloading system resources
    c) Blocking user authentication

d) Encrypting sensitive data

Answer: The total number of vulnerabilities and entry points that can be exploited

39. **How does connectivity impact network security?**

a) More connections increase potential entry points for attackers

b) Overloading system resources

c) Blocking user authentication

d) Encrypting sensitive data

Answer: More connections increase potential entry points for attackers

40. **What is the primary characteristic of a fail-open security control?**

a) It allows access when a system fails, prioritizing availability over security

b) It blocks access when a system fails

c) It encrypts sensitive data

d) It monitors network traffic

Answer: It allows access when a system fails, prioritizing availability over security

41. **What happens when a security system is configured to fail closed?**

a) It blocks access to maintain security when a failure occurs

b) It allows access when a system fails

c) It encrypts sensitive data

d) It monitors network traffic

Answer: It blocks access to maintain security when a failure occurs

42. **What is a key difference between active and passive security devices?**

a) Active devices take immediate action to block threats, while passive devices only monitor and log activity

b) Passive devices block threats, while active devices monitor activity

c) Active devices encrypt data, while passive devices monitor traffic

d) Passive devices allow access, while active devices block access

Answer: Active devices take immediate action to block threats, while passive devices only monitor and log activity

43. **What is a key characteristic of an inline security device compared to a tap monitor device?**

a) An inline device actively analyzes and blocks traffic in real time, while a tap monitor device only observes traffic

b) A tap monitor device blocks traffic, while an inline device observes traffic

c) An inline device encrypts data, while a tap monitor device monitors traffic

d) A tap monitor device allows access, while an inline device blocks access

Answer: An inline device actively analyzes and blocks traffic in real time, while a tap monitor device only observes traffic

44. **What is the primary function of a jump server in network security?**

a) It provides a secure intermediary system for accessing critical resources

b) It encrypts sensitive data

c) It monitors network traffic

d) It blocks unauthorized access

Answer: It provides a secure intermediary system for accessing critical resources

45. **How does a proxy server enhance network security?**
    a) It acts as an intermediary between users and web resources to filter and monitor traffic
    b) It encrypts sensitive data
    c) It blocks unauthorized access
    d) It monitors network traffic
    Answer: It acts as an intermediary between users and web resources to filter and monitor traffic
46. **What is the primary function of an Intrusion Prevention System (IPS)?**
    a) To actively detect and block malicious network activity in real time
    b) To monitor and log network activity
    c) To encrypt sensitive data
    d) To block unauthorized access
    Answer: To actively detect and block malicious network activity in real time
47. **What is the key difference between an Intrusion Detection System (IDS) and an Intrusion Prevention System (IPS)?**
    a) An IDS monitors and alerts on suspicious activity, while an IPS actively blocks threats
    b) An IPS monitors and alerts, while an IDS blocks threats
    c) An IDS encrypts data, while an IPS monitors traffic
    d) An IPS allows access, while an IDS blocks access
    Answer: An IDS monitors and alerts on suspicious activity, while an IPS actively blocks threats
48. **How does a load balancer improve network security and performance?**
    a) It distributes traffic across multiple servers to prevent overload and mitigate DoS attacks
    b) It encrypts sensitive data
    c) It monitors network traffic
    d) It blocks unauthorized access
    Answer: It distributes traffic across multiple servers to prevent overload and mitigate DoS attacks
49. **What is the function of sensors in network security?**
    a) They collect and analyze data to detect potential threats in real time
    b) They encrypt sensitive data
    c) They monitor network traffic
    d) They block unauthorized access
    Answer: They collect and analyze data to detect potential threats in real time
50. **What is the primary function of 802.1x in network security?**
    a) To provide port-based network access control using authentication mechanisms
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block unauthorized access
    Answer: To provide port-based network access control using authentication mechanisms
51. **Which authentication framework is used to support multiple authentication methods, including smart cards and biometrics?**

a) Extensible Authentication Protocol (EAP)
b) Transport Layer Security (TLS)
c) Internet Protocol Security (IPSec)
d) Secure Access Service Edge (SASE)
Answer: Extensible Authentication Protocol (EAP)

52. **Which type of firewall is specifically designed to protect web applications from threats like SQL injection and cross-site scripting?**
a) Web Application Firewall (WAF)
b) Next-Generation Firewall (NGFW)
c) Layer 4/Layer 7 firewall
d) Unified Threat Management (UTM)
Answer: Web Application Firewall (WAF)

53. **Which type of security appliance combines multiple security functions, such as firewall, intrusion prevention, and antivirus, in a single solution?**
a) Unified Threat Management (UTM)
b) Web Application Firewall (WAF)
c) Next-Generation Firewall (NGFW)
d) Layer 4/Layer 7 firewall
Answer: Unified Threat Management (UTM)

54. **What is a key advantage of a Next-Generation Firewall (NGFW) compared to traditional firewalls?**
a) NGFW includes deep packet inspection and advanced threat detection beyond simple port filtering
b) It encrypts sensitive data
c) It monitors network traffic
d) It blocks unauthorized access
Answer: NGFW includes deep packet inspection and advanced threat detection beyond simple port filtering

55. **Which type of firewall operates at both Layer 4 and Layer 7 of the OSI model for advanced traffic filtering?**
a) Layer 4/Layer 7 firewall
b) Web Application Firewall (WAF)
c) Next-Generation Firewall (NGFW)
d) Unified Threat Management (UTM)
Answer: Layer 4/Layer 7 firewall

56. **What is the primary function of a Virtual Private Network (VPN) in secure communications?**
a) To encrypt data traffic over public and private networks for secure remote access
b) To monitor network traffic
c) To block unauthorized access
d) To segment the network
Answer: To encrypt data traffic over public and private networks for secure remote access

57. **Which security mechanism allows users to securely connect to a private network from an external location?**
    a) Remote access
    b) Encryption
    c) Monitoring
    d) Segmentation
    Answer: Remote access
58. **What is the primary purpose of tunneling in network security?**
    a) To encapsulate data for secure transmission over untrusted networks
    b) To monitor network traffic
    c) To block unauthorized access
    d) To segment the network
    Answer: To encapsulate data for secure transmission over untrusted networks
59. **Which protocol is commonly used to encrypt web traffic and establish secure communication over the internet?**
    a) Transport Layer Security (TLS)
    b) Internet Protocol Security (IPSec)
    c) Extensible Authentication Protocol (EAP)
    d) Secure Access Service Edge (SASE)
    Answer: Transport Layer Security (TLS)
60. **Which security protocol is used to establish encrypted tunnels for secure data transmission between networks?**
    a) Internet Protocol Security (IPSec)
    b) Transport Layer Security (TLS)
    c) Extensible Authentication Protocol (EAP)
    d) Secure Access Service Edge (SASE)
    Answer: Internet Protocol Security (IPSec)
61. **How does Software-Defined Wide Area Network (SD-WAN) improve network security?**
    a) By dynamically routing traffic over multiple secure connections and enforcing security policies
    b) By monitoring network traffic
    c) By blocking unauthorized access
    d) By segmenting the network
    Answer: By dynamically routing traffic over multiple secure connections and enforcing security policies
62. **What is a key security benefit of Secure Access Service Edge (SASE)?**
    a) It integrates cloud-delivered security services with wide area networking
    b) It monitors network traffic
    c) It blocks unauthorized access
    d) It segments the network
    Answer: It integrates cloud-delivered security services with wide area networking

63. **What is the most important factor when selecting effective security controls for an organization?**
    a) Ensuring controls align with business needs and risk management strategies
    b) Overloading system resources
    c) Blocking user authentication
    d) Encrypting sensitive data
    Answer: Ensuring controls align with business needs and risk management strategies
64. **Which type of data is subject to government or industry regulations, such as GDPR or HIPAA?**
    a) Regulated data
    b) Trade secret
    c) Intellectual Property (IP)
    d) Legal information
    Answer: Regulated data
65. **Which type of data includes proprietary formulas, processes, or business strategies that provide a competitive advantage?**
    a) Trade secret
    b) Regulated data
    c) Intellectual Property (IP)
    d) Legal information
    Answer: Trade secret
66. **Which term refers to legally protected creations, such as patents, trademarks, and copyrights?**
    a) Intellectual Property (IP)
    b) Regulated data
    c) Trade secret
    d) Legal information
    Answer: Intellectual Property (IP)
67. **Which type of data includes contracts, agreements, and other documents that have legal significance?**
    a) Legal information
    b) Regulated data
    c) Trade secret
    d) Intellectual Property (IP)
    Answer: Legal information
68. **Which of the following best describes financial information in the context of security?**
    a) Data that includes banking details, credit card numbers, and financial statements
    b) Regulated data
    c) Trade secret
    d) Intellectual Property (IP)
    Answer: Data that includes banking details, credit card numbers, and financial statements

69. **Which of the following is an example of non-human readable data?**
    a) Encrypted binary code used for system authentication
    b) Financial statements
    c) Legal contracts
    d) Business strategies
    Answer: Encrypted binary code used for system authentication
70. **What is the purpose of data classification in cybersecurity?**
    a) To categorize data based on sensitivity and required security measures
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block unauthorized access
    Answer: To categorize data based on sensitivity and required security measures
71. **Which type of data classification applies to information that could cause harm if disclosed but is not highly sensitive?**
    a) Sensitive data
    b) Confidential
    c) Restricted
    d) Public
    Answer: Sensitive data
72. **Which classification label is typically applied to data that should only be accessed by authorized personnel due to its importance?**
    a) Confidential
    b) Sensitive data
    c) Restricted
    d) Public
    Answer: Confidential
73. **Which classification applies to data that is intended for general distribution and does not require security controls?**
    a) Public
    b) Sensitive data
    c) Confidential
    d) Restricted
    Answer: Public
74. **Which type of data classification is used for information that requires strict access control and should not be widely shared?**
    a) Restricted
    b) Sensitive data
    c) Confidential
    d) Public
    Answer: Restricted
75. **Which type of data classification applies to Personally Identifiable Information (PII) such as Social Security numbers and medical records?**
    a) Private

b) Sensitive data
c) Confidential
d) Restricted
Answer: Private

76. **Which classification is assigned to data that, if lost or compromised, would have a severe impact on business operations?**
a) Critical
b) Sensitive data
c) Confidential
d) Restricted
Answer: Critical

77. **Which of the following is a key consideration when handling data securely?**
a) Ensuring proper encryption and access controls are applied based on data sensitivity
b) Overloading system resources
c) Blocking user authentication
d) Monitoring network traffic
Answer: Ensuring proper encryption and access controls are applied based on data sensitivity

78. **What are three primary states of data in cybersecurity?**
a) Data at rest, data in transit, and data in use
b) Sensitive, confidential, and restricted
c) Public, private, and critical
d) Encrypted, hashed, and masked
Answer: Data at rest, data in transit, and data in use

79. **What term best describes data that is stored on a device, such as a hard drive or database, and not actively being transmitted?**
a) Data at rest
b) Data in transit
c) Data in use
d) Encrypted data
Answer: Data at rest

80. **Which security measure is most important for protecting data in transit?**
a) Encrypting data using protocols like TLS or IPSec
b) Monitoring network traffic
c) Blocking unauthorized access
d) Segmenting the network
Answer: Encrypting data using protocols like TLS or IPSec

81. **Which of the following best describes data in use?**
a) Data actively being processed by applications, memory, or CPUs
b) Data stored on a hard drive
c) Data transmitted over a network
d) Encrypted data
Answer: Data actively being processed by applications, memory, or CPUs

82. **What does data sovereignty refer to in cybersecurity?**
    a) The concept that data is subject to the laws and regulations of the country where it was collected or stored
    b) Encrypting sensitive data
    c) Monitoring network traffic
    d) Blocking unauthorized access
    Answer: The concept that data is subject to the laws and regulations of the country where it was collected or stored
83. **Which security feature allows organizations to track and enforce policies based on a device's physical location?**
    a) Geolocation
    b) Encryption
    c) Monitoring
    d) Segmentation
    Answer: Geolocation
84. **Which of the following is a common method to secure data?**
    a) Using encryption, access controls, and data masking
    b) Overloading system resources
    c) Blocking user authentication
    d) Monitoring network traffic
    Answer: Using encryption, access controls, and data masking
85. **What is the purpose of geographic restrictions in cybersecurity?**
    a) To limit access to data based on physical location and jurisdiction
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block unauthorized access
    Answer: To limit access to data based on physical location and jurisdiction
86. **Which security measure converts data into an unreadable format to protect it from unauthorized access?**
    a) Encryption
    b) Masking
    c) Tokenization
    d) Hashing
    Answer: Encryption
87. **What is the purpose of hashing in data security?**
    a) To create a unique, fixed-length representation of data for integrity verification
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block unauthorized access
    Answer: To create a unique, fixed-length representation of data for integrity verification
88. **Which method is used to hide part of a data value to protect sensitive information?**
    a) Masking
    b) Encryption

c) Tokenization
d) Hashing
Answer: Masking

89. **Which data protection technique replaces sensitive information with a non-sensitive equivalent?**
a) Tokenization
b) Encryption
c) Masking
d) Hashing
Answer: Tokenization

90. **What is the primary goal of obfuscation in cybersecurity?**
a) To make data or code difficult to understand while maintaining functionality
b) To encrypt sensitive data
c) To monitor network traffic
d) To block unauthorized access
Answer: To make data or code difficult to understand while maintaining functionality

91. **How does segmentation enhance security in a network?**
a) By dividing the network into isolated sections to limit unauthorized access
b) By encrypting sensitive data
c) By monitoring network traffic
d) By blocking unauthorized access
Answer: By dividing the network into isolated sections to limit unauthorized access

92. **What is the purpose of permission restrictions in data security?**
a) To enforce access controls based on user roles and responsibilities
b) To encrypt sensitive data
c) To monitor network traffic
d) To block unauthorized access
Answer: To enforce access controls based on user roles and responsibilities

93. **What is a key difference between load balancing and clustering in high availability architecture?**
a) Load balancing distributes traffic across multiple servers, while clustering ensures failover redundancy
b) Clustering distributes traffic, while load balancing ensures failover
c) Load balancing encrypts data, while clustering monitors traffic
d) Clustering blocks access, while load balancing allows access
Answer: Load balancing distributes traffic across multiple servers, while clustering ensures failover redundancy

94. **Which type of disaster recovery site is fully operational and can take over immediately in the event of a failure?**
a) Hot site
b) Warm site
c) Cold site

d) Backup site

Answer: Hot site

95. **Which disaster recovery site requires the most time and effort to become operational after a failure?**

a) Cold site

b) Hot site

c) Warm site

d) Backup site

Answer: Cold site

96. **Which type of disaster recovery site has some pre-configured infrastructure but requires additional setup before full operation?**

a) Warm site

b) Hot site

c) Cold site

d) Backup site

Answer: Warm site

97. **What is the primary benefit of geographic dispersion in disaster recovery planning?**

a) It reduces the impact of localized disasters by distributing resources across multiple locations

b) It encrypts sensitive data

c) It monitors network traffic

d) It blocks unauthorized access

Answer: It reduces the impact of localized disasters by distributing resources across multiple locations

98. **What is a security benefit of platform diversity in an organization's IT environment?**

a) It reduces the risk of widespread compromise by limiting reliance on a single system

b) It encrypts sensitive data

c) It monitors network traffic

d) It blocks unauthorized access

Answer: It reduces the risk of widespread compromise by limiting reliance on a single system

99. **What is a primary advantage of using a multi-cloud system?**

a) It enhances redundancy and reduces dependency on a single cloud provider

b) It encrypts sensitive data

c) It monitors network traffic

d) It blocks unauthorized access

Answer: It enhances redundancy and reduces dependency on a single cloud provider

100. **Which of the following best describes continuity of operations planning?**

a) Ensuring critical business functions can continue during and after a disaster or disruption

b) Encrypting sensitive data

c) Monitoring network traffic
d) Blocking unauthorized access
Answer: Ensuring critical business functions can continue during and after a disaster or disruption

101. **Why is capacity planning important for IT security?**
a) It ensures that resources are available to support current and future security needs
b) It encrypts sensitive data
c) It monitors network traffic
d) It blocks unauthorized access
Answer: It ensures that resources are available to support current and future security needs

102. **How does capacity planning impact personnel in an organization?**
a) It ensures the organization has enough trained staff to manage security operations effectively
b) It encrypts sensitive data
c) It monitors network traffic
d) It blocks unauthorized access
Answer: It ensures the organization has enough trained staff to manage security operations effectively

103. **Which factor should be considered when planning technology capacity for cybersecurity?**
a) Scalability of security infrastructure to handle increasing workloads
b) Encrypting sensitive data
c) Monitoring network traffic
d) Blocking unauthorized access
Answer: Scalability of security infrastructure to handle increasing workloads

104. **Why is infrastructure an important component of capacity planning?**
a) It ensures that network, storage, and compute resources can support security requirements
b) It encrypts sensitive data
c) It monitors network traffic
d) It blocks unauthorized access
Answer: It ensures that network, storage, and compute resources can support security requirements

105. **What is the primary purpose of a tabletop exercise in cybersecurity testing?**
a) To conduct a discussion-based walkthrough of incident response procedures
b) To encrypt sensitive data
c) To monitor network traffic
d) To block unauthorized access
Answer: To conduct a discussion-based walkthrough of incident response procedures

106. **What does a failover test evaluate in an IT environment?**
a) The ability of a system to switch to a backup or redundant system during a failure
b) Encrypting sensitive data

c) Monitoring network traffic

d) Blocking unauthorized access

Answer: The ability of a system to switch to a backup or redundant system during a failure

107. **What is the main goal of a cybersecurity simulation exercise?**

a) To create a controlled environment for testing security incident responses

b) To encrypt sensitive data

c) To monitor network traffic

d) To block unauthorized access

Answer: To create a controlled environment for testing security incident responses

108. **How does parallel processing support cybersecurity testing?**

a) By running a secondary system alongside the primary one to validate functionality before full deployment

b) By encrypting sensitive data

c) By monitoring network traffic

d) By blocking unauthorized access

Answer: By running a secondary system alongside the primary one to validate functionality before full deployment

109. **What is a key security benefit of maintaining both on-site and off-site backups?**

a) It ensures data is protected from local disasters while allowing fast recovery when needed

b) It encrypts sensitive data

c) It monitors network traffic

d) It blocks unauthorized access

Answer: It ensures data is protected from local disasters while allowing fast recovery when needed

110. **Why is backup frequency an important consideration in data protection?**

a) More frequent backups reduce potential data loss in case of a system failure

b) It encrypts sensitive data

c) It monitors network traffic

d) It blocks unauthorized access

Answer: More frequent backups reduce potential data loss in case of a system failure

111. **Why should backups be encrypted?**

a) To protect stored data from unauthorized access or theft

b) To monitor network traffic

c) To block unauthorized access

d) To segment the network

Answer: To protect stored data from unauthorized access or theft

112. **What is a snapshot in the context of data backups?**

a) A point-in-time copy of a system or data used for quick recovery

b) Encrypting sensitive data

c) Monitoring network traffic

d) Blocking unauthorized access

Answer: A point-in-time copy of a system or data used for quick recovery

113. **What is the primary goal of a recovery plan in cybersecurity?**

a) To restore systems and data to a functional state after an incident

b) To encrypt sensitive data

c) To monitor network traffic

d) To block unauthorized access

Answer: To restore systems and data to a functional state after an incident

114. **Which of the following best describes data replication in disaster recovery?**

a) The process of copying data to another system in real time or scheduled intervals for redundancy

b) Encrypting sensitive data

c) Monitoring network traffic

d) Blocking unauthorized access

Answer: The process of copying data to another system in real time or scheduled intervals for redundancy

115. **What is the purpose of journaling in data security?**

a) To keep a continuous log of changes to data for recovery and integrity verification

b) To encrypt sensitive data

c) To monitor network traffic

d) To block unauthorized access

Answer: To keep a continuous log of changes to data for recovery and integrity verification

116. **Why is power a critical consideration in cybersecurity and disaster recovery planning?**

a) Power failures can cause downtime, data loss, and security vulnerabilities

b) To encrypt sensitive data

c) To monitor network traffic

d) To block unauthorized access

Answer: Power failures can cause downtime, data loss, and security vulnerabilities

117. **What is the role of generators in disaster recovery planning?**

a) To provide backup power in case of a primary power failure

b) To encrypt sensitive data

c) To monitor network traffic

d) To block unauthorized access

Answer: To provide backup power in case of a primary power failure

118. **What is the primary function of Uninterruptible Power Supply (UPS) in cybersecurity?**

a) To provide temporary backup power to critical systems in case of an outage

b) To encrypt sensitive data

c) To monitor network traffic

d) To block unauthorized access

Answer: To provide temporary backup power to critical systems in case of an outage

Section Four : Security Operations

1. **What is the primary purpose of establishing a secure baseline in cyber security?**
   a) To define the minimum required security settings for all systems
   b) To overload system resources
   c) To block user authentication
   d) To encrypt sensitive data
   Answer: To define the minimum required security settings for all systems
2. **What is an important step when deploying a secure baseline?**
   a) Ensuring system settings match security policies before deployment
   b) Encrypting sensitive data
   c) Monitoring network traffic
   d) Blocking unauthorized access
   Answer: Ensuring system settings match security policies before deployment
3. **Why is it important to maintain a secure baseline over time?**
   a) To keep systems protected through regular updates and patches
   b) To overload system resources
   c) To block user authentication
   d) To encrypt sensitive data
   Answer: To keep systems protected through regular updates and patches
4. **Which of the following is an effective method for hardening mobile devices?**
   a) Using strong authentication and remote wipe
   b) Overloading system resources
   c) Blocking user authentication
   d) Encrypting sensitive data
   Answer: Using strong authentication and remote wipe
5. **What is a key security measure for hardening workstations?**
   a) Applying patches and disabling unneeded services
   b) Overloading system resources
   c) Blocking user authentication
   d) Encrypting sensitive data
   Answer: Applying patches and disabling unneeded services
6. **What is a recommended practice for securing network switches?**
   a) Disabling unused ports and using MAC filtering
   b) Encrypting sensitive data
   c) Monitoring network traffic
   d) Blocking unauthorized access
   Answer: Disabling unused ports and using MAC filtering
7. **Which of the following is an essential security measure for hardening routers?**
   a) Changing default credentials and disabling unnecessary services
   b) Overloading system resources
   c) Blocking user authentication

d) Encrypting sensitive data

Answer: Changing default credentials and disabling unnecessary services

8. **What is an important security consideration for cloud infrastructure?**
   a) Implementing strong identity and access management controls
   b) Overloading system resources
   c) Blocking user authentication
   d) Encrypting sensitive data
   Answer: Implementing strong identity and access management controls
9. **Which security control is essential for hardening servers?**
   a) Enforcing least privilege and disabling unnecessary services
   b) Overloading system resources
   c) Blocking user authentication
   d) Encrypting sensitive data
   Answer: Enforcing least privilege and disabling unnecessary services
10. **What is a major security risk associated with industrial control systems and SCADA?**
    a) ICS and SCADA often lack built-in security making them vulnerable
    b) Overloading system resources
    c) Blocking user authentication
    d) Encrypting sensitive data
    Answer: ICS and SCADA often lack built-in security making them vulnerable
11. **How can embedded systems be hardened against security threats?**
    a) Disabling unnecessary functions and applying firmware updates
    b) Overloading system resources
    c) Blocking user authentication
    d) Encrypting sensitive data
    Answer: Disabling unnecessary functions and applying firmware updates
12. **Which of the following is a security challenge associated with real time operating systems (RTOS)?**
    a) RTOS often prioritizes performance over security increasing vulnerability
    b) Overloading system resources
    c) Blocking user authentication
    d) Encrypting sensitive data
    Answer: RTOS often prioritizes performance over security increasing vulnerability
13. **Which of the following best describes a major security risk associated with IoT devices?**
    a) Many IoT devices lack strong security and are vulnerable to attacks
    b) Overloading system resources
    c) Blocking user authentication
    d) Encrypting sensitive data
    Answer: Many IoT devices lack strong security and are vulnerable to attacks
14. **What is a key security consideration when configuring wireless devices?**
    a) Enabling WPA3 encryption to protect data in transit

b) Overloading system resources
c) Blocking user authentication
d) Monitoring network traffic
Answer: Enabling WPA3 encryption to protect data in transit

15. **Why is it important to consider security during the installation of networking devices?**
a) To ensure devices are configured with encryption and access controls
b) Overloading system resources
c) Blocking user authentication
d) Monitoring network traffic
Answer: To ensure devices are configured with encryption and access controls

16. **What is the purpose of a wireless site survey?**
a) To analyze signal strength, interference, and coverage for optimal deployment
b) To encrypt sensitive data
c) To monitor network traffic
d) To block unauthorized access
Answer: To analyze signal strength, interference, and coverage for optimal deployment

17. **What does a heat map represent in a wireless network assessment?**
a) A visual representation of wireless signal strength and coverage areas
b) Encrypted data visualization
c) Network traffic monitoring
d) Unauthorized access detection
Answer: A visual representation of wireless signal strength and coverage areas

18. **What is the primary function of mobile device management (MDM) in an enterprise environment?**
a) To enforce security policies and remotely manage mobile devices
b) To encrypt sensitive data
c) To monitor network traffic
d) To block unauthorized access
Answer: To enforce security policies and remotely manage mobile devices

19. **Which of the following best describes the bring your own device (BYOD) deployment model?**
a) Employees use personal devices for work under security policies
b) Company-owned devices with limited personal use allowed
c) Employees select from approved devices
d) Devices are fully managed by the organization
Answer: Employees use personal devices for work under security policies

20. **How does the corporate-owned, personally enabled (COPE) deployment model differ from BYOD?**
a) Company-owned devices with limited personal use allowed
b) Employees use personal devices for work
c) Employees select from approved devices

d) Devices are fully managed by the organization

Answer: Company-owned devices with limited personal use allowed

21. **Which mobile device deployment model allows employees to select from a list of company approved devices?**
    a) Choose your own device (CYOD)
    b) Bring your own device (BYOD)
    c) Corporate-owned, personally enabled (COPE)
    d) Fully managed devices
    Answer: Choose your own device (CYOD)
22. **Which mobile connection method provides the most secure and reliable remote network access?**
    a) Cellular
    b) Public Wi-Fi
    c) Bluetooth
    d) USB tethering
    Answer: Cellular
23. **What is a common security risk when connecting to public Wi-Fi networks?**
    a) Man-in-the-middle (MITM) attacks that intercept data
    b) Overloading system resources
    c) Blocking user authentication
    d) Encrypting sensitive data
    Answer: Man-in-the-middle (MITM) attacks that intercept data
24. **Which of the following is a security concern when using Bluetooth connections?**
    a) Devices can be vulnerable to unauthorized pairing and interception
    b) Overloading system resources
    c) Blocking user authentication
    d) Encrypting sensitive data
    Answer: Devices can be vulnerable to unauthorized pairing and interception
25. **What is a key security improvement in Wi-Fi Protected Access 3 (WPA3) over WPA2?**
    a) WPA3 uses stronger encryption with Simultaneous Authentication of Equals
    b) WPA2 uses stronger encryption
    c) WPA3 blocks all network traffic
    d) WPA2 monitors network activity
    Answer: WPA3 uses stronger encryption with Simultaneous Authentication of Equals
26. **What is the primary function of AAA (Authentication, Authorization, and Accounting) in remote access security?**
    a) To enforce identity verification, permissions, and activity tracking
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block unauthorized access
    Answer: To enforce identity verification, permissions, and activity tracking

27. **Which of the following best describes the role of the RADIUS protocol?**
    a) It provides centralized authentication and authorization for remote users
    b) It encrypts sensitive data
    c) It monitors network traffic
    d) It blocks unauthorized access
    Answer: It provides centralized authentication and authorization for remote users
28. **Which cryptographic protocol is commonly used to secure web communications?**
    a) Transport Layer Security (TLS)
    b) Internet Protocol Security (IPSec)
    c) Extensible Authentication Protocol (EAP)
    d) Secure Access Service Edge (SASE)
    Answer: Transport Layer Security (TLS)
29. **Which of the following is a widely used authentication protocol for network access control?**
    a) Extensible Authentication Protocol (EAP)
    b) Transport Layer Security (TLS)
    c) Internet Protocol Security (IPSec)
    d) Secure Access Service Edge (SASE)
    Answer: Extensible Authentication Protocol (EAP)
30. **Why is input validation important for application security?**
    a) It prevents injection attacks by validating input data
    b) It encrypts sensitive data
    c) It monitors network traffic
    d) It blocks unauthorized access
    Answer: It prevents injection attacks by validating input data
31. **What is the purpose of secure cookies in web application security?**
    a) To prevent unauthorized access with encrypted cookies and proper attributes
    b) To monitor network traffic
    c) To block unauthorized access
    d) To encrypt sensitive data
    Answer: To prevent unauthorized access with encrypted cookies and proper attributes
32. **How does static code analysis improve application security?**
    a) By identifying vulnerabilities in source code before execution
    b) By encrypting sensitive data
    c) By monitoring network traffic
    d) By blocking unauthorized access
    Answer: By identifying vulnerabilities in source code before execution
33. **What is the main purpose of code signing in software security?**
    a) To verify software authenticity and integrity with digital signatures
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block unauthorized access
    Answer: To verify software authenticity and integrity with digital signatures

34. **What is the primary function of sandboxing in cyber security?**
    a) To isolate untrusted applications in a controlled environment to prevent threats
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block unauthorized access
    Answer: To isolate untrusted applications in a controlled environment to prevent threats
35. **Why is continuous monitoring important in cyber security?**
    a) It helps detect and respond to security threats in real time
    b) It encrypts sensitive data
    c) It monitors network traffic
    d) It blocks unauthorized access
    Answer: It helps detect and respond to security threats in real time
36. **What is a key security consideration in the acquisition and procurement process?**
    a) Evaluating vendors for security compliance and potential risks
    b) Encrypting sensitive data
    c) Monitoring network traffic
    d) Blocking unauthorized access
    Answer: Evaluating vendors for security compliance and potential risks
37. **Why is asset ownership important in cyber security?**
    a) It assigns responsibility for the protection and management of an asset
    b) It encrypts sensitive data
    c) It monitors network traffic
    d) It blocks unauthorized access
    Answer: It assigns responsibility for the protection and management of an asset
38. **What is the purpose of data classification in an organization?**
    a) To categorize data based on sensitivity and access requirements
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block unauthorized access
    Answer: To categorize data based on sensitivity and access requirements
39. **Why is asset inventory management important in cyber security?**
    a) It helps track and manage IT resources to identify unauthorized devices
    b) It encrypts sensitive data
    c) It monitors network traffic
    d) It blocks unauthorized access
    Answer: It helps track and manage IT resources to identify unauthorized devices
40. **What is the primary function of asset enumeration in cyber security?**
    a) To identify and catalog devices, services, and configurations on a network
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block unauthorized access
    Answer: To identify and catalog devices, services, and configurations on a network

41. **What is the purpose of sanitation in the disposal and decommissioning process?**
    a) To ensure that all sensitive data is removed from a device before disposal or reuse
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block unauthorized access
    Answer: To ensure that all sensitive data is removed from a device before disposal or reuse
42. **Which method ensures that a storage device is permanently destroyed and cannot be recovered?**
    a) Physical destruction like shredding or crushing
    b) Encrypting sensitive data
    c) Monitoring network traffic
    d) Blocking unauthorized access
    Answer: Physical destruction like shredding or crushing
43. **What is the purpose of certification in the context of data disposal?**
    a) To verify that the data was properly sanitized or destroyed per security standards
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block unauthorized access
    Answer: To verify that the data was properly sanitized or destroyed per security standards
44. **Why is data retention an important consideration in the disposal process?**
    a) To ensure data is kept for required compliance periods before secure disposal
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block unauthorized access
    Answer: To ensure data is kept for required compliance periods before secure disposal
45. **What is the primary function of a vulnerability scan in cyber security?**
    a) To identify and assess potential weaknesses in a system or network
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block unauthorized access
    Answer: To identify and assess potential weaknesses in a system or network
46. **What is the primary goal of static analysis in application security?**
    a) To analyze the application source code without execution to identify vulnerabilities
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block unauthorized access
    Answer: To analyze the application source code without execution to identify vulnerabilities
47. **How does dynamic analysis help improve application security?**
    a) By analyzing the application during execution to detect real-time vulnerabilities
    b) To encrypt sensitive data

c) To monitor network traffic

d) To block unauthorized access

Answer: By analyzing the application during execution to detect real-time vulnerabilities

48. **What is the purpose of package monitoring in application security?**

a) To track and analyze third-party dependencies for vulnerabilities

b) To encrypt sensitive data

c) To monitor network traffic

d) To block unauthorized access

Answer: To track and analyze third-party dependencies for vulnerabilities

49. **What is a threat feed in cyber security?**

a) A stream of updates on current and emerging cyber security threats

b) Encrypting sensitive data

c) Monitoring network traffic

d) Blocking unauthorized access

Answer: A stream of updates on current and emerging cyber security threats

50. **What does open-source intelligence (OSINT) involve in cyber security?**

a) Collecting public info from open sources to identify potential threats

b) Encrypting sensitive data

c) Monitoring network traffic

d) Blocking unauthorized access

Answer: Collecting public info from open sources to identify potential threats

51. **What is the primary concern when using proprietary versus third-party software in a security environment?**

a) Proprietary offers more control; third-party may introduce external risks

b) Encrypting sensitive data

c) Monitoring network traffic

d) Blocking unauthorized access

Answer: Proprietary offers more control; third-party may introduce external risks

52. **What is the purpose of an information-sharing organization in cyber security?**

a) To enable organizations to share threat intel and security best practices

b) To encrypt sensitive data

c) To monitor network traffic

d) To block unauthorized access

Answer: To enable organizations to share threat intel and security best practices

53. **What is a common risk associated when accessing information on the dark web?**

a) Exposure to illegal content, cyber crime, and harmful software

b) Encrypting sensitive data

c) Monitoring network traffic

d) Blocking unauthorized access

Answer: Exposure to illegal content, cyber crime, and harmful software

54. **What is the primary goal of penetration testing (pentesting) in cyber security?**

a) To identify vulnerabilities and weaknesses in a system by simulating attacks

b) To encrypt sensitive data

c) To monitor network traffic

d) To block unauthorized access

Answer: To identify vulnerabilities and weaknesses in a system by simulating attacks

55. **What is the purpose of a responsible disclosure program in cyber security?**

a) To let researchers report vulnerabilities ethically and in a controlled way

b) To encrypt sensitive data

c) To monitor network traffic

d) To block unauthorized access

Answer: To let researchers report vulnerabilities ethically and in a controlled way

56. **What is a bug bounty program?**

a) A program where organizations reward reports of security vulnerabilities

b) Encrypting sensitive data

c) Monitoring network traffic

d) Blocking unauthorized access

Answer: A program where organizations reward reports of security vulnerabilities

57. **What is the goal of a system or process audit in cyber security?**

a) To evaluate security controls, find vulnerabilities, and ensure compliance

b) To encrypt sensitive data

c) To monitor network traffic

d) To block unauthorized access

Answer: To evaluate security controls, find vulnerabilities, and ensure compliance

58. **What is the purpose of analysis in vulnerability management?**

a) To assess and understand the severity, impact, and risk of identified vulnerabilities

b) To encrypt sensitive data

c) To monitor network traffic

d) To block unauthorized access

Answer: To assess and understand the severity, impact, and risk of identified vulnerabilities

59. **What does confirmation mean in the context of vulnerability management?**

a) Verifying the existence of a vulnerability and determining its true impact

b) Encrypting sensitive data

c) Monitoring network traffic

d) Blocking unauthorized access

Answer: Verifying the existence of a vulnerability and determining its true impact

60. **What is a false positive in vulnerability scanning?**

a) When a vulnerability is incorrectly identified as present when it is not

b) When a vulnerability is missed

c) When a system is encrypted

d) When network traffic is monitored

Answer: When a vulnerability is incorrectly identified as present when it is not

61. **What does a false negative refer to in vulnerability scanning?**

a) When a vulnerability is missed or incorrectly marked as not present

b) When a vulnerability is identified correctly

c) When a system is encrypted

d) When network traffic is monitored

Answer: When a vulnerability is missed or incorrectly marked as not present

62. **What is the purpose of prioritizing vulnerabilities in a security environment?**

a) To focus on critical vulnerabilities first based on potential impact

b) To encrypt sensitive data

c) To monitor network traffic

d) To block unauthorized access

Answer: To focus on critical vulnerabilities first based on potential impact

63. **What does the Common Vulnerability Scoring System (CVSS) provide?**

a) A standardized method for rating the severity of vulnerabilities

b) Encrypting sensitive data

c) Monitoring network traffic

d) Blocking unauthorized access

Answer: A standardized method for rating the severity of vulnerabilities

64. **What is the Common Vulnerability Enumeration (CVE)?**

a) A database assigning unique IDs to known cyber security vulnerabilities

b) Encrypting sensitive data

c) Monitoring network traffic

d) Blocking unauthorized access

Answer: A database assigning unique IDs to known cyber security vulnerabilities

65. **What is vulnerability classification?**

a) Categorizing vulnerabilities by type, severity, and impact

b) Encrypting sensitive data

c) Monitoring network traffic

d) Blocking unauthorized access

Answer: Categorizing vulnerabilities by type, severity, and impact

66. **What does the exposure factor measure in risk management?**

a) Percentage of asset loss from a specific threat

b) Encrypting sensitive data

c) Monitoring network traffic

d) Blocking unauthorized access

Answer: Percentage of asset loss from a specific threat

67. **What are environmental variables in the context of vulnerability management?**

a) Physical factors like environment, climate, and location affecting risk

b) Encrypting sensitive data

c) Monitoring network traffic

d) Blocking unauthorized access

Answer: Physical factors like environment, climate, and location affecting risk

68. **What does industry or organizational impact refer to in risk management?**

a) The potential consequences a vulnerability may have on the business or industry

b) Encrypting sensitive data

c) Monitoring network traffic

d) Blocking unauthorized access

Answer: The potential consequences a vulnerability may have on the business or industry

69. **What is meant by risk tolerance in cyber security?**
    a) The level of risk an organization is willing to accept to meet goals
    b) Encrypting sensitive data
    c) Monitoring network traffic
    d) Blocking unauthorized access
    Answer: The level of risk an organization is willing to accept to meet goals
70. **What is the primary goal of vulnerability response and remediation?**
    a) To identify, prioritize, and fix vulnerabilities to reduce risk exposure
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block unauthorized access
    Answer: To identify, prioritize, and fix vulnerabilities to reduce risk exposure
71. **What is the purpose of patching in vulnerability management?**
    a) To apply updates and fixes to address known software or hardware vulnerabilities
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block unauthorized access
    Answer: To apply updates and fixes to address known software or hardware vulnerabilities
72. **How does insurance relate to vulnerability management?**
    a) It helps reduce financial loss from attacks but doesn't replace risk management
    b) It encrypts sensitive data
    c) It monitors network traffic
    d) It blocks unauthorized access
    Answer: It helps reduce financial loss from attacks but doesn't replace risk management
73. **What is the purpose of network segmentation in cyber security?**
    a) To divide a network into smaller segments to reduce the impact of a potential breach
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block unauthorized access
    Answer: To divide a network into smaller segments to reduce the impact of a potential breach
74. **What are compensating controls in security?**
    a) Alternative security measures implemented when the primary control cannot be applied
    b) Encrypting sensitive data
    c) Monitoring network traffic
    d) Blocking unauthorized access
    Answer: Alternative security measures implemented when the primary control cannot be applied

75. **What is the difference between exceptions and exemptions in vulnerability management?**
    a) Exceptions allow temporary deviations from security policies while exemptions remove policies entirely
    b) Exemptions allow temporary deviations while exceptions remove policies
    c) Exceptions encrypt data while exemptions monitor traffic
    d) Exemptions block access while exceptions allow access
    Answer: Exceptions allow temporary deviations from security policies while exemptions remove policies entirely
76. **What is the purpose of validating remediation efforts in cyber security?**
    a) To ensure that the fix addresses the vulnerability without adding new risks
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block unauthorized access
    Answer: To ensure that the fix addresses the vulnerability without adding new risks
77. **What does rescanning involve in vulnerability management?**
    a) Scanning after remediation to confirm issues are resolved
    b) Encrypting sensitive data
    c) Monitoring network traffic
    d) Blocking unauthorized access
    Answer: Scanning after remediation to confirm issues are resolved
78. **Why is an audit important in vulnerability management?**
    a) To verify the effectiveness of security controls, compliance, and remediation actions
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block unauthorized access
    Answer: To verify the effectiveness of security controls, compliance, and remediation actions
79. **What is the purpose of verification in vulnerability management?**
    a) To confirm vulnerabilities are remediated and security measures work
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block unauthorized access
    Answer: To confirm vulnerabilities are remediated and security measures work
80. **What is the primary purpose of reporting in vulnerability management?**
    a) To communicate vulnerability status, remediation, and impact to stakeholders
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block unauthorized access
    Answer: To communicate vulnerability status, remediation, and impact to stakeholders
81. **What is the main purpose of monitoring computing resources in an organization?**
    a) To track and manage system health, performance, and security
    b) To encrypt sensitive data

c) To monitor network traffic
d) To block unauthorized access
Answer: To track and manage system health, performance, and security

82. **What is the goal of monitoring applications in a network?**
a) To detect vulnerabilities, errors, and performance issues within the application
b) To encrypt sensitive data
c) To monitor network traffic
d) To block unauthorized access
Answer: To detect vulnerabilities, errors, and performance issues within the application

83. **Why is monitoring infrastructure important in cyber security?**
a) To ensure that the network and devices are functioning securely
b) To encrypt sensitive data
c) To monitor network traffic
d) To block unauthorized access
Answer: To ensure that the network and devices are functioning securely

84. **What is log aggregation in the context of monitoring activities?**
a) The process of collecting system logs into a central repository for analysis
b) Encrypting sensitive data
c) Monitoring network traffic
d) Blocking unauthorized access
Answer: The process of collecting system logs into a central repository for analysis

85. **What is the purpose of alerting in security monitoring?**
a) To notify admins of potential security events needing attention
b) To encrypt sensitive data
c) To monitor network traffic
d) To block unauthorized access
Answer: To notify admins of potential security events needing attention

86. **Why is scanning important in vulnerability management?**
a) To identify system and application vulnerabilities needing remediation
b) To encrypt sensitive data
c) To monitor network traffic
d) To block unauthorized access
Answer: To identify system and application vulnerabilities needing remediation

87. **What is the main purpose of reporting in security monitoring?**
a) To provide detailed analysis of incidents, vulnerabilities, and performance to stakeholders
b) To encrypt sensitive data
c) To monitor network traffic
d) To block unauthorized access
Answer: To provide detailed analysis of incidents, vulnerabilities, and performance to stakeholders

88. **Why is archiving logs important in security operations?**
a) To store historical data for compliance audits and future analysis

b) To encrypt sensitive data
c) To monitor network traffic
d) To block unauthorized access
Answer: To store historical data for compliance audits and future analysis

89. **What is the primary purpose of quarantine in alert response and remediation?**
a) To isolate potentially malicious files or devices to prevent further damage
b) To encrypt sensitive data
c) To monitor network traffic
d) To block unauthorized access
Answer: To isolate potentially malicious files or devices to prevent further damage

90. **What is alert tuning in the context of security operations?**
a) The use of alert thresholds to reduce false positives and highlight relevant alerts
b) Encrypting sensitive data
c) Monitoring network traffic
d) Blocking unauthorized access
Answer: The use of alert thresholds to reduce false positives and highlight relevant alerts

91. **What is the purpose of the Security Content Automation Protocol (SCAP)?**
a) To standardize security info format and automate compliance management
b) To encrypt sensitive data
c) To monitor network traffic
d) To block unauthorized access
Answer: To standardize security info format and automate compliance management

92. **How do security benchmarks help improve an organization's security posture?**
a) They offer best practices for securing systems and networks
b) They encrypt sensitive data
c) They monitor network traffic
d) They block unauthorized access
Answer: They offer best practices for securing systems and networks

93. **What is the difference between agent-based and agentless security monitoring?**
a) Agent-based needs software on the system; agentless does not
b) Agentless needs software; agent-based does not
c) Agent-based encrypts data; agentless monitors traffic
d) Agentless blocks access; agent-based allows access
Answer: Agent-based needs software on the system; agentless does not

94. **What is the role of Security Information and Event Management (SIEM) systems?**
a) To collect, correlate, and analyze security data to identify threats
b) To encrypt sensitive data
c) To monitor network traffic
d) To block unauthorized access
Answer: To collect, correlate, and analyze security data to identify threats

95. **What is the main function of a Security Information and Event Management (SIEM) system?**

a) To collect and analyze event data to detect and respond to threats
b) To encrypt sensitive data
c) To monitor network traffic
d) To block unauthorized access
Answer: To collect and analyze event data to detect and respond to threats

96. **What is the primary role of antivirus software in cyber security?**
a) To detect, block, and remove malware like viruses, worms, and trojans
b) To encrypt sensitive data
c) To monitor network traffic
d) To block unauthorized access
Answer: To detect, block, and remove malware like viruses, worms, and trojans

97. **How does Data Loss Prevention (DLP) help protect sensitive data?**
a) By restricting sensitive data movement inside and outside the network
b) By encrypting sensitive data
c) By monitoring network traffic
d) By blocking unauthorized access
Answer: By restricting sensitive data movement inside and outside the network

98. **What is the purpose of Simple Network Management Protocol (SNMP) traps?**
a) To send alerts to management systems about network device events or issues
b) To encrypt sensitive data
c) To monitor network traffic
d) To block unauthorized access
Answer: To send alerts to management systems about network device events or issues

99. **What is NetFlow used for in network security?**
a) To monitor and analyze traffic to detect unusual patterns or threats
b) To encrypt sensitive data
c) To monitor network traffic
d) To block unauthorized access
Answer: To monitor and analyze traffic to detect unusual patterns or threats

100. **What is the main purpose of vulnerability scanners in cyber security?**
a) To identify and assess vulnerabilities so that they can be remediated
b) To encrypt sensitive data
c) To monitor network traffic
d) To block unauthorized access
Answer: To identify and assess vulnerabilities so that they can be remediated

101. **What is the purpose of firewall rules in network security?**
a) To define allowed network traffic based on specific conditions
b) To encrypt sensitive data
c) To monitor network traffic
d) To block unauthorized access
Answer: To define allowed network traffic based on specific conditions

102. **What is the role of Access Control Lists (ACLs) in firewall configuration?**
a) To define rules to allow or deny traffic by IPs, subnets, and protocols

b) To encrypt sensitive data
c) To monitor network traffic
d) To block unauthorized access
Answer: To define rules to allow or deny traffic by IPs, subnets, and protocols

103. **How are ports and protocols used in firewall configuration?**
a) To control traffic based on port numbers and communication protocols
b) To encrypt sensitive data
c) To monitor network traffic
d) To block unauthorized access
Answer: To control traffic based on port numbers and communication protocols

104. **What is the purpose of a screened subnet in network security?**
a) To isolate internal networks from the internet using an intermediate firewall
b) To encrypt sensitive data
c) To monitor network traffic
d) To block unauthorized access
Answer: To isolate internal networks from the internet using an intermediate firewall

105. **What is a trend in Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)?**
a) The increasing use of machine learning and AI to detect and respond to network threats
b) Encrypting sensitive data
c) Monitoring network traffic
d) Blocking unauthorized access
Answer: The increasing use of machine learning and AI to detect and respond to network threats

106. **What is the role of signatures in IDS or IPS systems?**
a) To match known attack patterns to detect malicious traffic
b) To encrypt sensitive data
c) To monitor network traffic
d) To block unauthorized access
Answer: To match known attack patterns to detect malicious traffic

107. **What is the primary function of agent-based web filtering?**
a) To install agents on devices to monitor and restrict web traffic locally
b) To encrypt sensitive data
c) To monitor network traffic
d) To block unauthorized access
Answer: To install agents on devices to monitor and restrict web traffic locally

108. **What is the role of a centralized proxy in web filtering?**
a) To act as an intermediary to enforce security policies between users and web services
b) To encrypt sensitive data
c) To monitor network traffic
d) To block unauthorized access

Answer: To act as an intermediary to enforce security policies between users and web services

109. **What is the purpose of URL scanning in web filtering?**
    a) To examine URLs for malicious content, phishing, or inappropriate material before access
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block unauthorized access
    Answer: To examine URLs for malicious content, phishing, or inappropriate material before access
110. **How does content categorization enhance web filtering?**
    a) By classifying web content into categories to apply specific access rules
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block unauthorized access
    Answer: By classifying web content into categories to apply specific access rules
111. **What are block rules in web filtering?**
    a) Rules that prevent access to specific sites, content, or categories per security policies
    b) Encrypting sensitive data
    c) Monitoring network traffic
    d) Blocking unauthorized access
    Answer: Rules that prevent access to specific sites, content, or categories per security policies
112. **How does reputation-based web filtering work?**
    a) It evaluates website reputation using history, feedback, and security issues
    b) Encrypting sensitive data
    c) Monitoring network traffic
    d) Blocking unauthorized access
    Answer: It evaluates website reputation using history, feedback, and security issues
113. **What is the primary function of operating system security?**
    a) To protect the operating system from unauthorized access and attacks
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block unauthorized access
    Answer: To protect the operating system from unauthorized access and attacks
114. **How does group policy contribute to operating system security?**
    a) By enforcing security settings and configurations across network systems
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block unauthorized access
    Answer: By enforcing security settings and configurations across network systems
115. **What does SELinux provide in terms of operating system security?**
    a) A mandatory access control system that restricts process and user interactions with

resources
b) Encrypting sensitive data
c) Monitoring network traffic
d) Blocking unauthorized access
Answer: A mandatory access control system that restricts process and user interactions with resources

116. **Why is the implementation of secure protocols essential in network security?**
a) To ensure secure, confidential data transmission across the network
b) To encrypt sensitive data
c) To monitor network traffic
d) To block unauthorized access
Answer: To ensure secure, confidential data transmission across the network

117. **Which factor should be considered when selecting a network protocol?**
a) The security level, including encryption and authentication
b) Encrypting sensitive data
c) Monitoring network traffic
d) Blocking unauthorized access
Answer: The security level, including encryption and authentication

118. **What is an important consideration when selecting a port for network communication?**
a) The port security and whether or not it is commonly targeted by attackers
b) Encrypting sensitive data
c) Monitoring network traffic
d) Blocking unauthorized access
Answer: The port security and whether or not it is commonly targeted by attackers

119. **Why is transport method selection crucial in secure communications?**
a) It determines a secure data transmission method and prevents unauthorized access
b) Encrypting sensitive data
c) Monitoring network traffic
d) Blocking unauthorized access
Answer: It determines a secure data transmission method and prevents unauthorized access

120. **What is the main function of DNS filtering in network security?**
a) To block access to malicious websites by filtering DNS requests
b) To encrypt sensitive data
c) To monitor network traffic
d) To block unauthorized access
Answer: To block access to malicious websites by filtering DNS requests

121. **Why is email security important in protecting organizations from cyber threats?**
a) To prevent phishing, malware, and other malicious activities delivered through email
b) To encrypt sensitive data
c) To monitor network traffic
d) To block unauthorized access

Answer: To prevent phishing, malware, and other malicious activities delivered through email

122. **What is the purpose of Domain-based Message Authentication, Reporting, and Conformance (DMARC)?**
    a) To authenticate and report emails to prevent spoofing and phishing
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block unauthorized access
    Answer: To authenticate and report emails to prevent spoofing and phishing
123. **What does DomainKeys Identified Mail (DKIM) provide for email security?**
    a) It adds a digital signature to verify sender identity and message integrity
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block unauthorized access
    Answer: It adds a digital signature to verify sender identity and message integrity
124. **What is the function of Sender Policy Framework (SPF) in email security?**
    a) To define authorized mail servers to prevent domain spoofing
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block unauthorized access
    Answer: To define authorized mail servers to prevent domain spoofing
125. **What is a gateway in the context of network security?**
    a) A device or software that connects two networks and filters traffic
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block unauthorized access
    Answer: A device or software that connects two networks and filters traffic
126. **What is the primary purpose of File Integrity Monitoring (FIM) in cyber security?**
    a) To detect unauthorized changes to files and directories
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block unauthorized access
    Answer: To detect unauthorized changes to files and directories
127. **How does Data Loss Prevention (DLP) help protect sensitive information?**
    a) By blocking unauthorized transfer or sharing of sensitive data
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block unauthorized access
    Answer: By blocking unauthorized transfer or sharing of sensitive data
128. **What is the main purpose of Network Access Control (NAC) in cyber security?**
    a) To enforce security policies and control device access to the network
    b) To encrypt sensitive data
    c) To monitor network traffic

d) To block unauthorized access

Answer: To enforce security policies and control device access to the network

129. **What is the main difference between Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR)?**

a) XDR integrates data from multiple security layers; EDR focuses on endpoints only

b) EDR integrates multiple layers; XDR focuses on endpoints

c) XDR encrypts data; EDR monitors traffic

d) EDR blocks access; XDR allows access

Answer: XDR integrates data from multiple security layers; EDR focuses on endpoints only

130. **How do User Behavior Analytics (UBA) enhance cyber security?**

a) By analyzing user behavior to detect activities that may indicate a security breach

b) To encrypt sensitive data

c) To monitor network traffic

d) To block unauthorized access

Answer: By analyzing user behavior to detect activities that may indicate a security breach

131. **What is the purpose of provisioning and deprovisioning user accounts in an organization?**

a) To ensure users have proper access when joining or leaving the organization

b) To encrypt sensitive data

c) To monitor network traffic

d) To block unauthorized access

Answer: To ensure users have proper access when joining or leaving the organization

132. **What is the impact of incorrect permission assignments in an organization?**

a) It can lead to unauthorized access, data breaches, and compromised systems

b) To encrypt sensitive data

c) To monitor network traffic

d) To block unauthorized access

Answer: It can lead to unauthorized access, data breaches, and compromised systems

133. **What is the purpose of identity proofing in the context of cyber security?**

a) To verify that a user is who they claim to be before granting access to a system

b) To encrypt sensitive data

c) To monitor network traffic

d) To block unauthorized access

Answer: To verify that a user is who they claim to be before granting access to a system

134. **What is federation in identity management?**

a) The process of linking and sharing user identity information across systems or organizations

b) Encrypting sensitive data

c) Monitoring network traffic

d) Blocking unauthorized access

Answer: The process of linking and sharing user identity information across systems or organizations

135. **What is the advantage of Single Sign-On (SSO) in an organization's security system?**
a) It allows users to authenticate once to access multiple applications without repeated login
b) To encrypt sensitive data
c) To monitor network traffic
d) To block unauthorized access
Answer: It allows users to authenticate once to access multiple applications without repeated login

136. **What is the role of Lightweight Directory Access Protocol (LDAP) in identity management?**
a) It is used to query and modify directory services to store user and authentication information
b) To encrypt sensitive data
c) To monitor network traffic
d) To block unauthorized access
Answer: It is used to query and modify directory services to store user and authentication information

137. **What does Open Authorization (OAuth) provide in access management?**
a) It lets third-party applications access user resources without sharing passwords
b) To encrypt sensitive data
c) To monitor network traffic
d) To block unauthorized access
Answer: It lets third-party applications access user resources without sharing passwords

138. **What is the role of Security Assertion Markup Language (SAML) in Single Sign-On (SSO)?**
a) It enables the exchange of authentication and authorization data between identity and service providers
b) To encrypt sensitive data
c) To monitor network traffic
d) To block unauthorized access
Answer: It enables the exchange of authentication and authorization data between identity and service providers

139. **What does interoperability in cyber security refer to?**
a) The ability of systems, devices, or apps to work together and exchange info securely
b) To encrypt sensitive data
c) To monitor network traffic
d) To block unauthorized access
Answer: The ability of systems, devices, or apps to work together and exchange info securely

140. **What is the purpose of attestation in security?**
    a) To verify system integrity to ensure it hasn't been altered or tampered with
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block unauthorized access
    Answer: To verify system integrity to ensure it hasn't been altered or tampered with
141. **What is the primary goal of Mandatory Access Control (MAC)?**
    a) To enforce access restrictions via system policies that users can't override
    b) To allow owners to decide access
    c) To assign permissions based on roles
    d) To use attributes for access control
    Answer: To enforce access restrictions via system policies that users can't override
142. **What is the key characteristic of Discretionary Access Control (DAC)?**
    a) It allows owners of resources to decide who has access to their resources
    b) To enforce system policies
    c) To assign permissions based on roles
    d) To use attributes for access control
    Answer: It allows owners of resources to decide who has access to their resources
143. **What does Role-Based Access Control (RBAC) rely on for assigning permissions?**
    a) It assigns permissions based on a user's role in the organization
    b) System policies that users can't override
    c) Owners deciding access
    d) Attributes for access control
    Answer: It assigns permissions based on a user's role in the organization
144. **What is Rule-Based Access Control?**
    a) It enforces access based on predefined rules and policies, not users or roles
    b) Owners decide access
    c) Permissions based on roles
    d) Attributes for access control
    Answer: It enforces access based on predefined rules and policies, not users or roles
145. **What does Attribute-Based Access Control (ABAC) use to determine access?**
    a) It uses attributes like user traits, environment, and resources to determine access
    b) Owners decide access
    c) Permissions based on roles
    d) Predefined rules and policies
    Answer: It uses attributes like user traits, environment, and resources to determine access
146. **What is the function of time-of-day restrictions in access control?**
    a) To limit access to systems or resources based on the time of day or specific hours
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block unauthorized access

Answer: To limit access to systems or resources based on the time of day or specific hours

147. **What does the principle of least privilege ensure in access control?**
    a) It ensures users get only the minimum access needed to do their tasks
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block unauthorized access
    Answer: It ensures users get only the minimum access needed to do their tasks
148. **What is the main purpose of multi-factor authentication (MFA)?**
    a) It requires two or more verification methods to enhance security
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block unauthorized access
    Answer: It requires two or more verification methods to enhance security
149. **What is an example of an implementation of multi-factor authentication (MFA)?**
    a) Requiring both a password and a fingerprint scan to log in
    b) Encrypting sensitive data
    c) Monitoring network traffic
    d) Blocking unauthorized access
    Answer: Requiring both a password and a fingerprint scan to log in
150. **What is the primary advantage of using biometrics for authentication?**
    a) Biometrics provide a unique, hard-to-replicate verification using physical traits
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block unauthorized access
    Answer: Biometrics provide a unique, hard-to-replicate verification using physical traits
151. **What is the difference between hard and soft authentication tokens?**
    a) Hard tokens are physical devices; soft tokens are software-based applications for authentication
    b) Soft tokens are physical; hard tokens are software-based
    c) Hard tokens encrypt data; soft tokens monitor traffic
    d) Soft tokens block access; hard tokens allow access
    Answer: Hard tokens are physical devices; soft tokens are software-based applications for authentication
152. **What is the primary function of security keys in authentication?**
    a) Security keys are a physical device used to verify identity, often in two-factor authentication (2FA)
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block unauthorized access
    Answer: Security keys are a physical device used to verify identity, often in two-factor authentication (2FA)

153. **Which of the following is an example of something you know in authentication?**
a) A password or PIN that you must input during login
b) A smartphone for codes
c) A fingerprint scan
d) A GPS location
Answer: A password or PIN that you must input during login

154. **What is an example of something you have as a factor in authentication?**
a) A smartphone that generates authentication codes for login
b) A password or PIN
c) A fingerprint scan
d) A GPS location
Answer: A smartphone that generates authentication codes for login

155. **Which of the following is an example of something you are as a factor in authentication?**
a) A fingerprint scan that is unique to you
b) A password or PIN
c) A smartphone for codes
d) A GPS location
Answer: A fingerprint scan that is unique to you

156. **What is the purpose of somewhere you are as an authentication factor?**
a) To authenticate a user based on their physical location, often using GPS or IP address
b) To encrypt sensitive data
c) To monitor network traffic
d) To block unauthorized access
Answer: To authenticate a user based on their physical location, often using GPS or IP address

157. **Why is password length important in securing accounts?**
a) Longer passwords are harder to crack through brute force
b) To encrypt sensitive data
c) To monitor network traffic
d) To block unauthorized access
Answer: Longer passwords are harder to crack through brute force

158. **Which of the following is a password best practice for ensuring security?**
a) Using a combination of upper and lowercase letters, numbers, and special characters
b) Reusing passwords across systems
c) Using short passwords
d) Never changing passwords
Answer: Using a combination of upper and lowercase letters, numbers, and special characters

159. **What is the recommended password length for maximum security?**
a) At least 12 characters
b) 6 characters
c) 8 characters

d) 10 characters

Answer: At least 12 characters

160. **What does password complexity refer to in security?**

a) Using a mix of characters: uppercase and lowercase letters, numbers, and symbols

b) Reusing passwords across systems

c) Using short passwords

d) Never changing passwords

Answer: Using a mix of characters: uppercase and lowercase letters, numbers, and symbols

161. **Why is reusing passwords a security risk?**

a) Reusing passwords can threaten additional systems if one password is compromised

b) It encrypts sensitive data

c) It monitors network traffic

d) It blocks unauthorized access

Answer: Reusing passwords can threaten additional systems if one password is compromised

162. **What is the recommended practice for password expiration?**

a) Passwords should be changed periodically to reduce risk

b) Never change passwords

c) Reuse passwords across systems

d) Use short passwords

Answer: Passwords should be changed periodically to reduce risk

163. **What is the main reason to track password age in an organization?**

a) To ensure passwords are periodically updated to reduce the risk of being compromised

b) To encrypt sensitive data

c) To monitor network traffic

d) To block unauthorized access

Answer: To ensure passwords are periodically updated to reduce the risk of being compromised

164. **What is the primary function of a password manager?**

a) To securely store and manage passwords for various accounts

b) To encrypt sensitive data

c) To monitor network traffic

d) To block unauthorized access

Answer: To securely store and manage passwords for various accounts

165. **What is passwordless authentication?**

a) An authentication method without traditional passwords, using biometrics or tokens instead

b) Using short passwords

c) Reusing passwords across systems

d) Never changing passwords

Answer: An authentication method without traditional passwords, using biometrics or tokens instead

166. **What is the purpose of privileged access management (PAM) tools?**
    a) To control and monitor access to critical systems and data by privileged users
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block unauthorized access
    Answer: To control and monitor access to critical systems and data by privileged users
167. **What are just-in-time permissions?**
    a) Permissions granted to users only when necessary, often with expirations
    b) Permanent permissions for all users
    c) Encrypting sensitive data
    d) Monitoring network traffic
    Answer: Permissions granted to users only when necessary, often with expirations
168. **What is the primary function of password vaulting?**
    a) To securely store and manage passwords in an encrypted repository
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block unauthorized access
    Answer: To securely store and manage passwords in an encrypted repository
169. **What are ephemeral credentials used for?**
    a) To provide temporary access to systems, often with an expiration time
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block unauthorized access
    Answer: To provide temporary access to systems, often with an expiration time
170. **What is the primary use case for automation and scripting in security operations?**
    a) To automate repetitive security tasks
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block unauthorized access
    Answer: To automate repetitive security tasks
171. **What is the goal of user provisioning in an organization?**
    a) To assign appropriate access rights and permissions to users based on their roles
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block unauthorized access
    Answer: To assign appropriate access rights and permissions to users based on their roles
172. **What is the purpose of resource provisioning in IT security?**
    a) To allocate and manage resources like storage and servers
    b) To encrypt sensitive data
    c) To monitor network traffic

d) To block unauthorized access

Answer: To allocate and manage resources like storage and servers

173. **What are guardrails in the context of security operations?**

a) Predefined policies that prevent harmful actions while allowing flexibility

b) Encrypting sensitive data

c) Monitoring network traffic

d) Blocking unauthorized access

Answer: Predefined policies that prevent harmful actions while allowing flexibility

174. **What is the purpose of security groups in identity management?**

a) To group users with similar security needs to simplify management

b) To encrypt sensitive data

c) To monitor network traffic

d) To block unauthorized access

Answer: To group users with similar security needs to simplify management

175. **What is the role of ticket creation in a security incident management process?**

a) To document and track security issues for resolution and auditing

b) To encrypt sensitive data

c) To monitor network traffic

d) To block unauthorized access

Answer: To document and track security issues for resolution and auditing

176. **What is the purpose of escalation in incident response?**

a) To escalate incidents to authorities or specialized teams when necessary

b) To encrypt sensitive data

c) To monitor network traffic

d) To block unauthorized access

Answer: To escalate incidents to authorities or specialized teams when necessary

177. **What does enabling or disabling services and access mean in security operations?**

a) The process of granting or revoking access to services based on policies and roles

b) To encrypt sensitive data

c) To monitor network traffic

d) To block unauthorized access

Answer: The process of granting or revoking access to services based on policies and roles

178. **What is the purpose of continuous integration and testing in security operations?**

a) To detect security vulnerabilities early through automated testing during development

b) To encrypt sensitive data

c) To monitor network traffic

d) To block unauthorized access

Answer: To detect security vulnerabilities early through automated testing during development

179. **How do integrations in Application Programming Interfaces (APIs) contribute to security operations?**

a) They enable security tools to communicate and share data
b) To encrypt sensitive data
c) To monitor network traffic
d) To block unauthorized access
Answer: They enable security tools to communicate and share data

180. **What is a key benefit of automation in security operations?**
a) It increases efficiency by reducing manual operations
b) To encrypt sensitive data
c) To monitor network traffic
d) To block unauthorized access
Answer: It increases efficiency by reducing manual operations

181. **How does automation contribute to time savings in security operations?**
a) By streamlining repetitive tasks such as patch management and log analysis
b) To encrypt sensitive data
c) To monitor network traffic
d) To block unauthorized access
Answer: By streamlining repetitive tasks such as patch management and log analysis

182. **Why is enforcing baselines important in security operations?**
a) It ensures secure, consistent system and network configurations organization-wide
b) To encrypt sensitive data
c) To monitor network traffic
d) To block unauthorized access
Answer: It ensures secure, consistent system and network configurations organization-wide

183. **How do standard infrastructure configurations improve security?**
a) It ensures uniform system configurations to simplify security management
b) To encrypt sensitive data
c) To monitor network traffic
d) To block unauthorized access
Answer: It ensures uniform system configurations to simplify security management

184. **What is a secure way to scale an organization's infrastructure?**
a) By planning and applying security measures as the system grows
b) To encrypt sensitive data
c) To monitor network traffic
d) To block unauthorized access
Answer: By planning and applying security measures as the system grows

185. **What role does employee retention play in cyber security?**
a) Employee retention helps ensure security knowledge and expertise are retained
b) To encrypt sensitive data
c) To monitor network traffic
d) To block unauthorized access
Answer: Employee retention helps ensure security knowledge and expertise are retained

186. **Why is a fast reaction time important in security incident management?**
a) A quick response helps to mitigate the impact of security incidents
b) To encrypt sensitive data
c) To monitor network traffic
d) To block unauthorized access
Answer: A quick response helps to mitigate the impact of security incidents

187. **What is a workforce multiplier in the context of security operations?**
a) Using tools and automation to extend the abilities of a limited security team
b) Encrypting sensitive data
c) Monitoring network traffic
d) Blocking unauthorized access
Answer: Using tools and automation to extend the abilities of a limited security team

188. **Why is complexity an important consideration in security operations?**
a) Greater complexity makes systems harder to manage and more vulnerable
b) To encrypt sensitive data
c) To monitor network traffic
d) To block unauthorized access
Answer: Greater complexity makes systems harder to manage and more vulnerable

189. **What is a critical factor to consider when evaluating the cost of a security solution?**
a) Balance security benefits with implementation and maintenance costs
b) Encrypting sensitive data
c) Monitoring network traffic
d) Blocking unauthorized access
Answer: Balance security benefits with implementation and maintenance costs

190. **What is the risk of having a single point of failure in a network or system?**
a) Failure of a single component can disrupt service, affecting security and availability
b) Encrypting sensitive data
c) Monitoring network traffic
d) Blocking unauthorized access
Answer: Failure of a single component can disrupt service, affecting security and availability

191. **What is technical debt in the context of security?**
a) The accumulated cost of delaying updates or improvements, increasing future challenges
b) Encrypting sensitive data
c) Monitoring network traffic
d) Blocking unauthorized access
Answer: The accumulated cost of delaying updates or improvements, increasing future challenges

192. **Why is ongoing supportability important in the context of security systems?**
a) Ongoing support ensures that security systems are updated and maintained to handle emerging threats

b) Encrypting sensitive data
c) Monitoring network traffic
d) Blocking unauthorized access
Answer: Ongoing support ensures that security systems are updated and maintained to handle emerging threats

193. **What is the primary goal of the preparation phase in incident response?**
a) To develop and test incident response plans
b) To encrypt sensitive data
c) To monitor network traffic
d) To block unauthorized access
Answer: To develop and test incident response plans

194. **Which action is typically performed during the detection phase of an incident response?**
a) Analyze system logs and alerts
b) Encrypt sensitive data
c) Monitor network traffic
d) Block unauthorized access
Answer: Analyze system logs and alerts

195. **What is the main objective of the analysis phase in incident response?**
a) To understand the impact and scope of the incident
b) To encrypt sensitive data
c) To monitor network traffic
d) To block unauthorized access
Answer: To understand the impact and scope of the incident

196. **During the containment phase of an incident response, which action is performed?**
a) Isolate affected systems to prevent further damage
b) Encrypt sensitive data
c) Monitor network traffic
d) Block unauthorized access
Answer: Isolate affected systems to prevent further damage

197. **What is the goal of the eradication phase in incident response?**
a) To remove any malicious code and vulnerabilities
b) To encrypt sensitive data
c) To monitor network traffic
d) To block unauthorized access
Answer: To remove any malicious code and vulnerabilities

198. **Which of the following is a key action in the recovery phase of incident response?**
a) Restore systems and services to normal
b) Encrypt sensitive data
c) Monitor network traffic
d) Block unauthorized access
Answer: Restore systems and services to normal

199. **What is the main purpose of the lessons learned phase in incident response?**
    a) To improve the organization's ability to detect and respond to future incidents
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block unauthorized access
    Answer: To improve the organization's ability to detect and respond to future incidents
200. **What is the primary purpose of training in security operations?**
    a) To ensure employees understand their role in security
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block unauthorized access
    Answer: To ensure employees understand their role in security
201. **Which activity is performed during testing in security operations?**
    a) Real-time simulations of breaches
    b) Encrypting sensitive data
    c) Monitoring network traffic
    d) Blocking unauthorized access
    Answer: Real-time simulations of breaches
202. **What is the primary goal of a tabletop exercise in security testing?**
    a) To evaluate the response plan's effectiveness
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block unauthorized access
    Answer: To evaluate the response plan's effectiveness
203. **Which of the following best describes a simulation in security operations testing?**
    a) A live exercise to test security systems against attacks
    b) Encrypting sensitive data
    c) Monitoring network traffic
    d) Blocking unauthorized access
    Answer: A live exercise to test security systems against attacks
204. **What is the purpose of root cause analysis in incident response?**
    a) To identify the source of a security incident
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block unauthorized access
    Answer: To identify the source of a security incident
205. **Which of the following best describes threat hunting?**
    a) The proactive search for potential threats and security breaches
    b) Encrypting sensitive data
    c) Monitoring network traffic
    d) Blocking unauthorized access
    Answer: The proactive search for potential threats and security breaches

206. **What is the purpose of a legal hold in digital forensics?**
    a) To preserve evidence by preventing data deletion or alteration
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block unauthorized access
    Answer: To preserve evidence by preventing data deletion or alteration
207. **What does the chain of custody refer to in digital forensics?**
    a) The chronological documentation of the possession of evidence
    b) Encrypting sensitive data
    c) Monitoring network traffic
    d) Blocking unauthorized access
    Answer: The chronological documentation of the possession of evidence
208. **Which activity is performed during the acquisition phase of digital forensics?**
    a) Preserving digital evidence for analysis
    b) Encrypting sensitive data
    c) Monitoring network traffic
    d) Blocking unauthorized access
    Answer: Preserving digital evidence for analysis
209. **What is the main purpose of reporting in digital forensics?**
    a) To detail how evidence was acquired and analyzed
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block unauthorized access
    Answer: To detail how evidence was acquired and analyzed
210. **What does preservation of digital evidence ensure in digital forensics?**
    a) The integrity and authenticity of evidence over time
    b) Encrypting sensitive data
    c) Monitoring network traffic
    d) Blocking unauthorized access
    Answer: The integrity and authenticity of evidence over time
211. **What is the focus of e-discovery in digital forensics?**
    a) The search and retrieval of relevant digital evidence for legal cases
    b) Encrypting sensitive data
    c) Monitoring network traffic
    d) Blocking unauthorized access
    Answer: The search and retrieval of relevant digital evidence for legal cases
212. **What is the primary purpose of log data in security operations?**
    a) To record events and activities for security monitoring and analysis
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block unauthorized access
    Answer: To record events and activities for security monitoring and analysis

213. **Which of the following is most commonly found in firewall logs?**
    a) Traffic blocked or allowed based on security rules
    b) Encrypting sensitive data
    c) Monitoring network traffic
    d) Blocking unauthorized access
    Answer: Traffic blocked or allowed based on security rules
214. **What type of information is typically captured in application logs?**
    a) User activities and application performance issues
    b) Encrypting sensitive data
    c) Monitoring network traffic
    d) Blocking unauthorized access
    Answer: User activities and application performance issues
215. **What is the primary function of endpoint logs in a security context?**
    a) To record activities and events on user devices
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block unauthorized access
    Answer: To record activities and events on user devices
216. **Which type of logs are specifically tailored to the security features of an operating system?**
    a) OS specific security logs
    b) Firewall logs
    c) Application logs
    d) Network logs
    Answer: OS specific security logs
217. **What is the purpose of IPS and IDS logs?**
    a) To record malicious or suspicious activities detected
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block unauthorized access
    Answer: To record malicious or suspicious activities detected
218. **Which of the following is typically recorded in network logs?**
    a) Details of connections, protocols, and IP addresses
    b) Encrypting sensitive data
    c) Monitoring network traffic
    d) Blocking unauthorized access
    Answer: Details of connections, protocols, and IP addresses
219. **What does metadata in security logs provide information about?**
    a) The who, what, where, and when of data interaction
    b) Encrypting sensitive data
    c) Monitoring network traffic
    d) Blocking unauthorized access
    Answer: The who, what, where, and when of data interaction

220. **What is the primary purpose of vulnerability scans in security operations?**
    a) To identify security weaknesses and vulnerabilities
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block unauthorized access
    Answer: To identify security weaknesses and vulnerabilities
221. **What is an advantage of using automated reports in security monitoring?**
    a) They generate consistent, timely analysis of security data
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block unauthorized access
    Answer: They generate consistent, timely analysis of security data
222. **What is the role of dashboards in security operations?**
    a) To provide a visual interface for monitoring security metrics
    b) To encrypt sensitive data
    c) To monitor network traffic
    d) To block unauthorized access
    Answer: To provide a visual interface for monitoring security metrics
223. **What type of information is captured in packet captures?**
    a) Captured network traffic like headers and payloads
    b) Encrypting sensitive data
    c) Monitoring network traffic
    d) Blocking unauthorized access
    Answer: Captured network traffic like headers and payloads