SYSTEM MCQs COLLECTION

NSCT Prep

Free MCQ Practice for NSCT Test Preparation

Cyber Security

1440 Multiple Choice Questions

nsctprep.dev

This dataset is created and compiled by Muhammad Abdullah Awais

Easy Questions

480 questions

Q1. What is cyber security?

A. Assembling and configuring enterprise hardware components
B. Developing and deploying scalable application software
C. Architecting and building responsive web applications
D. Protecting computer systems, networks, and data from digital attacks

Answer: D

Q2. Which of the following is a goal of cyber security?

A. Improving user interface design
B. Increasing internet speed
C. Reducing hardware costs
D. Protecting confidentiality of data

Answer: D

Q3. What does the CIA triad stand for in cyber security?

A. Computer, Internet, Application
B. Confidentiality, Integrity, Availability
C. Central Intelligence Agency
D. Code, Integration, Authentication

Answer: B

Q4. Which of the following is an example of a cyber threat?

A. Phishing email
B. Power outage
C. Software update
D. Hardware upgrade

Answer: A

Q5. What is the primary purpose of a firewall?

A. Reduce file sizes through compression algorithms
B. Filter incoming and outgoing network traffic
C. Maintain redundant copies of critical data
D. Optimize internet speed and network throughput

Answer: B

Q6. Which of the following is considered personal identifiable information (PII)?

A. Public news article
B. National ID card number
C. Weather forecast
D. Open-source code

Answer: B

Q7. What is a vulnerability in the context of cyber security?

A. A security tool for scanning and detecting vulnerabilities
B. A category of self-replicating malicious software
C. A standard network communication protocol for data transfer
D. A weakness in a system that can be exploited

Answer: D

Q8. What is the role of antivirus software?

A. Detect and remove malicious software
B. Expand available system memory resources
C. Organize and catalog system file structures
D. Schedule and generate automated data backups

Answer: A

Q9. Which organization is responsible for cyber security standards globally?

A. ISO (International Organization for Standardization)
B. UNICEF within enterprise security environments
C. WHO within enterprise security environments
D. FIFA within enterprise security environments

Answer: A

Q10. What does the term 'threat' mean in cyber security?

A. A potential cause of an unwanted incident that may harm a system
B. A routine patch applied to update system software
C. A high-level language used for development
D. A hardware component inside wireless networking routers

Answer: A

Q11. What does confidentiality mean in information security?

A. Data is regularly backed up to remote locations
B. Data is continuously available to all authorized users
C. Data is only accessible to authorized individuals
D. Data remains unmodified and accurately preserved

Answer: C

Q12. What does integrity mean in information security?

A. Data remains accurate and unaltered during storage and transmission
B. Data is available 24/7 within enterprise security environments
C. Data is deleted after use within enterprise security environments
D. Data is always encrypted regardless of the specific situation or context

Answer: A

Q13. What does availability mean in the CIA triad?

A. Data can be accessed by anyone in security contexts
B. Data is encrypted within enterprise security environments
C. Data is stored in the cloud within enterprise security environments
D. Authorized users can access data and resources when needed

Answer: D

Q14. Which of the following is a strong password practice?

A. Using password123 within enterprise security environments
B. Using your name as password within enterprise security environments
C. Using a mix of uppercase, lowercase, numbers, and special characters
D. Using the same password for all accounts

Answer: C

Q15. What is encryption?

A. Deleting files permanently within enterprise security environments
B. Converting data into a coded format to prevent unauthorized access
C. Compressing files to save space within enterprise security environments
D. Backing up data to cloud within enterprise security environments

Answer: B

Q16. What is the purpose of a backup?

A. To encrypt files using established cryptographic standards
B. To speed up computer processing performance speed
C. To delete unnecessary files within the data management framework
D. To create a copy of data for recovery in case of data loss

Answer: D

Q17. Which of the following is a type of security control?

A. Gaming control
B. Preventive control
C. Marketing control
D. Advertising control

Answer: B

Q18. What is authentication?

A. Verifying the identity of a user or system
B. Applying cryptographic ciphers to protect data
C. Compressing files to reduce disk storage consumption
D. Architecting and building responsive web applications

Answer: A

Q19. What does a password manager do?

A. Attempts to crack and compromise stored passwords
B. Broadcasts and shares passwords on public platforms
C. Permanently removes and erases stored passwords
D. Securely stores and manages passwords for various accounts

Answer: D

Q20. Which is an example of 'something you know' in authentication?

A. Smart card
B. Retina scan
C. Password
D. Fingerprint

Answer: C

Q21. What is cryptography?

A. Study of databases within enterprise security environments
B. Study of networks within enterprise security environments
C. Study of computers within enterprise security environments
D. The practice of securing communication through encoding messages

Answer: D

Q22. What is plaintext in cryptography?

A. The original readable message before encryption
B. A cryptographic key applied to data protection workflows
C. A type of cipher applied to data protection workflows
D. Encrypted data within enterprise security environments

Answer: A

Q23. What is ciphertext?

A. A hash function within modern computing environments
B. A type of key within modern computing environments
C. A readable message within modern computing environments
D. The encrypted, unreadable form of a message

Answer: D

Q24. What is a cryptographic key?

A. A physical metal key for a locked server room
B. A piece of information used to encrypt and decrypt data
C. A strain of self-replicating malicious software programs
D. A physical cable used for network connections

Answer: B

Q25. Which of the following is a symmetric encryption algorithm?

A. RSA
B. ECC
C. Diffie-Hellman
D. AES

Answer: D

Q26. What is decryption?

A. Converting plaintext to ciphertext
B. Converting ciphertext back to plaintext
C. Compressing data files for reduced storage space consumption
D. Deleting encrypted data in security contexts

Answer: B

Q27. What is the Caesar cipher?

A. An asymmetric algorithm within modern computing environments
B. A hash function within modern computing environments
C. A modern encryption standard applied to data protection workflows
D. A simple substitution cipher that shifts letters by a fixed number

Answer: D

Q28. What is the purpose of a digital signature?

A. To compress files for reducing disk storage consumption
B. To sign documents physically within enterprise computing infrastructure
C. To verify the authenticity and integrity of a digital message
D. To encrypt all data using established cryptographic standards

Answer: C

Q29. Which of the following is an asymmetric encryption algorithm?

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

Answer: C

Q30. What is a public key in asymmetric cryptography?

A. A key that is freely shared and used for encrypting messages
B. A key that must be kept secret used in enterprise computing environments
C. A password within the identity management system
D. A physical key within modern computing environments

Answer: A

Q31. What is a firewall?

A. A physical fireproof barrier within a building structure
B. A category of self-replicating malicious software
C. A high-level language used for development used in enterprise computing environments
D. A network security device that monitors and filters network traffic

Answer: D

Q32. What does VPN stand for?

A. Very Personal Network
B. Verified Public Network
C. Virtual Private Network
D. Visual Processing Node

Answer: C

Q33. What is the purpose of a VPN?

A. To reduce data sizes through compression methods
B. To increase internet speed for improved operational efficiency
C. To block all websites within enterprise computing infrastructure
D. To create a secure, encrypted connection over a public network

Answer: D

Q34. What protocol is used for secure web browsing?

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

Answer: B

Q35. What is a network intrusion?

A. Adding new devices to a network
B. Upgrading network hardware
C. Unauthorized access to a computer network
D. Installing network software

Answer: C

Q36. Which port number is commonly used for HTTPS?

A. 21
B. 80
C. 25
D. 443

Answer: D

Q37. What is a DMZ in networking?

A. A network segment between internal and external networks to host public-facing services
B. A military zone within enterprise computing environments
C. A wireless network used in enterprise network infrastructure
D. A network routing device for managing enterprise traffic flows

Answer: A

Q38. What does IDS stand for in network security?

A. Integrated Development System
B. Internal Data Storage
C. Internet Download Service
D. Intrusion Detection System

Answer: D

Q39. What is packet filtering?

A. Encrypting all packets regardless of the specific situation or context
B. Deleting all packets regardless of the specific situation or context
C. Compressing network packets within enterprise security environments
D. Examining packets and allowing or blocking them based on defined rules

Answer: D

Q40. What is the function of a proxy server in security?

A. To act as an intermediary between users and the internet, providing anonymity and filtering
B. To directly connect to the internet within enterprise computing infrastructure
C. To create viruses for enterprise computing environments and management
D. To store passwords within enterprise computing infrastructure and management

Answer: A

Q41. What is OS hardening?

A. Making the OS run faster within enterprise security environments
B. Increasing storage capacity within enterprise security environments
C. Installing new applications within enterprise security environments
D. The process of securing an operating system by reducing its attack surface

Answer: D

Q42. Why is it important to keep operating systems updated?

A. To fix security vulnerabilities and improve system stability
B. To make the computer slower within enterprise computing infrastructure
C. To increase file storage within the data management framework
D. To change the wallpaper within enterprise computing infrastructure

Answer: A

Q43. What is a user account in operating system security?

A. A software application used for enterprise computing operations
B. A network connection used in enterprise network infrastructure
C. An identity used to access and interact with the OS with specific permissions
D. A social media profile within modern computing environments

Answer: C

Q44. What is the purpose of file permissions in an OS?

A. To compress files for reducing disk storage consumption
B. To encrypt all files automatically
C. To make files larger within the data management framework
D. To control who can read, write, or execute files

Answer: D

Q45. What is a system log?

A. A file that records events, errors, and activities within the operating system
B. A strain of self-replicating malicious software programs
C. A physical network cable used for connecting infrastructure devices
D. A physical security measure for protecting building infrastructure

Answer: A

Q46. What is the purpose of disabling unnecessary services on an OS?

A. To free up disk space only within enterprise computing infrastructure
B. To reduce the attack surface by eliminating potential entry points
C. To make the OS look cleaner within enterprise computing infrastructure
D. To speed up boot time only for improved operational efficiency

Answer: B

Q47. What is a security patch?

A. A software update that fixes a specific security vulnerability
B. A decorative element within modern computing environments
C. A physical patch on hardware installed within computing infrastructure
D. A category of self-replicating malicious software

Answer: A

Q48. Which is a basic OS security practice?

A. Disabling the firewall within enterprise security environments
B. Running all programs as administrator
C. Using strong passwords and enabling automatic updates
D. Sharing admin passwords within enterprise security environments

Answer: C

Q49. What is Windows Defender?

A. A built-in antimalware component of Windows operating system
B. A file manager for organizing system directories
C. A standard web browser for accessing internet sites
D. A first-person video game for entertainment

Answer: A

Q50. What is the root account in Linux?

A. The superuser account with unrestricted access to all commands and files
B. A regular user account within the identity management system
C. A temporary account within the identity management system
D. A guest account within the identity management system

Answer: A

Q51. What does HTTPS indicate in a website URL?

A. The website is an older legacy version of the platform
B. The website loads with higher overall speed performance
C. The website is free to access without any subscription
D. The website uses encrypted communication via SSL/TLS

Answer: D

Q52. What is a phishing website?

A. A government website providing official public services
B. A secure website verified by a certificate authority
C. A website about recreational fishing techniques and tips
D. A fake website designed to trick users into revealing personal information

Answer: D

Q53. What is a web application firewall (WAF)?

A. A standard web browser used for accessing internet-hosted content
B. An online platform used for creating and hosting web content
C. A physical barrier installed to protect building infrastructure
D. A security solution that filters and monitors HTTP traffic between a web app and the internet

Answer: D

Q54. What is the purpose of CAPTCHA on websites?

A. To deliberately slow down website page loading speed
B. To distinguish between human users and automated bots
C. To compress and optimize images for web page loading
D. To encrypt data using symmetric cipher algorithms

Answer: B

Q55. What is a cookie in web security?

A. A category of self-replicating malicious software
B. A small piece of data stored by a web browser for session management
C. A baked food snack or treat served at parties
D. A security tool for scanning and detecting vulnerabilities

Answer: B

Q56. Why check for a padlock icon in the browser address bar?

A. It shows the site operates without any advertisements
B. It means the site loads with high-performance speed
C. It means the site is popular and heavily visited
D. It indicates the connection is encrypted with SSL/TLS

Answer: D

Q57. What is a secure password practice for web accounts?

A. Using the same password everywhere
B. Using single-character passwords
C. Writing passwords on sticky notes
D. Using unique, strong passwords for each website

Answer: D

Q58. What is the purpose of two-factor authentication on websites?

A. To deliberately make the login process much slower
B. To completely block all users from accessing the site
C. To add an extra layer of security beyond just a password
D. To encrypt the entire website using a secret algorithm

Answer: C

Q59. What does 'session' mean in web security?

A. A formal class held at a school or university within modern computing environments
B. A software application used for enterprise computing operations
C. A period of interaction between a user and a web application, tracked by a session identifier
D. A physical cable used for network connections used in enterprise network infrastructure

Answer: C

Q60. What is input validation in web security?

A. Checking keyboard hardware functionality and connectivity
B. Verifying that user-submitted data meets expected criteria before processing
C. Formatting and styling text content on a web page
D. Compressing and reducing the size of input data

Answer: B

Q61. What is malware?

A. A physical hardware component inside computer systems
B. Software intentionally designed to cause damage to a computer, server, or network
C. Legitimate helpful software designed for user productivity
D. An operating system for managing system resources used in enterprise computing environments

Answer: B

Q62. What is a computer virus?

A. A written record or logbook for tracking daily operational activities
B. Malicious code that attaches to programs and replicates when the host program runs
C. A routine system update for improving stability used in enterprise computing environments
D. A self-replicating strain of malicious software targeting systems

Answer: B

Q63. What is a computer worm?

A. A physical hardware component used in computing infrastructure
B. Self-replicating malware that spreads across networks without needing a host program
C. A software application used for enterprise computing operations
D. A hardware component inside wireless networking routers

Answer: B

Q64. What is a Trojan horse in computing?

A. A physical hardware component used in computing infrastructure
B. Malware disguised as legitimate software to trick users into installing it
C. An antivirus program designed to detect known threats
D. A wooden horse artifact from ancient Greek history

Answer: B

Q65. What is ransomware?

A. Malware that encrypts files and demands payment for the decryption key
B. Free and open-source software available for download
C. A backup tool for creating copies of important data
D. An antivirus update that patches known vulnerabilities

Answer: A

Q66. What is spyware?

A. Software that secretly monitors and collects user information without consent
B. A security tool for scanning and detecting vulnerabilities
C. A telescope used for astronomical observation used in enterprise computing environments
D. A standard web browser for accessing internet sites

Answer: A

Q67. What is adware?

A. A security program designed to protect against malware
B. An advertising company that creates marketing campaigns
C. Software that automatically displays or downloads unwanted advertisements
D. A helpful tool for managing and organizing digital files

Answer: C

Q68. What is a phishing attack?

A. A routine security scan assessing system vulnerabilities used in enterprise computing environments
B. A standard network communication protocol for data transmission
C. A recreational fishing technique using specialized gear used in enterprise computing environments
D. A social engineering attack using deceptive messages to trick victims into revealing sensitive information

Answer: D

Q69. What is a Denial of Service (DoS) attack?

A. A network upgrade that improves bandwidth and throughput used in enterprise computing environments
B. Refusing customer service in a retail environment across computing environments
C. A software application used for enterprise computing operations
D. An attack that overwhelms a system with traffic to make it unavailable to legitimate users

Answer: D

Q70. What is the best defense against malware?

A. Completely avoiding and never using a computer at all
B. Only using free open-source software for all tasks
C. Permanently disconnecting the system from internet access
D. Using updated antivirus software and practicing safe computing habits

Answer: D

Q71. What is multi-factor authentication (MFA)?

A. Using multiple different passwords for one account
B. Using two or more different verification methods to confirm identity
C. Displaying multiple login screens for a single service
D. Using multiple different usernames for one account

Answer: B

Q72. What are the three main factors of authentication?

A. Name, address, phone within enterprise security environments
B. Hardware, software, firmware within enterprise security environments
C. Username, password, email within enterprise security environments
D. Something you know, something you have, something you are

Answer: D

Q73. What is a biometric authentication method?

A. Authenticating identity using a traditional password or passphrase
B. Using physical characteristics like fingerprints or facial recognition to verify identity
C. Using a smart card hardware token for two-factor authentication
D. Using a numeric PIN code for verifying user identity at login

Answer: B

Q74. What is role-based access control (RBAC)?

A. Access permissions assigned based on a user's role within the organization
B. No formal access control mechanism exists in the system
C. Everyone has the same unrestricted access to resources
D. Access is assigned randomly without specific criteria

Answer: A

Q75. What is a PIN (Personal Identification Number)?

A. A numeric password used to authenticate a user's identity
B. A symmetric key data encryption algorithm
C. A network identifier assigned to connected devices
D. A physical metal pin used for hardware components

Answer: A

Q76. What is single sign-on (SSO)?

A. An authentication scheme allowing a user to log in once and access multiple systems
B. A next-generation firewall for filtering network traffic flows
C. Creating a single user account for system administration
D. Using one password for everything without variation

Answer: A

Q77. What is the purpose of a username?

A. To speed up computer processing performance speed
B. To identify a specific user account in a system
C. To create automated backup copies of user data
D. To encrypt data using symmetric cipher algorithms

Answer: B

Q78. What is account lockout?

A. Normally logging out of an active and authenticated user session
B. A security mechanism that locks an account after too many failed login attempts
C. Permanently deleting and removing a user account from the system
D. Changing a user account password for improved security posture

Answer: B

Q79. What is a one-time password (OTP)?

A. A shared password used by multiple user accounts
B. A permanent password that never expires or changes
C. A password valid for only one login session or transaction
D. A master password that unlocks all system accounts

Answer: C

Q80. What is authorization?

A. Permanently deleting files and data from the system storage drives
B. Determining what resources and actions an authenticated user is allowed to access
C. Creating and provisioning a new user account entry in the directory
D. Verifying and confirming who you are as a user during the login process

Answer: B

Q81. What is secure software development?

A. Writing detailed technical documentation for all application code modules
B. Only testing for bugs and defects at the very end of the development cycle
C. Writing application code quickly without any formal quality review process
D. Integrating security measures throughout the entire software development lifecycle

Answer: D

Q82. What is the SDLC?

A. A high-level language used for development used in enterprise computing environments
B. A database management system for storing data records
C. A security tool for scanning and detecting vulnerabilities
D. A structured process for planning, creating, testing, and deploying software

Answer: D

Q83. Why is input validation important in secure coding?

A. To ensure user input is safe and prevent malicious data from being processed
B. To make the user interface look visually appealing
C. To speed up the application processing and response time
D. To reduce the overall file size of application resources

Answer: A

Q84. What is a software vulnerability?

A. A routine patch applied to update and improve existing system software
B. A category of self-replicating malicious software designed for harm
C. A weakness or flaw in software that can be exploited to compromise security
D. A planned and well-documented software feature built for end users

Answer: C

Q85. What is code review in secure development?

A. Copying code from the internet without attribution or proper licensing
B. Examining source code to identify security flaws, bugs, and code quality issues
C. Permanently deleting old obsolete source code from repository branches
D. Writing code faster without any verification of quality or correctness

Answer: B

Q86. What does 'security by design' mean?

A. Adding security measures only after production deployment
B. Building security into software from the earliest stages of development
C. Installing antivirus software on the development machine
D. Using only encryption as the single security measure

Answer: B

Q87. What is the purpose of error handling in secure coding?

A. To deliberately cause the application to crash on errors
B. To log all error details publicly for transparency
C. To ignore all errors and continue processing without alerts
D. To gracefully manage errors without exposing sensitive information

Answer: D

Q88. What is a security bug?

A. A physical hardware failure requiring component replacement
B. A network connectivity issue affecting system availability
C. A software defect that could be exploited to compromise system security
D. A planned feature request from the product stakeholders

Answer: C

Q89. What is the purpose of using HTTPS in web applications?

A. To block unwanted advertisements from displaying
B. To encrypt data transmitted between client and server
C. To compress web pages for reduced bandwidth usage
D. To optimize the website for faster loading performance

Answer: B

Q90. Why should default passwords be changed?

A. To comply with organizational branding requirements
B. To improve overall system performance and speed
C. To make the login process more difficult for users
D. Because default passwords are publicly known and easily exploited

Answer: D

Q91. What does Wi-Fi stand for?

A. Wide Firewall
B. Wired Finder
C. Wireless Fidelity
D. Wireless Firewall

Answer: C

Q92. What is the purpose of a Wi-Fi password?

A. To slow down the connection within enterprise computing infrastructure
B. To restrict network access to authorized users and encrypt wireless traffic
C. To identify the network name across the enterprise network infrastructure
D. To increase internet speed for improved operational efficiency

Answer: B

Q93. What is Bluetooth?

A. A short-range wireless technology for exchanging data between devices
B. A dental condition affecting tooth enamel coloring
C. A wired connection using physical Ethernet cables
D. A strain of self-replicating malicious software programs

Answer: A

Q94. Why should you avoid unknown public Wi-Fi networks?

A. They are always blocked by network providers
B. They always have slow data transfer speeds
C. They consume too much device battery power
D. They may be set up by attackers to intercept your data

Answer: D

Q95. What is the purpose of screen lock on a mobile device?

A. To speed up device processing and app performance
B. To conserve and extend device battery life span
C. To prevent unauthorized physical access to the device and its data
D. To improve the display quality and screen resolution

Answer: C

Q96. What is mobile device encryption?

A. Converting all data on the device into an unreadable format requiring authentication
B. Making the phone processor run faster and smoother
C. A screen saver that activates after inactivity timeout used in enterprise computing environments
D. Compressing files to reduce disk storage consumption

Answer: A

Q97. What should you do if your mobile device is lost or stolen?

A. Do nothing at all and wait patiently for the situation to resolve itself
B. Buy a new replacement device immediately without taking any other action
C. Use remote wipe and tracking features, change passwords, and report to authorities
D. Wait patiently for the lost or stolen device to be returned by someone

Answer: C

Q98. What is the risk of outdated mobile operating systems?

A. Known security vulnerabilities remain unpatched and exploitable
B. Newer wallpapers and themes are not available to install
C. Applications appear different with slightly changed layouts
D. The phone appears visually old and aesthetically outdated

Answer: A

Q99. What is an SSID in wireless networking?

A. A hardware component inside wireless networking routers
B. A symmetric key data encryption algorithm
C. A wireless security protocol for data encryption
D. The name that identifies a specific wireless network

Answer: D

Q100. Why should you keep Bluetooth off when not in use?

A. To reduce the attack surface and prevent unauthorized connections
B. To make phone calls connect and complete faster overall
C. To customize and change the phone color theme appearance
D. To improve camera quality and photo capture resolution

Answer: A

Q101. What is cloud computing?

A. A weather forecasting system using satellite data analysis
B. Storing files exclusively on your local desktop hard drive
C. Delivering computing services like servers, storage, and software over the internet
D. A type of external hard drive for portable data storage

Answer: C

Q102. What are the three main cloud service models?

A. Small, Medium, Large
B. RAM, CPU, GPU
C. IaaS, PaaS, SaaS
D. HTTP, FTP, SMTP

Answer: C

Q103. What is the shared responsibility model in cloud security?

A. Both the provider and customer share responsibility for different aspects of security
B. Only the customer is responsible for all security measures including infrastructure
C. The cloud provider is solely responsible for everything including customer data
D. No one is responsible for implementing security controls in cloud environments

Answer: A

Q104. What is a public cloud?

A. Cloud infrastructure shared among multiple organizations over the internet
B. A government-operated cloud for public sector agencies
C. A cloud deployment visible to everyone on the internet
D. A private physical server in an on-premises data center

Answer: A

Q105. What is a private cloud?

A. A secret cloud that nobody uses or accesses at all
B. Cloud infrastructure exclusively used by a single organization
C. A specific type of weather and atmospheric phenomena
D. A personal desktop computer used for individual tasks

Answer: B

Q106. Why is data encryption important in cloud computing?

A. To protect data confidentiality on shared infrastructure and during transmission
B. To organize files better with structured directory layouts
C. To make data load faster with improved performance speed
D. To reduce storage costs through efficient data management

Answer: A

Q107. What is multi-tenancy in cloud computing?

A. Multiple users connected to one physical computer terminal for shared access
B. Having multiple user accounts on different cloud services for various purposes
C. A cloud computing platform designed for hosting distributed enterprise workloads
D. Multiple customers sharing physical infrastructure while data remains logically isolated

Answer: D

Q108. What is a cloud access security broker (CASB)?

A. A next-generation firewall for filtering network traffic flows
B. A cloud provider offering infrastructure as a service
C. A security tool between users and cloud services to enforce security policies
D. An automated backup solution for enterprise data recovery needs

Answer: C

Q109. What is the risk of misconfigured cloud storage?

A. Faster data access speeds and improved system performance
B. Accidental public exposure of sensitive data due to incorrect access permissions
C. Better performance throughput for cloud-hosted applications
D. Lower costs for cloud infrastructure resource consumption

Answer: B

Q110. What is IAM in cloud security?

A. A framework for managing digital identities and controlling user access to cloud resources
B. A social media feature for managing online profile settings
C. A file management system for organizing stored documents used in enterprise computing environments
D. An email service for sending and receiving electronic messages

Answer: A

Q111. What is digital forensics?

A. Repairing damaged computers and replacing failed hardware components in infrastructure
B. A standard software application used for routine enterprise computing operations
C. Installing and configuring software applications on production computing systems
D. Collecting, analyzing, and preserving digital evidence from electronic devices for investigation

Answer: D

Q112. What is digital evidence?

A. A physical security measure for protecting building infrastructure
B. Physical fingerprints collected at a crime scene within enterprise security environments
C. A software application used for enterprise computing operations
D. Any data stored or transmitted using a computer that supports or refutes a theory in a legal case

Answer: D

Q113. Why is chain of custody important in digital forensics?

A. It reduces storage space required for evidence preservation
B. It makes the forensic investigation process faster
C. It ensures evidence integrity and admissibility by documenting who handled it and how
D. Continuous monitoring is not important for security for modern enterprise security environments

Answer: C

Q114. What is a forensic image?

A. A digital photograph taken with a camera for documentation
B. A bit-by-bit exact copy of a storage device for forensic examination
C. A screenshot captured from a computer display for reference
D. A photograph of a physical crime scene by investigators

Answer: B

Q115. What types of devices can contain digital evidence?

A. Only USB drives can contain relevant digital evidence for forensic investigation
B. Only desktop computers can contain relevant digital evidence for investigation
C. Only smartphones can contain relevant digital evidence for forensic investigation
D. Computers, smartphones, tablets, servers, IoT devices, USB drives, and any digital storage media

Answer: D

Q116. What is the first step in a digital forensics investigation?

A. Deleting suspicious files from the compromised system
B. Restarting the computer to clear temporary memory contents
C. Installing antivirus software on the compromised system
D. Identifying and securing the scene to prevent evidence tampering

Answer: D

Q117. What is file recovery in digital forensics?

A. Creating new files on the forensic examination workstation
B. Encrypting files within enterprise security environments
C. Retrieving deleted, damaged, or lost files from storage media
D. Compressing files to reduce disk storage consumption

Answer: C

Q118. What is metadata in digital forensics?

A. A high-level language used for development used in enterprise computing environments
B. A strain of self-replicating malicious software programs
C. Data about data, such as file creation date, author, and modification history
D. A standard network communication protocol for data transfer

Answer: C

Q119. What is a write blocker used for in forensics?

A. To block network traffic across the enterprise network infrastructure
B. To block websites within enterprise computing infrastructure
C. To prevent any write operations to the evidence drive during examination
D. To block writing on paper within enterprise computing infrastructure

Answer: C

Q120. What is the purpose of hashing in digital forensics?

A. To create a unique digital fingerprint of evidence to verify its integrity
B. To reduce data sizes through compression methods and management
C. To speed up computers for improved operational efficiency
D. To encrypt files using established cryptographic standards

Answer: A

Q121. What is an incident in cyber security?

A. A routine patch applied to update system software used in enterprise computing environments
B. An event that threatens the security, confidentiality, integrity, or availability of information assets
C. A physical hardware component used in computing infrastructure
D. A scheduled maintenance within enterprise computing environments

Answer: B

Q122. What is incident response?

A. An organized approach to addressing and managing a security breach to limit damage
B. Generating redundant backup copies of system data for disaster recovery
C. Installing routine software updates on regularly scheduled maintenance days
D. Ignoring security events and hoping they resolve on their own naturally

Answer: A

Q123. Why is having an incident response plan important?

A. It ensures quick, organized, and effective response to security incidents
B. Continuous monitoring is not important for security
C. It eliminates all threats regardless of the specific situation or context
D. It replaces security tools within enterprise security environments

Answer: A

Q124. What is the first phase of incident response?

A. Recovery
B. Containment
C. Preparation
D. Eradication

Answer: C

Q125. What is an incident response team?

A. A marketing team managing brand awareness campaigns used in enterprise computing environments
B. Trained personnel responsible for detecting, analyzing, and responding to security incidents
C. A software application used for enterprise computing operations
D. A group of malicious hackers targeting an organization used in enterprise computing environments

Answer: B

Q126. What should you do if you suspect a security incident?

A. Report it immediately to the appropriate security team
B. Try to fix it yourself without informing anyone
C. Delete all files to eliminate any potential evidence
D. Ignore it and continue with normal operations as usual

Answer: A

Q127. What is the purpose of incident documentation?

A. To blame someone specific for causing the incident
B. To delete evidence of the incident from all records
C. To create unnecessary bureaucratic paperwork and overhead
D. To maintain a detailed record of the incident, actions taken, and findings

Answer: D

Q128. What is the difference between an event and an incident?

A. Events are worse than incidents in terms of damage across computing environments
B. They are fundamentally identical concepts with no meaningful differences
C. Incidents are planned events scheduled by the security team
D. An event is any observable occurrence; an incident negatively impacts security or violates policy

Answer: D

Q129. What is the purpose of the containment phase?

A. To ignore the incident and let it resolve on its own
B. To limit the scope and damage by isolating affected systems
C. To start a new project unrelated to the current incident
D. To spread and propagate the incident to other systems

Answer: B

Q130. What is a security alert?

A. A fire alarm system installed in a physical building
B. A notification indicating a potential security event requiring investigation
C. A performance warning about high system resource usage
D. A software update notification from the operating system

Answer: B

Q131. What is security monitoring?

A. Monitoring attendance records for employee time tracking
B. Watching security guards on physical surveillance cameras
C. Continuous observation and analysis of systems and networks for security threats
D. A video surveillance system for monitoring building access

Answer: C

Q132. What is a security log?

A. A record of security-relevant events and activities within a system or network
B. A wooden log used for building physical fire structures
C. A login page for entering user authentication credentials
D. A security guard's written diary of daily activity notes

Answer: A

Q133. What is an alert in security monitoring?

A. A routine system update for improving stability used in enterprise computing environments
B. A user account type with specifically assigned access permissions
C. A notification when a security tool detects suspicious or potentially malicious activity
D. An alarm clock that wakes people up at a set time used in enterprise computing environments

Answer: C

Q134. What is the purpose of monitoring network traffic?

A. To count the total number of packets transmitted on network
B. To slow down overall network performance and throughput
C. To increase available bandwidth for improved download speeds
D. To detect unusual patterns, unauthorized access, and potential security threats

Answer: D

Q135. What is a dashboard in security monitoring?

A. A file manager for organizing system directories used in enterprise computing environments
B. A visual interface displaying real-time security metrics, alerts, and status information
C. A web browser application for accessing internet-hosted content
D. A car dashboard displaying vehicle speed and fuel information

Answer: B

Q136. Why is continuous monitoring important?

A. Continuous monitoring exists solely to use more electricity
B. Continuous monitoring is not important for security for modern enterprise security environments
C. Threats can occur at any time and continuous monitoring ensures quick detection
D. Continuous monitoring exists only to generate more data

Answer: C

Q137. What is log management?

A. Collecting, storing, analyzing, and retaining log data from various systems
B. Managing a personal blog for publishing online content
C. Managing a lumber yard for processing wood materials
D. A task management tool for organizing project work items

Answer: A

Q138. What type of events should be logged for security?

A. Login attempts, access to sensitive data, system changes, and privilege escalations
B. Only successful events should be logged for monitoring and compliance reporting
C. Only errors and crashes should be logged for security analysis and remediation
D. Only network events should be logged for analysis and security monitoring

Answer: A

Q139. What is a false positive in security monitoring?

A. A true security threat confirmed by analysis investigation
B. A false identity used for unauthorized system access
C. A system error causing application crashes or instability
D. An alert that incorrectly identifies normal activity as a security threat

Answer: D

Q140. What is the purpose of antivirus monitoring?

A. To continuously watch for and detect malware infections in real-time
B. To delete all files from the system storage permanently
C. To sell software licenses for antivirus subscriptions
D. To slow down the computer for detailed system analysis

Answer: A

Q141. What is cybercrime?

A. Playing computer games for recreational entertainment and leisure purposes
B. Criminal activity involving computers, networks, or digital devices as tools or targets
C. Using computers for normal everyday work productivity and communications
D. Building websites for establishing personal or commercial online presence

Answer: B

Q142. What is PECA 2016 in Pakistan?

A. An education policy for governing school curriculum standards
B. Pakistan's primary legislation addressing cybercrimes, data protection, and electronic fraud
C. A health regulation for managing public medical facilities used in enterprise computing environments
D. A traffic law regulating vehicle movement on roads used in enterprise computing environments

Answer: B

Q143. What is intellectual property in the digital context?

A. A physical hardware component used in computing infrastructure
B. Creative works, inventions, designs, and software protected by law from unauthorized use
C. Internet speed and bandwidth available for data transfers
D. Physical property like land and buildings owned by individuals

Answer: B

Q144. What is data privacy?

A. Making data public and freely accessible for anyone across computing environments
B. The right of individuals to control how their personal information is collected, used, and shared
C. Hiding your computer from others by placing it out of sight
D. Deleting all data from storage devices permanently across computing environments

Answer: B

Q145. What is unauthorized access in cyber law?

A. Logging into your own user account with correct credentials
B. Downloading free software from authorized official sources
C. Using public Wi-Fi for browsing the internet content
D. Accessing a computer system or network without permission

Answer: D

Q146. What is online harassment?

A. Using digital communication to threaten, intimidate, or harm another person
B. Social media marketing campaigns for brand awareness
C. Sending friendly emails to colleagues for collaboration
D. Online gaming with other players for entertainment purposes

Answer: A

Q147. What is software piracy?

A. Software testing for validating application feature quality
B. The unauthorized copying, distribution, or use of copyrighted software
C. Open-source development contributing code to public projects
D. Sailing ships equipped with computer navigation technology

Answer: B

Q148. What is digital consent?

A. A symmetric key data encryption algorithm applied to data protection workflows
B. A computer command executed from the terminal or console used in enterprise computing environments
C. A digital signature used for verifying message authenticity used in enterprise computing environments
D. Permission given by an individual for their personal data to be collected, processed, or shared

Answer: D

Q149. What is identity theft in the digital context?

A. Creating a new email account for personal communication
B. Changing your username on a social media platform account
C. Forgetting your password and requesting an account reset
D. Stealing personal information to impersonate someone for fraud or other crimes

Answer: D

Q150. What is the purpose of acceptable use policies (AUP)?

A. To deploy and install application software and management
B. To restrict all computer use for security purposes and management
C. To increase internet speed for improved operational efficiency
D. To define rules and guidelines for responsible and secure use of IT resources

Answer: D

Q151. What is AI in cyber security?

A. A next-generation firewall security appliance deployed across enterprise environments
B. The use of machine learning and intelligent algorithms to detect, prevent, and respond to threats
C. A physical security measure for protecting building infrastructure
D. A software application used for enterprise computing operations

Answer: B

Q152. What is the Internet of Things (IoT)?

A. A network of physical devices connected to the internet that collect and exchange data
B. A web browser application for accessing internet-hosted content
C. A social media platform for sharing posts and updates used in enterprise computing environments
D. A new internet service provider offering broadband access

Answer: A

Q153. Why are IoT devices a security concern?

A. They process data too fast for security tools to monitor
B. They consume too much electricity for normal household budgets
C. They are too expensive for consumers to purchase and use
D. Many have weak security, default passwords, and limited update capabilities

Answer: D

Q154. What is blockchain technology?

A. A next-generation firewall for filtering network traffic flows
B. A cryptographic algorithm used for protecting sensitive data
C. A distributed, immutable ledger that records transactions across many computers
D. A database backup system for creating redundant data copies

Answer: C

Q155. What is ransomware-as-a-service (RaaS)?

A. A backup service for managing enterprise data resources
B. A legitimate cloud service for hosting web applications
C. A data recovery service for restoring encrypted file backups
D. A criminal model where ransomware developers lease tools to other criminals

Answer: D

Q156. What is biometric authentication technology?

A. A standard network communication protocol for data transfer
B. A cryptographic algorithm used for protecting sensitive data
C. Using unique physical or behavioral characteristics for identity verification
D. Using only passwords for user identity verification login

Answer: C

Q157. What is cloud-native security?

A. A physical security measure specifically designed for protecting building infrastructure
B. Weather-based security monitoring using atmospheric sensors and satellite imaging data
C. Security approaches designed specifically for cloud environments including containers and serverless
D. A self-replicating strain of malicious software designed for targeting computing systems

Answer: C

Q158. What is a deepfake?

A. AI-generated synthetic media realistically depicting people saying or doing things they never did
B. A software application used for enterprise computing operations
C. A deep sea photograph taken underwater for marine research used in enterprise computing environments
D. A symmetric key data encryption algorithm applied to data protection workflows

Answer: A

Q159. What is 5G and why does it matter for security?

A. A strain of self-replicating malicious software programs
B. The fifth generation of personal computer hardware architecture
C. The fifth generation of mobile network technology bringing new security challenges
D. A security certification for mobile network professionals

Answer: C

Q160. What is cyber resilience?

A. A next-generation firewall for filtering network traffic flows
B. Never experiencing any cyber attacks or security incidents
C. An automated backup solution for enterprise data recovery needs
D. An organization's ability to continuously deliver outcomes despite adverse cyber events

Answer: D

Q161. What does the term 'attack surface' refer to in cyber security?

A. The graphical interface of a security application
B. The total number of employees in an organization
C. The set of points where an attacker can try to enter
D. The physical area covered by a wireless network

Answer: C

Q162. Which term describes an individual who attempts to gain unauthorized access to systems?

A. Developer
B. Hacker
C. Analyst
D. Administrator

Answer: B

Q163. What is the main purpose of security awareness training?

A. Training staff to configure enterprise-level firewalls
B. Teaching employees to write secure code for applications
C. Educating users to recognize and avoid security threats
D. Certifying professionals for network administration roles

Answer: C

Q164. Which of the following best describes a 'white hat' hacker?

A. A hacker who creates malware to disrupt critical services
B. An ethical hacker who tests systems with proper authorization
C. A malicious hacker who exploits systems for personal gain
D. A hacker who sells stolen data on underground marketplaces

Answer: B

Q165. What does 'data breach' mean in cyber security?

A. Authorized sharing of data between partner organizations
B. Unauthorized access and disclosure of sensitive information
C. Scheduled backup of organizational data to offsite storage
D. Routine migration of data between different server systems

Answer: B

Q166. What is the function of encryption in cyber security?

A. Deleting outdated files from the system permanently
B. Compressing files to reduce overall storage capacity
C. Converting data into unreadable format for protection
D. Scanning networks to detect unauthorized intrusions

Answer: C

Q167. Which type of cyber attack tricks users into revealing sensitive information via fake emails?

A. Sniffing
B. Phishing
C. Brute force
D. Keylogging

Answer: B

Q168. What is the purpose of a security policy in an organization?

A. Defining rules and procedures for protecting information assets
B. Listing hardware specifications for all organizational devices
C. Documenting employee performance reviews and evaluations
D. Recording financial transactions and quarterly budget reports

Answer: A

Q169. Which of the following is NOT a pillar of the CIA triad?

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

Answer: D

Q170. What does the term 'insider threat' refer to?

A. A natural disaster affecting the data center infrastructure
B. A hardware malfunction causing temporary system downtime
C. A security threat originating from within the organization
D. An external attacker probing the network from the internet

Answer: C

Q171. What is the purpose of access control in information security?

A. Monitoring hardware temperature for system stability
B. Compressing files to save disk storage space usage
C. Restricting who can view or use resources in a system
D. Speeding up data transfer across network connections

Answer: C

Q172. Which type of security control is a locked door to a server room?

A. Logical
B. Technical
C. Administrative
D. Physical

Answer: D

Q173. What does 'integrity' mean in the context of information security?

A. Keeping sensitive information hidden from unauthorized people
B. Providing fast network speeds for data transfer and access
C. Making sure systems are always available to authorized users
D. Ensuring data is accurate and has not been tampered with

Answer: D

Q174. What is a security baseline?

A. A software tool for scanning networks against vulnerabilities
B. A type of firewall used at the network perimeter gateway
C. A minimum set of security standards for systems to meet
D. The highest possible security level an organization uses

Answer: C

Q175. Which of the following is an example of a detective security control?

A. Audit log
B. Encryption
C. Backup
D. Firewall

Answer: A

Q176. What is the purpose of a password policy?

A. Documenting disaster recovery procedures for data centers
B. Defining rules for creating and managing strong passwords
C. Specifying network bandwidth allocation per each department
D. Listing all approved software applications for installation

Answer: B

Q177. What does 'availability' ensure in the CIA triad?

A. Data is hidden from all external network users at all times
B. Data cannot be modified by any internal user of the system
C. Systems and data are accessible when needed by authorized users
D. All network traffic is encrypted between source and destination

Answer: C

Q178. Which term describes the process of verifying a user's claimed identity?

A. Encryption
B. Accounting
C. Authorization
D. Authentication

Answer: D

Q179. What is social engineering in the context of security?

A. Building secure social media platforms for enterprise users
B. Creating automated social network bots for data collection
C. Manipulating people into revealing confidential information
D. Designing user-friendly interfaces for security applications

Answer: C

Q180. What is the primary function of a security patch?

A. Upgrading hardware components for better system performance
B. Adding new features and capabilities to existing software
C. Fixing known security vulnerabilities in software or systems
D. Migrating data from legacy storage to modern cloud services

Answer: C

Q181. What is plaintext in cryptography?

A. A hash value generated from a digital signature
B. Data that has been encrypted using a cipher algorithm
C. A secret key used for decrypting encoded messages
D. Original readable data before encryption is applied

Answer: D

Q182. Which type of cryptography uses the same key for encryption and decryption?

A. Steganography
B. Asymmetric
C. Symmetric
D. Hashing

Answer: C

Q183. What is the output of a hash function called?

A. Digest
B. Plaintext
C. Token
D. Ciphertext

Answer: A

Q184. Which algorithm is a widely used symmetric encryption standard?

A. AES
B. RSA
C. ECC
D. DSA

Answer: A

Q185. What is the primary purpose of a digital signature?

A. Verifying the authenticity and integrity of a message
B. Generating random encryption keys for secure sessions
C. Compressing data to reduce network bandwidth consumption
D. Encrypting the entire message content for confidentiality

Answer: A

Q186. What does RSA stand for in cryptography?

A. Rivest-Shamir-Adleman
B. Recursive Signing Architecture
C. Random Security Algorithm
D. Rapid Symmetric Authentication

Answer: A

Q187. What is a certificate authority (CA) responsible for?

A. Monitoring network traffic for suspicious activity and intrusions
B. Manufacturing hardware security modules for data center operations
C. Issuing and managing digital certificates for secure communications
D. Developing encryption algorithms for government security agencies

Answer: C

Q188. Which of the following is an asymmetric encryption algorithm?

A. DES
B. RSA
C. RC4
D. AES

Answer: B

Q189. What is the purpose of a cryptographic key?

A. A software license required to install encryption applications
B. A physical device used to unlock encrypted hardware storage units
C. A parameter that determines the output of a cryptographic algorithm
D. A network address assigned to encrypted communication channels

Answer: C

Q190. What property of hash functions means the output cannot be reversed to find the input?

A. Key derivation
B. Collision resistance
C. One-way property
D. Block chaining

Answer: C

Q191. What is the primary function of a network firewall?

A. Managing user accounts across the enterprise network
B. Storing backup copies of important network data files
C. Increasing the overall speed of network connections
D. Filtering traffic based on predefined security rules

Answer: D

Q192. What does a VPN provide for network communications?

A. Load balancing across multiple server instances
B. Faster download speeds for large file transfers
C. Encrypted tunnel for secure data transmission
D. Automatic virus scanning of all network traffic

Answer: C

Q193. What is a DMZ in network security?

A. A protocol for encrypting database connections between application server nodes
B. A tool for monitoring bandwidth usage across all organizational network links
C. A network segment that separates internal networks from untrusted external networks
D. A type of malware that spreads automatically across connected wireless networks

Answer: C

Q194. What does IDS stand for in network security?

A. Intrusion Detection System
B. Integrated Display Server
C. Internet Data Service
D. Internal Defense System

Answer: A

Q195. What is the purpose of network segmentation?

A. Dividing a network into smaller segments to improve security and performance
B. Removing all firewalls to simplify the overall network architecture
C. Increasing the physical cable length between network connected devices
D. Combining multiple small networks into one large unified network system

Answer: A

Q196. Which protocol provides secure web browsing by encrypting HTTP traffic?

A. HTTPS
B. SNMP
C. FTP
D. SMTP

Answer: A

Q197. What is a proxy server used for in network security?

A. Acting as an intermediary between users and the internet for security
B. Directly connecting users to the internet without any filtering
C. Replacing the router as the main network traffic forwarding device
D. Generating encryption keys for all network-connected user devices

Answer: A

Q198. What type of attack floods a server with traffic to make it unavailable?

A. DoS attack
B. SQL injection
C. Spoofing
D. Phishing

Answer: A

Q199. What does NAT stand for in networking?

A. Network Address Translation
B. Network Audit Technique
C. Network Access Terminal
D. Node Authentication Token

Answer: A

Q200. What is the purpose of an access control list (ACL) on a network device?

A. Recording the browsing history of all network users for auditing
B. Listing all devices currently connected to the network for inventory
C. Managing software licenses for applications installed on the server
D. Defining rules that permit or deny traffic based on specified criteria

Answer: D

Q201. What is the primary role of user account management in OS security?

A. Managing the color scheme and desktop wallpaper preferences
B. Controlling who can access the system and their permission levels
C. Increasing the processing speed of all running applications
D. Improving the graphical user interface design for better usability

Answer: B

Q202. What is the purpose of file permissions in an operating system?

A. Organizing files alphabetically in directory listings
B. Setting the default font size for text documents
C. Controlling who can read, write, or execute a file
D. Determining how fast files can be read from disk

Answer: C

Q203. What does the 'root' account represent in Linux operating systems?

A. A standard user account for regular daily computing tasks
B. A disabled account used only for emergency system recovery
C. The superuser account with full administrative privileges
D. A guest account with limited temporary access to the system

Answer: C

Q204. What is the purpose of operating system patching?

A. Adding new entertainment features to the operating system
B. Upgrading the hardware drivers for better graphics performance
C. Changing the default language settings of the operating system
D. Fixing security vulnerabilities and bugs in the OS software

Answer: D

Q205. What is a host-based firewall?

A. A centralized network device protecting the entire corporate network
B. A hardware appliance installed at the internet service provider
C. A firewall installed on individual computers to control their traffic
D. A cloud service that scans emails for malicious file attachments

Answer: C

Q206. What is the function of an OS audit log?

A. Compressing old files to free up available disk storage space
B. Speeding up the boot process by caching startup configurations
C. Recording system events and user activities for security review
D. Displaying real-time CPU usage statistics on the desktop screen

Answer: C

Q207. What is the purpose of disabling unnecessary services on a server?

A. Improving the visual appearance of the server management console
B. Increasing the amount of available RAM for user applications
C. Reducing the attack surface by eliminating potential entry points
D. Enabling faster network communication between all server nodes

Answer: C

Q208. What does UAC stand for in Windows security?

A. Unified Audit Console
B. Update Administration Center
C. User Account Control
D. Universal Access Code

Answer: C

Q209. What is the purpose of disk encryption on a laptop?

A. Protecting data if the laptop is lost or stolen by making it unreadable
B. Increasing the read and write speed of the hard drive significantly
C. Preventing the laptop from connecting to unsecured wireless networks
D. Reducing the storage capacity needed for files on the encrypted disk

Answer: A

Q210. What is a security hardening guide for an operating system?

A. A document providing steps to secure an OS by reducing vulnerabilities
B. A manual for repairing physical damage to computer hardware components
C. A guide for increasing internet connection speeds through OS tweaks
D. A tutorial for installing entertainment software on the operating system

Answer: A

Q211. What is cross-site scripting (XSS)?

A. A protocol for sharing authentication tokens between different websites
B. An attack that injects malicious scripts into web pages viewed by users
C. A method for optimizing website loading speed across browsers
D. A technique for cross-browser testing of web application functionality

Answer: B

Q212. What is SQL injection?

A. A method of creating structured database tables and indexes
B. An attack that inserts malicious SQL code into application queries
C. A tool for migrating data between different database platforms
D. A database optimization technique for faster query results

Answer: B

Q213. What does HTTPS provide that HTTP does not?

A. Faster page loading speeds for all website resources
B. Larger file upload limits for web form submissions
C. Encrypted communication between browser and server
D. Better search engine rankings for website content

Answer: C

Q214. What is a web application firewall (WAF)?

A. A security tool that filters and monitors HTTP traffic to web applications
B. A network switch that connects multiple web servers in a data center
C. A device that increases the bandwidth available to web server connections
D. A software program that designs web page layouts and visual templates

Answer: A

Q215. What is the purpose of input validation in web applications?

A. Converting user input into different languages automatically
B. Improving the visual appearance of input fields on web forms
C. Ensuring user input meets expected formats before processing it
D. Speeding up form submission by compressing input data first

Answer: C

Q216. What does CSRF stand for in web security?

A. Cached Session Recovery Feature
B. Cross-Site Request Forgery
C. Central Server Response Filter
D. Client-Side Resource Failure

Answer: B

Q217. What is the purpose of the same-origin policy in web browsers?

A. Preventing web pages from making requests to different domains than their origin
B. Ensuring all web pages load at the same speed regardless of server location
C. Requiring all websites to use identical CSS stylesheets for consistent design
D. Blocking users from opening multiple browser tabs at the same time period

Answer: A

Q218. What is a session token used for in web applications?

A. Measuring the loading time of web pages for performance optimization
B. Encrypting all data stored in the web application's backend database
C. Generating random numbers for CAPTCHA verification on login forms
D. Identifying and maintaining a user's authenticated session with the server

Answer: D

Q219. What is clickjacking?

A. Tricking users into clicking hidden elements overlaid on legitimate web pages
B. A technique for optimizing click-through rates on web advertisements
C. Stealing user passwords by recording their keyboard strokes while typing
D. A method of bypassing CAPTCHA challenges using automated mouse clicks

Answer: A

Q220. What is the OWASP Top 10?

A. A ranking of the top ten fastest web servers available for commercial purchase
B. A list of the ten most critical web application security risks updated regularly
C. A collection of ten programming languages recommended for web development
D. A standard defining ten required features for modern web browser software

Answer: B

Q221. What is a computer virus?

A. A software tool used for optimizing computer system performance
B. A program that replicates by attaching itself to other programs or files
C. A hardware component that protects computers from power surges
D. A network protocol designed for secure file transfer operations

Answer: B

Q222. What is ransomware?

A. Malware that encrypts files and demands payment for decryption
B. A tool that helps organize files into categorized folder systems
C. A program that provides free access to premium software licenses
D. Software that speeds up internet browsing on older computers

Answer: A

Q223. How does a worm differ from a virus?

A. A worm only affects hardware while a virus only affects software
B. A worm requires user interaction while a virus spreads automatically
C. A worm spreads independently without needing to attach to host files
D. A worm is harmless while a virus always causes system destruction

Answer: C

Q224. What is a Trojan horse in cyber security?

A. A security tool that automatically detects and removes all known viruses
B. Malware disguised as legitimate software to trick users into installing it
C. An encryption method used to protect files during network transmission
D. A firewall configuration that blocks all incoming network traffic completely

Answer: B

Q225. What is spyware designed to do?

A. Improve computer performance by monitoring resource usage patterns
B. Protect sensitive files by creating encrypted backup copies of data
C. Secretly collect information about a user's activities without consent
D. Block malicious websites from loading in the user's web browser

Answer: C

Q226. What is a botnet?

A. A secure private network used by government agencies for communications
B. A legitimate network of robots used in manufacturing and automation
C. A network of compromised computers controlled remotely by an attacker
D. A high-speed connection linking multiple data centers across regions

Answer: C

Q227. What is a keylogger?

A. A device that locks the keyboard to prevent unauthorized system access
B. A feature that creates keyboard shortcuts for frequently used programs
C. A program that records every keystroke made by the user on a computer
D. A tool that tests keyboard hardware for mechanical defects and issues

Answer: C

Q228. What is adware?

A. A service that manages advertising campaigns across multiple platforms
B. Software that displays unwanted advertisements on the user's device
C. A program that blocks all advertisements while browsing the internet
D. A tool used by marketers to create professional advertisement designs

Answer: B

Q229. What is a brute force attack?

A. Exploiting software bugs to gain unauthorized access to a database
B. Physically damaging computer hardware to disrupt system operations
C. Trying every possible combination to guess a password or encryption key
D. Flooding a network with traffic to deny service to legitimate users

Answer: C

Q230. What is a man-in-the-middle attack?

A. A strategy for overwhelming servers with simultaneous connection requests
B. A technique for bypassing firewalls by tunneling through allowed ports
C. A method of hiding malware inside legitimate software update packages
D. An attack where the attacker intercepts communication between two parties

Answer: D

Q231. What is multi-factor authentication (MFA)?

A. Logging into multiple applications with a single set of credentials
B. Creating multiple user accounts for the same person in a system
C. Using two or more verification methods to confirm a user's identity
D. Setting up multiple passwords for a single user account for safety

Answer: C

Q232. What is single sign-on (SSO)?

A. A technique for creating unique passwords for every individual application
B. A security measure requiring users to sign in separately to each application
C. A method of encrypting passwords before storing them in the user database
D. A system allowing users to access multiple applications with one login credential

Answer: D

Q233. What is a biometric authentication method?

A. Creating long and complex passwords that are difficult for attackers to guess
B. Using a physical security token device to generate one-time access codes
C. Using physical characteristics like fingerprints or facial features to verify identity
D. Sending a verification code to a registered phone number for confirmation

Answer: C

Q234. What is the purpose of account lockout policies?

A. Preventing users from accessing their accounts outside of regular business hours
B. Forcing users to change their passwords after every single successful login event
C. Temporarily disabling accounts after multiple failed login attempts to stop attacks
D. Permanently deleting user accounts that have been inactive for over twelve months

Answer: C

Q235. What are the three factors of authentication?

A. First name, last name, and date of birth for verification
B. Something you know, something you have, and something you are
C. Email address, phone number, and physical mailing address
D. Username, password, and security question answer combination

Answer: B

Q236. What is role-based access control (RBAC)?

A. Giving every user in the organization identical access rights to all resources
B. Restricting access based on the time of day the user attempts to log in
C. Assigning permissions to users based on their organizational role or job function
D. Allowing users to choose which resources they want to access independently

Answer: C

Q237. What is a one-time password (OTP)?

A. A password that can be used unlimited times until the user changes it
B. A default system password assigned to all new employee user accounts
C. A permanent password set during initial account creation for the user
D. A password that is valid for only one login session or transaction

Answer: D

Q238. What is the principle of least privilege in access control?

A. Restricting access to systems only during designated working hours daily
B. Requiring users to request permission for every individual file they access
C. Granting users only the minimum access needed for their specific job duties
D. Providing all users with administrator-level access for operational convenience

Answer: C

Q239. What is a CAPTCHA used for?

A. Tracking user browsing behavior across different websites for analytics
B. Measuring the loading speed of web pages for performance optimization
C. Encrypting user passwords before storing them in the application database
D. Distinguishing human users from automated bots during online interactions

Answer: D

Q240. What is an access control list (ACL)?

A. A list defining which users or groups have permission to access specific resources
B. A catalog of all software applications installed on the organizational network
C. A record of all users who have ever logged into the system since installation
D. A directory listing all hardware devices connected to the computer network

Answer: A

Q241. What is secure software development?

A. Writing code that prioritizes speed over all other quality attributes
B. Creating software that focuses exclusively on user interface design
C. Building software with security integrated throughout the development lifecycle
D. Developing software as quickly as possible without any testing phases

Answer: C

Q242. What is the purpose of code review in secure development?

A. Measuring the execution speed of individual functions in code
B. Formatting code to follow consistent visual styling conventions
C. Translating code from one programming language to another one
D. Examining code to find security flaws and bugs before deployment

Answer: D

Q243. What does SDLC stand for in software development?

A. System Data Logging Control
B. Software Development Life Cycle
C. Secure Database Login Credentials
D. Standard Digital Library Catalog

Answer: B

Q244. What is input sanitization in secure coding?

A. Formatting input data to display it in a more readable user interface
B. Cleaning user input to remove or escape potentially harmful characters
C. Converting all input text to uppercase for consistent data storage
D. Compressing input data to reduce the database storage requirements

Answer: B

Q245. What is the principle of 'secure by default' in software design?

A. Software should allow all features by default for maximum user flexibility
B. Software should disable all functionality until security is configured
C. Software should require users to manually enable all security features
D. Software should be configured with the most secure settings out of the box

Answer: D

Q246. What is a buffer overflow vulnerability?

A. When a hard drive runs out of storage space preventing new files from being saved
B. When a network connection transfers more data than the bandwidth can accommodate
C. When a database table exceeds its maximum number of allowed records or entries
D. When a program writes more data to a buffer than it can hold causing memory corruption

Answer: D

Q247. What is static application security testing (SAST)?

A. Testing a running application by sending malicious requests to endpoints
B. Monitoring application behavior in production for suspicious activity
C. Analyzing source code without executing it to find security vulnerabilities
D. Scanning network traffic for signs of application-level security attacks

Answer: C

Q248. Why should sensitive data like passwords never be stored in plain text?

A. Because plain text passwords can be read directly if the database is compromised
B. Because plain text passwords cannot be validated during the login process flow
C. Because plain text takes up more storage space than encrypted text in databases
D. Because plain text is incompatible with modern database management systems today

Answer: A

Q249. What is the purpose of error handling in secure coding?

A. Displaying all error details to help users troubleshoot their problems
B. Managing errors gracefully without revealing sensitive system information
C. Ignoring errors so the application continues running without interruption
D. Logging errors only to the browser console for developer convenience

Answer: B

Q250. What is the purpose of using version control in secure development?

A. Compiling code into executable format for production server deployment
B. Tracking code changes enabling rollback and audit trail of modifications
C. Encrypting all source code files to prevent unauthorized code access
D. Automatically fixing security vulnerabilities found in application code

Answer: B

Q251. What is the most secure wireless encryption protocol currently available?

A. WPA
B. WEP
C. WPS
D. WPA3

Answer: D

Q252. What is a rogue access point?

A. A legitimate access point that has been configured with a strong password
B. A backup access point that activates when the primary one stops working
C. A guest network access point provided for visitors in a corporate office
D. An unauthorized wireless access point connected to a network without approval

Answer: D

Q253. What is the purpose of a mobile device management (MDM) solution?

A. Providing free mobile applications to all employees for personal usage
B. Upgrading the hardware components inside company-issued mobile phones
C. Increasing the battery life of mobile devices through power optimization
D. Centrally managing and securing mobile devices used within an organization

Answer: D

Q254. What is Bluetooth security's main concern?

A. Excessive battery drain caused by Bluetooth hardware power consumption
B. Slow data transfer speeds compared to modern WiFi network connections
C. Unauthorized pairing and data interception over short-range connections
D. Incompatibility between different Bluetooth device manufacturers products

Answer: C

Q255. What is the risk of connecting to public WiFi networks?

A. Attackers can intercept unencrypted data transmitted over the shared network
B. Public WiFi networks require stronger passwords than private home networks
C. Public WiFi networks always provide faster speeds than private connections
D. Public WiFi automatically installs security software on connected devices

Answer: A

Q256. What does BYOD stand for in mobile security?

A. Backup Your Online Data
B. Build Your Own Database
C. Bring Your Own Device
D. Browse Your Own Domain

Answer: C

Q257. What is the purpose of remote wipe capability on mobile devices?

A. Cleaning the device screen remotely using an automated cleaning mechanism
B. Deleting old text messages to free up storage space on the mobile device
C. Removing unused applications to improve the mobile device's performance
D. Erasing all data on a lost or stolen device to prevent unauthorized access

Answer: D

Q258. What is an evil twin attack in wireless security?

A. Connecting two identical routers to the same network causing IP address conflicts
B. Creating a fake WiFi access point that mimics a legitimate one to steal data
C. Sending duplicate data packets across a wireless network to cause congestion
D. Installing two antivirus programs that conflict with each other on a device

Answer: B

Q259. What is the security risk of jailbreaking or rooting a mobile device?

A. It enables the device to connect to more WiFi networks simultaneously
B. It removes built-in security controls making the device vulnerable to malware
C. It increases the device's processing speed by unlocking hidden CPU features
D. It improves battery life by disabling unnecessary background system processes

Answer: B

Q260. What is the purpose of a VPN on a mobile device?

A. Increasing mobile data speed by compressing all network traffic packets
B. Encrypting network traffic to protect data when using untrusted networks
C. Extending the WiFi range of the device to connect to distant networks
D. Blocking all incoming phone calls from unknown or unregistered numbers

Answer: B

Q261. What is the shared responsibility model in cloud security?

A. A model where the cloud provider handles all security with no customer involvement
B. A model where the customer handles all security without any provider assistance
C. A model where security responsibilities are split between the cloud provider and customer
D. A model where third-party vendors manage all security for both provider and customer

Answer: C

Q262. What are the three main cloud service models?

A. LAN, WAN, and MAN
B. CPU, RAM, and SSD
C. IaaS, PaaS, and SaaS
D. HTTP, FTP, and SMTP

Answer: C

Q263. What is a cloud access security broker (CASB)?

A. A person who negotiates cloud service contracts on behalf of organizations
B. A network device that routes traffic between different cloud provider data centers
C. A certification program for cloud security professionals in the IT industry
D. A security tool that sits between users and cloud services to enforce policies

Answer: D

Q264. What is the risk of misconfigured cloud storage buckets?

A. Data transfer speeds decrease significantly making applications unusable
B. Sensitive data may be exposed publicly if access controls are not properly set
C. Cloud storage costs increase dramatically due to inefficient configuration
D. The cloud provider revokes the organization's account for policy violations

Answer: B

Q265. What is multi-tenancy in cloud computing?

A. A customer maintaining separate accounts for each department within an organization
B. Multiple customers sharing the same physical infrastructure in a cloud environment
C. A single customer using multiple cloud providers simultaneously for redundancy
D. Multiple data centers connected together to form one large computing cluster

Answer: B

Q266. What is the purpose of identity and access management (IAM) in cloud environments?

A. Backing up all cloud data to local on-premises servers for redundancy
B. Monitoring the physical security of data centers operated by cloud providers
C. Optimizing the performance of applications running on cloud infrastructure
D. Managing who can access cloud resources and what actions they can perform

Answer: D

Q267. What is data sovereignty in cloud computing?

A. The cloud provider having complete ownership of all customer data stored
B. Data being subject to the laws of the country where it is physically stored
C. Users having the ability to access their data from any country worldwide
D. Data being automatically encrypted by the cloud provider at all times

Answer: B

Q268. What is the purpose of encryption at rest in cloud storage?

A. Reducing the overall cost of cloud storage by compressing encrypted data
B. Speeding up data retrieval from cloud storage by compressing encrypted files
C. Preventing cloud administrators from modifying data stored in the cloud
D. Protecting stored data from unauthorized access even if storage is compromised

Answer: D

Q269. What is a virtual private cloud (VPC)?

A. An isolated section of cloud infrastructure dedicated to a single customer
B. A private data center that does not connect to any public cloud service
C. A cloud-based VPN service for encrypting all internet traffic globally
D. A virtual machine running antivirus software in the cloud environment

Answer: A

Q270. What is shadow IT in the context of cloud security?

A. Employees using unauthorized cloud services without IT department approval
B. IT staff working remotely from home offices instead of the corporate campus
C. Cloud services that operate only during nighttime hours for cost savings
D. Backup cloud infrastructure that remains inactive until primary systems fail

Answer: A

Q271. What is digital forensics?

A. The technique of building databases for storing criminal record information
B. The process of collecting and analyzing digital evidence from electronic devices
C. The method of encrypting court documents for secure legal proceedings
D. The practice of designing user interfaces for law enforcement applications

Answer: B

Q272. Why is preserving the chain of custody important in digital forensics?

A. It ensures evidence integrity and admissibility in legal proceedings
B. It speeds up the analysis process by organizing evidence chronologically
C. It prevents investigators from accessing evidence until trial begins
D. It reduces the cost of forensic investigations by limiting evidence scope

Answer: A

Q273. What is a forensic image of a hard drive?

A. A compressed backup of only the active files on the hard drive
B. A log file recording all read and write operations on the drive
C. A bit-for-bit exact copy of the entire drive including deleted data
D. A photograph taken of the physical hard drive for documentation

Answer: C

Q274. What is a write blocker used for in digital forensics?

A. Limiting the number of files that can be saved on a USB drive
B. Stopping malware from writing malicious files to the hard drive
C. Preventing any modification to evidence media during examination
D. Blocking users from writing documents on shared network drives

Answer: C

Q275. What type of evidence can be found in computer RAM?

A. Permanent files that remain stored even after the computer is completely shut down
B. Hardware serial numbers and manufacturer information for all installed components
C. Running processes, encryption keys, and temporary data that disappears when powered off
D. Operating system installation files that are needed only during the initial setup

Answer: C

Q276. What is the purpose of hashing in digital forensics?

A. Compressing evidence data to save storage space on forensic servers
B. Verifying that evidence has not been altered by comparing hash values
C. Converting binary evidence data into human-readable text documents
D. Encrypting evidence files to prevent unauthorized access by others

Answer: B

Q277. What is volatile data in forensic investigations?

A. Data that is stored in cloud services and accessible from anywhere
B. Data that is lost when a device is powered off such as RAM contents
C. Data that is permanently stored on hard drives and never changes
D. Data that is encrypted and cannot be accessed without proper keys

Answer: B

Q278. What are log files used for in forensic analysis?

A. Managing software licenses for forensic tools used during analysis
B. Storing user passwords in an encrypted format for secure retrieval
C. Recording system events that help reconstruct activities and timelines
D. Tracking the physical location of all devices on the network map

Answer: C

Q279. What is metadata in the context of digital evidence?

A. Encrypted data that requires a special key to read and understand
B. Data about data, such as file creation dates, authors, and modification times
C. Backup copies of files stored on a separate external storage device
D. The main content of a document file like the text or images within it

Answer: B

Q280. What is the first step a forensic investigator should take at a crime scene?

A. Immediately turning off all computers to preserve the current state
B. Securing the scene and documenting the state of all devices present
C. Deleting unnecessary files to focus the investigation on key evidence
D. Connecting all devices to the internet for remote forensic analysis

Answer: B

Q281. What is an incident response plan?

A. A training syllabus for teaching new employees about organizational policies at work
B. A schedule for performing regular system maintenance and software update installations
C. A financial plan for budgeting cyber security spending across all fiscal year quarters
D. A documented strategy for detecting, responding to, and recovering from security incidents

Answer: D

Q282. What is the first phase of the incident response lifecycle according to NIST?

A. Preparation
B. Eradication
C. Containment
D. Recovery

Answer: A

Q283. What is the purpose of incident containment?

A. Shutting down the entire organization's network permanently until the threat is gone
B. Deleting all data on affected systems to remove any traces of the attack completely
C. Limiting the spread and impact of a security incident to prevent further damage
D. Notifying the media about the security incident for public awareness and transparency

Answer: C

Q284. What is a CSIRT?

A. Central Server Infrastructure Review Tool
B. Cyber Security Integration and Reporting Technology
C. Computer Security Incident Response Team
D. Cloud Service Infrastructure Recovery Technique

Answer: C

Q285. What is the purpose of a lessons learned review after an incident?

A. Assigning blame to the individuals who caused or failed to prevent the incident
B. Deleting all records of the incident to protect the organization's public reputation
C. Calculating the exact financial bonus for team members who resolved the incident
D. Identifying improvements to prevent similar incidents and enhance response processes

Answer: D

Q286. What is the difference between an event and an incident in cyber security?

A. An event is always malicious while an incident is always a harmless system occurrence
B. An event is any observable occurrence while an incident is an event that harms security
C. An event requires investigation while an incident is resolved automatically by tools
D. An event only happens on servers while an incident only happens on user workstations

Answer: B

Q287. What is the role of incident triage?

A. Automatically resolving all incidents using predefined scripts without human input
B. Prioritizing incidents based on severity and impact to allocate resources effectively
C. Forwarding all incidents to external law enforcement for criminal investigation
D. Permanently closing all incident tickets without any investigation or resolution

Answer: B

Q288. What is eradication in incident response?

A. Notifying affected users about the incident and providing credit monitoring services
B. Removing the root cause of the incident and any attacker artifacts from systems
C. Documenting the incident for future reference and compliance reporting purposes
D. Restoring systems to normal operation after the threat has been fully eliminated

Answer: B

Q289. What is the purpose of an incident response communication plan?

A. Scheduling regular team meetings for discussing non-security project deliverables
B. Creating social media posts about the organization's daily business operations
C. Marketing the organization's security capabilities to attract potential customers
D. Defining who to notify, when, and how during a security incident for coordination

Answer: D

Q290. What is the recovery phase in incident response?

A. Documenting all evidence collected during the investigation for legal review
B. Identifying the initial attack vector used by the threat actor to gain access
C. Purchasing new hardware to replace all systems affected by the security breach
D. Restoring affected systems to normal operation and verifying they are secure

Answer: D

Q291. What is a SIEM system?

A. A tool that collects and analyzes security event data from across the network
B. A protocol for encrypting email communications between users securely
C. A physical device that blocks malware at the network perimeter gateway
D. A type of firewall specifically designed for protecting cloud environments

Answer: A

Q292. What is the purpose of security log monitoring?

A. Deleting old log files to free up storage space on the server hard drives
B. Converting log files into PDF documents for printing and physical archival
C. Detecting suspicious activities and security incidents by reviewing system logs
D. Creating backup copies of log files for disaster recovery planning purposes

Answer: C

Q293. What is a security alert?

A. A notification generated when a monitoring system detects potentially suspicious activity
B. A marketing email from a security vendor promoting their latest product features
C. A scheduled reminder for IT staff to change their passwords at regular intervals
D. A system notification about available software updates that need to be installed

Answer: A

Q294. What is a false positive in security monitoring?

A. A system error that prevents the monitoring tool from generating any alerts
B. A genuine security incident that was correctly detected by the monitoring system
C. An alert triggered by normal activity that is incorrectly identified as malicious
D. A disabled alert rule that no longer triggers on any type of security event

Answer: C

Q295. What is network traffic analysis used for in security?

A. Testing network cable quality to ensure reliable physical connections work
B. Monitoring network communications to identify anomalies and potential threats
C. Designing new network architectures for improved organizational connectivity
D. Increasing network bandwidth by optimizing data packet routing efficiency

Answer: B

Q296. What is endpoint detection and response (EDR)?

A. A process for repairing damaged endpoint hardware components like keyboards and screens
B. A method for deploying software updates to all endpoint devices simultaneously
C. A system for tracking the physical location of all laptop devices issued to employees
D. A security tool that monitors endpoints for threats and provides investigation capabilities

Answer: D

Q297. What is log aggregation?

A. Distributing log data across multiple servers for redundant backup storage
B. Converting log files from text format to binary format for faster reading
C. Deleting duplicate log entries to reduce the overall volume of stored data
D. Collecting logs from multiple sources into a centralized location for analysis

Answer: D

Q298. What is a security dashboard?

A. A physical panel of buttons used to arm and disarm building security alarms
B. A software application for managing employee access badges and ID cards
C. A visual display showing security metrics, alerts, and system status in real time
D. A printed report summarizing monthly security statistics for executive review

Answer: C

Q299. What is vulnerability scanning?

A. Testing network cable connections for signal quality and potential interference issues
B. Automated scanning of systems to identify known security weaknesses and misconfigurations
C. Physically inspecting server hardware for signs of tampering or unauthorized modifications
D. Manually reviewing source code to find programming errors and logic flaws in software

Answer: B

Q300. What is the purpose of a security operations center (SOC)?

A. Providing technical support to employees experiencing computer problems
B. Developing new software applications for the organization's customers
C. Managing the physical security of the building including locks and guards
D. Centrally monitoring and responding to security events across the organization

Answer: D

Q301. What is the primary purpose of data protection laws?

A. Setting minimum salary requirements for IT professionals in organizations
B. Increasing internet speeds for all citizens within a country's borders
C. Regulating the manufacturing standards for computer hardware products
D. Protecting individuals' personal data from misuse and unauthorized processing

Answer: D

Q302. What does GDPR stand for?

A. General Digital Privacy Regulation
B. Global Digital Privacy Requirement
C. General Data Protection Regulation
D. Government Data Processing Rules

Answer: C

Q303. What is intellectual property in the context of cyber law?

A. Employee skills and knowledge that are gained through professional training programs
B. Network bandwidth that is allocated to a specific organization by an internet provider
C. Physical computer hardware that is owned by an organization and stored in data centers
D. Creations of the mind like inventions, designs, and software that are legally protected

Answer: D

Q304. What is the purpose of a privacy policy on a website?

A. Displaying advertisements that are relevant to the user's browsing history
B. Informing users how their personal data is collected, used, and protected
C. Preventing users from accessing certain pages on the website based on age
D. Encrypting all data transmitted between the user's browser and the server

Answer: B

Q305. What is ethical hacking?

A. Hacking into systems without permission to demonstrate security weaknesses publicly
B. Using social engineering to test employee awareness without organizational approval
C. Creating malware for research purposes without deploying it in real environments
D. Authorized testing of systems to find vulnerabilities before malicious hackers exploit them

Answer: D

Q306. What is a non-disclosure agreement (NDA) used for in cyber security?

A. Allowing employees to share company secrets with competitors for personal benefit
B. Disclosing all security vulnerabilities publicly to raise awareness about threats
C. Legally binding parties to keep shared confidential information private and secure
D. Granting customers full access to the organization's proprietary source code

Answer: C

Q307. What does the term 'compliance' mean in cyber security?

A. Completing all security training courses within the required time period
B. Competing with other organizations to achieve the highest security ratings
C. Following established laws, regulations, and standards for information security
D. Purchasing the most expensive security tools available on the market today

Answer: C

Q308. What is responsible disclosure in cyber security?

A. Publishing all discovered vulnerabilities immediately on social media platforms
B. Ignoring discovered vulnerabilities to avoid any potential legal consequences
C. Selling vulnerability information to the highest bidder on dark web forums
D. Reporting vulnerabilities to the vendor privately before making them public

Answer: D

Q309. What is the purpose of cyber crime laws?

A. Providing free internet access to all citizens as a fundamental digital right
B. Defining illegal cyber activities and establishing penalties for those who commit them
C. Mandating that all organizations must use open-source software exclusively
D. Regulating the prices of cyber security software products sold in the market

Answer: B

Q310. What is digital consent in data privacy?

A. Allowing any organization to access user data without requiring authorization
B. Obtaining user permission before collecting and processing their personal data
C. Storing user data indefinitely regardless of whether consent was ever provided
D. Automatically collecting user data without informing them about the practice

Answer: B

Q311. What is the Internet of Things (IoT) in cyber security?

A. A cloud storage service that allows unlimited data storage for connected devices
B. A security protocol designed to protect web browsers from malicious website content
C. A new type of internet connection that is faster than traditional broadband service
D. Network of connected devices that collect and exchange data creating security challenges

Answer: D

Q312. What is artificial intelligence's role in cyber security?

A. Enhancing threat detection, automating responses, and analyzing large security datasets
B. Replacing all human security professionals with fully autonomous robot defenders
C. Creating new types of encryption that are impossible to break by any method
D. Eliminating all cyber threats permanently through advanced predictive algorithms

Answer: A

Q313. What is blockchain technology's relevance to cyber security?

A. Eliminating the need for encryption because blockchain is inherently secure
B. Providing tamper-resistant record-keeping and decentralized trust mechanisms
C. Replacing all existing databases with faster and cheaper storage solutions
D. Creating untraceable communications that cannot be monitored by anyone

Answer: B

Q314. What is quantum computing's potential impact on cyber security?

A. Eliminating all cyber threats because quantum computers cannot be compromised
B. Making all existing security tools obsolete and completely useless immediately
C. Threatening current encryption methods by potentially breaking widely used algorithms
D. Having no impact on cyber security because quantum computing is only theoretical

Answer: C

Q315. What is zero trust architecture?

A. A network design that eliminates all firewalls to simplify security management
B. A security model that trusts no one by default and verifies every access request
C. A framework that trusts all internal users and only verifies external connections
D. A policy requiring zero passwords for user authentication across all systems

Answer: B

Q316. What is DevSecOps?

A. Integrating security practices into the DevOps software development pipeline
B. A cloud service that automatically secures deployed applications and databases
C. A specialized operating system designed for security-focused development work
D. A certification for developers who specialize in building secure applications

Answer: A

Q317. What is ransomware-as-a-service (RaaS)?

A. A legitimate cloud service that helps organizations recover from ransomware attacks
B. A government program providing free ransomware decryption tools to affected organizations
C. A business model where ransomware developers sell or lease their tools to other criminals
D. A cybersecurity insurance product that covers ransomware payment costs for businesses

Answer: C

Q318. What is edge computing and its security implications?

A. A computing approach that only works with wired connections and cannot use wireless links
B. A method of strengthening network perimeter defenses at the edge of the corporate network
C. A technique for storing backup data at the geographical edges of a country's territory
D. Processing data closer to where it is generated, creating new distributed security challenges

Answer: D

Q319. What is a deepfake?

A. A backup copy of data that is stored in a deeply encrypted format for maximum security
B. A social media account that pretends to be a real person for legitimate marketing goals
C. A type of encryption that creates fake data to confuse attackers during a breach event
D. AI-generated synthetic media that can convincingly impersonate real people in video or audio

Answer: D

Q320. What is cyber resilience?

A. The speed at which an internet connection recovers after a temporary service outage
B. The physical durability of computer hardware against environmental damage threats
C. A software feature that automatically restarts applications after an unexpected crash
D. An organization's ability to prepare for, respond to, and recover from cyber incidents

Answer: D

Q321. What does the term 'cyber hygiene' refer to?

A. Cleaning computer hardware regularly
B. Routine practices to maintain system health and security
C. Installing only free software
D. Using the internet only during business hours

Answer: B

Q322. Which of the following is an example of a cyber attack?

A. Backing up files to a cloud server
B. Sending an encrypted email
C. Deploying ransomware on a network
D. Installing a security patch

Answer: C

Q323. What is the primary goal of information security?

A. Making systems run faster
B. Protecting information from unauthorized access, use, or destruction
C. Reducing hardware costs
D. Increasing internet bandwidth

Answer: B

Q324. What does the term 'exploit' mean in cyber security?

A. A security certification program
B. A piece of software or technique that takes advantage of a vulnerability
C. A type of antivirus software
D. A network monitoring tool

Answer: B

Q325. Which professional is responsible for protecting an organization's computer systems?

A. Database administrator
B. Cyber security analyst
C. Graphic designer
D. Help desk technician

Answer: B

Q326. What is a 'patch' in the context of cyber security?

A. A physical repair to damaged hardware
B. A software update that fixes security vulnerabilities
C. A type of network cable
D. A backup storage device

Answer: B

Q327. What does 'authentication' verify in cyber security?

A. The speed of a network connection
B. The identity of a user or system
C. The size of a file
D. The cost of a software license

Answer: B

Q328. Which of the following is a common indicator of a phishing email?

A. The email comes from a known colleague
B. The email has a professional signature
C. The email contains urgent language and suspicious links
D. The email is about a scheduled meeting

Answer: C

Q329. What is a 'risk' in cyber security?

A. Any computer connected to the internet
B. The potential for loss or damage when a threat exploits a vulnerability
C. A type of encryption algorithm
D. A network protocol

Answer: B

Q330. What is the purpose of a security awareness program?

A. To train employees on recognizing and responding to security threats
B. To install firewalls on every computer
C. To replace antivirus software
D. To encrypt all company emails automatically

Answer: A

Q331. What is a security incident?

A. A scheduled system update
B. An event that threatens the confidentiality, integrity, or availability of information
C. A routine password change
D. A planned network maintenance window

Answer: B

Q332. What is the purpose of a firewall in network security?

A. To increase internet speed
B. To monitor and control incoming and outgoing network traffic based on security rules
C. To store backup files
D. To manage email accounts

Answer: B

Q333. What is the difference between a threat and a vulnerability?

A. They are the same thing
B. A threat is a potential danger while a vulnerability is a weakness that can be exploited
C. A vulnerability is more dangerous than a threat
D. Threats only exist online while vulnerabilities are physical

Answer: B

Q334. What does 'non-repudiation' ensure in information security?

A. That data is always available
B. That a user cannot deny having performed a specific action
C. That passwords are never reused
D. That firewalls block all traffic

Answer: B

Q335. What is a security policy?

A. A type of antivirus software
B. A document that outlines an organization's rules and procedures for protecting information
C. A hardware device for encrypting files
D. A programming language for security tools

Answer: B

Q336. Which of the following is a preventive security control?

A. Security camera
B. Intrusion detection system
C. Access control lock on a door
D. Audit log review

Answer: C

Q337. What is data classification in information security?

A. Sorting data alphabetically
B. Categorizing data based on its sensitivity level to apply appropriate protection
C. Deleting old data from servers
D. Compressing data to save storage space

Answer: B

Q338. What does the term 'least privilege' mean in security?

A. Giving all users administrator access
B. Granting users only the minimum access necessary to perform their job functions
C. Removing all access permissions from users
D. Using the cheapest security software available

Answer: B

Q339. What is two-factor authentication (2FA)?

A. Using two different passwords
B. A security method requiring two different types of verification to prove identity
C. Logging in from two different devices
D. Having two user accounts

Answer: B

Q340. What is the purpose of an acceptable use policy (AUP)?

A. To define how employees may use organizational IT resources
B. To list all software installed on company computers
C. To track employee internet browsing history
D. To set pricing for IT services

Answer: A

Q341. What is the difference between encryption and hashing?

A. They are the same process
B. Encryption is reversible with a key while hashing is a one-way process
C. Hashing is always faster than encryption
D. Encryption does not use keys

Answer: B

Q342. What is a private key in asymmetric cryptography?

A. A key shared with everyone publicly
B. A key kept secret by the owner and used for decryption or signing
C. A key used only for hashing
D. A password used to log into websites

Answer: B

Q343. What is the purpose of SSL/TLS in web communications?

A. To speed up website loading times
B. To encrypt communications between a web browser and web server
C. To compress images on websites
D. To block advertisements on web pages

Answer: B

Q344. Which of the following is an example of a hash algorithm?

A. AES
B. RSA
C. SHA-256
D. Diffie-Hellman

Answer: C

Q345. What does 'key length' refer to in cryptography?

A. The physical length of a USB security key
B. The number of bits in a cryptographic key, which affects encryption strength
C. The number of characters in a password
D. The duration a key remains valid

Answer: B

Q346. What is a digital certificate used for?

A. To store encrypted files permanently
B. To verify the identity of a website or entity and bind a public key to that identity
C. To block malware from downloading
D. To increase internet connection speed

Answer: B

Q347. What does symmetric encryption mean?

A. Different keys are used for encryption and decryption
B. The same key is used for both encryption and decryption
C. No key is needed for encryption
D. Only the sender needs a key

Answer: B

Q348. What is a cryptographic protocol?

A. A type of computer virus
B. A set of rules that governs how cryptographic operations are performed in communications
C. A hardware device for encryption
D. A programming language for writing security software

Answer: B

Q349. Why should encryption keys be kept secret?

A. Because keys are expensive to generate
B. Because anyone with the key can decrypt the protected data
C. Because keys expire after one use
D. Because keys take up storage space

Answer: B

Q350. What is end-to-end encryption?

A. Encrypting only the first and last packets of a transmission
B. Encrypting data at the sender's end so that only the intended recipient can decrypt it
C. Encrypting data only when stored on a server
D. Using two firewalls at each end of a network

Answer: B

Q351. What is an IP address used for in networking?

A. To encrypt data on a network
B. To uniquely identify a device on a network
C. To increase network speed
D. To store files on a server

Answer: B

Q352. What is a router's role in network security?

A. It only provides wireless internet access
B. It directs network traffic between networks and can enforce security policies through access control lists
C. It stores all network passwords
D. It replaces the need for firewalls

Answer: B

Q353. What is the purpose of network address translation (NAT) in security?

A. To speed up internet connections significantly
B. To hide internal IP addresses from external networks
C. To encrypt all outgoing network packets
D. To replace the need for antivirus software

Answer: B

Q354. What does the term 'bandwidth' refer to in networking?

A. The physical width of a network cable
B. The maximum amount of data that can be transmitted over a network connection in a given time
C. The number of computers on a network
D. The strength of a WiFi signal

Answer: B

Q355. What is the purpose of a network switch in a local area network?

A. To connect a network to the internet
B. To connect multiple devices within a network and forward data to the correct destination device
C. To encrypt all network traffic
D. To scan for viruses on the network

Answer: B

Q356. What is network monitoring used for?

A. To increase the speed of all network connections
B. To observe and analyze network traffic for performance issues and security threats
C. To replace all security controls
D. To generate encryption keys

Answer: B

Q357. What does DNS stand for and what is its primary function?

A. Data Network Storage; stores files on a network
B. Domain Name System; translates domain names into IP addresses
C. Digital Network Security; encrypts network traffic
D. Direct Network Service; manages network connections

Answer: B

Q358. What is a network protocol?

A. A hardware device used to connect networks
B. A set of rules governing how data is transmitted and received over a network
C. A type of network cable
D. A software program for browsing the internet

Answer: B

Q359. What is the function of an Intrusion Prevention System (IPS)?

A. To provide wireless internet access
B. To detect and actively block malicious network traffic in real time
C. To create backups of network data
D. To assign IP addresses to devices

Answer: B

Q360. What is a VLAN used for in network security?

A. To increase the physical range of a WiFi network
B. To logically segment a network into separate broadcast domains for improved security and management
C. To encrypt all data on the network
D. To replace physical firewalls

Answer: B

Q361. What is a one-time pad in cryptography?

A. A cipher that uses a random key as long as the message and is used only once
B. A reusable encryption key for multiple messages
C. A type of hash function
D. A digital certificate format

Answer: A

Q362. Which type of encryption is faster for large amounts of data: symmetric or asymmetric?

A. Asymmetric encryption
B. Both are equally fast
C. Neither can handle large data
D. Symmetric encryption

Answer: D

Q363. What does the term 'key pair' refer to in asymmetric cryptography?

A. Two identical keys used for encryption
B. A public key and a corresponding private key
C. Two symmetric keys shared between parties
D. A key and its backup copy

Answer: B

Q364. What is the purpose of Base64 encoding?

A. To encrypt data securely
B. To compress data for storage
C. To represent binary data in an ASCII string format
D. To generate cryptographic hashes

Answer: C

Q365. What does the acronym AES stand for?

A. Asymmetric Encryption System
B. Advanced Encryption Standard
C. Automated Encoding Scheme
D. Applied Encryption Software

Answer: B

Q366. What is a cryptographic hash collision?

A. When two different inputs produce the same hash output
B. When a hash function fails to produce output
C. When encryption and decryption keys match
D. When two users share the same password

Answer: A

Q367. What is the role of a random number generator in cryptography?

A. To create user passwords automatically
B. To generate unpredictable values for keys, nonces, and IVs
C. To speed up encryption algorithms
D. To compress data before encryption

Answer: B

Q368. What is the difference between encoding and encryption?

A. They are the same thing
B. Encoding transforms data for usability while encryption transforms data for confidentiality
C. Encoding is more secure than encryption
D. Encryption is faster than encoding

Answer: B

Q369. Which of the following is NOT a symmetric encryption algorithm?

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

Answer: D

Q370. What is a digital envelope in cryptography?

A. A physical container for cryptographic keys
B. A method combining symmetric and asymmetric encryption to securely transmit data
C. A type of email encryption only
D. A digital signature format

Answer: B

Q371. What is the purpose of a firewall built into an operating system?

A. To speed up internet connections
B. To filter incoming and outgoing network traffic based on security rules
C. To defragment the hard drive
D. To manage user passwords

Answer: B

Q372. What is the principle of least privilege in operating system security?

A. Giving all users administrator access
B. Users and programs should only have the minimum permissions needed to perform their tasks
C. Disabling all user accounts except root
D. Removing all security software

Answer: B

Q373. What is a software update in the context of OS security?

A. A new version of a video game
B. A patch or fix released to address security vulnerabilities or bugs in the OS
C. A change to the desktop wallpaper
D. An increase in storage capacity

Answer: B

Q374. What does antivirus software do on an operating system?

A. Increases internet speed
B. Detects, prevents, and removes malicious software
C. Manages file storage
D. Creates system backups

Answer: B

Q375. Why should users avoid running programs as administrator unnecessarily?

A. It makes the computer slower
B. Programs running with admin privileges can make system-wide changes that could be harmful if compromised
C. Admin accounts have fewer features
D. There is no reason to avoid it

Answer: B

Q376. What is a strong password policy for OS user accounts?

A. Using the word 'password' for all accounts
B. Requiring passwords with minimum length, complexity, and regular changes
C. Allowing blank passwords for convenience
D. Using the same password for all accounts

Answer: B

Q377. What is a boot password in OS security?

A. A password required before the operating system loads
B. The default password for all applications
C. A password used only for email
D. A password for internet browsing

Answer: A

Q378. What happens when automatic updates are disabled on an OS?

A. The system becomes faster
B. The system may miss critical security patches and remain vulnerable to known threats
C. Nothing changes
D. The system automatically becomes more secure

Answer: B

Q379. What is a guest account on an operating system?

A. The main administrator account
B. A limited-privilege account for temporary users with restricted access
C. An account with full system permissions
D. A hidden account used by hackers

Answer: B

Q380. Why is it important to lock your computer screen when stepping away?

A. To save electricity only
B. To prevent unauthorized physical access to your active session and data
C. It is not important
D. To improve display quality

Answer: B

Q381. What is a web browser's address bar padlock icon used to indicate?

A. The website is free of malware
B. The connection to the website is encrypted using HTTPS
C. The website content is verified as accurate
D. The website loads faster than others

Answer: B

Q382. What is the purpose of the robots.txt file on a website?

A. To block all hackers from accessing the site
B. To instruct search engine crawlers which parts of the site to avoid indexing
C. To encrypt website data
D. To manage user passwords

Answer: B

Q383. What is a URL redirect vulnerability?

A. When a website loads too slowly
B. When a website redirects users to a malicious site using unvalidated redirect parameters
C. When a website's URL is too long
D. When a website changes its domain name

Answer: B

Q384. Why should sensitive forms on websites use POST requests instead of GET?

A. POST requests are faster
B. GET requests include data in the URL which can be cached, logged, and visible in browser history
C. POST requests do not require a server
D. GET requests cannot carry data

Answer: B

Q385. What is the purpose of rate limiting on a web application?

A. To make the website faster
B. To restrict the number of requests a user can make in a given time period to prevent abuse
C. To increase server storage
D. To improve website appearance

Answer: B

Q386. What is a Content Delivery Network (CDN) and does it improve security?

A. A type of encryption algorithm
B. A distributed network of servers that can improve performance and provide basic DDoS protection
C. A database management system
D. A web programming language

Answer: B

Q387. What is an HTTP cookie used for in web applications?

A. To encrypt web pages
B. To store small pieces of data on the client's browser for session management, preferences, and tracking
C. To speed up DNS resolution
D. To compress web traffic

Answer: B

Q388. What is cross-origin resource sharing (CORS)?

A. A type of web attack
B. A mechanism that allows web pages to request resources from a different domain than the one that served the page
C. A database query language
D. A server-side scripting language

Answer: B

Q389. Why is it important to use prepared statements when interacting with databases in web applications?

A. They make queries run faster
B. They prevent SQL injection by separating SQL code from user data
C. They reduce database storage usage
D. They are required by all programming languages

Answer: B

Q390. What does the HttpOnly flag on a cookie do?

A. Makes the cookie work only over HTTP, not HTTPS
B. Prevents the cookie from being accessed by client-side JavaScript
C. Encrypts the cookie value
D. Deletes the cookie after the browser closes

Answer: B

Q391. What is a password manager and why should you use one?

A. A tool that remembers only one password
B. A tool that generates and securely stores unique complex passwords for all your accounts
C. A tool that removes password requirements
D. A tool that shares passwords with others

Answer: B

Q392. What does 'something you know' refer to as an authentication factor?

A. A fingerprint scan
B. A smart card
C. Knowledge-based credentials such as a password, PIN, or security question answer
D. A one-time code from an app

Answer: C

Q393. What is the difference between a PIN and a password?

A. There is no difference
B. A PIN is typically a short numeric code while a password is usually longer and can contain letters, numbers, and symbols
C. A PIN is more secure than a password
D. A password can only contain numbers

Answer: B

Q394. What is session timeout and why is it important for security?

A. When a website permanently deletes your account
B. Automatically ending a user's session after a period of inactivity to prevent unauthorized access
C. When the server crashes from too many users
D. When your internet connection drops

Answer: B

Q395. What is two-step verification?

A. Creating two separate accounts
B. An authentication process that requires two separate verification steps, typically a password and a code sent to your device
C. Logging in twice with the same password
D. Using two different browsers

Answer: B

Q396. What is the purpose of a security question during account recovery?

A. To make the login process slower
B. To verify identity by asking a question that only the legitimate account owner should be able to answer
C. To test the user's general knowledge
D. To encrypt the user's data

Answer: B

Q397. What is the difference between logging in and logging out?

A. They are the same action
B. Logging in authenticates a user and creates a session; logging out ends the session and revokes access
C. Logging out gives more access than logging in
D. Only administrators can log out

Answer: B

Q398. Why should you not share your passwords with others?

A. Shared passwords use more server resources
B. Sharing passwords means others can access your accounts, and you lose control over who does what with your credentials
C. Passwords stop working when shared
D. It is only a recommendation, not important

Answer: B

Q399. What is a brute-force attack on a login page?

A. A physical attack on the server
B. An automated attack that systematically tries all possible password combinations until the correct one is found
C. Refreshing the login page repeatedly
D. Typing the password very quickly

Answer: B

Q400. What is an authenticator app used for?

A. To browse the web securely
B. To generate time-based one-time passwords (TOTP) for two-factor authentication
C. To manage email accounts
D. To encrypt files on your phone

Answer: B

Q401. What is a code vulnerability?

A. A feature that makes code run faster
B. A weakness or flaw in software code that could be exploited by an attacker
C. A type of programming language
D. A software license agreement

Answer: B

Q402. Why should developers avoid hardcoding secrets like API keys in source code?

A. Hardcoded keys make the code too long
B. Hardcoded secrets can be exposed in version control systems, making them accessible to anyone with code access
C. Hardcoded keys improve performance
D. There is no reason to avoid it

Answer: B

Q403. What is the purpose of logging in application development?

A. To slow down the application
B. To record events, errors, and user activities for debugging, monitoring, and security auditing
C. To encrypt application data
D. To manage database connections

Answer: B

Q404. What is dependency management in software development?

A. Managing the development team
B. Tracking and managing the external libraries and frameworks a project relies on to ensure they are secure and up-to-date
C. Managing database dependencies
D. Organizing code files into folders

Answer: B

Q405. What is a security requirement in software development?

A. A request for more developers
B. A specification that defines the security features and controls a software application must implement
C. A requirement to use a specific programming language
D. A deadline for project completion

Answer: B

Q406. Why is it important to handle errors properly in secure coding?

A. Error handling makes code longer
B. Proper error handling prevents sensitive information from being exposed in error messages and maintains application stability
C. Error handling is only for debugging
D. Error handling slows down the application

Answer: B

Q407. What is the purpose of unit testing in secure development?

A. To test the entire application at once
B. To test individual components or functions in isolation to verify they behave correctly, including security-related behavior
C. To test network performance
D. To test user interface design

Answer: B

Q408. What is the concept of 'defense in depth' in application development?

A. Using one very strong security control
B. Implementing multiple layers of security controls so that if one layer fails, others still provide protection
C. Defending only the database
D. Developing applications quickly without testing

Answer: B

Q409. What is the difference between authentication and input validation in secure coding?

A. They are the same concept
B. Authentication verifies user identity while input validation ensures data meets expected format and constraints before processing
C. Input validation replaces the need for authentication
D. Authentication validates all input automatically

Answer: B

Q410. Why should developers use parameterized queries instead of string concatenation for database queries?

A. Parameterized queries are shorter to write
B. Parameterized queries separate SQL code from data, preventing SQL injection attacks that string concatenation enables
C. String concatenation is faster
D. There is no practical difference

Answer: B

Q411. What is airplane mode on a mobile device?

A. A mode that makes the phone look like an airplane
B. A setting that disables all wireless communications including cellular, WiFi, and Bluetooth
C. A mode that increases battery life by 10 times
D. A special mode for use during flights only

Answer: B

Q412. Why should you verify WiFi network names before connecting?

A. To ensure the fastest connection
B. Attackers can create fake networks with similar names to legitimate ones to intercept your data
C. WiFi names affect download speeds
D. Network names determine the security level automatically

Answer: B

Q413. What is the purpose of app permissions on mobile devices?

A. To make apps run faster
B. To control which device resources and data an app can access, such as camera, location, and contacts
C. To manage app storage size
D. To determine which users can install the app

Answer: B

Q414. What is a hotspot on a mobile device?

A. A device that gets physically hot
B. A feature that shares the device's cellular data connection with other devices via WiFi
C. A location with the strongest cell signal
D. A type of malware

Answer: B

Q415. Why should you download apps only from official app stores?

A. Official apps are always free
B. Official app stores review apps for malware and security issues, reducing the risk of installing malicious software
C. Unofficial apps have better features
D. It makes no difference where you download apps

Answer: B

Q416. What is NFC on a mobile device?

A. New Firewall Configuration
B. Near Field Communication, a short-range wireless technology used for contactless payments and data transfer
C. Network Frequency Controller
D. Next-gen File Compression

Answer: B

Q417. What does encryption of mobile device storage protect against?

A. App crashes
B. Unauthorized access to data on the device if it is lost, stolen, or physically accessed by an attacker
C. Slow internet speeds
D. Battery drain

Answer: B

Q418. What is a wireless access point?

A. A wired ethernet port
B. A hardware device that allows wireless devices to connect to a wired network using WiFi
C. A type of mobile application
D. A satellite internet receiver

Answer: B

Q419. Why is it important to keep your mobile device's operating system updated?

A. Updates only add new emojis
B. Updates include security patches that fix known vulnerabilities that attackers could exploit
C. Updates always make the device slower
D. Updates are optional and unimportant

Answer: B

Q420. What is a SIM card in a mobile phone?

A. A security camera
B. A small chip that identifies the subscriber and allows the phone to connect to the cellular network
C. A type of mobile storage for photos
D. A screen protector

Answer: B

Q421. What is a cloud storage service?

A. A physical warehouse for storing computers
B. An online service that allows users to store, access, and share files over the internet
C. A type of local hard drive
D. A mobile application for photography

Answer: B

Q422. What is the difference between a public cloud and a private cloud?

A. There is no difference
B. A public cloud shares infrastructure among multiple organizations while a private cloud is dedicated to a single organization
C. Public clouds are free while private clouds are paid
D. Private clouds do not use the internet

Answer: B

Q423. What is a hybrid cloud environment?

A. A cloud that only works during certain hours
B. A combination of public and private cloud infrastructure that allows data and applications to be shared between them
C. A cloud service that does not use encryption
D. A backup-only cloud solution

Answer: B

Q424. Why is it important to use strong passwords for cloud accounts?

A. Cloud services do not support strong passwords
B. Weak passwords can be easily guessed or cracked, giving attackers access to all your cloud-stored data and services
C. Strong passwords are only needed for local accounts
D. Password strength does not affect cloud security

Answer: B

Q425. What is a cloud service level agreement (SLA)?

A. A type of cloud encryption
B. A contract between the cloud provider and customer that defines the expected level of service, availability, and security responsibilities
C. A programming language for cloud apps
D. A cloud storage format

Answer: B

Q426. What is data backup in cloud computing?

A. Deleting old data from the cloud
B. Creating copies of data stored in the cloud to protect against data loss from accidental deletion, corruption, or attacks
C. Moving all data to a local hard drive
D. Encrypting data at rest

Answer: B

Q427. What is the role of encryption in transit for cloud services?

A. It makes data transfer faster
B. It protects data while it is being transmitted between your device and the cloud server, preventing eavesdropping
C. It compresses data for storage
D. It is only used for email

Answer: B

Q428. What is a cloud region in cloud computing?

A. A marketing term with no technical meaning
B. A geographic area containing data centers where cloud resources are hosted, affecting latency and data residency compliance
C. A type of cloud pricing model
D. The cloud provider's headquarters location

Answer: B

Q429. What is multi-factor authentication's importance for cloud services?

A. MFA is not useful for cloud services
B. MFA adds extra security layers beyond passwords for cloud accounts, significantly reducing the risk of unauthorized access even if passwords are compromised
C. MFA slows down cloud performance
D. MFA is only for on-premises systems

Answer: B

Q430. What is a cloud compliance requirement?

A. A requirement to use only one cloud provider
B. Regulatory standards and laws that organizations must follow when storing and processing data in the cloud, such as data protection and privacy regulations
C. A requirement to back up data daily
D. A cloud provider's internal policy only

Answer: B

Q431. What is the purpose of taking photographs at a digital crime scene?

A. For social media posts
B. To document the state of evidence including screen displays, cable connections, and device locations before any changes are made
C. To test the camera equipment
D. For marketing materials

Answer: B

Q432. What is a forensic copy different from a regular file copy?

A. They are exactly the same thing
B. A forensic copy is a bit-for-bit exact duplicate of an entire storage device including deleted files and empty space, while a regular copy only copies visible files
C. A forensic copy is smaller in size
D. A regular copy includes more data than a forensic copy

Answer: B

Q433. What role does a hash value play in digital forensics?

A. It encrypts the evidence
B. It creates a unique digital fingerprint of evidence that can be used to verify the evidence has not been altered
C. It compresses evidence files
D. It translates evidence into different languages

Answer: B

Q434. What is a forensic workstation?

A. Any regular office computer
B. A specialized computer configured for analyzing digital evidence with forensic tools, write-blocking capabilities, and proper security controls
C. A computer used only for word processing
D. A server that stores websites

Answer: B

Q435. Why is it important to document every step during a forensic investigation?

A. For billing purposes only
B. To maintain a detailed record that supports the integrity of evidence and can be presented in legal proceedings
C. Documentation is optional in forensics
D. To create a user manual for the software

Answer: B

Q436. What are the common sources of digital evidence in a computer investigation?

A. Only the hard drive
B. Hard drives, RAM, network logs, email, browser history, USB devices, cloud accounts, and mobile devices
C. Only printed documents
D. Only internet browsing history

Answer: B

Q437. What is the difference between logical and physical acquisition in digital forensics?

A. They are the same method
B. Logical acquisition copies files and folders accessible by the OS, while physical acquisition copies the entire storage media bit-by-bit including deleted data
C. Logical acquisition is always better
D. Physical acquisition only copies visible files

Answer: B

Q438. What is an evidence bag used for in digital forensics?

A. To carry personal items
B. An anti-static, tamper-evident container used to store and transport physical digital evidence while maintaining chain of custody
C. A regular plastic bag
D. A bag for storing paper documents

Answer: B

Q439. What is deleted file recovery in digital forensics?

A. Permanently destroying files
B. The process of recovering files that have been deleted by users, as the data may still exist on the storage device until overwritten
C. Downloading files from the internet
D. Creating backup copies of files

Answer: B

Q440. What is the role of an expert witness in digital forensics?

A. To hack into the suspect's computer
B. A qualified professional who presents and explains digital evidence and forensic findings in court in a way that judges and juries can understand
C. To destroy evidence after the trial
D. To represent the defendant

Answer: B

Q441. What is the goal of incident response in cybersecurity?

A. To prevent all incidents from ever occurring
B. To systematically handle security incidents to minimize damage, reduce recovery time, and learn from the experience
C. To blame individuals for security failures
D. To shut down all systems permanently after an attack

Answer: B

Q442. Who should be notified when a security incident is detected?

A. Only the IT department
B. The incident response team, management, and potentially affected parties as defined in the incident response plan
C. No one, to avoid causing panic
D. Only external media

Answer: B

Q443. What is the purpose of an incident response plan?

A. To create work for the IT team
B. To provide a structured, pre-defined approach for handling security incidents so the team can respond quickly and effectively
C. To document past projects
D. To track employee attendance

Answer: B

Q444. What should an employee do if they receive a suspicious email?

A. Forward it to all colleagues to warn them
B. Report it to the IT security team and do not click any links or open attachments
C. Delete it and forget about it
D. Reply to the sender asking if it is legitimate

Answer: B

Q445. What is incident containment?

A. Putting all computers in a sealed room
B. Taking immediate actions to limit the scope and damage of a security incident, such as isolating affected systems from the network
C. Ignoring the incident until it resolves itself
D. Deleting all data from affected systems

Answer: B

Q446. What is the recovery phase of incident response?

A. Recovering the cost of the incident from insurance
B. Restoring affected systems and services to normal operation after the threat has been eliminated
C. Recovering deleted emails
D. Recovering employee passwords

Answer: B

Q447. Why should an organization conduct post-incident reviews?

A. To assign blame to individuals
B. To analyze what happened, identify what worked well and what needs improvement, and update procedures to better handle future incidents
C. Post-incident reviews are a waste of time
D. To create a public news report about the incident

Answer: B

Q448. What is the role of backup systems in incident response?

A. Backups are not related to incident response
B. Backups provide clean copies of data and systems that can be used to restore operations after an incident like ransomware or data corruption
C. Backups only store old, unnecessary data
D. Backups are used only for testing purposes

Answer: B

Q449. What is a security incident log?

A. A wooden log used for physical security
B. A record that documents the details of a security incident including timeline, actions taken, evidence collected, and people involved
C. A log of employee login times
D. A record of software purchases

Answer: B

Q450. What is the difference between a security event and a security incident?

A. They mean exactly the same thing
B. A security event is any observable occurrence in a system; a security incident is an event that actually threatens or breaches security policies
C. An event is more serious than an incident
D. An incident always involves data loss

Answer: B

Q451. What is the purpose of an intrusion detection system (IDS)?

A. To speed up network performance
B. To monitor network traffic or system activity for malicious behavior or policy violations and generate alerts
C. To encrypt all network traffic
D. To manage user passwords

Answer: B

Q452. What is a security baseline in monitoring?

A. The lowest level of security an organization can have
B. A documented standard of normal system behavior and configuration that deviations from can indicate security issues
C. The first security tool purchased
D. A baseline measurement of network speed

Answer: B

Q453. What is the purpose of monitoring failed login attempts?

A. To count how many employees forget their passwords
B. To detect potential brute-force attacks, unauthorized access attempts, or compromised accounts
C. Failed logins do not need to be monitored
D. To measure system performance

Answer: B

Q454. What is a security information and event management (SIEM) alert?

A. A marketing email from a security vendor
B. A notification generated when the SIEM detects activity matching predefined rules or patterns that may indicate a security threat
C. A reminder to update passwords
D. An error message in the SIEM software

Answer: B

Q455. Why is it important to monitor both inbound and outbound network traffic?

A. Only inbound traffic needs monitoring
B. Inbound monitoring detects incoming attacks while outbound monitoring detects data exfiltration, malware communication, and compromised systems beaconing to attacker infrastructure
C. Outbound traffic is always safe
D. Monitoring both directions is too expensive to be worthwhile

Answer: B

Q456. What is a false negative in security monitoring?

A. A false alarm about a security threat
B. A real security threat that the monitoring system fails to detect, allowing the attack to proceed without alerting the security team
C. A negative review of security software
D. A test alert used during security drills

Answer: B

Q457. What is the purpose of monitoring privileged account activity?

A. Privileged accounts do not need monitoring
B. Privileged accounts have elevated access that can cause significant damage if misused; monitoring their activity detects unauthorized use, insider threats, and compromised admin accounts
C. Monitoring privileged accounts violates privacy
D. Only guest accounts need monitoring

Answer: B

Q458. What is real-time monitoring versus periodic monitoring?

A. They are the same approach with different names
B. Real-time monitoring continuously analyzes events as they occur for immediate detection, while periodic monitoring reviews data at scheduled intervals
C. Real-time monitoring is less effective
D. Periodic monitoring catches more threats

Answer: B

Q459. What is the role of antivirus alerts in security monitoring?

A. Antivirus alerts are always false positives
B. Antivirus alerts notify security teams when malware is detected on endpoints, enabling investigation and response to potential infections
C. Antivirus alerts only matter for personal computers
D. Antivirus alerts replace the need for other monitoring

Answer: B

Q460. What is unauthorized access to a computer system?

A. Using your own computer at home
B. Accessing a computer system or network without permission from the owner, which is illegal in most jurisdictions
C. Installing software with admin approval
D. Browsing a public website

Answer: B

Q461. What is the purpose of a terms of service agreement for online services?

A. To make registration more complicated
B. To define the rules, rights, and responsibilities for using an online service, forming a legal agreement between the user and the provider
C. To collect user email addresses
D. To slow down the sign-up process

Answer: B

Q462. What is cyber harassment?

A. Asking someone a question online
B. Using digital communications to threaten, intimidate, or repeatedly harass another person, which is a punishable offense under cyber laws
C. Sending a friend request on social media
D. Posting a restaurant review online

Answer: B

Q463. What is the purpose of a privacy notice on a website?

A. To decorate the website footer
B. To inform users about what personal data is collected, how it is used, stored, and shared, and what rights users have regarding their data
C. To increase website traffic
D. To prevent users from leaving the website

Answer: B

Q464. What is digital copyright?

A. The right to copy any digital content freely
B. Legal protection that gives creators exclusive rights to their original digital works such as software, music, videos, and written content
C. A license to hack into copyrighted systems
D. A type of Creative Commons license only

Answer: B

Q465. Why is it important to obtain consent before collecting personal data?

A. Consent is only a recommendation, not a requirement
B. Data protection laws require organizations to obtain informed consent before collecting and processing personal data to respect individual privacy rights
C. Consent is only needed for government organizations
D. Collecting data without consent is always allowed

Answer: B

Q466. What is an acceptable use policy (AUP)?

A. A marketing document for software products
B. A set of rules that define how an organization's IT resources may be used, covering permitted activities, prohibited behaviors, and consequences for violations
C. A software installation guide
D. A network speed guarantee

Answer: B

Q467. What is the legal consequence of sending spam emails in many jurisdictions?

A. There are no legal consequences for spam
B. Sending unsolicited commercial emails can result in fines and penalties under anti-spam legislation such as CAN-SPAM Act, GDPR, or PECA 2016
C. Spam is only illegal if it contains malware
D. Only governments can send bulk emails

Answer: B

Q468. What does it mean to report a cybercrime?

A. Posting about the crime on social media
B. Formally notifying law enforcement authorities (like FIA in Pakistan) about a cyber crime so they can investigate and take legal action
C. Telling your friends about the incident
D. Writing a blog post about the experience

Answer: B

Q469. What is a smart device in the context of cybersecurity?

A. Any device that uses electricity
B. A device connected to the internet that can collect, send, and receive data, such as smart speakers, thermostats, and cameras
C. A device that is physically large
D. A computer without internet access

Answer: B

Q470. What is the concept of zero trust in simple terms?

A. Trusting no technology at all and using only paper
B. A security model based on the principle of 'never trust, always verify' where every access request is authenticated and authorized regardless of location
C. Trusting all internal users but not external ones
D. A model where security is not needed

Answer: B

Q471. What is a supply chain attack in cybersecurity?

A. An attack on physical delivery trucks
B. An attack that targets a less-secure element in the supply chain (like a software vendor or service provider) to gain access to a larger target organization
C. An attack that only affects manufacturers
D. Stealing products from a warehouse

Answer: B

Q472. What is automation in cybersecurity?

A. Replacing all security staff with robots
B. Using technology to automatically perform security tasks like scanning for vulnerabilities, responding to alerts, and updating security rules without manual intervention
C. Making all passwords automatic
D. Automating the creation of cyber attacks

Answer: B

Q473. What is a digital twin in technology?

A. A twin sibling who works in technology
B. A virtual replica of a physical system, process, or device that can be used for simulation, testing, and monitoring
C. A backup copy of a digital file
D. A second computer monitor

Answer: B

Q474. What is the role of machine learning in detecting cyber threats?

A. Machine learning creates cyber threats
B. Machine learning can analyze large volumes of data to identify patterns and anomalies that may indicate cyber threats, helping detect attacks that traditional rule-based systems might miss
C. Machine learning replaces all cybersecurity professionals
D. Machine learning only works for email filtering

Answer: B

Q475. What is the dark web?

A. The internet when your screen brightness is low
B. A part of the internet that requires special software (like Tor) to access and is not indexed by standard search engines, often associated with illegal activities
C. Any website with a dark color scheme
D. A private corporate network

Answer: B

Q476. What is multi-cloud strategy?

A. Using many computers in one office
B. Using services from multiple cloud providers to avoid vendor lock-in, improve resilience, and leverage different providers' strengths
C. Running the same application multiple times
D. Having multiple internet connections

Answer: B

Q477. What is an intrusion prevention system (IPS) capable of doing beyond detection?

A. Only generating reports
B. Automatically blocking or preventing detected malicious traffic in real-time before it reaches the target
C. Encrypting all network traffic
D. Managing user accounts

Answer: B

Q478. What is online fraud in the context of cyber law?

A. Selling products online at a discount
B. Using deceptive practices on the internet to illegally obtain money, data, or other benefits from victims
C. Creating a website for a legitimate business
D. Posting product reviews online

Answer: B

Q479. What is wearable technology and what security concerns does it raise?

A. Clothing made from special fabrics
B. Internet-connected devices worn on the body like smartwatches and fitness trackers that collect personal health and location data, raising privacy and data security concerns
C. Any technology that is portable
D. Protective equipment for construction workers

Answer: B

Q480. What is the significance of 5G technology for cybersecurity?

A. 5G only improves download speeds with no security impact
B. 5G introduces new attack surfaces due to network slicing, massive IoT connectivity, and edge computing, but also provides improved security features over 4G
C. 5G eliminates all cybersecurity concerns
D. 5G technology is identical to WiFi

Answer: B

Medium Questions

480 questions

Q481. Which of the following best describes 'defense in depth'?

A. Using only encryption as the single security method
B. Layering multiple security controls throughout a system
C. Depending solely on firewalls for perimeter protection
D. Relying on only one strong security control measure

Answer: B

Q482. What is the difference between a threat and a risk in cyber security?

A. A risk is a type of malware designed for compromising system integrity
B. They are the same thing with no meaningful distinction between them
C. A threat only applies to hardware targeting enterprise network infrastructure
D. A threat is a potential danger while risk is the likelihood and impact of that threat

Answer: D

Q483. Which of the following is an example of a physical security control?

A. Intrusion detection system
B. Data-at-rest symmetric encryption
C. Biometric access to server room
D. Network firewall rule configuration

Answer: C

Q484. What is the purpose of a security policy in an organization?

A. To define rules and guidelines for protecting information assets
B. To minimize infrastructure and hardware expenditures
C. To expand network bandwidth allocation and throughput
D. To design and build user-facing application interfaces

Answer: A

Q485. Which cyber security principle states that users should only have the minimum access necessary?

A. Principle of least privilege
B. Defense in depth
C. Security by obscurity
D. Separation of duties

Answer: A

Q486. What is social engineering in cyber security?

A. Manipulating people into revealing confidential information
B. Engineering software for social platforms
C. Building social media applications
D. Designing social networks within enterprise security environments

Answer: A

Q487. Which of the following is a component of the NIST Cybersecurity Framework?

A. Identify, Protect, Detect, Respond, Recover
B. Design, Build, Test, Deploy lifecycle
C. Input, Process, Output data flow model
D. Plan, Do, Check, Act continuous cycle

Answer: A

Q488. What is the purpose of a risk assessment in cyber security?

A. To design new websites for enterprise computing environments
B. To identify, analyze, and evaluate security risks
C. To install antivirus software and management
D. To write application code and management

Answer: B

Q489. What does 'non-repudiation' mean in information security?

A. Ensuring a party cannot deny having performed an action
B. Denying access to all users regardless of the specific situation or context
C. Blocking network traffic within enterprise security environments
D. Encrypting all messages regardless of the specific situation or context

Answer: A

Q490. Which of the following best describes an 'attack surface'?

A. The total sum of vulnerabilities accessible to an attacker
B. A strain of self-replicating malicious software programs
C. A security certification for mobile network professionals
D. The physical area of a computer across computing environments

Answer: A

Q491. What is the difference between symmetric and asymmetric encryption?

A. Symmetric uses two keys, asymmetric uses one across computing environments
B. There is no difference in any deployment scenario or context
C. Symmetric is always stronger regardless of the specific situation or context
D. Symmetric uses one key for both encryption and decryption, asymmetric uses a key pair

Answer: D

Q492. What is a hash function used for in security?

A. Applying symmetric ciphers for secure data transfer
B. Generating a fixed-size output from input data for integrity verification
C. Generating redundant backup copies of system data
D. Compressing files to reduce disk storage consumption

Answer: B

Q493. Which is an example of a detective security control?

A. Intrusion Detection System (IDS)
B. Firewall within enterprise security environments
C. Data-at-rest symmetric encryption
D. Access control list in security contexts

Answer: A

Q494. What is the purpose of an access control list (ACL)?

A. To define which users or systems are granted access to specific resources
B. To encrypt data using symmetric cipher algorithms
C. To compress files for reducing disk storage consumption
D. To generate comprehensive network topology diagrams

Answer: A

Q495. What is the difference between identification and authentication?

A. Neither is used in security within enterprise security environments
B. They are fundamentally the same thing in security
C. Identification claims an identity, authentication proves it
D. Authentication comes before identification

Answer: C

Q496. What is a security token in authentication?

A. A backup device for managing enterprise data resources
B. A physical or digital device that generates one-time passwords for authentication
C. A network firewall rule for filtering inbound traffic
D. A software application used for enterprise computing operations

Answer: B

Q497. What is the purpose of security auditing?

A. To deploy and install application software across enterprise computing systems
B. To architect and design new information systems and management
C. To increase available bandwidth for improved download speeds
D. To systematically evaluate the security of a system by testing against established criteria

Answer: D

Q498. Which security principle involves dividing critical tasks among multiple people?

A. Need to know
B. Least privilege
C. Defense in depth
D. Separation of duties

Answer: D

Q499. What is a security baseline?

A. A next-generation firewall security appliance
B. A backup schedule for creating regular recovery snapshots
C. The fastest network speed within enterprise security environments
D. A minimum set of security controls required for a system

Answer: D

Q500. What type of attack targets the availability component of the CIA triad?

A. Network eavesdropping attack
B. Denial of Service (DoS)
C. Spear phishing email attack
D. Credential data theft attack

Answer: B

Q501. What is the key size of AES-256?

A. 256 bits
B. 192 bits
C. 512 bits
D. 128 bits

Answer: A

Q502. What is a block cipher?

A. A cipher that encrypts one bit at a time
B. A cryptographic algorithm used for protecting sensitive data
C. A cipher that encrypts fixed-size blocks of data at a time
D. A cipher that uses no key applied to data protection workflows

Answer: C

Q503. What is a stream cipher?

A. A cipher that encrypts entire files at once
B. A cipher that encrypts data one bit or byte at a time
C. A cipher that uses block processing
D. A cipher that only works with video

Answer: B

Q504. What is the Diffie-Hellman key exchange used for?

A. Hashing passwords within enterprise security environments
B. Compressing data files for reduced storage space consumption
C. Encrypting data directly within enterprise security environments
D. Securely exchanging cryptographic keys over an insecure channel

Answer: D

Q505. Which hash algorithm produces a 256-bit output?

A. SHA-256
B. SHA-512
C. MD5
D. SHA-1

Answer: A

Q506. What is a digital certificate?

A. A cryptographic algorithm used for protecting sensitive data
B. An electronic document that uses a digital signature to bind a public key with an identity
C. A software application used for enterprise computing operations
D. A physical security measure for protecting building infrastructure

Answer: B

Q507. What is the role of a Certificate Authority (CA)?

A. To design websites for enterprise computing environments
B. To develop software across enterprise computing systems
C. To design and distribute malicious software programs
D. To issue, manage, and revoke digital certificates

Answer: D

Q508. Why is MD5 considered insecure for cryptographic purposes?

A. It requires too much memory within enterprise security environments
B. It is too slow within enterprise security environments
C. It is vulnerable to collision attacks where two different inputs produce the same hash
D. It produces too long an output within enterprise security environments

Answer: C

Q509. What is the purpose of a nonce in cryptography?

A. A number used only once to prevent replay attacks
B. To compress files for reducing disk storage consumption
C. To create automated backup copies of user data
D. To encrypt data using symmetric cipher algorithms

Answer: A

Q510. What is PKI (Public Key Infrastructure)?

A. A next-generation firewall for filtering network traffic flows
B. A framework for managing digital certificates and public-key encryption
C. A category of self-replicating malicious software
D. A standard network communication protocol for data transfer

Answer: B

Q511. What is the difference between an IDS and an IPS?

A. IDS only detects and alerts while IPS can also block malicious traffic
B. They are the same thing with no meaningful distinction between them
C. IPS is slower than IDS within enterprise security environments
D. IDS blocks traffic while IPS only detects

Answer: A

Q512. What is network segmentation?

A. Deleting network components within enterprise security environments
B. A type of network attack used in enterprise network infrastructure
C. Dividing a network into smaller segments to improve security and performance
D. Combining all networks into one regardless of the specific situation or context

Answer: C

Q513. What is ARP spoofing?

A. An attack where fake ARP messages link an attacker's MAC address with a legitimate IP
B. A symmetric key data encryption algorithm applied to data protection workflows
C. A firewall configuration deployed across enterprise environments
D. A legitimate network technique used in enterprise network infrastructure

Answer: A

Q514. What is the purpose of network access control (NAC)?

A. To speed up the network across the enterprise network infrastructure
B. To restrict access to a network based on device compliance and user identity
C. To install network cables across the enterprise network infrastructure
D. To generate comprehensive network topology diagrams

Answer: B

Q515. What is a honeypot in network security?

A. A decoy system designed to attract attackers and study their methods
B. A network switch used in enterprise network infrastructure
C. A strain of self-replicating malicious software programs
D. A type of firewall for filtering wireless network traffic

Answer: A

Q516. What is SSL/TLS used for?

A. Optimal network routing and efficient packet forwarding across systems
B. Persistent data storage and streamlined data retrieval management
C. Providing encrypted communication between a client and server over a network
D. Lossless data file compression techniques for long-term storage optimization

Answer: C

Q517. What is a VLAN and how does it improve security?

A. A Virtual LAN that logically segments a network, isolating traffic between groups
B. A virtual private network encrypted tunnel connection
C. A next-generation firewall for filtering network traffic flows
D. A software application used for enterprise computing operations

Answer: A

Q518. What is port scanning?

A. Sending packets to specific ports to discover which services are running
B. A cryptographic algorithm used for protecting sensitive data
C. A physical inspection of ports within modern computing environments
D. A backup method for managing enterprise data resources

Answer: A

Q519. What is a stateful firewall?

A. A firewall without rules deployed across enterprise environments
B. A firewall that tracks the state of active connections and makes decisions based on context
C. A software-only firewall deployed across enterprise environments
D. A firewall that only checks packet headers deployed across enterprise environments

Answer: B

Q520. What is DNS security and why is it important?

A. Continuous monitoring is not important for security for modern enterprise security environments
B. It is only about encrypting DNS without any additional considerations needed
C. Protecting DNS infrastructure from attacks like DNS spoofing to ensure correct domain name resolution
D. DNS security only affects speed without any additional considerations needed

Answer: C

Q521. What is mandatory access control (MAC) in operating systems?

A. The OS enforces access rules based on security labels that users cannot override
B. Users set their own permissions within enterprise security environments
C. All users have equal access with no meaningful distinction between them
D. No access control is needed in any deployment scenario or context

Answer: A

Q522. What is Address Space Layout Randomization (ASLR)?

A. A standard network communication protocol for data transmission
B. A file management technique for organizing directories used in enterprise computing environments
C. A symmetric key data encryption algorithm applied to data protection workflows
D. A security technique that randomly arranges memory address space of processes to prevent exploitation

Answer: D

Q523. What is the purpose of SELinux?

A. To provide mandatory access control security policies in Linux
B. To install and manage software packages efficiently
C. To optimize and speed up the Linux kernel performance
D. To create and manage virtual machine environments

Answer: A

Q524. What is a chroot jail in Linux security?

A. An operation that changes the root directory for a process, isolating it from the rest of the file system
B. A physical jail or correctional facility structure within modern computing environments
C. A network configuration for firewall rule settings deployed across enterprise environments
D. A specific type of user account with limited access within the identity management system

Answer: A

Q525. What is the purpose of Windows Group Policy?

A. To centrally manage and configure OS settings, user permissions, and security policies
B. To create social media groups for enterprise communication
C. To logically group related files within directories and management
D. To organize and arrange desktop icons into folders and management

Answer: A

Q526. What is Data Execution Prevention (DEP)?

A. An automated feature for scheduling data backups for managing enterprise data resources
B. A security feature that marks memory regions as non-executable to prevent code execution from those areas
C. A built-in file encryption tool for data protection applied to data protection workflows
D. A network traffic monitoring feature for analysis used in enterprise network infrastructure

Answer: B

Q527. What is the Windows Registry and why is it important for security?

A. An automated backup solution for enterprise data recovery needs
B. A user account type with specifically assigned access permissions
C. A hierarchical database storing OS and application settings that if compromised can affect system security
D. A next-generation firewall security appliance deployed across enterprise environments

Answer: C

Q528. What is process isolation in operating systems?

A. Keeping each process's memory space separate to prevent unauthorized access between processes
B. A specific type of preemptive multitasking method used in enterprise computing environments
C. Running all system processes in shared memory space across computing environments
D. Immediately stopping and terminating all processes across computing environments

Answer: A

Q529. What is the purpose of audit logging in an OS?

A. To record security-relevant events for monitoring, investigation, and compliance
B. To identify and remove obsolete system files and management
C. To add computational overhead slowing the system and management
D. To reduce data sizes through compression methods and management

Answer: A

Q530. What is sandboxing in OS security?

A. Playing in a physical sandbox recreation area across computing environments
B. A type of data encryption applied to data protection workflows
C. Running applications in an isolated environment to limit their access to system resources
D. A next-generation firewall for filtering network traffic flows

Answer: C

Q531. What is Cross-Site Scripting (XSS)?

A. A responsive web design technique used for structuring and organizing page layouts
B. A front-end JavaScript framework commonly used for building interactive web applications
C. A vulnerability where malicious scripts are injected into trusted websites and executed in browsers
D. A written record or logbook used by teams for tracking daily operational activities

Answer: C

Q532. What is SQL injection?

A. An attack that inserts malicious SQL code through user input to manipulate the database
B. A database management system for storing structured records
C. A software application used for enterprise computing operations
D. An optimization technique for improving SQL query speed used in enterprise computing environments

Answer: A

Q533. What is Cross-Site Request Forgery (CSRF)?

A. An attack that tricks a browser into making unintended requests to a site where the user is authenticated
B. A form validation technique for checking user inputs within the identity management system
C. A standard type of user login authentication system within the identity management system
D. A type of HTTP cookie used for session tracking within modern computing environments

Answer: A

Q534. What is the Same-Origin Policy?

A. A web browser application for accessing internet-hosted content
B. A security mechanism restricting scripts from one origin from accessing resources of another origin
C. An intellectual property copyright protection law within modern computing environments
D. A common website design pattern for page layout within modern computing environments

Answer: B

Q535. What is Content Security Policy (CSP)?

A. An HTTP header specifying which content sources are allowed to be loaded by a web page
B. A cascading style sheets framework for responsive page layouts
C. A front-end JavaScript library for dynamic web development
D. A content management system for organizing digital resources

Answer: A

Q536. What is the purpose of HTTP security headers?

A. To format and style web content for visual presentation and management
B. To compress and optimize images for web page loading and management
C. To instruct browsers to enable security features protecting against common web attacks
D. To make websites load faster with better performance and management

Answer: C

Q537. What is session hijacking?

A. Properly logging out of an active user session across computing environments
B. Creating a new user session for web interaction across computing environments
C. An attack where an attacker takes over a valid user session by stealing the session ID
D. An automated session timeout after inactivity period used in enterprise computing environments

Answer: C

Q538. What is the OWASP Top 10?

A. A ranked list of the most widely used web browsers
B. A programming framework for building web app front-ends
C. A curated list of the top ten most popular websites
D. A regularly updated list of the most critical web application security risks

Answer: D

Q539. What is clickjacking?

A. A software application used for enterprise computing operations
B. A gaming technique for improving response speed used in enterprise computing environments
C. An attack tricking users into clicking hidden elements by layering invisible frames
D. A user account type with specifically assigned access permissions

Answer: C

Q540. What is the purpose of parameterized queries?

A. To separate SQL code from user data, ensuring input is treated as data not code
B. To compress and reduce the size of database stored data
C. To improve and optimize query execution performance speed
D. To format and style the output of database query results

Answer: A

Q541. What is a keylogger?

A. A tool for managing and organizing cryptographic keys
B. Software or hardware that records keystrokes to capture sensitive information
C. A software application used for enterprise computing operations
D. A cryptographic algorithm used for protecting sensitive data

Answer: B

Q542. What is a botnet?

A. A helpful automated robot network for task assistance used in enterprise computing environments
B. A chat bot service providing automated customer support used in enterprise computing environments
C. A network monitoring tool for tracking bandwidth utilization
D. A network of compromised computers controlled remotely for coordinated malicious activities

Answer: D

Q543. How does a DDoS attack differ from DoS?

A. DDoS attacks are generally considered less dangerous than standard single-source DoS attacks
B. DDoS uses multiple compromised systems to flood the target, making it harder to mitigate
C. They are functionally identical attack frameworks with no meaningful differences between them
D. DoS attacks typically use significantly more compromised systems than DDoS attacks

Answer: B

Q544. What is a rootkit?

A. A disk utility for managing storage partitions used in enterprise computing environments
B. Malware designed to gain unauthorized root-level access and hide its presence
C. A legitimate system administration tool for configuration
D. A standard operating system boot loader for initialization

Answer: B

Q545. What is social engineering?

A. A software application suite used for enterprise computing operations and communications
B. Building and developing social media networking platforms for public user interaction
C. Psychological manipulation to trick people into making security mistakes or revealing information
D. Engineering and designing interactive social interaction systems for enterprise organizations

Answer: C

Q546. What is a drive-by download attack?

A. A software application used for enterprise computing operations
B. A standard file transfer method between connected systems used in enterprise computing environments
C. Downloading files while driving in a moving vehicle
D. Automatic download of malware when visiting a compromised website without user interaction

Answer: D

Q547. What is a watering hole attack?

A. A water cooling attack damaging hardware cooling systems
B. Attacking municipal water supply infrastructure systems
C. Compromising websites frequently visited by a targeted group to infect their computers
D. A network flooding attack using volumetric traffic used in enterprise computing environments

Answer: C

Q548. What is fileless malware?

A. A clean program verified by security code audit analysis
B. Malware that operates without any source code at all
C. Malware that operates entirely in memory without writing files to disk
D. A type of antivirus program for real-time scanning

Answer: C

Q549. What is a man-in-the-middle (MITM) attack?

A. A professional mediator in business negotiations within modern computing environments
B. A software application used for enterprise computing operations
C. An attack where the attacker secretly intercepts and possibly alters communication between two parties
D. A proxy server that forwards requests between systems used in enterprise computing environments

Answer: C

Q550. What are indicators of compromise (IOCs)?

A. Performance metrics for measuring system throughput
B. Signs indicating system improvement and optimization
C. Software licensing keys for verifying installations
D. Observable artifacts or evidence suggesting a system has been breached

Answer: D

Q551. What is the difference between authentication and authorization?

A. Neither process is used in modern security frameworks
B. Authentication verifies identity, authorization determines permissions
C. Authorization always comes before the authentication phase
D. They are functionally identical frameworks with no differences

Answer: B

Q552. What is LDAP used for in access control?

A. A file format used for structured data storage for managing enterprise data resources
B. A high-level language used for development within modern computing environments
C. A software application used for enterprise computing operations
D. A protocol for accessing distributed directory information services for centralized authentication

Answer: D

Q553. What is attribute-based access control (ABAC)?

A. Access control decisions based solely on user age and demographics
B. Access control evaluating attributes of users, resources, actions, and environment
C. Randomized access control without any defined criteria or policies
D. Access control based on file system attributes exclusively without context

Answer: B

Q554. What is a federated identity?

A. A physical security measure for protecting building infrastructure
B. A fake identity created for fraudulent purposes used in enterprise computing environments
C. A temporary identity assigned for a single session used in enterprise computing environments
D. A system allowing users to use the same identity credentials across multiple organizations

Answer: D

Q555. What is the purpose of a RADIUS server?

A. To provide centralized authentication, authorization, and accounting for network access
B. To measure and calculate distances between network nodes and management
C. To increase and optimize overall network throughput speed
D. To create and deploy enterprise wireless network infrastructure

Answer: A

Q556. What is privilege escalation?

A. Installing new software applications on the system
B. Gaining elevated access rights beyond what was initially authorized
C. Receiving a job promotion or advancement opportunity
D. Creating a new user account with default permissions

Answer: B

Q557. What is the purpose of access control matrices?

A. To define access rights of subjects to objects in a structured format
B. To encrypt data using symmetric cipher algorithms
C. To compress files for reducing disk storage consumption
D. To create and format data management spreadsheets

Answer: A

Q558. What is SAML (Security Assertion Markup Language)?

A. A high-level language used for development within modern computing environments
B. A software application used for enterprise computing operations
C. An XML-based standard for exchanging authentication and authorization data between providers
D. A database management system for storing structured records

Answer: C

Q559. What is the purpose of session management in authentication?

A. To schedule tasks within enterprise computing infrastructure
B. To securely maintain a user's authenticated state throughout their interaction
C. To manage network sessions across the enterprise network infrastructure
D. To manage computer memory within enterprise computing infrastructure

Answer: B

Q560. What is adaptive authentication?

A. A biometric method within enterprise computing environments
B. An approach adjusting security requirements based on risk factors like location and behavior
C. A credential management mechanism for user authentication flows
D. Fixed authentication rules within enterprise security environments

Answer: B

Q561. What is the OWASP Secure Coding Practices guide?

A. A high-level language used for development within modern computing environments
B. A database design guide for managing enterprise data resources
C. A comprehensive checklist of secure coding practices organized by vulnerability category
D. A software application used for enterprise computing operations

Answer: C

Q562. What is threat modeling in software development?

A. Testing application performance under heavy load conditions
B. Creating threat actors for penetration testing exercises
C. Running antivirus scans on development machine environments
D. A structured approach to identifying and addressing security threats during design

Answer: D

Q563. What is static application security testing (SAST)?

A. Testing network performance under heavy traffic loads
B. Testing user interfaces for usability and accessibility
C. Analyzing source code without executing it to find security vulnerabilities
D. Testing the application while it is actively running

Answer: C

Q564. What is dynamic application security testing (DAST)?

A. Testing database query performance under heavy loads
B. Testing a running application by simulating attacks to find vulnerabilities
C. Testing source code without running it across computing environments
D. Testing code compilation for syntax errors and warnings

Answer: B

Q565. What is the principle of fail-safe defaults?

A. Logging all defaults regardless of the specific situation or context
B. Ignoring security failures within enterprise security environments
C. Always granting access by default in security contexts
D. Denying access by default and requiring explicit permission grants

Answer: D

Q566. What is dependency management in secure development?

A. Managing and coordinating team members across projects
B. Tracking, updating, and securing third-party libraries and components
C. Managing and configuring enterprise server infrastructure
D. Managing database servers and optimizing query performance

Answer: B

Q567. What is the purpose of security testing in the SDLC?

A. To deliberately delay the project delivery timeline
B. To create comprehensive technical documentation materials
C. To identify and fix security vulnerabilities before deployment to production
D. To test and validate hardware components for compatibility

Answer: C

Q568. What is 'shift left' in security?

A. Integrating security practices earlier in the development lifecycle
B. Moving project deadlines earlier in the release timeline
C. Moving physical servers to the left of the data center
D. Changing code alignment and formatting in source files

Answer: A

Q569. What is secure session management?

A. Properly creating, maintaining, and destroying sessions to prevent hijacking and fixation
B. Sharing sessions between multiple users simultaneously
C. Deleting all cookies immediately after each page request
D. Never creating sessions for any user interactions at all regardless of the deployment context or scenario

Answer: A

Q570. What is the purpose of output encoding?

A. Making output look visually pretty and well-formatted
B. Compressing output data for reduced bandwidth consumption
C. Encrypting output using symmetric cipher key algorithms
D. Converting output to a safe format to prevent injection attacks like XSS

Answer: D

Q571. What is WPA3?

A. A web application framework for building online services
B. A mobile application for managing device Wi-Fi settings
C. The latest Wi-Fi security protocol with stronger encryption and forward secrecy
D. A Bluetooth version for short-range wireless communication

Answer: C

Q572. What is an evil twin attack?

A. A physical hardware component used in computing infrastructure
B. A mirrored display for screen sharing purposes used in enterprise computing environments
C. A twin SIM card used for dual number support used in enterprise computing environments
D. A rogue access point mimicking a legitimate Wi-Fi network to intercept traffic

Answer: D

Q573. What is Mobile Device Management (MDM)?

A. A physical hardware component used within enterprise computing infrastructure systems
B. A standard software application used for routine enterprise computing operations
C. A mobile device application designed for portable computing operations and tasks
D. Software allowing organizations to remotely manage, secure, and enforce policies on mobile devices

Answer: D

Q574. What are the risks of jailbreaking or rooting a mobile device?

A. It improves battery life and extends usage time
B. It removes built-in security protections and exposes the device to malware
C. It makes the phone processor run significantly faster
D. There are no security risks at all from this practice

Answer: B

Q575. What is a rogue access point?

A. An officially authorized network infrastructure device
B. A Bluetooth device used for short-range data exchange
C. An unauthorized wireless access point installed without administrator knowledge
D. A mobile device application for portable computing operations

Answer: C

Q576. What is WEP and why is it insecure?

A. An outdated wireless encryption protocol with known vulnerabilities crackable in minutes
B. A physical hardware component used in computing infrastructure
C. A cryptographic algorithm used for protecting sensitive data
D. A next-generation firewall for filtering network traffic flows

Answer: A

Q577. What is app sandboxing on mobile devices?

A. Playing games in a sandbox within enterprise security environments
B. A testing method for validating application functionality
C. Isolating each app in its own environment to prevent unauthorized data access
D. A game development technique for creating mobile games

Answer: C

Q578. What is SIM swapping?

A. Upgrading SIM cards to a newer generation of mobile network technology standard
B. Sharing SIM cards between multiple mobile phone devices for network access
C. An attack convincing a carrier to transfer a victim's number to a new SIM for account takeover
D. Changing phone cases for a different physical appearance and improved protection

Answer: C

Q579. What is the purpose of a VPN on a mobile device?

A. To encrypt internet traffic when using public or untrusted networks
B. To make phone calls cheaper through VoIP routing
C. To speed up mobile data transfer download bandwidth
D. To improve camera quality and photo capture resolution

Answer: A

Q580. What is BYOD and its security implications?

A. A software application used for enterprise computing operations
B. A policy allowing personal devices for work, creating data separation and security challenges
C. A physical hardware component used in computing infrastructure
D. A music streaming service platform for audio content used in enterprise computing environments

Answer: B

Q581. What is the difference between IaaS, PaaS, and SaaS security responsibilities?

A. Customer always manages everything in every cloud model
B. Security is not needed in any cloud computing environment for modern enterprise security environments
C. In IaaS customer manages most; in PaaS provider manages more; in SaaS provider manages most
D. Provider manages everything in all cloud service models

Answer: C

Q582. What is cloud workload protection?

A. A backup solution for creating redundant data recovery copies
B. A load balancing technique for distributing network traffic used in enterprise computing environments
C. Security solutions protecting workloads including VMs, containers, and serverless functions
D. Physical security of data center server hardware infrastructure

Answer: C

Q583. What is DLP in cloud environments?

A. Encrypting all data using symmetric cipher algorithm keys
B. Compressing data files for reduced storage space consumption
C. Creating redundant copies of data for backup recovery
D. Technologies preventing sensitive data from being inappropriately shared or exposed

Answer: D

Q584. What is cloud security posture management (CSPM)?

A. A standard software application used for routine enterprise computing operations
B. A cloud infrastructure provider offering a range of core computing service options
C. An automated solution monitoring cloud infrastructure for misconfigurations and compliance violations
D. A cloud storage manager designed for organizing and managing hosted data resources

Answer: C

Q585. What is server-side encryption in cloud storage?

A. The cloud provider encrypts data at rest on the server before storing it
B. Encrypting data on the client device before transmission
C. A next-generation firewall for filtering network traffic flows
D. A compression method for reducing cloud storage data sizes

Answer: A

Q586. What is the purpose of cloud audit logging?

A. To record all activities and API calls for security monitoring and compliance
B. To manage and administer user accounts and access rights
C. To add computational overhead slowing the system and management
D. To increase storage usage for expanded data capacity

Answer: A

Q587. What is a virtual private cloud (VPC)?

A. A logically isolated section of public cloud where resources launch in a customer-defined virtual network
B. A physical hardware component used in computing infrastructure
C. A virtual private network encrypted tunnel connection used in enterprise computing environments
D. A physical security measure for protecting building infrastructure

Answer: A

Q588. What is container security in cloud environments?

A. An automated backup solution designed for enterprise data recovery needs and processes
B. Protecting containerized apps through image scanning, runtime protection, and secure orchestration
C. Securing physical shipping containers during transportation across global supply chains
D. A physical security measure designed for protecting building infrastructure and premises

Answer: B

Q589. What are cloud security groups?

A. User groups for managing organizational access permissions
B. Social media groups for enterprise team communication
C. A type of cloud storage for archiving large data volumes
D. Virtual firewalls controlling inbound and outbound traffic to cloud resources

Answer: D

Q590. What is least privilege in cloud IAM?

A. Using shared credentials for all users in the environment
B. Granting only the minimum permissions necessary for specific tasks
C. Completely blocking all access to cloud resources
D. Giving everyone administrator access to all resources

Answer: B

Q591. What is volatile evidence in digital forensics?

A. Evidence that is explosive within enterprise security environments
B. Evidence that never changes in any deployment scenario or context
C. Physical evidence within enterprise security environments
D. Data in temporary storage like RAM that is lost when the system is powered off

Answer: D

Q592. What is the order of volatility in evidence collection?

A. Collect backup data first within enterprise security environments
B. The order does not matter in any deployment scenario or context
C. Collect most volatile data first: registers, cache, RAM, disk, then remote logs
D. Collect hard drive data first within enterprise security environments

Answer: C

Q593. What is steganography analysis in digital forensics?

A. Detecting and extracting hidden data concealed within files like images or audio
B. Network analysis within enterprise security environments
C. Analyzing dinosaur fossils within enterprise security environments
D. Photo editing within enterprise security environments

Answer: A

Q594. What is network forensics?

A. Designing networks within enterprise security environments
B. Capture, recording, and analysis of network traffic to investigate security incidents
C. Installing network cables within enterprise security environments
D. Configuring routers within enterprise security environments

Answer: B

Q595. What is a forensic toolkit?

A. A physical toolbox used in enterprise computing environments
B. A development environment within modern computing environments
C. A collection of software tools for digital evidence collection, analysis, and reporting
D. A repair kit within enterprise computing environments

Answer: C

Q596. What is timeline analysis in digital forensics?

A. A project management technique within modern computing environments
B. Creating project schedules within enterprise security environments
C. Reconstructing a chronological sequence of events using timestamps from multiple sources
D. A time management tool used in enterprise computing environments

Answer: C

Q597. What is email forensics?

A. Writing and composing emails within enterprise security environments for communication
B. Examining email headers, content, attachments, and metadata to trace origin and authenticity
C. Reading and reviewing emails within enterprise security environments for monitoring
D. Deleting and archiving emails within enterprise security environments for compliance

Answer: B

Q598. What is the role of a forensic examiner's report?

A. A detailed document presenting methodology, findings, and conclusions for legal proceedings
B. A blog post published online for broad public readership review and engagement
C. A news article published within enterprise computing environments for staff awareness
D. A personal diary used for recording daily reflections and activities for reference

Answer: A

Q599. What is memory forensics?

A. Testing memory speed and latency within enterprise security environments for capacity
B. Analysis of RAM contents to find evidence of malware, connections, and encryption keys
C. A memory stress test within enterprise computing environments to evaluate stability
D. Adding more RAM modules within enterprise security environments for performance

Answer: B

Q600. What is anti-forensics?

A. A type of forensic analysis technique within enterprise computing environments
B. A standard software application used for enterprise computing operations and tasks
C. Techniques used to prevent or obstruct forensic investigation, such as data wiping and timestamp manipulation
D. Good forensic practices applied within enterprise security environments for compliance

Answer: C

Q601. What are the six phases of the NIST incident response lifecycle?

A. Design, Develop, Test, Release, Maintain, Retire across computing environments
B. Preparation, Detection and Analysis, Containment, Eradication, Recovery, Post-Incident Activity
C. None of these in any deployment scenario or context across computing environments
D. Plan, Build, Test, Deploy, Monitor, Retire within enterprise security environments

Answer: B

Q602. What is triage in incident response?

A. A network tool used in enterprise network infrastructure
B. Prioritizing incidents based on severity, impact, and urgency to allocate resources
C. A strain of self-replicating malicious software programs
D. Medical treatment within enterprise security environments

Answer: B

Q603. What is the eradication phase?

A. Deleting the incident report within enterprise security environments
B. Removing the root cause including malware, compromised accounts, and exploited vulnerabilities
C. Erasing all data regardless of the specific situation or context
D. Shutting down all systems regardless of the specific situation or context

Answer: B

Q604. What is the recovery phase?

A. Restoring affected systems to normal operation and monitoring for recurrence
B. Recovering deleted emails within enterprise security environments
C. A data backup process for managing enterprise data resources
D. Finding lost items within enterprise security environments

Answer: A

Q605. What is a lessons learned review?

A. A post-incident analysis of what happened, what worked, what failed, and how to improve
B. A security audit deployed across enterprise environments used in enterprise computing environments
C. A training course within enterprise computing environments
D. A school exam within enterprise computing environments

Answer: A

Q606. What is the role of a CISO during a major incident?

A. To write code within enterprise computing infrastructure and management
B. To provide strategic leadership, coordinate response, and make critical containment decisions
C. To fix computers within enterprise computing infrastructure and management
D. To design websites for enterprise computing environments and management

Answer: B

Q607. What is a playbook in incident response?

A. A game manual within modern computing environments
B. A software manual used in enterprise computing environments
C. A children's book within modern computing environments
D. Predefined procedures for responding to specific types of security incidents

Answer: D

Q608. What is the purpose of incident classification?

A. To categorize incidents by type and severity for appropriate response and resource allocation
B. To file paperwork within the data management framework and management
C. To rank team members within enterprise computing infrastructure and management
D. To organize files within the data management framework and management

Answer: A

Q609. What is threat hunting?

A. A recreational entertainment application for consumer devices
B. Hunting animals within enterprise security environments
C. Proactively searching through networks to detect threats that evaded existing controls
D. Installing antivirus software on the development machine

Answer: C

Q610. What is the importance of communication during incident response?

A. Communication should wait until after resolution
B. Clear, timely communication with stakeholders is essential for effective coordination
C. Only technical communication matters without any additional considerations needed
D. Communication is not needed in any deployment scenario or context

Answer: B

Q611. What is a SIEM system?

A. A physical hardware component used in computing infrastructure
B. Security Information and Event Management: aggregates, correlates, and analyzes security data
C. A next-generation firewall security appliance deployed across enterprise environments
D. A physical cable used for network connections used in enterprise network infrastructure

Answer: B

Q612. What is the difference between signature-based and anomaly-based detection?

A. Anomaly-based detection only works effectively in offline analysis and forensic modes
B. Signature-based detection is always considered better than anomaly-based detection methods
C. They are functionally identical detection frameworks with no meaningful differences at all
D. Signature-based matches known patterns; anomaly-based detects deviations from normal behavior

Answer: D

Q613. What is a Security Operations Center (SOC)?

A. A software company that develops security products deployed across enterprise environments
B. A physical hardware component used in computing infrastructure
C. A centralized facility where a team continuously monitors, detects, and responds to security incidents
D. A cloud computing platform for hosting enterprise workloads

Answer: C

Q614. What is log correlation?

A. Deleting old logs to free up storage space on servers
B. Sorting logs alphabetically for easier navigation across computing environments
C. Comparing log file sizes for storage capacity planning
D. Analyzing and connecting related events across multiple sources to identify threat patterns

Answer: D

Q615. What is UEBA?

A. Security analytics using machine learning to establish baselines and detect anomalous user behavior
B. A social media management tool used for content scheduling tasks and engagement tracking
C. A user interface design tool used for creating web application page layouts and mockups
D. An email analytics tool used for tracking message delivery metrics and campaign performance

Answer: A

Q616. What is the purpose of vulnerability scanning?

A. To automatically identify known security weaknesses in systems and configurations
B. To compress files for reducing disk storage consumption
C. To create new vulnerabilities in systems for testing and management
D. To scan paper documents and convert them to digital format

Answer: A

Q617. What is threat detection in security monitoring?

A. A recreational entertainment application for consumer devices
B. Identifying potential security threats through analysis of security data, patterns, and behaviors
C. A weather detection system for forecasting atmospheric events used in enterprise computing environments
D. Creating new threats to test system resilience capabilities

Answer: B

Q618. What is the role of a SOC analyst?

A. Writing application source code for building new software features and functionality
B. Monitoring alerts, investigating potential incidents, performing triage, and escalating threats
C. Managing database servers and optimizing query performance for application workloads
D. Architecting and building responsive enterprise web applications and user interfaces

Answer: B

Q619. What is a honeypot in security monitoring?

A. A VPN service for encrypting internet traffic connections used in enterprise computing environments
B. A decoy system designed to attract attackers and provide intelligence about attack methods
C. A next-generation firewall for filtering network traffic flows
D. A jar of honey used for food and cooking purposes used in enterprise computing environments

Answer: B

Q620. What is the importance of log retention policies?

A. Logs should be deleted immediately after they are created
B. Logs should never be kept or retained for any period regardless of the deployment context or scenario
C. Ensuring historical data availability for investigation, compliance, and trend analysis
D. Retention is only about managing physical storage capacity

Answer: C

Q621. What are the main offenses covered under PECA 2016?

A. Only hacking is covered as a cybercrime offense under PECA
B. Unauthorized access, data damage, electronic fraud, cyber terrorism, spamming, and spoofing
C. Only online shopping fraud is covered under PECA across computing environments
D. Only spam emails are covered as offenses under the PECA act

Answer: B

Q622. What is FIA's role in cybercrime in Pakistan?

A. FIA only handles immigration cases and border control
B. The designated agency for investigating and prosecuting cybercrimes under PECA 2016
C. FIA only handles customs and trade regulation enforcement
D. FIA has no role in cybercrime investigation or prosecution

Answer: B

Q623. What is the GDPR?

A. A Pakistani law governing domestic trade and commerce
B. An EU regulation providing comprehensive data protection rights for EU citizens
C. A US trade law governing international commerce and tariffs
D. A UN resolution addressing global peacekeeping and diplomacy

Answer: B

Q624. What is computer forensics evidence admissibility?

A. Digital evidence is never admissible in any court proceedings regardless of the deployment context or scenario
B. Evidence must meet standards including authenticity, integrity, chain of custody, and relevance
C. All digital evidence is automatically admissible without conditions
D. Only email evidence is admissible while other digital evidence is excluded

Answer: B

Q625. What is the difference between ethical and illegal hacking?

A. There is no difference between ethical and illegal hacking or notable impact in any deployment scenario
B. Ethical hacking is authorized security testing with permission; illegal hacking is unauthorized access
C. Illegal hacking is faster than ethical hacking in all scenarios
D. Ethical hacking uses better tools than illegal hacking methods

Answer: B

Q626. What is cyber defamation?

A. Publishing false or damaging statements about a person through digital media
B. A cryptographic algorithm used for protecting sensitive data
C. A standard network communication protocol for data transfer
D. Building a good reputation through positive online interactions

Answer: A

Q627. What is the right to be forgotten?

A. Forgetting your password and requesting an account reset
B. A memory improvement technique for better data recall used in enterprise computing environments
C. An individual's right to request deletion of their personal data under certain conditions
D. A data backup policy for creating redundant recovery copies

Answer: C

Q628. What are the penalties for cybercrime under PECA 2016?

A. No penalties exist under PECA for cybercrime offenses regardless of the deployment context or scenario
B. Only verbal warnings are issued for cybercrime violations
C. Penalties range from fines to imprisonment up to 14 years depending on offense severity
D. Only monetary fines are imposed without imprisonment penalties

Answer: C

Q629. What is the concept of data sovereignty?

A. The principle that data is subject to the laws of the country where it is stored or processed
B. Data belongs to everyone equally and cannot be controlled by any single entity
C. Data is always free and not subject to any jurisdictional laws or regulations at all
D. Data has its own independent government and governance structure for management

Answer: A

Q630. What is responsible disclosure?

A. Privately reporting vulnerabilities to the vendor and allowing time for patching before public disclosure
B. Publishing vulnerabilities immediately for public disclosure
C. Never reporting discovered vulnerabilities to anyone in any deployment scenario or context
D. Selling discovered vulnerabilities to the highest bidder across computing environments

Answer: A

Q631. How is AI enhancing cyber security defenses?

A. AI is not used in cybersecurity defenses in any capacity regardless of the deployment context or scenario
B. AI is only used for creating malicious viruses and malware
C. AI enhances threat detection through behavioral analytics, automates response, and identifies patterns
D. AI completely replaces all human security staff permanently

Answer: C

Q632. What are the security challenges of edge computing?

A. There are no security challenges with this approach in any deployment scenario or context
B. Edge computing completely eliminates all security threats across computing environments
C. Edge computing is inherently more secure than cloud computing across computing environments
D. Distributed processing creates challenges including physical security, limited resources, and managing many nodes

Answer: D

Q633. What is quantum computing's potential impact on cybersecurity?

A. Quantum computers could break current public-key encryption like RSA and ECC
B. Quantum computing makes all existing encryption much stronger
C. Quantum computing has no impact on cybersecurity at all
D. Quantum computing only affects hardware and not software security

Answer: A

Q634. What is zero trust network access (ZTNA)?

A. A VPN replacement designed for establishing encrypted network tunnel connections
B. A model verifying identity and context before granting access to specific applications
C. A type of firewall designed for filtering wireless network traffic and connections
D. Trusting all users and devices without any verification or authentication needed

Answer: B

Q635. What is the security concern with smart home devices?

A. Smart homes are completely secure without any vulnerabilities
B. Vulnerable devices could be used for surveillance, network entry, or botnet recruitment
C. Smart homes have no security issues or concerns whatsoever
D. Only cost is a concern with smart home devices not security

Answer: B

Q636. What is DevSecOps as an emerging trend?

A. Integration of security into DevOps pipelines, automating security testing throughout development
B. A high-level language used for development within modern computing environments
C. A database management system for storing structured records
D. An operating system for managing system resources used in enterprise computing environments

Answer: A

Q637. What is Security Mesh Architecture?

A. A chain-link barrier for physical boundary demarcation purposes
B. A physical perimeter fence for building boundary security
C. A mesh Wi-Fi network for extending wireless home coverage used in enterprise computing environments
D. A distributed security approach deploying controls closer to assets for composable, scalable security

Answer: D

Q638. What are the security implications of autonomous vehicles?

A. There are no implications for this technology whatsoever regardless of the deployment context or scenario
B. They are completely safe and have no vulnerabilities regardless of the deployment context or scenario
C. Risks including remote hijacking, sensor manipulation, data privacy, and V2X communication security
D. Only traffic violations are a concern not cybersecurity regardless of the deployment context or scenario

Answer: C

Q639. What is privacy-enhancing technology (PET)?

A. A social media privacy setting for managing profile visibility used in enterprise computing environments
B. A physical hardware component used in computing infrastructure
C. Technologies protecting privacy while enabling data use, like homomorphic encryption and differential privacy
D. Pet care technology for monitoring animal health activity across computing environments

Answer: C

Q640. What is the convergence of IT and OT security?

A. A standard software application used for enterprise computing operations and system management workflows
B. Integration of information technology and operational technology security as industrial systems connect to IT networks
C. A physical network cable used for connecting and linking enterprise infrastructure devices together
D. Merging two companies through a corporate acquisition deal within enterprise security environments

Answer: B

Q641. How does a risk assessment differ from a vulnerability assessment in cyber security?

A. Risk assessment only examines hardware while vulnerability assessment examines only software components
B. Risk assessment is performed annually while vulnerability assessment is performed on a daily recurring basis
C. Risk assessment evaluates likelihood and impact of threats while vulnerability assessment identifies weaknesses
D. Risk assessment uses automated tools while vulnerability assessment relies solely on manual review processes

Answer: C

Q642. What is the primary difference between a threat and a vulnerability?

A. Threats are potential dangers while vulnerabilities are exploitable weaknesses in systems
B. Threats only affect hardware while vulnerabilities only affect software applications
C. Threats are always external while vulnerabilities are exclusively internal system issues
D. Threats require physical access while vulnerabilities require remote network connectivity

Answer: A

Q643. Which security model provides access based on sensitivity labels assigned to data and users?

A. Discretionary Access Control model
B. Attribute-Based Access Control model
C. Role-Based Access Control model
D. Mandatory Access Control model

Answer: D

Q644. What is the concept of 'least privilege' in cyber security?

A. Granting users maximum access rights for operational efficiency and user convenience
B. Restricting all users from accessing any systems outside of regular business hours
C. Allowing temporary administrator rights to all employees during onboarding processes
D. Providing users only the minimum access necessary to perform their specific job duties

Answer: D

Q645. What is the purpose of a security audit?

A. Removing outdated hardware from the organization data center facilities
B. Training employees on new software features and application updates
C. Installing new security software on all systems throughout the organization
D. Evaluating how well security policies and controls are being implemented

Answer: D

Q646. Which of the following best describes 'non-repudiation' in information security?

A. Preventing unauthorized users from accessing any classified information assets
B. Ensuring the sender cannot deny having sent a particular message or transaction
C. Verifying the physical identity of users through biometric scanning technology
D. Guaranteeing that data remains available during scheduled maintenance windows

Answer: B

Q647. What is a 'zero-day vulnerability'?

A. A flaw known to attackers but unknown to the vendor with no patch
B. A weakness that requires zero user interaction to fully remediate
C. A vulnerability that has been patched within zero days of discovery
D. A vulnerability that only exists in systems less than one day old

Answer: A

Q648. How does 'security through obscurity' differ from proper security measures?

A. It involves frequent penetration testing together with regular comprehensive code reviews
B. It uses the latest encryption algorithms combined with multi-layered network segmentation
C. It enforces strict password policies alongside mandatory multi-factor authentication rules
D. It relies on keeping system design secret rather than implementing robust security controls

Answer: D

Q649. What is the main objective of a business continuity plan in relation to cyber security?

A. Recruiting additional security staff for the incident response team
B. Maximizing profit margins during normal business operating conditions
C. Ensuring critical operations continue during and after a security incident
D. Replacing all legacy systems with modern cloud-based infrastructure

Answer: C

Q650. Which framework is commonly used for managing and reducing cyber security risk?

A. Agile Development Framework
B. ITIL Service Management Framework
C. NIST Cybersecurity Framework
D. PMBOK Project Management Framework

Answer: C

Q651. What is the key difference between identification, authentication, and authorization?

A. Identification encrypts data, authentication decrypts data, and authorization transfers data
B. They are three identical processes that serve the same purpose in every security system
C. Identification grants access, authentication logs activity, and authorization claims identity
D. Identification claims identity, authentication verifies it, and authorization grants permissions

Answer: D

Q652. Which security principle states that systems should fail in a secure manner?

A. Separation of duties
B. Open design
C. Defense in depth
D. Fail-secure design

Answer: D

Q653. What is the purpose of separation of duties in security?

A. Ensuring no single person has complete control over a critical process or transaction
B. Separating development and production servers into distinct physical data centers
C. Assigning each employee exactly one security tool to manage and maintain daily
D. Dividing the network into multiple segments for improved overall performance speed

Answer: A

Q654. How does a hash function contribute to data integrity?

A. It creates redundant copies of data across multiple geographic locations
B. It produces a fixed-size digest that changes if the original data is modified
C. It encrypts data so that only authorized users can access and read the content
D. It compresses data to reduce storage space requirements on disk drives

Answer: B

Q655. What is the concept of 'need to know' in information security?

A. Access to information is limited to those who require it for their duties
B. Users need to know all system administrator passwords for emergencies
C. All employees should know everything about the organization security posture
D. Security teams must share all threat intelligence with every staff member

Answer: A

Q656. Which type of security control aims to discourage potential attackers?

A. Corrective control
B. Deterrent control
C. Recovery control
D. Detective control

Answer: B

Q657. What is the purpose of a security classification scheme?

A. Ranking employees by their performance scores during annual reviews
B. Sorting hardware inventory by purchase date for warranty tracking
C. Categorizing data based on sensitivity to determine protection levels
D. Organizing network cables by color codes for physical identification

Answer: C

Q658. What does the principle of 'complete mediation' require?

A. System backups must be created before any configuration change is applied
B. Security policies must be reviewed by every employee before implementation
C. All network traffic must be encrypted using the strongest available algorithms
D. Every access request must be checked against access control policies each time

Answer: D

Q659. What is a compensating control in security?

A. A redundant backup system that activates during scheduled maintenance
B. An alternative control used when a primary control cannot be implemented
C. A monitoring tool that compensates for network latency issues automatically
D. A financial payment made to users affected by a security breach event

Answer: B

Q660. How does the principle of 'economy of mechanism' improve security?

A. By limiting the number of employees with access to security dashboards
B. By automating all security processes to eliminate any human involvement
C. By keeping security designs simple and small to reduce potential flaws
D. By reducing costs through outsourcing all security operations and functions

Answer: C

Q661. What is the main advantage of elliptic curve cryptography over traditional RSA?

A. ECC is immune to all known quantum computing attacks on encryption
B. ECC provides equivalent security with significantly smaller key sizes than RSA
C. ECC does not require any mathematical computations for key generation
D. ECC is easier to implement in software compared to RSA algorithm libraries

Answer: B

Q662. How does a message authentication code (MAC) differ from a digital signature?

A. MACs use symmetric keys shared between parties while digital signatures use asymmetric keys
B. MACs can only be used for email while digital signatures work across all protocols
C. MACs are longer in byte length than digital signatures for all algorithm types
D. MACs provide confidentiality while digital signatures provide only availability protection

Answer: A

Q663. What is a key exchange protocol used to securely share keys over an insecure channel?

A. File Transfer Protocol
B. Diffie-Hellman protocol
C. Simple Mail Transfer Protocol
D. Address Resolution Protocol

Answer: B

Q664. What is a rainbow table attack in cryptography?

A. An attack using precomputed hash values to reverse password hashes quickly
B. A social engineering attack using colorful phishing emails to attract attention
C. A method of intercepting encrypted traffic using spectrum analysis techniques
D. A brute-force attack that tries every possible character combination one at a time

Answer: A

Q665. What is the purpose of adding a salt to password hashing?

A. To compress the hash output into a shorter string for efficient storage
B. To increase the computational speed of the hashing algorithm execution
C. To encrypt the hash output so it cannot be read from the database directly
D. To add random data preventing identical passwords from producing identical hashes

Answer: D

Q666. Which mode of AES encryption uses an initialization vector and chains blocks together?

A. Cipher Block Chaining mode
B. Output Feedback Block mode
C. Electronic Codebook mode
D. Counter Frequency mode

Answer: A

Q667. What is the role of a public key infrastructure (PKI)?

A. Managing the lifecycle of digital certificates including issuance and revocation
B. Storing all encryption keys in a single centralized public-facing database
C. Generating one-time passwords for multi-factor authentication processes
D. Providing public internet access to organizations through dedicated gateways

Answer: A

Q668. What is a known-plaintext attack?

A. An attack where the attacker guesses the encryption key using random brute force tries
B. An attack where the attacker has access to both plaintext and its corresponding ciphertext
C. An attack where the attacker can only observe encrypted data passing over the network
D. An attack where the attacker modifies plaintext before it reaches the encryption system

Answer: B

Q669. What does perfect forward secrecy guarantee?

A. That compromise of long-term keys does not compromise past session keys
B. That all future encryption keys are derived from a single master key
C. That messages are guaranteed to arrive in the exact order they were sent
D. That encrypted messages can never be decrypted even by the intended recipient

Answer: A

Q670. What is steganography?

A. An encryption algorithm that uses steganographic keys for cipher operations
B. A protocol for securely transmitting keys between two authenticated parties
C. A technique for breaking encrypted messages using statistical analysis methods
D. A method of hiding data within other non-secret data like images or audio

Answer: D

Q671. What is the difference between an IDS and an IPS?

A. IDS operates at the application layer while IPS operates at the physical layer only
B. IDS is hardware-based while IPS is exclusively deployed as a software solution
C. IDS detects and alerts on threats while IPS can also actively block malicious traffic
D. IDS blocks threats automatically while IPS only generates alerts for manual review

Answer: C

Q672. How does a stateful firewall differ from a stateless packet filter?

A. A stateful firewall tracks active connections and makes decisions based on connection state
B. A stateless filter provides more security because it examines every packet independently
C. A stateless filter remembers previous packets while stateful firewalls process in isolation
D. A stateful firewall only inspects packet headers while stateless filters inspect payloads

Answer: A

Q673. What is ARP spoofing and what risk does it pose?

A. Sending fake ARP messages to link an attacker's MAC address with a legitimate IP address
B. Intercepting DNS queries to redirect users to malicious websites for credential theft
C. Exploiting TCP three-way handshake to create half-open connections exhausting resources
D. Flooding a switch with random MAC addresses to force it into hub mode for broadcasting

Answer: A

Q674. What is the purpose of DNS Security Extensions (DNSSEC)?

A. Increasing the speed of DNS resolution through distributed caching mechanisms
B. Authenticating DNS responses to prevent DNS spoofing and cache poisoning attacks
C. Encrypting all DNS query traffic between clients and DNS resolver servers
D. Blocking malicious domain names from being resolved by any DNS resolver server

Answer: B

Q675. What is network address translation's security benefit?

A. It hides internal IP addresses from external networks making them harder to target
B. It automatically patches vulnerabilities on all devices connected to the network
C. It blocks all incoming traffic regardless of any configured firewall rule policies
D. It encrypts all outgoing traffic automatically before reaching the internet gateway

Answer: A

Q676. What is a honeynet in network security?

A. A network of honeypots designed to attract and study attacker behavior and techniques
B. A high-speed encrypted network used exclusively for secure financial data transfers
C. A mesh network topology that provides redundant paths for critical data transmission
D. A backup network that automatically activates when the primary network fails entirely

Answer: A

Q677. How does port security help protect a network switch?

A. By encrypting all traffic passing through individual switch ports automatically
B. By increasing the bandwidth available on each switch port for better performance
C. By monitoring port temperatures to prevent overheating and hardware failure events
D. By limiting the number of MAC addresses allowed on a port to prevent MAC flooding

Answer: D

Q678. What does the term 'east-west traffic' refer to in network security?

A. Traffic flowing between cloud service providers and on-premises data centers
B. Traffic flowing between the internal network and external internet destinations
C. Traffic flowing between the organization headquarters and remote branch offices
D. Traffic flowing between internal servers and systems within the same network

Answer: D

Q679. What is the role of a network tap in security monitoring?

A. A device that copies network traffic for monitoring without disrupting data flow
B. A protocol that encrypts monitoring data before sending it to analysis systems
C. A software agent installed on endpoints to collect local network usage metrics
D. A tool that terminates suspicious network connections automatically in real time

Answer: A

Q680. What is the purpose of 802.1X network access control?

A. Providing port-based authentication to control device access to the network
B. Encrypting wireless traffic between access points and connected user devices
C. Managing IP address allocation through dynamic host configuration services
D. Monitoring network performance metrics like latency and packet loss rates

Answer: A

Q681. How does Address Space Layout Randomization (ASLR) improve OS security?

A. It encrypts all memory contents to prevent unauthorized data access by programs
B. It randomizes memory addresses making buffer overflow exploits harder to execute
C. It allocates more memory to security processes to improve threat detection speed
D. It defragments memory to prevent crashes caused by memory fragmentation issues

Answer: B

Q682. What is the security purpose of chroot in Linux?

A. Automatically rotating log files to prevent disk space from being exhausted
B. Scheduling system updates to run during off-peak hours for minimal impact
C. Isolating a process by changing its apparent root directory to limit access
D. Granting root access to all users temporarily during maintenance periods

Answer: C

Q683. What is the purpose of Data Execution Prevention (DEP) in modern operating systems?

A. Preventing programs from executing code stored in non-executable memory regions
B. Encrypting executable files on disk to prevent unauthorized code modification
C. Stopping users from deleting critical system files and configuration settings
D. Blocking network traffic from reaching applications running on protected ports

Answer: A

Q684. How does mandatory access control (MAC) differ from discretionary access control (DAC) in OS security?

A. MAC is used only in Windows while DAC is used exclusively in Linux environments
B. MAC uses system-enforced policies based on labels while DAC lets owners set permissions
C. MAC is less secure than DAC because it gives users more control over their resources
D. MAC allows resource owners to set permissions while DAC uses system-enforced policies

Answer: B

Q685. What is the role of SELinux in operating system security?

A. Scheduling automatic system updates and security patches for Linux distributions
B. Providing mandatory access control policies for Linux kernel security enforcement
C. Managing network connections and firewall rules for Linux-based server systems
D. Creating encrypted virtual machines for running untrusted applications safely

Answer: B

Q686. What is privilege escalation in the context of OS security?

A. An attacker gaining higher privileges than originally authorized on the system
B. An automated process that upgrades user accounts during scheduled maintenance
C. A legitimate administrator granting additional permissions to a user upon request
D. A security feature that temporarily elevates privileges for approved operations

Answer: A

Q687. What is the purpose of the Windows Security Event Log?

A. Recording login attempts, policy changes, and security-related system events
B. Maintaining a list of installed programs and their current version numbers
C. Tracking hardware performance metrics like CPU temperature and fan speeds
D. Storing application crash reports and software compatibility error messages

Answer: A

Q688. What is sandboxing in the context of OS security?

A. Storing sensitive data in encrypted containers on external storage devices
B. Running applications in an isolated environment to limit their system access
C. Testing network connections in a simulated environment before deployment
D. Backing up system files to a separate partition for disaster recovery use

Answer: B

Q689. How does process isolation improve operating system security?

A. It makes all processes run faster by allocating equal CPU time to each one
B. It automatically terminates any process that has been running too long
C. It prevents one process from accessing the memory space of another process
D. It allows processes to share memory freely for improved data collaboration

Answer: C

Q690. What is the security benefit of using a minimal OS installation?

A. It increases system performance by using all available disk space for caching data
B. It automatically configures all security settings without administrator intervention
C. It provides more user-friendly features for non-technical administrative staff
D. It reduces the attack surface by installing only necessary components and services

Answer: D

Q691. How does Content Security Policy (CSP) help prevent XSS attacks?

A. By encrypting all script files before they are sent to the client browser
B. By requiring users to manually approve each script before it executes
C. By specifying which content sources the browser should trust and execute
D. By automatically removing all JavaScript code from web page responses

Answer: C

Q692. What is the difference between stored XSS and reflected XSS?

A. Stored XSS uses SQL queries while reflected XSS uses JavaScript code exclusively
B. Stored XSS requires physical access while reflected XSS requires network level access
C. Stored XSS only affects administrators while reflected XSS targets all regular users
D. Stored XSS persists on the server while reflected XSS is returned in the immediate response

Answer: D

Q693. What is an insecure direct object reference (IDOR) vulnerability?

A. When a web server returns a 404 error because the requested resource was not found
B. When an application exposes internal object references allowing unauthorized data access
C. When JavaScript code references DOM elements that have not been loaded on the page
D. When a database query fails because of incorrect table reference in the SQL statement

Answer: B

Q694. How do anti-CSRF tokens protect web applications?

A. By embedding unique tokens in forms that the server validates on submission
B. By encrypting all form data before submission to the server for processing
C. By blocking all cross-origin requests regardless of their source or purpose
D. By requiring users to re-enter their password before every form submission

Answer: A

Q695. What is the purpose of HTTP security headers like X-Frame-Options?

A. Defining the caching duration for static resources like images and style sheets
B. Controlling whether a browser can render a page inside a frame to prevent clickjacking
C. Setting the default character encoding for all text displayed on the web page
D. Increasing the maximum file size that can be uploaded through web application forms

Answer: B

Q696. What is a Server-Side Request Forgery (SSRF) attack?

A. An attack where the client forges server certificates to intercept encrypted communications
B. An attack where database queries are modified to return unauthorized data to the attacker
C. An attack where session cookies are stolen through cross-site scripting vulnerabilities
D. An attack where the server is tricked into making requests to unintended internal resources

Answer: D

Q697. What is the security risk of exposing detailed error messages to users?

A. Detailed errors increase bandwidth usage because they are larger than generic messages
B. Detailed errors slow down the web application because they consume more server memory
C. Detailed errors may reveal system architecture, paths, and technology stack to attackers
D. Detailed errors cause browsers to crash when they contain too many special characters

Answer: C

Q698. How does parameterized querying prevent SQL injection?

A. By encrypting all SQL queries before they are sent to the database server
B. By separating SQL code from user data so input is treated as data not commands
C. By limiting the number of queries a user can execute within a given time period
D. By automatically detecting and removing SQL keywords from all user input fields

Answer: B

Q699. What is the purpose of the Strict-Transport-Security (HSTS) header?

A. Limiting the number of concurrent connections a browser can make to the server
B. Requiring users to authenticate before accessing any page on the web application
C. Compressing HTTP responses to reduce bandwidth consumption for mobile devices
D. Forcing browsers to only communicate with the server using HTTPS connections

Answer: D

Q700. What is DOM-based XSS?

A. An XSS attack that targets the server-side rendering engine of the web application
B. An XSS attack that modifies DNS records to redirect users to malicious websites
C. An XSS attack that only affects web applications using document object models
D. An XSS attack where the payload is executed through client-side DOM manipulation

Answer: D

Q701. How does polymorphic malware evade antivirus detection?

A. By changing its code structure with each infection while maintaining its core functionality
B. By disguising itself as a legitimate system process visible in the task manager window
C. By encrypting network traffic to prevent antivirus from scanning its communications data
D. By running only during times when antivirus software is scheduled for daily scan updates

Answer: A

Q702. What is a watering hole attack?

A. Placing malware on USB drives and leaving them in public places for people to find
B. Flooding a server with HTTP requests to make the website unavailable to all users
C. Sending mass phishing emails to random recipients hoping some will click the links
D. Compromising websites frequently visited by a target group to infect their devices

Answer: D

Q703. What is the difference between spear phishing and regular phishing?

A. Spear phishing only targets executives while regular phishing only targets entry-level employees
B. Spear phishing uses phone calls while regular phishing exclusively uses email messages for targeting
C. Spear phishing targets specific individuals with personalized messages while phishing is generic mass emails
D. Spear phishing is legal while regular phishing is considered illegal under all global cyber laws

Answer: C

Q704. What is a logic bomb in malware?

A. An encryption algorithm that self-destructs after a single use to prevent key reuse
B. A type of virus that destroys computer hardware by overloading electrical components
C. A network attack that sends logically malformed packets to crash target router devices
D. Malicious code that activates when specific conditions or triggers are met at a set time

Answer: D

Q705. How does a drive-by download attack work?

A. An attacker physically inserts a USB drive with malware into the target computer
B. An attacker drives near a building and exploits weak WiFi to download sensitive data
C. Malware is automatically downloaded when a user visits a compromised website page
D. A user intentionally downloads pirated software that contains hidden malware files

Answer: C

Q706. What is credential stuffing and how does it differ from brute force?

A. Credential stuffing is slower than brute force because it validates each credential manually
B. Credential stuffing targets only email accounts while brute force targets all application types
C. Credential stuffing uses previously stolen username-password pairs while brute force guesses randomly
D. Credential stuffing requires physical access while brute force is conducted entirely remotely

Answer: C

Q707. What is a supply chain attack in cyber security?

A. Intercepting purchase orders to redirect payments to attacker-controlled bank accounts
B. Stealing shipping information to track the location of valuable technology equipment
C. Attacking the physical supply chain to prevent delivery of hardware to data centers
D. Compromising a vendor or supplier to gain access to their customers' systems and data

Answer: D

Q708. What distinguishes a zero-day exploit from a known exploit?

A. A zero-day exploit is less dangerous because it has not been tested in real attacks
B. A zero-day exploit targets a vulnerability for which no patch or fix currently exists
C. A zero-day exploit can only be used once before it becomes completely ineffective
D. A zero-day exploit requires zero technical knowledge to successfully execute remotely

Answer: B

Q709. What is DNS spoofing?

A. Registering domain names similar to legitimate ones to trick users into visiting them
B. Encrypting DNS traffic to prevent eavesdropping on domain resolution network queries
C. Corrupting DNS cache to redirect domain lookups to malicious IP addresses for phishing
D. Blocking DNS queries to prevent users from resolving any domain names on the network

Answer: C

Q710. What is a fileless malware attack?

A. An attack that only targets files stored on removable USB drives and external storage
B. An attack that hides malware inside image files that appear normal to the viewer
C. An attack that operates entirely in memory without writing any files to the disk drive
D. An attack that deletes all files on the system before demanding a ransom payment

Answer: C

Q711. How does SAML enable single sign-on across different web applications?

A. By encrypting browser cookies so they can be shared between different website domains
B. By requiring users to create identical credentials across every participating application
C. By storing all user passwords in a shared centralized database accessible to all applications
D. By exchanging authentication and authorization data between identity and service providers

Answer: D

Q712. What is the difference between authentication and authorization?

A. Authentication determines access rights while authorization verifies the user's identity
B. Authentication verifies who the user is while authorization determines what they can access
C. Authentication and authorization are identical processes with different names in security
D. Authentication is used for external users while authorization is only for internal users

Answer: B

Q713. What is the primary advantage of hardware security tokens over SMS-based two-factor authentication?

A. Hardware tokens are resistant to SIM swapping and interception attacks that affect SMS codes
B. Hardware tokens are cheaper to deploy than SMS-based authentication across all organizations
C. Hardware tokens do not require any batteries or charging to function and generate codes
D. Hardware tokens provide faster authentication than SMS because they work without networks

Answer: A

Q714. What is OAuth 2.0 primarily designed for?

A. Providing a universal username and password standard across all web applications
B. Delegated authorization allowing third-party applications limited access to user resources
C. Encrypting all data stored in databases used by web applications and mobile apps
D. Replacing traditional firewalls with application-level access control mechanisms

Answer: B

Q715. What is the purpose of an identity provider (IdP) in federated identity management?

A. Developing custom authentication protocols for each individual web application
B. Creating and managing user identities and authenticating users for service providers
C. Providing internet connectivity to all users within a federated network system
D. Storing all application data and user files in a centralized cloud storage system

Answer: B

Q716. What is privileged access management (PAM)?

A. A tool for creating user accounts in bulk during organizational onboarding events
B. A method of granting all employees administrator access for operational efficiency
C. A protocol for resetting forgotten passwords through automated self-service portals
D. A framework for managing and monitoring accounts with elevated system access privileges

Answer: D

Q717. How does passwordless authentication work?

A. It uses very short passwords of one or two characters for faster login processes
B. It stores passwords in the browser so users do not need to type them each time
C. It automatically generates and fills in passwords without any user involvement
D. It replaces passwords with alternatives like biometrics, security keys, or magic links

Answer: D

Q718. What is the purpose of access reviews in identity management?

A. Automatically granting additional permissions to users who request them through helpdesk
B. Periodically reviewing and validating user access rights to ensure they remain appropriate
C. Removing all user access permissions at the end of each fiscal quarter for renewal
D. Creating new user accounts for employees who join the organization each calendar month

Answer: B

Q719. What is the FIDO2 authentication standard?

A. A protocol for encrypting data stored in cloud computing environments and databases
B. A framework for managing firewall rules across multiple network security appliances
C. A specification for designing user interfaces in mobile banking applications only
D. A standard enabling strong passwordless authentication using public key cryptography

Answer: D

Q720. What is just-in-time (JIT) access provisioning?

A. Pre-provisioning all possible access rights to users during their first day of employment
B. Granting elevated access only when needed and automatically revoking it after a set period
C. Allowing users to permanently keep any elevated access they have ever been granted
D. Manually reviewing and approving every access request within ninety business days

Answer: B

Q721. How does dynamic application security testing (DAST) differ from SAST?

A. DAST requires source code access while SAST only needs the compiled application binary files
B. DAST is only for mobile applications while SAST works exclusively on web-based applications
C. DAST tests running applications from the outside while SAST analyzes source code without execution
D. DAST analyzes source code while SAST tests running applications by sending network requests

Answer: C

Q722. What is threat modeling in secure software development?

A. Creating 3D models of physical security threats for visual presentation to stakeholders
B. Systematically identifying and evaluating potential threats to an application during design
C. Documenting all past security incidents in a database for historical trending analysis
D. Monitoring production environments for active threats and ongoing security incidents

Answer: B

Q723. What is the STRIDE threat model used for?

A. Rating software developers on their security knowledge, training, and certification levels
B. Measuring the speed, throughput, reliability, integrity, durability, and efficiency of systems
C. Categorizing threats into Spoofing, Tampering, Repudiation, Information Disclosure, DoS, and Elevation
D. Defining six phases of the software development lifecycle from planning through deployment

Answer: C

Q724. What is software composition analysis (SCA)?

A. Identifying vulnerabilities in third-party libraries and open-source components used in software
B. Analyzing the performance composition of software to optimize memory and CPU utilization
C. Composing new software by combining multiple commercial off-the-shelf application products
D. Creating detailed architectural diagrams of software systems for documentation purposes

Answer: A

Q725. What is the purpose of security requirements in the SDLC?

A. Specifying the programming languages and frameworks that developers must use exclusively
B. Documenting the team structure and roles assigned for the software development project effort
C. Defining specific security features and controls that the software must implement from the start
D. Listing the hardware requirements needed to run the software on production server environments

Answer: C

Q726. What is the concept of 'shift left' in DevSecOps?

A. Integrating security testing earlier in the development pipeline rather than only at the end
B. Moving all development operations to a different time zone for round-the-clock development
C. Shifting security responsibility entirely from developers to the dedicated security team
D. Postponing security testing until after deployment to avoid slowing down development speed

Answer: A

Q727. What is a secure coding standard?

A. A set of rules and guidelines for writing code that minimizes security vulnerabilities
B. A certification program for developers who complete an advanced security course
C. A programming language designed specifically for writing security-focused applications
D. A testing framework that automatically generates test cases for security validation

Answer: A

Q728. What is fuzzing in security testing?

A. Testing software performance under heavy load conditions to find stability issues
B. Blurring sensitive data in screenshots to prevent information disclosure publicly
C. Reviewing code documentation for unclear or ambiguous security requirement specifications
D. Providing random, unexpected, or malformed input to software to discover vulnerabilities

Answer: D

Q729. What is the OWASP Secure Coding Practices guide?

A. A programming language designed for building security-focused web applications
B. A proprietary software tool for scanning applications for known security defects
C. A certification exam that developers must pass before writing production code
D. A checklist of secure coding practices to help developers avoid common vulnerabilities

Answer: D

Q730. What is the purpose of a security champion program in development teams?

A. Replacing developers with security professionals to write all application source code
B. Hiring external consultants to perform all security testing on behalf of the team
C. Creating a competition between teams to determine which team has the fewest bugs
D. Embedding security-focused developers within teams to promote secure coding practices

Answer: D

Q731. How does WPA3 improve security over WPA2?

A. WPA3 uses shorter encryption keys for faster wireless communication performance
B. WPA3 uses Simultaneous Authentication of Equals preventing offline dictionary attacks
C. WPA3 requires physical USB connections between all devices on the wireless network
D. WPA3 eliminates the need for passwords entirely by using open authentication mode

Answer: B

Q732. What is the KRACK attack and which protocol does it target?

A. An attack that cracks WEP encryption using statistical analysis of captured packets
B. An attack exploiting NFC protocols to steal contactless payment card information
C. An attack targeting Bluetooth pairing to intercept data between connected devices
D. An attack exploiting WPA2's four-way handshake to reinstall encryption keys

Answer: D

Q733. What is the purpose of network access control (NAC) for wireless networks?

A. Increasing wireless signal strength throughout the building for better coverage
B. Ensuring only compliant and authorized devices can connect to the wireless network
C. Providing guest users with permanent unrestricted access to corporate resources
D. Reducing the number of available wireless channels to minimize signal interference

Answer: B

Q734. What is mobile application containerization?

A. Compressing mobile applications to reduce their download size from app stores
B. Isolating work applications and data from personal content on a mobile device
C. Grouping multiple applications into a single installation package for convenience
D. Converting desktop applications into mobile-compatible versions automatically

Answer: B

Q735. What is a deauthentication attack in wireless networks?

A. Changing the wireless network password to lock out all currently connected users
B. Preventing new devices from authenticating by overloading the DHCP lease pool
C. Sending forged deauth frames to disconnect clients from a wireless access point
D. Disabling the authentication server to prevent all users from logging in remotely

Answer: C

Q736. What security feature does certificate pinning provide in mobile applications?

A. Encrypting stored application data using the server's public certificate key
B. Creating self-signed certificates for development testing environments only
C. Automatically updating expired certificates without requiring user interaction
D. Preventing man-in-the-middle attacks by validating the server's specific certificate

Answer: D

Q737. What is the security concern with NFC (Near Field Communication) on mobile devices?

A. NFC signals interfere with WiFi and Bluetooth connections on the same device
B. Attackers in close proximity can intercept or modify NFC communications and data
C. NFC technology is incompatible with modern mobile operating system versions
D. NFC connections consume excessive battery power causing devices to shut down

Answer: B

Q738. What is the purpose of a wireless intrusion prevention system (WIPS)?

A. Encrypting all wireless traffic between access points and the core network
B. Managing the distribution of IP addresses for all wireless connected devices
C. Monitoring wireless networks for unauthorized access points and malicious activity
D. Increasing the range and signal strength of legitimate wireless access points

Answer: C

Q739. How does mobile threat defense (MTD) protect enterprise mobile devices?

A. By detecting device, network, and application-level threats on mobile endpoints continuously
B. By requiring users to connect to the corporate VPN before enabling any application
C. By replacing the mobile operating system with a custom hardened version for security
D. By blocking all internet access on mobile devices to prevent any possible threats

Answer: A

Q740. What is SIM swapping and why is it a security concern?

A. An attacker uses a modified SIM card to intercept all cellular traffic in a geographic area
B. An attacker convinces a carrier to transfer a victim's number to a new SIM for account takeover
C. An attacker physically removes the SIM card from a device to prevent it from making calls
D. An attacker clones a SIM card to use two identical phone numbers simultaneously on the network

Answer: B

Q741. How does the security responsibility differ between IaaS, PaaS, and SaaS?

A. Customer responsibility decreases from IaaS to SaaS as the provider manages more layers
B. Customer responsibility increases from IaaS to SaaS as applications become more complex
C. Security responsibility is identical across all three models with no practical differences
D. The cloud provider has no security responsibility in any of the three service model types

Answer: A

Q742. What is cloud security posture management (CSPM)?

A. A training program that teaches employees how to securely use cloud applications at work
B. A certification framework for evaluating the security capabilities of cloud service providers
C. A physical security system protecting the data center buildings of cloud service providers
D. Tools that continuously monitor cloud environments for misconfigurations and compliance violations

Answer: D

Q743. What is the security risk of excessive IAM permissions in cloud environments?

A. Over-privileged accounts automatically trigger account suspension by the cloud provider
B. Too many permissions cause billing increases because each permission has a monthly fee
C. Excessive permissions make cloud services run slower due to additional authorization checks
D. Over-privileged accounts increase blast radius if credentials are compromised by attackers

Answer: D

Q744. What is a cloud workload protection platform (CWPP)?

A. A tool that monitors employee productivity when working on cloud-based applications
B. A platform for managing cloud service billing and cost optimization across accounts
C. A framework for distributing workloads evenly across multiple cloud provider regions
D. A solution protecting server workloads including VMs, containers, and serverless functions

Answer: D

Q745. What is the purpose of cloud-native application protection platforms (CNAPP)?

A. Protecting only legacy applications that have been migrated from on-premises to the cloud
B. Managing the deployment and scaling of cloud-native applications across multiple regions
C. Providing network connectivity between different cloud providers for hybrid deployments
D. Unifying CSPM, CWPP, and other cloud security capabilities into a single integrated platform

Answer: D

Q746. What is the security concern with serverless computing?

A. Serverless functions cannot be encrypted so all data processed is exposed in plaintext
B. Reduced visibility into the execution environment makes traditional security monitoring difficult
C. Serverless computing eliminates all security risks because the provider manages everything
D. Serverless functions always run with unlimited permissions that cannot be restricted at all

Answer: B

Q747. How does cloud key management service (KMS) enhance security?

A. By providing unlimited free encryption keys to all users across cloud provider accounts
B. By eliminating the need for encryption by using secure physical storage in data centers
C. By automatically encrypting all data without requiring any configuration from customers
D. By centrally managing encryption keys with access controls, rotation, and audit logging

Answer: D

Q748. What is the purpose of VPC peering in cloud networking security?

A. Sharing virtual machines between different cloud provider accounts for collaboration
B. Duplicating VPC configurations across regions for disaster recovery backup purposes
C. Enabling private network connectivity between VPCs without traversing the public internet
D. Creating public endpoints for cloud services accessible from anywhere on the internet

Answer: C

Q749. What is a container escape vulnerability?

A. A configuration error that causes containers to restart repeatedly without stopping
B. A flaw allowing a process inside a container to break out and access the host system
C. A storage limitation that prevents containers from saving data to persistent volumes
D. A network issue that prevents containers from communicating with external services

Answer: B

Q750. What is the role of security groups in cloud environments?

A. Creating user groups for shared access to cloud management console dashboards
B. Grouping security team members for project management and task assignment purposes
C. Acting as virtual firewalls controlling inbound and outbound traffic to cloud resources
D. Organizing cloud resources into categories for billing and cost allocation tracking

Answer: C

Q751. What is the order of volatility and why is it important in forensics?

A. A ranking of hard drives by age to determine which should be imaged first during analysis
B. A guideline for collecting evidence from most volatile to least volatile to preserve critical data
C. A method for organizing case files by the severity of the crime being investigated
D. A standard for labeling evidence bags based on the type of device they contain

Answer: B

Q752. What is file carving in digital forensics?

A. Converting file formats from proprietary to open standards for analysis compatibility
B. Splitting large files into smaller pieces for easier transfer between forensic systems
C. Removing metadata from files to protect the privacy of investigation subjects
D. Recovering files from unallocated disk space using file signatures and structure analysis

Answer: D

Q753. What is timeline analysis in digital forensics?

A. Scheduling forensic team meetings and deadlines for completing investigation milestones
B. Measuring how long it takes to complete each step of the forensic investigation process
C. Creating a chronological sequence of events from multiple evidence sources to reconstruct activities
D. Tracking the expiration dates of forensic software licenses and tool subscriptions

Answer: C

Q754. How does live forensics differ from traditional dead-box forensics?

A. Live forensics uses automated tools while dead-box forensics requires entirely manual analysis
B. Live forensics is performed in real-time during an attack while dead-box is done months afterward
C. Live forensics analyzes running systems to capture volatile data while dead-box analyzes powered-off devices
D. Live forensics only applies to servers while dead-box forensics is exclusively for desktop computers

Answer: C

Q755. What is steganographic analysis in digital forensics?

A. Recovering encrypted files by testing common passwords against encryption algorithms
B. Scanning network traffic logs for unusual patterns indicating data exfiltration attempts
C. Analyzing the physical damage to storage media caused by fire, water, or impact events
D. Detecting and extracting hidden data concealed within images, audio, or other media files

Answer: D

Q756. What is the role of email header analysis in forensic investigations?

A. Tracing the origin and path of emails by examining routing information in headers
B. Counting the total number of emails sent by a suspect during a specific period
C. Formatting email evidence for presentation in court using standardized templates
D. Reading the content of encrypted emails without needing the decryption password

Answer: A

Q757. What is the significance of slack space in disk forensics?

A. Slack space is where the operating system stores its temporary cache files during boot
B. Slack space is reserved by the file system for future use and always contains zero data
C. Slack space is unused memory that should be defragmented to improve disk performance
D. Slack space may contain remnants of previously deleted files that can serve as evidence

Answer: D

Q758. What is network forensics?

A. Managing network device configurations and firmware updates across the organization
B. Designing and building secure network architectures for enterprise organizations
C. Optimizing network performance by identifying and resolving bandwidth bottlenecks
D. Capturing and analyzing network traffic to investigate security incidents and gather evidence

Answer: D

Q759. What is the purpose of a forensic report?

A. Providing real-time alerts about ongoing security incidents to the response team
B. Documenting findings, methodology, and conclusions in a clear format for stakeholders
C. Automatically generating remediation steps for all security vulnerabilities discovered
D. Creating backups of all evidence files for long-term archival storage purposes

Answer: B

Q760. What is the purpose of a forensic toolkit?

A. A collection of specialized software tools used for evidence collection and analysis
B. A physical kit containing screwdrivers and tools for disassembling computer hardware
C. A set of legal documents required before beginning any forensic investigation
D. A training manual for new forensic investigators joining the digital forensics team

Answer: A

Q761. How should an incident response team handle evidence during a ransomware attack?

A. Immediately paying the ransom to recover files before collecting any forensic evidence
B. Deleting the ransom note to prevent panic among employees and organizational leadership
C. Formatting all affected systems right away to eliminate the ransomware infection quickly
D. Preserving encrypted files and ransom notes as evidence before attempting any recovery

Answer: D

Q762. What is the difference between short-term and long-term containment?

A. Short-term involves rebuilding systems while long-term involves monitoring for threat recurrence
B. Short-term takes days to implement while long-term is applied within the first few minutes
C. Short-term stops immediate damage while long-term implements durable fixes allowing investigation
D. Short-term is performed by management while long-term is handled by the technical team

Answer: C

Q763. What is the purpose of tabletop exercises in incident response?

A. Testing network bandwidth by sending large amounts of simulated attack traffic
B. Simulating incident scenarios through discussion to test plans and identify gaps
C. Training new employees on how to use desktop computers and office applications
D. Reviewing the physical layout of office furniture to optimize workspace ergonomics

Answer: B

Q764. What is an indicator of compromise (IoC)?

A. A financial indicator showing the cost of recovering from a security breach event
B. Observable evidence that a system or network may have been breached by an attacker
C. A metric measuring the overall compromise between security and user convenience
D. A performance metric tracking system uptime percentage across all business hours

Answer: B

Q765. When should law enforcement be notified during an incident response?

A. When the incident involves criminal activity, data breaches with legal requirements, or national security
B. Only after the incident has been fully resolved and all systems have been restored to normal
C. Law enforcement should never be notified as it could compromise the internal investigation
D. Immediately for every security event regardless of severity or type of incident detected

Answer: A

Q766. What is the purpose of incident severity classification?

A. Categorizing incidents by impact level to determine appropriate response and resource allocation
B. Ranking incident response team members by their seniority within the organizational hierarchy
C. Sorting incident tickets alphabetically by the name of the person who reported them
D. Classifying incidents by the time of day they occurred for shift scheduling optimization

Answer: A

Q767. What is the role of threat intelligence in incident response?

A. Providing context about threats, attacker tactics, and IoCs to improve detection and response
B. Generating marketing reports about the organization's security posture for stakeholders
C. Replacing the need for incident response teams by using artificial intelligence for defense
D. Automatically blocking all threats without requiring any human intervention or analysis

Answer: A

Q768. What is a playbook in incident response?

A. A predefined set of procedures for handling specific types of security incidents consistently
B. A report template used for documenting the final results of completed investigations
C. A catalog of all security tools and their license keys used by the response team
D. A training manual for new employees covering general workplace policies and procedures

Answer: A

Q769. What is the purpose of an incident response retainer with a third-party provider?

A. Hiring permanent full-time security staff through a third-party recruitment agency partner
B. Ensuring expert incident response resources are available on-demand when a major incident occurs
C. Purchasing cyber insurance to cover the financial costs of future data breach events
D. Outsourcing all daily security monitoring operations to a third-party managed service provider

Answer: B

Q770. What is a war room in incident response?

A. A dedicated space where the response team coordinates and manages a major incident together
B. A secure server room where all critical infrastructure is housed during normal operations
C. A virtual meeting room used for daily stand-up meetings about project status and updates
D. A training facility where employees practice responding to simulated physical emergencies

Answer: A

Q771. How does user and entity behavior analytics (UEBA) enhance security monitoring?

A. By monitoring only privileged user accounts and ignoring standard employee activities
B. By replacing SIEM systems entirely with machine learning based threat detection tools
C. By blocking all user activities that deviate from a predefined list of approved actions
D. By establishing behavioral baselines and detecting anomalies that indicate potential threats

Answer: D

Q772. What is the difference between signature-based and anomaly-based detection?

A. Signature-based matches known patterns while anomaly-based detects deviations from normal behavior
B. Signature-based requires more computing resources than anomaly-based detection methods do
C. Signature-based is used for network monitoring while anomaly-based is used only for endpoints
D. Signature-based detects unknown threats while anomaly-based only detects previously seen attacks

Answer: A

Q773. What is the purpose of log correlation in SIEM systems?

A. Connecting related events from different sources to identify complex attack patterns
B. Converting all logs into a single standardized format for easier visual reading
C. Backing up log data to secondary storage for disaster recovery preparedness
D. Removing duplicate log entries to reduce storage space requirements on servers

Answer: A

Q774. What is the role of threat intelligence feeds in security monitoring?

A. Automatically patching all vulnerabilities found across the organization's infrastructure
B. Generating monthly compliance reports for regulatory auditors and board presentations
C. Providing up-to-date indicators of compromise to enhance detection rules and alert accuracy
D. Replacing human analysts by automatically investigating and resolving all security alerts

Answer: C

Q775. What is a honeypot used for in security monitoring?

A. Storing encrypted passwords securely in a protected database for authentication use
B. Providing backup internet connectivity when the primary connection fails completely
C. Distributing security patches to all endpoints across the organizational network
D. Attracting attackers to a decoy system to study their techniques and detect intrusions

Answer: D

Q776. What is the challenge of alert fatigue in security operations?

A. Alerts being displayed in colors that are difficult for analysts to distinguish on screens
B. Alerts arriving too slowly for analysts to respond before the threat window has closed
C. Overwhelming analysts with too many alerts causing them to miss genuine threats in the volume
D. Alert systems consuming too much network bandwidth reducing application performance speed

Answer: C

Q777. What is the purpose of a security baseline in monitoring?

A. Establishing normal behavior patterns so deviations can be identified as potential threats
B. Setting the minimum hardware requirements for running security monitoring software tools
C. Defining the maximum number of security alerts allowed per day before system shutdown
D. Creating a template for security reports that must be submitted to regulatory authorities

Answer: A

Q778. What is the role of packet capture (PCAP) in security monitoring?

A. Recording raw network packets for detailed analysis of network communications and attacks
B. Compressing network traffic to reduce bandwidth usage across organizational network links
C. Encrypting network packets to protect data confidentiality during transit between systems
D. Blocking malicious packets from reaching their intended destination on the network

Answer: A

Q779. What is extended detection and response (XDR)?

A. A unified platform integrating detection across endpoints, network, cloud, and email sources
B. A compliance tool that extends audit reporting to cover international regulatory frameworks
C. An advanced firewall that extends network protection to include wireless access points
D. A backup system that extends data retention periods beyond standard policy requirements

Answer: A

Q780. What is the purpose of dark web monitoring for organizations?

A. Purchasing threat intelligence tools that are exclusively available on dark web forums
B. Blocking all organizational users from accessing dark web sites through network filters
C. Detecting if organizational data, credentials, or assets appear on dark web marketplaces
D. Monitoring the dark web to recruit security researchers who operate on hidden platforms

Answer: C

Q781. How does GDPR's 'right to be forgotten' impact organizations?

A. Organizations can ignore deletion requests if the data is stored in encrypted backup archives
B. Organizations must delete all data about a person including legally required financial records
C. Organizations must delete personal data upon request when there is no legitimate reason to retain it
D. The right to be forgotten only applies to social media companies and not other organizations

Answer: C

Q782. What is the difference between data privacy and data security?

A. Privacy is a technical control while security is a legal requirement enforced by regulators
B. Privacy only applies to digital data while security only applies to physical document records
C. Privacy governs how data should be handled while security implements protections against unauthorized access
D. Privacy and security are identical concepts with no meaningful distinction between them in practice

Answer: C

Q783. What is a Data Protection Impact Assessment (DPIA)?

A. An assessment evaluating privacy risks of data processing activities before implementation
B. A financial audit calculating the total cost of data protection measures for budgeting
C. A training evaluation assessing employee knowledge of organizational privacy policies
D. A performance test measuring how fast data protection systems process user requests

Answer: A

Q784. What is the Computer Fraud and Abuse Act (CFAA)?

A. An international treaty establishing global standards for ethical hacking practices
B. A state-level law in California that requires breach notification within 24 hours
C. A European regulation that mandates encryption for all cross-border data transfers
D. A US federal law that criminalizes unauthorized access to protected computer systems

Answer: D

Q785. What is the role of a Data Protection Officer (DPO)?

A. Managing the physical security of the organization's data center facilities full time
B. Selling the organization's data to third parties for approved marketing purposes
C. Overseeing compliance with data protection regulations and serving as a point of contact
D. Developing and maintaining all software applications used by the organization directly

Answer: C

Q786. What is the purpose of PCI DSS?

A. Establishing security standards for organizations that handle credit card payment data
B. Regulating the manufacturing and distribution of personal computer hardware devices
C. Defining standards for physical security of government classified information systems
D. Setting requirements for environmental sustainability in data center construction

Answer: A

Q787. What is the concept of data minimization in privacy law?

A. Collecting only the minimum personal data necessary for the specified legitimate purpose
B. Minimizing the number of employees who know about the organization's privacy practices
C. Compressing personal data to minimize the storage space required on organizational servers
D. Deleting all personal data immediately after collection regardless of business requirements

Answer: A

Q788. What are bug bounty programs and their legal considerations?

A. Programs that penalize employees financially for introducing bugs into production code
B. Programs that pay hackers to attack competitor organizations to find their security weaknesses
C. Programs rewarding researchers for finding vulnerabilities with clear legal scope and authorization
D. Programs offering rewards for reporting software bugs related to user interface design only

Answer: C

Q789. What is the purpose of HIPAA in the United States?

A. Establishing standards for highway infrastructure protection against cyber attacks
B. Protecting the privacy and security of patient health information in healthcare organizations
C. Defining rules for international trade of technology products between countries
D. Regulating the hiring practices of technology companies across the United States market

Answer: B

Q790. What is the legal concept of 'reasonable security measures'?

A. Security controls that are appropriate and proportionate to the risk and data sensitivity involved
B. Security measures dictated entirely by the IT department without legal guidance or oversight
C. The maximum possible security measures regardless of cost or impact on business operations
D. Only the most basic security measures such as passwords without any additional protections

Answer: A

Q791. How does the convergence of IT and OT create new security challenges?

A. OT systems were designed for isolated networks and connecting them to IT increases their attack surface
B. IT and OT convergence eliminates all security risks by combining the strengths of both domains
C. IT and OT convergence only affects manufacturing companies and has no impact on other sectors
D. OT systems are inherently more secure than IT systems and improve the overall security posture

Answer: A

Q792. What is the security concern with large language models (LLMs) in cyber security?

A. LLMs can generate phishing content, discover vulnerabilities, and create malicious code at scale
B. LLMs eliminate all social engineering threats by educating users automatically at all times
C. LLMs cannot process security-related queries and are completely useless for cyber attacks
D. LLMs are only used for defensive security purposes and have no offensive applications whatsoever

Answer: A

Q793. What is Secure Access Service Edge (SASE)?

A. A physical security perimeter around data centers using advanced biometric access controls
B. A software development methodology focused on creating secure edge computing applications
C. A network protocol designed to replace TCP/IP with more secure communication mechanisms
D. A cloud architecture combining network security and WAN capabilities into a single service model

Answer: D

Q794. How does 5G technology introduce new cyber security challenges?

A. 5G networks are slower than 4G making them less attractive targets for cyber attackers
B. 5G only affects mobile phone security and has no impact on enterprise network security
C. Increased device density, network slicing complexity, and expanded attack surface from IoT proliferation
D. 5G eliminates all existing cyber threats through its built-in advanced security architecture

Answer: C

Q795. What is the concept of security mesh architecture?

A. A physical mesh network used for building security camera systems in large corporate offices
B. A decorative pattern used in security badge design for employee identification purposes
C. A distributed security approach that extends controls around individuals and assets regardless of location
D. A single centralized security platform that manages all security controls from one location

Answer: C

Q796. What is the security impact of digital twins in industrial environments?

A. Digital twins can be used to simulate attacks and test defenses without risking physical systems
B. Digital twins automatically patch vulnerabilities in physical systems they are connected to
C. Digital twins are identical copies of malware used by security researchers in sandboxed environments
D. Digital twins eliminate all physical security requirements for industrial control systems completely

Answer: A

Q797. What is privacy-enhancing technology (PET)?

A. Software that automatically deletes all browsing history and cookies after each web session
B. Physical barriers installed around servers to prevent unauthorized personnel from viewing screens
C. Technologies that enable data processing while minimizing personal data exposure and privacy risks
D. Traditional encryption methods that have been rebranded with a more modern marketing name

Answer: C

Q798. How does autonomous vehicle security present unique cyber security challenges?

A. Autonomous vehicles use isolated systems with no network connectivity eliminating all cyber risks
B. Autonomous vehicle security is identical to traditional computer security with no unique requirements
C. Compromised vehicle systems could endanger physical safety, requiring real-time security with minimal latency
D. Autonomous vehicles are immune to cyber attacks because they use proprietary operating systems

Answer: C

Q799. What is the concept of cyber-physical systems security?

A. Securing the physical locks and barriers that protect server rooms from unauthorized entry
B. Protecting integrated systems where digital components interact with and control physical processes
C. Installing physical firewalls in the walls of data centers to prevent electromagnetic leaks
D. Developing software applications that run on both mobile phones and desktop computers

Answer: B

Q800. What is the emerging concept of security-as-code?

A. Defining and managing security policies and controls as code within the development pipeline
B. Replacing all security hardware appliances with software-only solutions running on general servers
C. Writing malware using programming languages instead of using automated malware creation tools
D. Teaching security professionals how to write code for developing custom vulnerability scanners

Answer: A

Q801. What is the primary distinction between a vulnerability scan and a penetration test?

A. Vulnerability scans are illegal while penetration tests are legal
B. Vulnerability scans identify weaknesses while penetration tests actively exploit them
C. Vulnerability scans are more expensive than penetration tests
D. Penetration tests only check for viruses

Answer: B

Q802. In the context of cyber security, what is 'due diligence'?

A. Ignoring minor security incidents
B. The practice of thoroughly investigating and understanding security risks before making decisions
C. Using only open-source security tools
D. Delegating all security to third parties

Answer: B

Q803. What distinguishes a 'grey hat' hacker from a 'white hat' and 'black hat' hacker?

A. Grey hats only hack government systems
B. Grey hats may find vulnerabilities without authorization but do not have malicious intent
C. Grey hats only use automated tools
D. Grey hats exclusively perform social engineering

Answer: B

Q804. What is the purpose of a cyber security maturity model?

A. To measure internet speed across an organization
B. To assess an organization's security capabilities and identify areas for improvement
C. To rank employees by technical skill
D. To determine which antivirus to purchase

Answer: B

Q805. How does 'defense in depth' differ from relying on a single security control?

A. Defense in depth uses only physical controls
B. Defense in depth employs multiple layers of security so that if one fails, others still protect
C. Single security controls are always more effective
D. Defense in depth only applies to cloud environments

Answer: B

Q806. What role does asset management play in cyber security?

A. It only tracks the financial value of equipment
B. It helps organizations identify what needs protecting and ensures proper security controls are applied
C. It replaces the need for access controls
D. It is only relevant for physical security

Answer: B

Q807. What is the difference between a proactive and reactive security approach?

A. Proactive security responds after an incident while reactive security prevents them
B. Proactive security anticipates and prevents threats before they occur, while reactive responds after an incident
C. There is no difference between the two approaches
D. Reactive security is always more cost-effective

Answer: B

Q808. What is the significance of compliance frameworks like ISO 27001 in cyber security?

A. They eliminate all cyber threats automatically
B. They provide standards and guidelines for establishing information security management systems
C. They are only applicable to government organizations
D. They replace the need for technical security controls

Answer: B

Q809. What is a security control in the context of cyber security?

A. A device used to lock server rooms only
B. A safeguard or countermeasure to avoid, detect, or minimize security risks
C. A type of malware detection algorithm
D. A firewall brand name

Answer: B

Q810. Why is third-party risk management important in cyber security?

A. Third parties never pose security risks
B. Vendors and partners with access to your systems can introduce vulnerabilities if not properly managed
C. It is only needed for financial institutions
D. Third-party risks only affect large enterprises

Answer: B

Q811. What is the difference between a corrective and a compensating security control?

A. They are identical in function
B. A corrective control restores systems after an incident, while a compensating control provides an alternative when a primary control cannot be implemented
C. Corrective controls prevent incidents while compensating controls detect them
D. Compensating controls are always more expensive than corrective controls

Answer: B

Q812. How does the principle of 'defense in depth' apply to data protection?

A. By using only one very strong encryption algorithm
B. By applying multiple layers of security controls such as encryption, access controls, monitoring, and backups
C. By relying solely on physical security measures
D. By giving all employees access to all data for transparency

Answer: B

Q813. What is the purpose of a business impact analysis (BIA) in information security?

A. To determine the salary of security staff
B. To identify critical business functions and the impact of disruptions on the organization
C. To select antivirus software vendors
D. To audit employee attendance records

Answer: B

Q814. What distinguishes a technical control from an administrative control in security?

A. Technical controls are always more effective
B. Technical controls are implemented through technology while administrative controls are implemented through policies and procedures
C. Administrative controls are not used in modern security
D. Technical controls do not require any maintenance

Answer: B

Q815. What is the concept of 'security by design' in information security?

A. Adding security features only after deployment
B. Integrating security considerations into every phase of system design and development from the beginning
C. Designing systems with no security to keep them simple
D. Using only open-source security tools in design

Answer: B

Q816. How does quantitative risk analysis differ from qualitative risk analysis?

A. Quantitative analysis uses numerical values and financial metrics while qualitative uses descriptive categories like high, medium, and low
B. Qualitative analysis is always more accurate
C. Quantitative analysis does not consider financial impact
D. They produce identical results using different terminology

Answer: A

Q817. What is the purpose of a data retention policy?

A. To keep all data indefinitely for compliance
B. To define how long data should be stored, when it should be deleted, and how disposal should occur
C. To prevent any data from being deleted
D. To maximize storage utilization on servers

Answer: B

Q818. What is the 'need to know' principle and how does it complement least privilege?

A. It means everyone needs to know everything for transparency
B. It restricts access to information based on job necessity, working alongside least privilege to limit both permissions and information access
C. It only applies to classified government information
D. It replaces the need for access control lists

Answer: B

Q819. What is the role of a security operations center (SOC) in an organization?

A. To develop new software applications
B. To centrally monitor, detect, analyze, and respond to security incidents in real time
C. To manage human resources records
D. To handle customer billing inquiries

Answer: B

Q820. What is the difference between data at rest, data in transit, and data in use?

A. They all refer to the same state of data
B. Data at rest is stored, data in transit is being transmitted, and data in use is actively being processed in memory
C. Data in use is always more secure than data at rest
D. Data in transit cannot be encrypted

Answer: B

Q821. What is the primary difference between a block cipher and a stream cipher in terms of data processing?

A. Block ciphers are always more secure
B. Block ciphers encrypt fixed-size blocks of data while stream ciphers encrypt data one bit or byte at a time
C. Stream ciphers cannot use keys
D. Block ciphers do not use initialization vectors

Answer: B

Q822. What is a certificate revocation list (CRL) used for?

A. To list all valid certificates in use
B. To publish a list of digital certificates that have been revoked before their expiration date
C. To generate new cryptographic keys
D. To store encrypted email messages

Answer: B

Q823. How does the Diffie-Hellman key exchange enable secure communication without prior shared secrets?

A. It sends the encryption key in plaintext
B. It allows two parties to jointly establish a shared secret over an insecure channel using mathematical operations
C. It requires a trusted third party to distribute keys
D. It only works on encrypted networks

Answer: B

Q824. What is the purpose of a message digest in cryptography?

A. To compress messages for faster transmission
B. To produce a fixed-length fingerprint of data that can verify its integrity
C. To encrypt messages using symmetric keys
D. To generate random encryption keys

Answer: B

Q825. What is the Online Certificate Status Protocol (OCSP) and how does it differ from CRL?

A. OCSP replaces encryption entirely
B. OCSP provides real-time certificate validation by querying the CA directly, unlike CRLs which are periodically published lists
C. OCSP is a type of symmetric encryption
D. OCSP and CRL are identical mechanisms

Answer: B

Q826. Why is AES considered more secure than DES for modern encryption needs?

A. AES uses shorter keys than DES
B. AES supports key lengths of 128, 192, and 256 bits while DES uses only 56-bit keys, making DES vulnerable to brute-force attacks
C. DES is newer than AES
D. AES is an asymmetric algorithm while DES is symmetric

Answer: B

Q827. What is key escrow and what security concern does it raise?

A. Key escrow means destroying keys after use
B. Key escrow involves storing copies of encryption keys with a trusted third party, raising concerns about unauthorized access to those keys
C. Key escrow is a method of key generation
D. Key escrow only applies to physical locks

Answer: B

Q828. What is a chosen-plaintext attack in cryptanalysis?

A. An attack where the attacker can only observe ciphertext
B. An attack where the attacker can choose arbitrary plaintexts and obtain their corresponding ciphertexts to deduce the key
C. An attack that only targets hash functions
D. An attack that requires physical access to the encryption device

Answer: B

Q829. What is the role of an initialization vector (IV) in encryption?

A. It replaces the encryption key
B. It adds randomness to the encryption process so that identical plaintexts produce different ciphertexts
C. It determines the key length
D. It is used only in hash functions

Answer: B

Q830. What is envelope encryption and where is it commonly used?

A. Encrypting physical mail envelopes
B. A technique where data is encrypted with a data key, and the data key is then encrypted with a master key, commonly used in cloud services
C. Using two different symmetric algorithms simultaneously
D. Encrypting only email attachments

Answer: B

Q831. What is the difference between a network-based IDS and a host-based IDS?

A. They monitor the same traffic in the same way
B. A network-based IDS monitors network traffic on a network segment, while a host-based IDS monitors activity on an individual host system
C. Host-based IDS is always more effective
D. Network-based IDS can only monitor wireless traffic

Answer: B

Q832. How does network address translation (NAT) provide a layer of security?

A. NAT encrypts all outgoing traffic
B. NAT hides internal IP addresses from external networks, making it harder for attackers to directly target internal devices
C. NAT replaces the need for firewalls entirely
D. NAT increases network bandwidth

Answer: B

Q833. What is the purpose of a network demilitarized zone (DMZ) architecture?

A. To eliminate the need for internal firewalls
B. To place public-facing services in an isolated network segment between the external and internal networks
C. To directly expose internal servers to the internet
D. To increase internal network speeds

Answer: B

Q834. What is SSL stripping and how does it compromise network security?

A. Removing physical cables from network equipment
B. A man-in-the-middle technique that downgrades HTTPS connections to HTTP, exposing data in plaintext
C. A method of improving SSL performance
D. A technique for updating SSL certificates

Answer: B

Q835. What is the purpose of network flow analysis in security monitoring?

A. To increase network throughput
B. To collect and analyze metadata about network connections (source, destination, ports, protocols, volume) to detect anomalies and threats
C. To encrypt all network traffic
D. To replace packet capture entirely

Answer: B

Q836. How does a proxy firewall (application-level gateway) differ from a packet-filtering firewall?

A. Proxy firewalls are always slower and less secure
B. A proxy firewall inspects traffic at the application layer and acts as an intermediary, while a packet filter only examines packet headers
C. Packet-filtering firewalls provide more granular inspection
D. Proxy firewalls cannot filter web traffic

Answer: B

Q837. What is MAC address spoofing and why is it a security concern?

A. It is a method of encrypting MAC addresses
B. An attacker changes their device's MAC address to impersonate another device, potentially bypassing MAC-based access controls
C. MAC addresses cannot be changed
D. MAC spoofing only affects wireless networks

Answer: B

Q838. What is the security benefit of implementing network segmentation with micro-segmentation?

A. It eliminates the need for any firewalls
B. It limits lateral movement by creating granular security zones around individual workloads, even within the same network segment
C. Micro-segmentation only applies to cloud environments
D. It increases network latency without security benefits

Answer: B

Q839. What is DNS cache poisoning and what risk does it pose?

A. Clearing the DNS cache for performance
B. An attack that inserts fraudulent DNS entries into a resolver's cache, redirecting users to malicious websites
C. A method of improving DNS performance
D. DNS caches cannot be manipulated

Answer: B

Q840. What is the purpose of implementing 802.1Q VLAN tagging?

A. To encrypt VLAN traffic
B. To identify which VLAN a frame belongs to as it traverses trunk links between switches, enabling logical network separation
C. To replace IP addressing on the network
D. To increase the maximum number of physical ports on a switch

Answer: B

Q841. What is the primary difference between CBC and CTR modes of operation in block ciphers?

A. CBC encrypts blocks independently while CTR chains them together
B. CTR mode turns a block cipher into a stream cipher allowing parallel encryption
C. CBC is faster than CTR in all cases
D. CTR requires a larger key size than CBC

Answer: B

Q842. What is the purpose of key derivation functions like HKDF?

A. To compress encryption keys for storage
B. To derive one or more cryptographic keys from a source of key material
C. To generate public-private key pairs
D. To verify digital signatures

Answer: B

Q843. How does authenticated encryption differ from standard encryption?

A. Authenticated encryption is slower but uses smaller keys
B. Authenticated encryption requires two separate algorithms always
C. Authenticated encryption provides both confidentiality and integrity/authenticity in a single operation
D. Authenticated encryption only works with asymmetric algorithms

Answer: C

Q844. What is the security implication of using a predictable initialization vector (IV)?

A. It has no security impact
B. It can enable chosen-plaintext attacks and leak information about encrypted data
C. It only affects performance, not security
D. It makes decryption impossible

Answer: B

Q845. What is Galois/Counter Mode (GCM) and why is it preferred for modern encryption?

A. A hash function that replaces SHA-256
B. An authenticated encryption mode providing both confidentiality and integrity with high performance
C. A key exchange protocol replacing Diffie-Hellman
D. A digital signature algorithm

Answer: B

Q846. What is the purpose of a cryptographic nonce and how does it differ from an IV?

A. They are identical concepts with no difference
B. A nonce is used only once and may not need to be random, while an IV typically needs to be unpredictable
C. A nonce is always longer than an IV
D. An IV is used in symmetric encryption while a nonce is for asymmetric only

Answer: B

Q847. What is the Diffie-Hellman key exchange vulnerable to without authentication?

A. Brute force attacks
B. Man-in-the-middle attacks
C. Replay attacks
D. Dictionary attacks

Answer: B

Q848. What is the role of a Merkle tree in cryptography?

A. To store encryption keys hierarchically
B. To efficiently verify data integrity using a tree of hashes
C. To generate random numbers
D. To perform key exchange between multiple parties

Answer: B

Q849. Why is SHA-1 considered deprecated for security purposes?

A. It produces output that is too long
B. It is too slow for modern systems
C. Practical collision attacks have been demonstrated against it
D. It only works with symmetric encryption

Answer: C

Q850. What is the concept of crypto-agility?

A. The ability to switch between encryption algorithms quickly without major system changes
B. Using multiple encryption algorithms simultaneously on all data
C. Encrypting data faster than real-time
D. The ability to break any encryption algorithm

Answer: A

Q851. What is the role of AppArmor in Linux security?

A. A firewall management tool
B. A mandatory access control system that restricts programs' capabilities based on per-program profiles
C. A disk encryption utility
D. A network monitoring tool

Answer: B

Q852. What is the difference between discretionary access control (DAC) and role-based access control (RBAC)?

A. DAC and RBAC are identical
B. In DAC, the resource owner sets permissions; in RBAC, permissions are assigned based on organizational roles
C. DAC is more secure than RBAC in all cases
D. RBAC allows users to share permissions freely

Answer: B

Q853. What is a privilege escalation attack and what are its two types?

A. An attack that only affects network devices, divided into internal and external
B. An attack that gains elevated access, divided into horizontal (accessing other users' resources) and vertical (gaining higher privileges)
C. An attack that targets passwords only, divided into online and offline
D. An attack on physical security, divided into tailgating and piggybacking

Answer: B

Q854. What is Windows BitLocker and what does it protect against?

A. A network firewall for Windows
B. Full disk encryption that protects data on lost or stolen devices by encrypting the entire volume
C. An antivirus program
D. A password manager

Answer: B

Q855. How does the Linux sudo command enhance security compared to logging in as root?

A. sudo is less secure than root login
B. sudo provides temporary elevated privileges with logging and accountability, reducing the risk of accidental system-wide damage
C. sudo grants permanent root access
D. sudo disables all security features

Answer: B

Q856. What is the purpose of System Integrity Protection (SIP) in macOS?

A. To encrypt user files
B. To restrict the root account from modifying protected system files and processes
C. To manage network connections
D. To install system updates

Answer: B

Q857. What are cgroups in Linux and how do they contribute to security?

A. A type of firewall rule
B. Control groups that limit, account for, and isolate the resource usage of process groups
C. A user authentication mechanism
D. A file encryption method

Answer: B

Q858. What is the security purpose of UEFI Secure Boot?

A. To speed up the boot process
B. To ensure only trusted, digitally signed software can run during the boot process, preventing bootkits
C. To encrypt the hard drive
D. To manage user accounts at boot time

Answer: B

Q859. What is the purpose of audit policies in Windows operating systems?

A. To track software licenses
B. To define which security events are recorded in the event log for monitoring and forensics
C. To manage desktop appearances
D. To control internet bandwidth

Answer: B

Q860. How does memory protection through W^X (Write XOR Execute) policy improve OS security?

A. It doubles available memory
B. It ensures memory pages are either writable or executable but never both, preventing code injection attacks
C. It encrypts all memory contents
D. It speeds up memory access

Answer: B

Q861. What is the security purpose of the X-Content-Type-Options header?

A. To encrypt content between browser and server
B. To prevent browsers from MIME-sniffing a response away from the declared content-type, stopping content-type confusion attacks
C. To compress HTTP responses
D. To cache web pages more effectively

Answer: B

Q862. How does a web application firewall (WAF) differ from a traditional network firewall?

A. They are identical in function
B. A WAF inspects HTTP/HTTPS traffic at the application layer to detect attacks like XSS and SQL injection, while network firewalls operate at lower layers
C. A WAF only blocks IP addresses
D. Network firewalls can inspect application-layer content better

Answer: B

Q863. What is the security risk of exposing source maps in a production web application?

A. Source maps slow down the server
B. Source maps reveal original source code structure and logic, aiding attackers in finding vulnerabilities
C. Source maps corrupt the database
D. Source maps have no security impact

Answer: B

Q864. What is a Server-Side Template Injection (SSTI) attack?

A. Injecting CSS into server templates
B. Injecting malicious code into server-side template engines that gets executed on the server, potentially leading to remote code execution
C. Injecting JavaScript into the client browser
D. Modifying HTML templates in a text editor

Answer: B

Q865. What is the purpose of the SameSite cookie attribute and what values can it take?

A. It determines cookie expiration time with values of Short, Medium, and Long
B. It controls when cookies are sent with cross-site requests, with values Strict, Lax, and None, helping prevent CSRF attacks
C. It sets the cookie's encryption strength
D. It determines which users can see the cookie

Answer: B

Q866. What is an XML External Entity (XXE) attack?

A. A cross-site scripting attack using XML
B. An attack exploiting XML parsers that process external entity references, potentially leading to file disclosure, SSRF, or denial of service
C. An attack that replaces XML with JSON
D. A SQL injection through XML queries

Answer: B

Q867. What is the security concern with JWT tokens stored in localStorage?

A. localStorage is too small for JWT tokens
B. JWTs in localStorage are accessible to JavaScript and vulnerable to XSS attacks, unlike HttpOnly cookies
C. localStorage automatically encrypts JWTs
D. There are no concerns with this approach

Answer: B

Q868. What is a subdomain takeover vulnerability?

A. When a subdomain loads too slowly
B. When an attacker claims a subdomain that points to an external service the organization no longer uses, enabling phishing or cookie theft
C. When a subdomain uses a different TLS certificate
D. When subdomains share the same database

Answer: B

Q869. How does Content Security Policy (CSP) report-only mode help in deploying security headers?

A. It blocks all violations immediately
B. It logs policy violations without enforcing them, allowing developers to test and refine CSP rules before enforcement
C. It only works in development environments
D. It disables all scripts on the page

Answer: B

Q870. What is a broken access control vulnerability in web applications?

A. When the login page does not load properly
B. When users can access resources or perform actions beyond their intended permissions due to improper authorization checks
C. When CSS styles are not applied correctly
D. When the server cannot handle multiple users

Answer: B

Q871. What is credential stuffing and how does it differ from brute-force attacks?

A. They are the same type of attack
B. Credential stuffing uses stolen username-password pairs from data breaches to try on other services, while brute-force tries random combinations
C. Credential stuffing only targets email accounts
D. Brute-force uses stolen credentials while credential stuffing does not

Answer: B

Q872. How does TOTP (Time-Based One-Time Password) authentication work?

A. It sends a password via email each time
B. It uses a shared secret and current time to generate a unique code that is valid for a short period, typically 30 seconds
C. It uses facial recognition technology
D. It generates a permanent second password

Answer: B

Q873. What is the difference between RBAC and ABAC in terms of flexibility?

A. RBAC is more flexible than ABAC
B. ABAC is more flexible because it can use multiple attributes (user, resource, environment, action) for access decisions, while RBAC is based only on predefined roles
C. They are equally flexible
D. Neither is flexible

Answer: B

Q874. What is the purpose of a challenge-response authentication protocol?

A. To test the user's typing speed
B. To verify identity by requiring the client to correctly respond to a random challenge from the server, proving knowledge without transmitting the secret
C. To challenge users with security questions only
D. To respond to denial-of-service attacks

Answer: B

Q875. What is identity federation and what problem does it solve?

A. Creating multiple identities for one user
B. Allowing users to authenticate across multiple organizations using a single identity from a trusted identity provider, reducing credential sprawl
C. Combining all passwords into one
D. Disabling authentication for external users

Answer: B

Q876. What is the security risk of using SMS-based two-factor authentication?

A. SMS 2FA has no security risks
B. SMS messages can be intercepted through SIM swapping, SS7 protocol vulnerabilities, or phone number porting, compromising the second factor
C. SMS 2FA is the most secure method available
D. SMS 2FA only works on smartphones

Answer: B

Q877. What is the concept of separation of duties in access control?

A. Giving all duties to one person
B. Dividing critical tasks among multiple users so no single person has complete control over a sensitive process, preventing fraud and errors
C. Separating work and personal accounts
D. Dividing the network into segments

Answer: B

Q878. What is an access token in the context of API authentication?

A. A physical token used to enter a building
B. A digital credential that represents the authorization granted to a client to access specific API resources on behalf of a user
C. A password stored in plain text
D. A certificate installed on the server

Answer: B

Q879. How does multi-factor authentication using a hardware security key work?

A. The key stores the user's password
B. The key uses public-key cryptography to create a unique credential per site, signing challenges without transmitting secrets
C. The key generates random passwords
D. The key connects to the internet to verify identity

Answer: B

Q880. What is the purpose of an identity governance and administration (IGA) platform?

A. To manage website content
B. To automate identity lifecycle management, access certifications, and policy enforcement across an organization
C. To encrypt all user data
D. To monitor network bandwidth

Answer: B

Q881. What is the DREAD threat rating model used for?

A. Ranking programming languages by security
B. Assessing and prioritizing threats based on Damage, Reproducibility, Exploitability, Affected Users, and Discoverability
C. Rating the performance of security tools
D. Evaluating developer skill levels

Answer: B

Q882. What is the purpose of a security code review and how does it differ from a regular code review?

A. They are identical processes
B. A security code review specifically focuses on identifying security vulnerabilities, insecure patterns, and compliance issues in addition to regular code quality concerns
C. Security code reviews only look at encryption code
D. Regular code reviews already cover all security concerns

Answer: B

Q883. What is the principle of fail-secure versus fail-open in software design?

A. They mean the same thing
B. Fail-secure denies access when a failure occurs, maintaining security; fail-open allows access during failures, prioritizing availability over security
C. Fail-secure means the system never fails
D. Fail-open means the system is always secure

Answer: B

Q884. How does a software composition analysis (SCA) tool help secure development?

A. By writing code automatically
B. By identifying known vulnerabilities in open-source dependencies and third-party libraries used in the project
C. By testing network security
D. By managing development team schedules

Answer: B

Q885. What is the security benefit of implementing Content Security Policy headers during development?

A. CSP speeds up page loading
B. CSP restricts which resources the browser can load, reducing the impact of XSS attacks by preventing execution of unauthorized scripts
C. CSP encrypts HTTP traffic
D. CSP manages user sessions

Answer: B

Q886. What is the role of a CI/CD security gate and what checks should it include?

A. It blocks all deployments permanently
B. It enforces automated security checks in the build pipeline including SAST, dependency scanning, and secret detection before code can be deployed
C. It only checks code formatting
D. It is a physical security checkpoint

Answer: B

Q887. What is the OWASP Application Security Verification Standard (ASVS)?

A. A programming language standard
B. A framework providing a basis for testing web application security controls through three levels of security verification requirements
C. A network protocol standard
D. A hardware security specification

Answer: B

Q888. What is the security concern with using eval() or similar dynamic code execution functions?

A. eval() is too slow for production use
B. eval() executes strings as code, and if user input reaches eval(), it enables arbitrary code execution attacks
C. eval() only works in specific languages
D. eval() causes memory leaks

Answer: B

Q889. What is the security purpose of input allowlisting versus blocklisting?

A. Blocklisting is always more secure than allowlisting
B. Allowlisting defines what input IS permitted (more secure), while blocklisting defines what IS NOT permitted (prone to bypasses through new attack patterns)
C. Allowlisting blocks all input
D. They provide identical security

Answer: B

Q890. What is the purpose of security regression testing in the SDLC?

A. Testing if the application runs on older systems
B. Verifying that previously fixed security vulnerabilities have not been reintroduced by new code changes
C. Testing the application's speed under load
D. Checking if old features still work

Answer: B

Q891. What is the security difference between WPA2-Personal and WPA2-Enterprise?

A. There is no security difference
B. WPA2-Personal uses a shared passphrase for all users while WPA2-Enterprise uses individual credentials authenticated through a RADIUS server, providing better accountability
C. WPA2-Personal is more secure
D. WPA2-Enterprise is only for home networks

Answer: B

Q892. What is a captive portal and what security risks does it present?

A. A portal that captures all network traffic permanently
B. A web page that requires user interaction before granting network access; risks include credential theft on fake portals and unencrypted initial connections
C. A firewall configuration tool
D. A type of network encryption

Answer: B

Q893. How does mobile application sandboxing protect the operating system?

A. It runs all apps in a virtual sandbox visual environment
B. Each app runs in its own isolated environment with restricted access to system resources and other apps' data, containing any malicious behavior
C. It prevents apps from using the internet
D. It only protects pre-installed apps

Answer: B

Q894. What is a wireless deauthentication attack and how does it work?

A. An attack that changes WiFi passwords
B. An attack that sends forged deauthentication frames to disconnect clients from a WiFi network, often used as a precursor to evil twin attacks
C. An attack that disables Bluetooth only
D. An attack that overheats wireless routers

Answer: B

Q895. What is the security purpose of mobile device attestation?

A. Verifying the user's identity
B. Cryptographically verifying the integrity and security state of a mobile device (that it has not been rooted, jailbroken, or tampered with) before granting access to resources
C. Attesting to the device's warranty status
D. Checking the device's battery health

Answer: B

Q896. What is the role of 802.1X in wireless network security?

A. It defines WiFi frequency bands
B. It provides port-based network access control requiring devices to authenticate before being granted network access, using EAP methods and a RADIUS server
C. It sets maximum WiFi speeds
D. It determines wireless signal range

Answer: B

Q897. What are the security implications of using public USB charging stations for mobile devices?

A. Public USB chargers are always safe
B. They pose a risk of 'juice jacking' where modified charging stations can install malware or steal data through the USB data connection
C. They charge devices faster than private chargers
D. They only affect older devices

Answer: B

Q898. What is WiFi Protected Setup (WPS) and why is it considered a security risk?

A. WPS provides the highest WiFi security available
B. WPS simplifies WiFi setup but its PIN-based method is vulnerable to brute-force attacks due to a design flaw that splits the 8-digit PIN into two halves
C. WPS only works with WPA3
D. WPS is required for all modern routers

Answer: B

Q899. How does a mobile VPN protect data on public WiFi networks?

A. It makes the WiFi network faster
B. It creates an encrypted tunnel between the mobile device and the VPN server, protecting all data from eavesdropping on the local network
C. It blocks all incoming calls
D. It only protects web browsing, not apps

Answer: B

Q900. What is the purpose of MAC address randomization on mobile devices?

A. To improve WiFi speed
B. To prevent tracking of the device across different WiFi networks by changing the hardware address used during scanning and connecting
C. To authenticate to WiFi networks
D. To encrypt wireless traffic

Answer: B

Q901. What is the principle of shared responsibility in cloud security and how does it vary by service model?

A. The cloud provider is responsible for all security
B. In IaaS, customers manage OS and application security; in PaaS, the provider manages the platform; in SaaS, the provider handles nearly everything except user access and data classification
C. The customer is responsible for all security
D. Shared responsibility means both parties do the same tasks

Answer: B

Q902. What is the security risk of overly permissive S3 bucket policies in AWS?

A. S3 buckets cannot be made public
B. Overly permissive policies can expose sensitive data to the public internet, leading to data breaches as seen in numerous high-profile incidents
C. Permissive policies improve performance
D. S3 bucket policies do not affect security

Answer: B

Q903. What is cloud-native logging and monitoring and why is it critical for security?

A. It is the same as traditional on-premises logging
B. Cloud-native logging aggregates logs from distributed cloud services (API calls, access events, resource changes) for security monitoring, threat detection, and compliance auditing
C. It only monitors server uptime
D. It replaces the need for security controls

Answer: B

Q904. What is a service mesh in cloud-native architecture and how does it enhance security?

A. A physical network of cloud servers
B. An infrastructure layer that handles service-to-service communication with built-in security features like mutual TLS, access policies, and traffic encryption without application code changes
C. A type of cloud storage
D. A mesh WiFi network for cloud data centers

Answer: B

Q905. What are cloud access security brokers (CASBs) and what four pillars of functionality do they provide?

A. CASBs only block cloud access
B. CASBs provide visibility, data security, threat protection, and compliance for cloud services by acting as intermediaries between users and cloud providers
C. CASBs are a type of cloud storage
D. CASBs only monitor bandwidth usage

Answer: B

Q906. What is infrastructure as code (IaC) security scanning and why is it important?

A. It scans physical infrastructure for defects
B. It analyzes IaC templates (Terraform, CloudFormation) for security misconfigurations before deployment, preventing insecure infrastructure from being provisioned
C. It scans code for programming errors only
D. It is only used for cost optimization

Answer: B

Q907. What is the blast radius concept in cloud architecture and how can it be minimized?

A. The physical distance a cloud data center's explosion can reach
B. The extent of damage that can result from a security incident; minimized through network segmentation, separate accounts, least privilege, and micro-segmentation
C. The WiFi signal range of cloud servers
D. The number of users affected by a cloud outage

Answer: B

Q908. What is the security purpose of a cloud-native web application firewall versus a traditional WAF?

A. They are identical in functionality
B. Cloud-native WAFs are designed for dynamic cloud environments with auto-scaling, API protection, bot management, and integration with cloud provider services and DevOps pipelines
C. Cloud-native WAFs are less capable than traditional WAFs
D. Traditional WAFs work better in cloud environments

Answer: B

Q909. What is a landing zone in cloud architecture and how does it relate to security?

A. A physical location where cloud servers are installed
B. A pre-configured, secure baseline environment with account structure, networking, IAM, logging, and security controls that serves as the foundation for cloud deployments
C. A backup storage location
D. A cloud provider's customer support portal

Answer: B

Q910. What is the security risk of using long-lived access keys for cloud service accounts?

A. Long-lived keys are the most secure option
B. Long-lived access keys that are not rotated can be leaked or stolen, providing persistent access; short-lived credentials and role-based access with temporary tokens are preferred
C. Long-lived keys automatically rotate
D. There is no risk with long-lived keys

Answer: B

Q911. What is the role of timestamps (MAC times) in forensic timeline reconstruction?

A. Timestamps are unreliable and never used
B. Modified, Accessed, and Created timestamps on files help establish when events occurred, reconstruct user activities, and build a chronological timeline of events
C. Timestamps only show the current date
D. MAC times refer to Apple computer forensics only

Answer: B

Q912. What is the difference between volatile and non-volatile evidence, and why does collection order matter?

A. All evidence has the same priority for collection
B. Volatile evidence (RAM, running processes, network connections) is lost when power is removed and must be collected first; non-volatile evidence (hard drives) persists and can be collected later
C. Non-volatile evidence must always be collected first
D. The collection order does not affect the investigation

Answer: B

Q913. How does file carving work and when is it necessary in forensic analysis?

A. File carving is a wood-working term not related to forensics
B. File carving recovers files from unallocated disk space by searching for file signatures (headers and footers) without relying on file system metadata, useful when files are deleted or file system is damaged
C. File carving only works on image files
D. File carving requires the original file names

Answer: B

Q914. What is a forensic triage and when is it performed?

A. The final step of a forensic investigation
B. A rapid preliminary assessment of digital evidence to identify the most relevant devices and data, prioritize investigation efforts, and determine the scope of a full forensic examination
C. A medical procedure unrelated to forensics
D. A method of permanently deleting evidence

Answer: B

Q915. What is registry analysis in Windows forensics and what type of evidence can it reveal?

A. Registry analysis only shows software license keys
B. Windows Registry analysis reveals system configuration, recently accessed files, USB device history, installed software, user accounts, network connections, and user activity patterns
C. The registry contains no useful forensic data
D. Registry analysis is only possible on Linux systems

Answer: B

Q916. What is the purpose of using EnCase or FTK in digital forensics?

A. They are video editing software
B. They are comprehensive digital forensic suites that provide evidence acquisition, analysis, search, bookmark, and reporting capabilities for forensic investigations
C. They are antivirus programs
D. They are network monitoring tools

Answer: B

Q917. What is network packet capture (PCAP) analysis in forensic investigations?

A. A method of capturing physical evidence
B. Analysis of recorded network traffic data to identify communications, data transfers, malware command-and-control traffic, and evidence of network-based attacks
C. A technique for capturing screenshots
D. A method of printing network diagrams

Answer: B

Q918. What is the significance of examining browser artifacts in a forensic investigation?

A. Browser artifacts only show bookmarks
B. Browser artifacts including history, cookies, cache, downloads, saved passwords, autofill data, and session data can reveal user activities, communications, and intent
C. Browser data is automatically deleted and cannot be recovered
D. Only the last visited website can be determined

Answer: B

Q919. What is the role of hash sets in forensic analysis?

A. Hash sets encrypt evidence for storage
B. Known hash sets (like NSRL) help forensic investigators quickly identify and filter known-good files (operating system files) and known-bad files (malware) from the evidence
C. Hash sets are random number generators
D. Hash sets delete duplicate files

Answer: B

Q920. What is the difference between a forensic investigation for civil versus criminal cases?

A. There is no difference in forensic methodology
B. Criminal cases require higher standards of evidence (beyond reasonable doubt), stricter chain of custody, and may involve law enforcement; civil cases use preponderance of evidence and may be conducted by private firms
C. Civil cases require more evidence than criminal cases
D. Digital forensics is only used in criminal cases

Answer: B

Q921. What is the role of threat intelligence in improving incident response capabilities?

A. Threat intelligence is not useful for incident response
B. Threat intelligence provides context about adversary tactics, techniques, and procedures (TTPs) that helps IR teams detect, attribute, and respond to incidents more effectively
C. Threat intelligence only helps with marketing
D. Threat intelligence replaces the need for incident response

Answer: B

Q922. How do tabletop exercises improve incident response preparedness?

A. They test physical security of table-mounted servers
B. They simulate incident scenarios through discussion-based exercises, testing communication, decision-making, and plan effectiveness without disrupting actual systems
C. They are physical fitness exercises for the IR team
D. They only test technical controls

Answer: B

Q923. What is the importance of establishing communication channels before an incident occurs?

A. Communication planning is not important for incident response
B. Pre-established out-of-band communication channels ensure the IR team can communicate securely during an incident, even if the attacker has compromised normal communication systems
C. Only email communication is needed
D. Communication should only be planned during the incident

Answer: B

Q924. What is the difference between eradication and remediation in incident response?

A. They are identical concepts
B. Eradication removes the immediate threat (malware, attacker access) while remediation addresses the underlying vulnerability or weakness that allowed the incident to occur
C. Eradication is a permanent solution while remediation is temporary
D. Remediation happens before eradication

Answer: B

Q925. What is a cyber incident severity classification system and why is it important?

A. It classifies incidents by the day of the week they occur
B. A framework that categorizes incidents by impact level to determine response priority, resource allocation, escalation requirements, and notification obligations
C. It only applies to government organizations
D. Severity classification slows down the response

Answer: B

Q926. How should evidence be handled during incident response to ensure it is admissible in court?

A. Evidence handling procedures do not matter for legal proceedings
B. Evidence must be collected following proper procedures including maintaining chain of custody, using write-protected copies, documenting all actions, and preserving original evidence integrity
C. Only digital copies of evidence are needed in court
D. Evidence should be modified to make it clearer for the judge

Answer: B

Q927. What is the role of a crisis communications plan in incident response?

A. It handles technical remediation steps
B. It defines how the organization communicates about the incident to stakeholders, media, customers, and regulators, managing reputation and meeting notification obligations
C. It is only needed for public companies
D. Communication is not part of incident response

Answer: B

Q928. What is the purpose of maintaining an asset inventory for incident response?

A. To track office furniture
B. An up-to-date inventory of all IT assets helps IR teams quickly identify affected systems, understand their criticality, determine blast radius, and prioritize response efforts
C. Asset inventories are only for accounting
D. It is not relevant to incident response

Answer: B

Q929. What is the concept of 'containment before eradication' in incident response?

A. Eradication should always come before containment
B. The incident must be contained (preventing further spread or damage) before eradication begins, because premature eradication may alert the attacker and lose evidence
C. Containment and eradication happen simultaneously always
D. Neither containment nor eradication is necessary

Answer: B

Q930. What is log normalization and why is it important for SIEM effectiveness?

A. Log normalization deletes unnecessary log entries
B. Log normalization converts logs from different sources into a consistent format, enabling effective correlation, analysis, and searching across heterogeneous data sources in a SIEM
C. Log normalization encrypts log data
D. Normalization is only needed for network logs

Answer: B

Q931. What is the MITRE ATT&CK framework's role in creating SIEM detection rules?

A. MITRE ATT&CK is not related to SIEM detection
B. ATT&CK provides a comprehensive matrix of adversary tactics and techniques that can be mapped to specific SIEM detection rules, helping identify coverage gaps and prioritize detection development
C. ATT&CK replaces SIEM systems entirely
D. ATT&CK only covers network-level attacks

Answer: B

Q932. How does network flow analysis (NetFlow/sFlow) complement full packet capture for security monitoring?

A. Flow analysis and packet capture provide identical information
B. Flow analysis provides metadata about communications (who talked to whom, when, how much data) at scale, while full packet capture provides content details; together they provide both breadth and depth of visibility
C. Flow analysis replaces the need for packet capture
D. Packet capture is always superior to flow analysis

Answer: B

Q933. What is the concept of security monitoring use cases and how should they be prioritized?

A. Use cases are user stories for software development
B. Security monitoring use cases define specific threat scenarios to detect (e.g., brute force, lateral movement), and should be prioritized based on threat likelihood, business impact, and available log sources
C. All use cases should be implemented simultaneously
D. Use cases are only needed for compliance

Answer: B

Q934. What is the difference between agent-based and agentless monitoring for endpoints?

A. They produce identical results with no trade-offs
B. Agent-based monitoring installs software on endpoints for deep visibility and real-time detection, while agentless monitoring uses network traffic or remote queries with less endpoint impact but potentially less visibility
C. Agent-based monitoring is always less secure
D. Agentless monitoring provides better endpoint visibility

Answer: B

Q935. What is a SIEM correlation rule and how does it reduce false positives?

A. Correlation rules only forward raw logs
B. Correlation rules combine multiple individual events across different sources to identify attack patterns, reducing false positives by requiring multiple conditions to be met before triggering an alert
C. Correlation rules increase false positives
D. Correlation is only used for compliance reporting

Answer: B

Q936. What is threat hunting and how does it differ from traditional alert-based security monitoring?

A. Threat hunting and alert-based monitoring are identical
B. Threat hunting is a proactive approach where analysts actively search for hidden threats that may have evaded automated detection, using hypotheses and data analysis rather than waiting for alerts
C. Threat hunting only looks for known malware signatures
D. Threat hunting replaces the need for SIEM

Answer: B

Q937. What is the purpose of a SOC analyst playbook for specific alert types?

A. Playbooks are scripts that automatically fix all security issues
B. Playbooks provide standardized investigation and response procedures for specific alert types, ensuring consistent analysis, reducing response time, and enabling junior analysts to handle complex alerts
C. Playbooks are only used for documentation
D. Playbooks replace the need for skilled analysts

Answer: B

Q938. What is the significance of DNS monitoring in security operations?

A. DNS monitoring only measures internet speed
B. DNS monitoring detects malicious domains, DNS tunneling for data exfiltration, domain generation algorithms (DGA) used by malware, and DNS-based command-and-control communications
C. DNS is too basic to be useful for security
D. DNS monitoring only applies to web servers

Answer: B

Q939. What is the role of data loss prevention (DLP) in security monitoring?

A. DLP only prevents accidental file deletion
B. DLP monitors and controls data movement to detect and prevent unauthorized transmission of sensitive data outside the organization, covering email, web, endpoints, and cloud services
C. DLP replaces encryption
D. DLP only works for physical documents

Answer: B

Q940. What is the extraterritorial jurisdiction challenge in cybercrime prosecution?

A. Cybercrime only occurs within one country
B. Cybercrimes often cross national boundaries, creating challenges in determining which country's laws apply, obtaining evidence from foreign jurisdictions, and securing cooperation between different legal systems
C. Extraterritorial jurisdiction is not relevant to cybercrime
D. All countries have identical cybercrime laws

Answer: B

Q941. What is the difference between data controller and data processor under data protection laws?

A. They are the same entity with different names
B. A data controller determines the purposes and means of data processing, while a data processor processes data on behalf of the controller according to their instructions
C. A data processor has more authority than a controller
D. Only data controllers are regulated by law

Answer: B

Q942. What is the principle of data minimization in privacy law?

A. Minimizing the quality of data collected
B. Organizations should only collect and process the minimum amount of personal data necessary for the specified purpose, avoiding excessive data collection
C. Collecting as much data as possible for future use
D. Minimizing the storage cost of data

Answer: B

Q943. What obligations do organizations have under breach notification laws?

A. Organizations have no obligation to disclose breaches
B. Organizations must notify affected individuals and/or regulatory authorities within specified timeframes when personal data breaches occur, with details about the breach and mitigation measures
C. Only breaches involving financial data require notification
D. Notification is only required if data is published publicly

Answer: B

Q944. What is the legal concept of reasonable security measures in cybersecurity?

A. There is no legal standard for security measures
B. The legal standard requiring organizations to implement security measures appropriate to the sensitivity of data they handle and the risks they face, considered in negligence and liability cases
C. Only government agencies must implement security measures
D. Reasonable security means using the most expensive solutions

Answer: B

Q945. What is the safe harbor provision in cybersecurity law?

A. A physical safe for storing digital evidence
B. Legal protections that shield organizations from liability if they follow specific security frameworks, standards, or practices as defined by applicable law
C. A harbor where cyber criminals are safe from prosecution
D. A type of data encryption standard

Answer: B

Q946. What are the legal implications of employee monitoring in the workplace?

A. Employers can monitor employees without any restrictions
B. Employee monitoring must balance the employer's legitimate security interests with employee privacy rights, often requiring notice, consent, and proportionality under applicable labor and privacy laws
C. Employee monitoring is illegal in all jurisdictions
D. Only IT staff can be monitored

Answer: B

Q947. What is the legal status of ethical hacking and penetration testing?

A. All hacking is illegal regardless of intent
B. Ethical hacking and penetration testing are legal when performed with explicit written authorization from the system owner, defining scope, methods, and timeframes
C. Ethical hackers never need permission
D. Penetration testing is illegal in all countries

Answer: B

Q948. What are the regulatory requirements of PCI DSS for organizations handling payment card data?

A. PCI DSS is optional for all organizations
B. PCI DSS mandates security requirements including network segmentation, encryption of cardholder data, access controls, vulnerability management, and regular security testing for organizations that process, store, or transmit payment card data
C. PCI DSS only applies to banks
D. PCI DSS only covers physical card transactions

Answer: B

Q949. What is the role of the Federal Investigation Agency (FIA) in cybercrime enforcement in Pakistan?

A. FIA has no authority over cybercrimes
B. FIA's National Response Centre for Cyber Crime (NR3C) is responsible for investigating and prosecuting cybercrimes under PECA 2016, including unauthorized access, data theft, online fraud, and cyber harassment
C. FIA only handles physical crimes
D. FIA delegates all cybercrime cases to provincial police

Answer: B

Q950. How does Secure Access Service Edge (SASE) architecture change traditional network security?

A. SASE replaces the internet with private networks
B. SASE converges network security functions (firewall, CASB, ZTNA, SWG) with WAN capabilities into a cloud-delivered service, providing security at the edge closer to users and devices regardless of location
C. SASE is a type of VPN
D. SASE only works for on-premises networks

Answer: B

Q951. What is the security concern with generative AI tools like large language models in enterprise environments?

A. Generative AI has no security concerns
B. Risks include data leakage through prompts, prompt injection attacks, generation of convincing phishing content, AI hallucination producing incorrect security advice, and employees sharing sensitive data with external AI services
C. Generative AI is perfectly secure for all enterprise use
D. Only the AI developer faces security risks

Answer: B

Q952. What is the concept of software-defined networking (SDN) and its security implications?

A. SDN is a type of physical network cable
B. SDN separates the network control plane from the data plane, enabling programmatic network management; security implications include centralized security policy enforcement but also a single point of failure if the controller is compromised
C. SDN has no impact on network security
D. SDN eliminates the need for firewalls

Answer: B

Q953. How do deepfakes pose a threat to cybersecurity beyond misinformation?

A. Deepfakes are only used for entertainment
B. Deepfakes enable advanced social engineering attacks including voice cloning for CEO fraud, video impersonation for identity verification bypass, and synthetic media for blackmail and manipulation
C. Deepfakes can only create images, not video or audio
D. Deepfakes are easily detected by all security systems

Answer: B

Q954. What is the security challenge of operational technology (OT) and IT convergence?

A. OT and IT convergence has no security challenges
B. OT systems were designed for isolated environments with different priorities (availability over confidentiality), and connecting them to IT networks exposes them to cyber threats they were not designed to withstand, while patching and updating is difficult due to uptime requirements
C. OT systems are naturally more secure than IT systems
D. IT security tools work identically in OT environments

Answer: B

Q955. What is the 'harvest now, decrypt later' threat in quantum computing?

A. A quantum computing farming technique
B. Adversaries are collecting and storing encrypted data today with the expectation that future quantum computers will be able to decrypt it, threatening long-term data confidentiality
C. A data backup strategy
D. A machine learning training approach

Answer: B

Q956. What is extended detection and response (XDR) and how does it evolve beyond EDR?

A. XDR is just a marketing term for EDR
B. XDR extends EDR by correlating and analyzing security data across multiple security layers (endpoints, network, cloud, email) to provide unified threat detection and response with broader visibility than endpoint-only EDR
C. XDR only monitors network traffic
D. XDR replaces all other security tools

Answer: B

Q957. What is the emerging concept of cybersecurity mesh architecture (CSMA)?

A. A physical mesh network for security devices
B. CSMA is a composable architecture approach where security controls are deployed as modular, interoperable services that can be distributed across the IT environment, enabling consistent security policy regardless of asset location
C. CSMA is a type of encryption
D. CSMA only applies to wireless networks

Answer: B

Q958. What is the role of threat intelligence platforms (TIPs) in modern cybersecurity?

A. TIPs generate cyber attacks for testing
B. TIPs aggregate, correlate, and operationalize threat intelligence from multiple sources, enabling organizations to contextualize threats, share intelligence, and integrate IoCs into security controls for proactive defense
C. TIPs only provide news articles about cyber threats
D. TIPs replace the need for security analysts

Answer: B

Q959. What is the security implication of edge computing for data protection?

A. Edge computing eliminates all security concerns
B. Edge computing processes data closer to the source, creating challenges in securing distributed processing nodes, ensuring consistent security policies across many edge locations, and protecting data at locations with potentially less physical security
C. Edge computing is more secure than cloud computing
D. Edge computing does not handle sensitive data

Answer: B

Q960. What is the purpose of conducting a gap analysis of the incident response plan?

A. To find physical gaps in server room security
B. To identify weaknesses and areas for improvement in the current IR plan by comparing it against best practices and frameworks
C. To measure network bandwidth gaps
D. To find gaps in employee schedules

Answer: B

Hard Questions

480 questions

Q961. In the STRIDE threat model, what does the 'E' stand for?

A. Elevation of Privilege
B. Exploitation in security contexts
C. Enumeration in security contexts
D. Data-at-rest symmetric encryption

Answer: A

Q962. Which is a key difference between ISO 27001 and ISO 27002?

A. ISO 27001 specifies requirements for an ISMS, ISO 27002 provides implementation guidelines
B. ISO 27001 is for networks, ISO 27002 is for applications
C. ISO 27001 is outdated within enterprise security environments
D. They are identical standards with no meaningful distinction between them

Answer: A

Q963. What is the primary purpose of the MITRE ATT&CK framework?

A. To design websites for enterprise computing environments
B. To develop antivirus software across enterprise computing systems
C. To provide a knowledge base of adversary tactics, techniques, and procedures
D. To generate comprehensive network topology diagrams

Answer: C

Q964. In cyber security, what does APT stand for?

A. Active Port Tunneling
B. Application Protocol Transfer
C. Advanced Persistent Threat
D. Automated Penetration Testing

Answer: C

Q965. Which best describes the concept of 'zero trust' architecture?

A. Using zero encryption within enterprise security environments
B. Trusting all internal network traffic regardless of the specific situation or context
C. Never trusting any entity by default and always verifying regardless of location
D. Blocking all external connections regardless of the specific situation or context

Answer: C

Q966. What is the purpose of a threat intelligence platform (TIP)?

A. To manage employee records within enterprise computing infrastructure
B. To create backup systems for enterprise computing environments
C. To collect, aggregate, and analyze threat data from multiple sources
D. To design and build user-facing application interfaces

Answer: C

Q967. Which regulation specifically addresses data protection for EU citizens?

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

Answer: D

Q968. What is the 'kill chain' model in cyber security?

A. A network topology used in enterprise network infrastructure
B. A method to physically destroy hardware installed within computing infrastructure
C. A type of encryption algorithm applied to data protection workflows
D. A framework describing the stages of a cyber attack from reconnaissance to exfiltration

Answer: D

Q969. What is the role of a Security Operations Center (SOC)?

A. To continuously monitor, detect, analyze, and respond to security incidents
B. To design network hardware across the enterprise network infrastructure
C. To develop new software products across enterprise computing systems
D. To sell security products within enterprise computing infrastructure

Answer: A

Q970. In Pakistan, which law primarily addresses cybercrime?

A. Industrial Relations Act in security contexts
B. Prevention of Electronic Crimes Act (PECA) 2016
C. Foreign Exchange Act within enterprise security environments
D. Pakistan Penal Code only in security contexts

Answer: B

Q971. What is the Bell-LaPadula security model primarily designed to protect?

A. Confidentiality
B. Non-repudiation
C. Integrity
D. Availability

Answer: A

Q972. Which security model uses 'no read down, no write up' to protect integrity?

A. Brewer-Nash
B. Clark-Wilson
C. Biba Model
D. Bell-LaPadula

Answer: C

Q973. What is the Clark-Wilson integrity model based on?

A. Discretionary access control in security contexts
B. Mandatory access control within enterprise security environments
C. Well-formed transactions and separation of duties
D. Role-based access control in security contexts

Answer: C

Q974. In security, what is a 'rainbow table'?

A. A precomputed table for reversing cryptographic hash functions
B. A type of firewall configuration for security management
C. A network topology map used in enterprise network infrastructure
D. A colorful network diagram used in enterprise network infrastructure

Answer: A

Q975. What is the purpose of 'salting' in password hashing?

A. Making passwords taste better within enterprise security environments
B. Compressing the password within enterprise security environments
C. Adding random data to the password before hashing to prevent rainbow table attacks
D. Encrypting the password twice within enterprise security environments

Answer: C

Q976. What is the Kerckhoffs principle in cryptography?

A. Encryption is unnecessary within enterprise security environments
B. A system should be secure even if everything except the key is public knowledge
C. Keys should be shared publicly within enterprise security environments
D. All algorithms should be secret regardless of the specific situation or context

Answer: B

Q977. What is the difference between DAC and MAC access control models?

A. MAC allows users to share freely within enterprise security environments
B. DAC allows owners to set permissions, MAC enforces system-wide policies based on classification labels
C. They are fundamentally identical concepts with no meaningful differences
D. DAC is more restrictive than MAC within enterprise security environments

Answer: B

Q978. Which describes 'security through obscurity'?

A. Relying on secrecy of implementation rather than sound design for security
B. Implementing zero trust within enterprise security environments
C. Using strong encryption within enterprise security environments
D. Using multiple firewalls within enterprise security environments

Answer: A

Q979. What is a Common Vulnerability Scoring System (CVSS)?

A. A cryptographic algorithm used for protecting sensitive data
B. A standard network communication protocol for data transfer
C. A type of malware scanner designed for compromising system integrity
D. A standardized framework for rating the severity of security vulnerabilities

Answer: D

Q980. What does TCB (Trusted Computing Base) refer to?

A. An automated backup solution designed for enterprise-level data recovery and restoration
B. A physical network cable used for connecting devices within the network infrastructure
C. The totality of protection mechanisms within a computer system responsible for enforcing security policy
D. A cloud computing platform used for hosting and managing distributed enterprise workloads

Answer: C

Q981. What mathematical problem does RSA encryption rely on?

A. The traveling salesman optimization problem
B. The difficulty of factoring large prime numbers
C. The discrete logarithm mathematical problem
D. Elliptic curve mathematical computation

Answer: B

Q982. What is an Initialization Vector (IV) in block cipher modes?

A. A type of hash function within modern computing environments
B. A random value used with a key to ensure identical plaintexts produce different ciphertexts
C. The first encryption key within enterprise security environments
D. A decryption algorithm within enterprise computing environments

Answer: B

Q983. Which block cipher mode is considered insecure for encrypting multiple blocks?

A. CBC (Cipher Block Chaining)
B. ECB (Electronic Codebook)
C. GCM (Galois/Counter Mode)
D. CTR (Counter) in security contexts

Answer: B

Q984. What is elliptic curve cryptography (ECC)?

A. A data compression technique that reduces file sizes within enterprise computing environments
B. A cryptographic hashing algorithm used within enterprise computing environments for integrity
C. A symmetric block cipher algorithm widely used for protecting sensitive data at rest
D. An asymmetric approach using elliptic curves over finite fields for smaller key sizes with equivalent security

Answer: D

Q985. What is a man-in-the-middle attack on key exchange?

A. A brute force attack targeting enterprise network infrastructure used in enterprise computing environments
B. A dictionary attack targeting enterprise network infrastructure used in enterprise computing environments
C. An attacker intercepting and altering communication between two parties who believe they are communicating directly
D. Physically stealing keys within enterprise security environments

Answer: C

Q986. What is perfect forward secrecy (PFS)?

A. Using only symmetric encryption without any additional considerations needed
B. Using the same key forever with no meaningful distinction between them
C. Never changing encryption keys in any deployment scenario or context
D. A property ensuring that compromise of long-term keys does not compromise past session keys

Answer: D

Q987. What is the purpose of HMAC?

A. To reduce data sizes through compression methods and management
B. To verify both data integrity and authenticity using a hash function and secret key
C. To encrypt messages using established cryptographic standards
D. To generate random numbers within enterprise computing infrastructure

Answer: B

Q988. Which is a post-quantum cryptographic approach?

A. Lattice-based cryptography
B. AES-128 symmetric block cipher
C. SHA-256 cryptographic hashing
D. RSA-2048 key exchange scheme

Answer: A

Q989. What is the purpose of key stretching algorithms like PBKDF2 and bcrypt?

A. To speed up encryption using established cryptographic standards
B. To compress encryption keys using established cryptographic standards
C. To make brute-force attacks on passwords computationally expensive by adding iterations
D. To make keys shorter within enterprise computing infrastructure

Answer: C

Q990. What is homomorphic encryption?

A. Encryption that only works on text without any additional considerations needed
B. A method to compress encrypted data for managing enterprise data resources
C. Encryption that allows computations on ciphertext without decrypting it first
D. A type of symmetric encryption applied to data protection workflows

Answer: C

Q991. What is a next-generation firewall (NGFW)?

A. Same as a traditional firewall with no meaningful distinction between them regardless of the deployment context or scenario
B. Only works with IPv6 without any additional considerations needed
C. Combines traditional firewall with application awareness, deep packet inspection, and integrated threat intelligence
D. Does not filter traffic in any deployment scenario or context regardless of the deployment context or scenario

Answer: C

Q992. What is the purpose of 802.1X network authentication?

A. To increase and optimize overall network throughput speed and management
B. To create and deploy enterprise wireless network infrastructure
C. To provide port-based network access control requiring authentication before granting access
D. To compress network traffic across the enterprise network infrastructure

Answer: C

Q993. What is deep packet inspection (DPI)?

A. Checking only packet headers without any additional considerations needed
B. Examining the full content of network packets including the data payload for threats
C. A type of compression within modern computing environments
D. A routing protocol used in enterprise network infrastructure

Answer: B

Q994. What is network forensics?

A. Designing and deploying new network topologies across enterprise security infrastructure
B. The capture, recording, and analysis of network events to discover the source of security attacks
C. Configuring and managing enterprise routers across enterprise security infrastructure
D. Installing and configuring network cables across enterprise security infrastructure environments

Answer: B

Q995. What is the purpose of a SIEM system in network security?

A. To speed up network traffic across the enterprise network infrastructure
B. To provide real-time analysis of security alerts from network hardware and applications
C. To compress log files within the data management framework and management
D. To generate comprehensive network topology diagrams and management

Answer: B

Q996. What is microsegmentation in network security?

A. A type of network cable used in enterprise network infrastructure
B. A standard network communication protocol for data transmission
C. Creating fine-grained security zones to isolate workloads and apply granular security policies
D. Dividing networks into very large segments within enterprise security environments

Answer: C

Q997. What is a network tap used for in security monitoring?

A. A network routing device for managing enterprise traffic flows
B. A way to steal water within modern computing environments
C. A passive device that copies network traffic for monitoring without affecting data flow
D. A wireless access point within modern computing environments

Answer: C

Q998. What is BGP hijacking?

A. A legitimate routing practice within modern computing environments
B. A symmetric key data encryption algorithm applied to data protection workflows
C. An attack where an AS falsely announces ownership of IP prefixes to redirect internet traffic
D. A next-generation firewall for filtering network traffic flows

Answer: C

Q999. What is the purpose of NetFlow in security analysis?

A. To encrypt traffic using established cryptographic standards and management
B. To collect and record IP traffic flow data for analysis of patterns and anomaly detection
C. To block websites within enterprise computing infrastructure and management
D. To increase available bandwidth for improved download speeds

Answer: B

Q1000. What is a zero-day vulnerability?

A. A vulnerability that has been patched within modern computing environments
B. A previously unknown vulnerability exploited before the vendor has released a fix
C. A vulnerability that only affects old networks used in enterprise computing environments
D. A vulnerability in outdated software used in enterprise computing environments

Answer: B

Q1001. What is a kernel-level rootkit?

A. A next-generation firewall security appliance deployed across enterprise environments
B. A legitimate administrative system utility tool used in enterprise computing environments
C. A standard user-space application for management within the identity management system
D. Malware that operates at the kernel level, hiding its presence and having unrestricted system access

Answer: D

Q1002. What is Trusted Platform Module (TPM)?

A. A wired network interface adapter for connectivity used in enterprise computing environments
B. A next-generation firewall for filtering network traffic flows
C. A hardware-based security chip that provides cryptographic functions and secure key storage
D. A type of volatile random access memory module used in enterprise computing environments

Answer: C

Q1003. What is Secure Boot?

A. A UEFI feature ensuring only signed and trusted software loads during boot, preventing bootkits
B. A symmetric key data encryption algorithm applied to data protection workflows
C. An automated feature for creating data backups for managing enterprise data resources
D. An option to boot the system more quickly within modern computing environments

Answer: A

Q1004. What is the purpose of Control Flow Integrity (CFI)?

A. To ensure program execution follows the intended control flow graph, preventing code-reuse attacks
B. To manage file systems within the data management framework and management
C. To control user access within enterprise computing infrastructure and management
D. To control traffic flow on networks across the enterprise network infrastructure

Answer: A

Q1005. What is a race condition vulnerability in OS security?

A. A concurrency competition between processes commonly found within modern computing environments
B. A type of scheduling algorithm used to manage processes within enterprise computing environments
C. A flaw where the outcome depends on timing, allowing exploitation of the window between check and use
D. A fast parallel processing technique used within enterprise computing environments for tasks

Answer: C

Q1006. What is namespace isolation in Linux containers?

A. Naming convention for files within enterprise security environments in security contexts
B. A kernel feature providing isolated views of system resources for processes, forming the basis of container security
C. A DNS configuration within modern computing environments for security management
D. A programming concept used in enterprise computing environments for security management

Answer: B

Q1007. What is integrity measurement architecture (IMA) in Linux?

A. Detecting unauthorized file changes by maintaining and verifying cryptographic hashes
B. Measuring and reporting available disk storage capacity on server devices
C. Improving overall system performance throughput and resource utilization
D. Compressing files to reduce disk storage consumption across system drives

Answer: A

Q1008. What is credential guard in Windows 10/11?

A. A standard software application used for routine enterprise computing operation tasks
B. A user account type with specifically assigned and managed access permissions
C. A feature using virtualization-based security to isolate and protect credential secrets from theft
D. A next-generation firewall solution for filtering and monitoring network traffic

Answer: C

Q1009. What is eBPF and how is it used in OS security?

A. A standard network communication protocol for data transmission
B. A symmetric key data encryption algorithm applied to data protection workflows
C. An in-kernel virtual machine allowing sandboxed programs for security monitoring without modifying kernel source
D. A file format used for structured data storage for managing enterprise data resources

Answer: C

Q1010. What is the difference between Type 1 and Type 2 hypervisors in security?

A. Type 1 runs directly on hardware providing better isolation, Type 2 runs on a host OS adding extra attack surface
B. Type 1 is software-only without any additional considerations needed
C. Type 2 is more secure within enterprise security environments across computing environments
D. No security difference in any deployment scenario or context or notable impact in any deployment scenario

Answer: A

Q1011. What is Server-Side Request Forgery (SSRF)?

A. A type of load balancing technique for traffic distribution used in enterprise computing environments
B. A server performance optimization technique for scaling within modern computing environments
C. An attack that abuses server functionality to make requests to internal resources the attacker cannot directly access
D. A server configuration method for managing network access used in enterprise network infrastructure

Answer: C

Q1012. What is a JSON Web Token (JWT) and its security considerations?

A. A database management system for storing structured records
B. A compact token format for secure claims transfer requiring proper validation and strong algorithms
C. A CSS preprocessor for advanced stylesheet development used in enterprise computing environments
D. A web browser application for accessing internet-hosted content

Answer: B

Q1013. What is the purpose of Subresource Integrity (SRI)?

A. To improve and optimize page load speed performance and management
B. To compress and minify JavaScript and CSS scripts within enterprise computing infrastructure
C. To allow browsers to verify fetched resources have not been tampered with using cryptographic hashes
D. To organize and manage web page static resources within enterprise computing infrastructure

Answer: C

Q1014. What is insecure deserialization?

A. A database schema problem causing data integrity errors for managing enterprise data resources
B. A vulnerability where untrusted data abuses deserialization logic, potentially leading to remote code execution
C. Slow and inefficient data loading performance issues within enterprise security environments
D. A data format compatibility issue between API versions for managing enterprise data resources

Answer: B

Q1015. What is a race condition vulnerability in web applications?

A. A performance optimization for improving application speed
B. A flaw where concurrent requests exploit timing gaps in security checks
C. A caching problem causing stale data to be served
D. A load balancing issue affecting resource distribution

Answer: B

Q1016. What is HTTP Request Smuggling?

A. A load balancing technique used for efficiently distributing incoming network traffic
B. A server-side caching mechanism designed for improving web page loading performance
C. A content delivery method used for efficiently distributing static web assets globally
D. An attack exploiting differences in how front-end and back-end servers parse HTTP requests

Answer: D

Q1017. What is a blind SQL injection attack?

A. A properly secured and parameterized SQL database query for managing enterprise data resources
B. An SQL injection where the attacker infers information by observing application behavior rather than direct output
C. A database backup technique for creating data snapshots for managing enterprise data resources
D. A standard SQL query that returns no data results for managing enterprise data resources

Answer: B

Q1018. What is the purpose of the HSTS header?

A. To compress and reduce the size of HTTP request headers
B. To force browsers to only use HTTPS, preventing protocol downgrade attacks
C. To block and prevent all incoming and outgoing traffic
D. To improve and speed up web connection establishment

Answer: B

Q1019. What is DOM-based XSS?

A. It is identical in behavior to reflected cross-site scripting across computing environments
B. Reflected XSS is exclusively a client-side vulnerability within enterprise security environments
C. DOM-based XSS is a server-side vulnerability entirely within enterprise security environments
D. XSS that executes entirely in the browser by manipulating the DOM, unlike reflected XSS which involves the server

Answer: D

Q1020. What is the purpose of OAuth 2.0 in web security?

A. To provide delegated authorization allowing third-party apps limited access without sharing credentials
B. To compress and reduce the size of transmitted web data and management
C. To completely block all unauthorized users from access and management
D. To encrypt all web traffic using symmetric cipher algorithms and management

Answer: A

Q1021. What is a polymorphic virus?

A. A virus designed for running on multiple hardware platforms
B. A virus that infects only once and does not replicate further
C. Malware that changes its code signature each time it replicates to evade detection
D. A benign virus that enhances system security posture overall

Answer: C

Q1022. What is a supply chain attack?

A. A written record or logbook for tracking daily operational activities
B. An attack compromising a trusted vendor or software update mechanism to distribute malware
C. A procurement process for purchasing IT equipment used in enterprise computing environments
D. Attacking physical supply chains and logistics routes

Answer: B

Q1023. What is an APT lifecycle?

A. A system update cycle for deploying maintenance patches within modern computing environments
B. A backup schedule for creating regular recovery snapshots for managing enterprise data resources
C. A multi-stage attack process involving reconnaissance, initial access, persistence, lateral movement, and exfiltration
D. A standard software development lifecycle methodology used in enterprise computing environments

Answer: C

Q1024. What is living-off-the-land (LOTL) technique?

A. Environmental computing initiatives for reducing power usage
B. A green IT practice focused on sustainable computing used in enterprise computing environments
C. Agricultural computing systems for managing farming operations
D. Using legitimate system tools already present on the target system to carry out malicious activities

Answer: D

Q1025. What is a logic bomb?

A. Malicious code that remains dormant until triggered by a specific condition like a date or event
B. A physical hardware component used in computing infrastructure
C. A written record or logbook for tracking daily operational activities
D. A software application used for enterprise computing operations

Answer: A

Q1026. What is DNS tunneling used for in attacks?

A. A DNS caching technique for reducing query response time used in enterprise computing environments
B. Encoding data within DNS queries to establish a covert communication channel bypassing firewalls
C. A DNS optimization technique for faster name resolution used in enterprise computing environments
D. Improving DNS resolution speed and performance latency

Answer: B

Q1027. What is steganography in cyber attacks?

A. A type of prehistoric dinosaur classification study used in enterprise computing environments
B. A printing technique for high-resolution image output used in enterprise computing environments
C. Hiding malicious data or communications within ordinary-looking files like images or audio
D. A photography method for capturing wide-angle images used in enterprise computing environments

Answer: C

Q1028. What is a metamorphic virus?

A. A virus that migrates and spreads between different host operating systems and platforms
B. A virus that executes only once on a system and then immediately self-terminates
C. Malware that completely rewrites its own code with each iteration while maintaining functionality
D. A benign virus variant that improves overall system security posture and performance

Answer: C

Q1029. What is the MITRE ATT&CK technique T1055 (Process Injection)?

A. A standard software development pattern used for organizing code into modules
B. A performance optimization technique for accelerating overall application speed
C. A technique where malicious code is injected into the address space of a legitimate process
D. A runtime debugging technique used for identifying and resolving code defects

Answer: C

Q1030. What is command and control (C2) infrastructure?

A. A network management tool used in enterprise network infrastructure
B. The communication framework attackers use to maintain control over compromised systems
C. A software development platform for building applications
D. A military headquarters facility for coordinating operations

Answer: B

Q1031. What is Kerberos authentication protocol?

A. A software application used for enterprise computing operations
B. A ticket-based network authentication protocol using symmetric key cryptography and a trusted third party
C. A standard web browser for accessing internet sites within modern computing environments
D. A standard network communication protocol for data transmission

Answer: B

Q1032. What is the difference between RBAC and ABAC in scalability?

A. Neither is scalable within enterprise security environments
B. RBAC is always more scalable regardless of the specific situation or context
C. ABAC is more scalable for complex environments as it uses attributes rather than requiring new roles
D. They scale identically with no meaningful distinction between them

Answer: C

Q1033. What is the FIDO2 authentication standard?

A. A passwordless authentication standard using public-key cryptography with hardware authenticators
B. A standard network communication protocol for data transmission
C. A credential management mechanism for user authentication flows
D. A file format used for structured data storage for managing enterprise data resources

Answer: A

Q1034. What is just-in-time (JIT) access provisioning?

A. A type of SSO used across multiple services within enterprise computing environments
B. Permanent access granted for all users regardless of the specific situation or context
C. Fast login systems used for authentication within enterprise security environments
D. Granting privileged access only when needed for a specific duration, then automatically revoking it

Answer: D

Q1035. What is the OAuth 2.0 authorization code flow?

A. A flow where the client receives an authorization code exchanged for tokens via a back-channel
B. A file transfer process within enterprise computing environments
C. A simple password exchange within the identity management system
D. A database query method for managing enterprise data resources

Answer: A

Q1036. What is the purpose of Privileged Access Management (PAM)?

A. To create user accounts for enterprise computing environments
B. To manage email accounts within enterprise computing infrastructure
C. To secure, manage, and monitor privileged accounts and access to critical systems
D. To design websites for enterprise computing environments and management

Answer: C

Q1037. What is a pass-the-hash attack?

A. A hashing algorithm used for data integrity within enterprise computing environments
B. Sharing passwords openly across teams within enterprise security environments for access
C. A credential management mechanism designed for enterprise user authentication flows
D. An attack where captured password hashes are used directly to authenticate without knowing the password

Answer: D

Q1038. What is continuous authentication?

A. Logging into the system repeatedly at regular intervals across computing environments
B. A type of multi-factor authentication using OTP tokens used in enterprise computing environments
C. Continuously verifying identity throughout a session using behavioral biometrics and contextual signals
D. A session timeout feature that logs users out within the identity management system

Answer: C

Q1039. What is claim-based identity?

A. A type of insurance policy covering liability damages used in enterprise computing environments
B. Using assertions about a user made by a trusted identity provider for authentication and authorization
C. A file management system for organizing stored documents used in enterprise computing environments
D. Filing legal claims in a court of law or tribunal within enterprise security environments

Answer: B

Q1040. What is certificate-based authentication?

A. A training certification program for development used in enterprise computing environments
B. Using digital certificates (X.509) to verify identity, preferred for machine-to-machine communication
C. A structured file format used for data storage and exchange
D. Using paper certificates for physical identity verification

Answer: B

Q1041. What is the Microsoft Security Development Lifecycle (SDL)?

A. A Microsoft commercial product for endpoint security used in enterprise computing environments
B. A testing framework for automated unit testing of code used in enterprise computing environments
C. A high-level language used for development within modern computing environments
D. A process integrating security into every SDLC phase including training, design, and verification

Answer: D

Q1042. What is a Software Bill of Materials (SBOM)?

A. A project plan for scheduling development milestones used in enterprise computing environments
B. A software application used for enterprise computing operations
C. A software license for managing application access rights
D. A comprehensive inventory of all components, libraries, and dependencies in software

Answer: D

Q1043. What is Interactive Application Security Testing (IAST)?

A. Manual code review conducted by human security reviewers
B. A software application used for enterprise computing operations
C. A hybrid combining SAST and DAST using instrumentation agents within the running application
D. A type of unit test for verifying individual code functions used in enterprise computing environments

Answer: C

Q1044. What is Runtime Application Self-Protection (RASP)?

A. A programming pattern used in enterprise computing environments
B. Security technology built into an application that detects and prevents attacks in real-time
C. A self-replicating strain of malicious software targeting systems
D. A software application used for enterprise computing operations

Answer: B

Q1045. What is the purpose of fuzz testing (fuzzing)?

A. Load testing application performance under heavy traffic
B. Providing random, unexpected, or malformed data as input to discover vulnerabilities
C. Testing user experience through usability research sessions
D. Testing application inputs with soft expected normal values

Answer: B

Q1046. What is taint analysis in secure development?

A. Tracking untrusted data through an application to identify where it reaches sensitive operations unsanitized
B. A color analysis tool for evaluating interface themes used in enterprise computing environments
C. Source code formatting and style standardization practices across computing environments
D. A code obfuscation method for protecting intellectual property used in enterprise computing environments

Answer: A

Q1047. What is the concept of 'secure defaults'?

A. Having no security settings or controls enabled at all regardless of the deployment context or scenario
B. Using default vendor passwords for all system accounts across computing environments
C. Shipping applications with the most secure configuration, requiring users to explicitly reduce security
D. Applications require no configuration at all to operate regardless of the deployment context or scenario

Answer: C

Q1048. What is a security champion program in DevSecOps?

A. Embedding security-trained developers within teams to advocate for security practices
B. A competitive security skills competition between teams used in enterprise computing environments
C. A hiring initiative for recruiting security professionals
D. A certification program for professional security credentials

Answer: A

Q1049. What is the purpose of a bug bounty program?

A. Paying developers to write application source code faster and more efficiently
B. Incentivizing external researchers to find and responsibly report vulnerabilities for rewards
C. An automated software testing service for quality assurance and code validation
D. A code quality improvement program focused on long-term maintainability goals

Answer: B

Q1050. What is DevSecOps?

A. Integrating security into DevOps pipelines through automation, making security a shared responsibility
B. A software application used for enterprise computing operations
C. A next-generation firewall security appliance deployed across enterprise environments
D. A high-level language used for development within modern computing environments

Answer: A

Q1051. What is the KRACK vulnerability?

A. A software application used for enterprise computing operations
B. A defect in wireless network adapter hardware components
C. A type of physical screen damage on mobile device displays
D. A vulnerability in WPA2's four-way handshake allowing nonce reuse and traffic decryption

Answer: D

Q1052. What is 802.11w (Protected Management Frames)?

A. A wireless speed standard for improving data throughput used in enterprise computing environments
B. A physical network cable used for connecting infrastructure devices
C. A physical hardware component used in computing infrastructure
D. An amendment providing integrity protection for management frames, preventing deauthentication attacks

Answer: D

Q1053. What is mobile application wrapping?

A. Gift wrapping services for physical phone accessories and mobile device peripherals
B. Encrypting app names for the purpose of obscuring installed applications on devices
C. Adding a management layer around apps to enforce security policies without modifying source code
D. Compressing mobile apps for reduced storage space consumption on user devices

Answer: C

Q1054. What is BLE security vulnerability tracking?

A. A fitness tracker feature for monitoring health activity
B. Monitoring BLE implementations for vulnerabilities like BlueBorne, KNOB, and BIAS
C. A battery monitoring tool for optimizing power consumption
D. Tracking the location of lost Bluetooth headphones

Answer: B

Q1055. What is certificate pinning in mobile applications?

A. A user account type with specifically assigned access permissions
B. Physically pinning paper certificates to a bulletin board
C. A file attachment method for sending documents via email used in enterprise computing environments
D. Hardcoding a host's expected certificate to prevent MITM attacks using fraudulent certificates

Answer: D

Q1056. What is the security risk of SS7 protocol vulnerabilities?

A. There is no risk at all from this vulnerability in any deployment scenario or context
B. A physical hardware component used in computing infrastructure
C. A mobile device application for portable computing operations
D. SS7 flaws allow interception of calls, SMS messages, and location tracking of mobile users globally

Answer: D

Q1057. What is containerization in enterprise mobile security?

A. A storage method for archiving large data file volumes used in enterprise computing environments
B. Physical shipping containers for transporting goods
C. A charging technique for optimizing battery power cycles used in enterprise computing environments
D. Creating isolated encrypted workspaces separating corporate and personal data on devices

Answer: D

Q1058. What is a man-in-the-disk attack on Android?

A. An attack exploiting insecure external storage use by apps to maliciously modify data
B. A network attack exploiting wireless protocol vulnerabilities
C. A disk cleaning tool for removing temporary cached files
D. A hardware attack targeting physical disk drive components

Answer: A

Q1059. What is a Wireless Intrusion Prevention System (WIPS)?

A. A mobile device application used for managing and configuring Wi-Fi network settings
B. A system monitoring wireless spectrum for unauthorized access and automatically taking countermeasures
C. A network routing device used for managing enterprise traffic flows across infrastructure
D. A Bluetooth peripheral device used for short-range data communication between systems

Answer: B

Q1060. What is the security significance of baseband processor vulnerabilities?

A. A battery concern related to excessive power consumption used in enterprise computing environments
B. A display issue causing visual glitches and rendering problems used in enterprise computing environments
C. Baseband vulnerabilities can allow remote code execution bypassing all OS-level security controls
D. Supply chain attacks have no significance in software security regardless of the deployment context or scenario

Answer: C

Q1061. What is a confused deputy problem in cloud security?

A. A confused employee who cannot follow security procedures used in enterprise computing environments
B. A next-generation firewall for filtering network traffic flows
C. A privilege escalation where a trusted service is tricked into performing unauthorized actions
D. A DNS issue causing incorrect domain name resolution used in enterprise computing environments

Answer: C

Q1062. What is CNAPP?

A. A web development framework designed for building scalable application frontend interfaces
B. An integrated security platform combining CSPM, CWPP, and application security for cloud-native apps
C. A mobile application store platform for downloading and distributing software packages
D. A cloud computing platform used for hosting and managing distributed enterprise workloads

Answer: B

Q1063. What is the NIST Cloud Computing Reference Architecture?

A. A framework defining five major actors and their roles in cloud computing
B. A cloud provider offering infrastructure as a service
C. A security tool for scanning and detecting vulnerabilities
D. A programming standard for writing cloud application code

Answer: A

Q1064. What are the security implications of serverless computing?

A. No security is needed because there are no significant threats regardless of the deployment context or scenario
B. This is completely secure by default without configuration across computing environments
C. Same security profile as traditional server hosting with no meaningful distinction between them
D. Reduced OS attack surface but increased function-level risks including injection and insecure dependencies

Answer: D

Q1065. What is cloud key management service (KMS)?

A. A managed service for creating and managing cryptographic keys for cloud data encryption
B. A music streaming service platform for audio content used in enterprise computing environments
C. A file management tool for organizing cloud storage resources
D. A network routing service for directing cloud data traffic

Answer: A

Q1066. What is cloud infrastructure entitlements management (CIEM)?

A. Managing cloud storage volumes and tracking data capacity limits across regions
B. Creating and provisioning new cloud user accounts across multiple environments
C. Managing cloud billing and implementing cost optimization strategies for budgets
D. Detecting and remediating excessive or unused permissions across multi-cloud environments

Answer: D

Q1067. What is CSA STAR certification?

A. An astronomy certification for studying celestial objects used in enterprise computing environments
B. A web browser application for accessing internet-hosted content
C. A movie rating classification for content age suitability used in enterprise computing environments
D. A third-party assessment of a cloud provider's security posture based on the Cloud Controls Matrix

Answer: D

Q1068. What is the blast radius concept in cloud security?

A. A network speed measurement using bandwidth throughput used in enterprise computing environments
B. The potential scope of damage if a security component is compromised, minimized through segmentation
C. A storage capacity metric for measuring disk volume sizes used in enterprise computing environments
D. A physical security measure for protecting building infrastructure

Answer: B

Q1069. What are immutable infrastructure security benefits?

A. There are no security benefits from this approach regardless of the deployment context or scenario
B. Faster server performance through hardware optimization
C. Permanent servers that never change with no security benefit regardless of the deployment context or scenario
D. Servers are never modified after deployment, reducing configuration drift and persistent threats

Answer: D

Q1070. What is the security challenge of multi-cloud environments?

A. Managing consistent security policies and visibility across multiple providers with different tools
B. Multi-cloud eliminates all security risks through redundancy
C. There are no challenges with this approach at all in any deployment scenario or context
D. Multi-cloud is inherently more secure than single-cloud

Answer: A

Q1071. What is a YARA rule?

A. A next-generation firewall for filtering network traffic flows
B. A programming language rule used in enterprise computing environments
C. A database management system for storing structured records
D. A pattern-matching tool for describing malware families based on textual or binary patterns

Answer: D

Q1072. What is the Sleuth Kit and Autopsy platform?

A. A security scanner deployed across enterprise environments for security management
B. An open-source digital forensics framework for file system analysis, timeline creation, and keyword searching
C. A detective game within modern computing environments for security management
D. A network monitor used in enterprise network infrastructure for security management

Answer: B

Q1073. What is file carving in digital forensics?

A. Physically cutting a hard drive within enterprise security environments
B. Wood carving with a computer within enterprise security environments
C. Editing file names within enterprise security environments
D. Recovering files from unallocated space by identifying file headers and footers without metadata

Answer: D

Q1074. What is the difference between live and dead forensics?

A. Live forensics analyzes a running system for volatile data; dead forensics examines a powered-off system
B. One involves living organisms within enterprise security environments
C. There is no difference in any deployment scenario or context or notable impact in any deployment scenario
D. One is more dangerous within enterprise security environments

Answer: A

Q1075. What is Windows Registry forensics?

A. Fixing Registry errors and resolving system conflicts within enterprise security environments
B. Registering Windows products and managing software licenses within enterprise security environments
C. Creating Registry backups and restoration points within enterprise security environments
D. Analyzing the Registry to extract evidence of user activities, installed software, and USB history

Answer: D

Q1076. What is the significance of slack space?

A. Unused RAM within enterprise security environments across computing environments
B. Empty space on a desk within enterprise security environments
C. Space between end of a file and end of disk cluster, which may contain remnants of previous data
D. A software application used for enterprise computing operations

Answer: C

Q1077. What is artifact analysis in mobile forensics?

A. Examining mobile-specific data like SMS databases, call logs, app caches, and location data
B. Analyzing phone hardware within enterprise security environments
C. Repairing mobile devices within enterprise security environments
D. Studying ancient artifacts within enterprise security environments

Answer: A

Q1078. What is the Volatility framework?

A. A database tool used in enterprise computing environments
B. A network scanner used in enterprise network infrastructure
C. Measuring system performance within enterprise security environments
D. An advanced memory forensics framework for extracting digital artifacts from RAM dumps

Answer: D

Q1079. What is evidence spoliation?

A. A chain of custody step within modern computing environments
B. Intentional or negligent destruction or alteration of evidence, leading to legal sanctions
C. Proper evidence handling within enterprise security environments
D. A forensic technique within enterprise computing environments

Answer: B

Q1080. What is cloud forensics and its challenges?

A. A standard software application used for enterprise computing operations and workflows
B. Weather analysis and atmospheric monitoring within enterprise security environments
C. An automated backup solution designed for enterprise data recovery and restoration needs
D. Forensic investigation in cloud environments facing data distribution, multi-jurisdiction, and limited access

Answer: C

Q1081. How does the SANS incident response framework differ from NIST?

A. SANS has only 3 steps within enterprise security environments without additional considerations
B. SANS emphasizes Identification vs. NIST's Detection and Analysis, and is more practitioner-oriented
C. They are fundamentally identical concepts with no meaningful differences between them at all
D. NIST has 10 distinct steps within enterprise security environments for incident handling

Answer: B

Q1082. What is a CSIRT and its key functions?

A. A specialized team handling incident monitoring, triage, analysis, coordination, and advisory services
B. A software application used for enterprise computing operations
C. A user account type with specifically assigned access permissions
D. A network administration team managing infrastructure used in enterprise computing environments

Answer: A

Q1083. What is cyber insurance?

A. An automated backup solution designed for enterprise data recovery and restoration needs
B. Insurance covering financial losses from cyber incidents including forensics, legal fees, and notification
C. Car insurance for covering vehicle damage and repair costs resulting from accidents
D. Health insurance covering IT staff medical expenses, benefits, and wellness programs

Answer: B

Q1084. What is the role of threat intelligence in incident response?

A. A type of self-replicating malicious software designed for system infiltration attacks
B. Generating and distributing threats against specifically targeted computing systems
C. Providing context about threat actors, TTPs, and IOCs to accelerate detection and guide response
D. A compliance reporting tool designed for generating audit documentation and reports

Answer: C

Q1085. What is SOAR?

A. A next-generation firewall security appliance deployed across enterprise environments
B. A software application used for enterprise computing operations
C. A technology stack integrating security tools, automating response tasks, and orchestrating workflows
D. A music platform for streaming and listening to audio used in enterprise computing environments

Answer: C

Q1086. What are the legal considerations during incident response?

A. Evidence preservation, regulatory notification requirements, privacy laws, and law enforcement coordination
B. Only criminal law applies without any specific legislation across computing environments
C. Only privacy laws matter during incident response without any additional considerations needed
D. No legal considerations exist during incident response regardless of the deployment context or scenario

Answer: A

Q1087. What is the purpose of tabletop exercises?

A. Playing board games for team building recreation purposes across computing environments
B. Discussion-based exercises to test plans, identify gaps, and improve coordination without operational impact
C. A physical security measure for protecting building infrastructure
D. Testing table strength and durability for furniture quality across computing environments

Answer: B

Q1088. What is the 'assume breach' concept?

A. Accepting all risks without any mitigation efforts across computing environments
B. Planning with the assumption that breaches will occur, focusing on detection, response, and recovery
C. Disabling all security controls for maximum performance across computing environments
D. Ignoring security entirely without any protective measures

Answer: B

Q1089. What is the role of digital forensics in incident response?

A. An activity reserved only for law enforcement investigators used in enterprise computing environments
B. A separate unrelated discipline with no connection within modern computing environments
C. Completely replacing incident response with alternatives across computing environments
D. Providing scientific examination of evidence to understand attack vector, scope, timeline, and attribution

Answer: D

Q1090. What is the difference between an incident and a data breach?

A. They are functionally identical frameworks with no differences in any deployment scenario or context
B. A breach is less serious than a standard incident within modern computing environments
C. An incident only involves malware and no other threats designed for compromising system integrity
D. An incident is any event threatening security; a breach specifically involves confirmed unauthorized access to sensitive data

Answer: D

Q1091. What is a SOC maturity model?

A. A project management tool for tracking development milestones
B. A software development model for iterative feature delivery
C. A framework for assessing and improving SOC capabilities across people, processes, and technology
D. A hiring framework for recruiting security team personnel used in enterprise computing environments

Answer: C

Q1092. What is SOAR in security monitoring?

A. A software application used for enterprise computing operations
B. A flight control system used in aviation navigation within modern computing environments
C. A platform integrating security tools, automating response workflows, and orchestrating incident handling
D. A cloud computing platform for hosting enterprise workloads

Answer: C

Q1093. What is MITRE ATT&CK's role in security monitoring?

A. A next-generation firewall security appliance deployed across enterprise environments
B. A vulnerability scanner for identifying system weaknesses used in enterprise computing environments
C. A software application used for enterprise computing operations
D. Providing a matrix of adversary tactics and techniques to guide detection rule creation and coverage assessment

Answer: D

Q1094. What is Extended Detection and Response (XDR)?

A. A display resolution specification for mobile devices installed within computing infrastructure
B. A unified platform integrating data from endpoints, networks, cloud, and email for holistic threat detection
C. A network routing device for managing enterprise traffic flows
D. A physical hardware component used in computing infrastructure

Answer: B

Q1095. What is deception technology?

A. Social media manipulation campaigns designed for spreading misinformation and propaganda
B. A magic show performance with illusion tricks for entertainment and audience engagement
C. A VPN technology used for creating encrypted tunnel connections across networks securely
D. Using decoys, breadcrumbs, and traps to detect attackers who bypassed perimeter defenses

Answer: D

Q1096. What are MTTD and MTTR?

A. Time to reboot systems within enterprise security environments
B. Average time to build software within enterprise security environments
C. Time to install updates regardless of the specific situation or context
D. Key SOC metrics measuring average time to detect (MTTD) and to contain and resolve (MTTR) incidents

Answer: D

Q1097. What is a purple team exercise?

A. A standard software application commonly used for enterprise computing operations and tasks
B. A collaborative exercise where offensive and defensive teams work together to improve detection
C. A training exercise specifically designed for improving team coordination and basic skills
D. A color-themed social event designed for team-building and recreational group activities

Answer: B

Q1098. What is network detection and response (NDR)?

A. A network routing device for managing enterprise traffic flows
B. A DNS service for resolving domain names to IP addresses used in enterprise computing environments
C. A solution monitoring network traffic using behavioral analytics and ML to detect and respond to threats
D. A network speed test for measuring bandwidth throughput used in enterprise computing environments

Answer: C

Q1099. What is the role of machine learning in security monitoring?

A. Replacing all human security analysts with automation across computing environments
B. Machine learning is used only for spam filtering without any additional considerations needed
C. Enhancing detection of novel threats, reducing false positives, and automating large-scale data analysis
D. Making systems slower through additional processing overhead

Answer: C

Q1100. What is a detection engineering program?

A. Building physical detectors for environmental monitoring
B. An electrical engineering course covering power distribution used in enterprise computing environments
C. A systematic approach to developing, testing, and measuring effectiveness of security detection rules
D. A physical hardware component used in computing infrastructure

Answer: C

Q1101. How does PECA 2016 address cyber terrorism?

A. Only monetary fines are imposed for cyber terrorism under PECA across computing environments
B. Only verbal warnings are issued for cyber terrorism under PECA across computing environments
C. Section 10 criminalizes using information systems for terrorism with penalties up to 14 years and 50 million rupees
D. PECA does not address terrorism in any of its provisions in any deployment scenario or context

Answer: C

Q1102. What is the Budapest Convention on Cybercrime?

A. A European trade agreement governing international commerce used in enterprise computing environments
B. A military alliance treaty for coordinating national defense used in enterprise computing environments
C. The first international treaty addressing cybercrime with a framework for international cooperation
D. A climate agreement for addressing global environmental change used in enterprise computing environments

Answer: C

Q1103. What are the challenges of cross-border cybercrime investigation?

A. There are no challenges with this approach at all or notable impact in any deployment scenario
B. Only language barriers present challenges for investigation
C. Only time zone differences present challenges for investigation
D. Jurisdictional conflicts, varying laws, evidence preservation across borders, and MLAT delays

Answer: D

Q1104. What is the legal framework for digital evidence in Pakistan?

A. Qanun-e-Shahadat Order 1984, PECA 2016, and Electronic Transactions Ordinance 2002 collectively govern it
B. Only criminal law applies without any specific legislation
C. No legal framework exists for digital evidence in Pakistan regardless of the deployment context or scenario
D. Only PECA applies without any other relevant legislation across computing environments

Answer: A

Q1105. What is the legal principle of proportionality in cyber security law?

A. Minimum security is always sufficient regardless of threat across computing environments
B. No security is needed because there are no significant threats regardless of the deployment context or scenario
C. Maximum security should always be applied regardless of risk
D. Security measures and penalties should be proportionate to the actual risk, balancing security with rights

Answer: D

Q1106. What is the legal status of encryption in different jurisdictions?

A. Encryption is mandatory everywhere in the world without exception
B. Legality varies: some countries mandate it, others restrict or require key escrow
C. There are no laws about encryption in any country worldwide
D. Encryption is illegal everywhere in the world without exception

Answer: B

Q1107. What is the NIS2 Directive?

A. A physical hardware component widely used in enterprise computing infrastructure systems
B. A standard software application used for routine enterprise computing operations tasks
C. A standard network communication protocol used for transmitting data across systems
D. An EU directive expanding cybersecurity requirements with risk management and incident reporting mandates

Answer: D

Q1108. What is 'duty of care' in cybersecurity?

A. The legal obligation to implement reasonable security measures to protect stakeholders from foreseeable harm
B. Only governments have a duty of care not private organizations regardless of the deployment context or scenario
C. Duty of care is only a medical concept with no legal relevance regardless of the deployment context or scenario
D. Having no responsibility for security is the accepted standard regardless of the deployment context or scenario

Answer: A

Q1109. What are the implications of the Schrems II decision?

A. There are no implications for this technology whatsoever regardless of the deployment context or scenario
B. It invalidated EU-US Privacy Shield and requires assessment of destination country data protection adequacy
C. It only affects social media platforms and no other services without impacting any other system components
D. It only affects banking institutions and no other organizations without impacting any other system components

Answer: B

Q1110. What is Pakistan's Personal Data Protection Bill?

A. An education policy for governing school curriculum standards used in enterprise computing environments
B. It has been fully enacted and is currently in force as law across computing environments
C. A banking regulation governing financial institution operations used in enterprise computing environments
D. A proposed legislation establishing data protection rights, consent requirements, and a regulatory authority

Answer: D

Q1111. What is post-quantum cryptography?

A. Encryption methods used after quantum computers become obsolete across computing environments
B. A standard cryptographic algorithm used for protecting sensitive data in transit and at rest
C. Algorithms resistant to quantum attacks; NIST is standardizing lattice-based algorithms like CRYSTALS-Kyber
D. Current encryption methods that are already widely deployed across enterprise computing environments

Answer: C

Q1112. What is confidential computing?

A. A privacy policy document for governing data handling used in enterprise computing environments
B. Hardware-based technology protecting data in use through trusted execution environments (TEEs)
C. Keeping computer use private from other household members
D. A secret language used for encoding confidential communications

Answer: B

Q1113. What is the significance of supply chain attacks in software?

A. Compromising trusted development tools or dependencies to distribute malware through legitimate channels
B. Supply chain attacks only affect physical goods and shipping without impacting any other system components
C. Supply chain attacks have no significance in software security regardless of the deployment context or scenario
D. Supply chain attacks only affect shipping and transportation without impacting any other system components

Answer: A

Q1114. What is cyber-physical systems security?

A. A gym security system for monitoring facility access points used in enterprise computing environments
B. Securing physical buildings with locks and access controls across computing environments
C. Protecting systems where computational elements control physical processes, where attacks cause physical damage
D. A fitness tracker for monitoring personal health activity used in enterprise computing environments

Answer: C

Q1115. What is adversarial machine learning?

A. Training ML models faster using distributed computing across computing environments
B. Techniques exploiting ML model vulnerabilities through adversarial inputs causing misclassification
C. A competitive tournament between different ML implementations used in enterprise computing environments
D. A type of supervised learning for classification tasks used in enterprise computing environments

Answer: B

Q1116. What is digital sovereignty in cybersecurity?

A. Owning a domain name for a personal website registration across computing environments
B. A nation's ability to control its digital infrastructure, data, and technology without foreign dependency
C. Online voting rights for participating in digital elections
D. A type of digital currency for online financial transactions used in enterprise computing environments

Answer: B

Q1117. What is the role of STIX/TAXII in threat intelligence?

A. Email services for sending and receiving electronic messages
B. Social media platforms for sharing posts and content within enterprise security environments
C. Standardized formats and protocols for sharing structured cyber threat intelligence between organizations
D. File sharing platforms for distributing documents and media

Answer: C

Q1118. What are the security implications of quantum key distribution (QKD)?

A. QKD weakens security by introducing new attack vectors across computing environments
B. There are no implications for this technology whatsoever regardless of the deployment context or scenario
C. QKD uses quantum mechanics for theoretically unbreakable key exchange, as eavesdropping is detectable
D. QKD replaces all existing encryption methods entirely across computing environments

Answer: C

Q1119. What is security chaos engineering?

A. Creating chaos and deliberate disruption in security team operations and workflow
B. Disabling all security controls to test overall system resilience under attack
C. Intentionally injecting security failures to proactively identify weaknesses and validate controls
D. Random penetration testing performed without any defined methodology or test plan

Answer: C

Q1120. What is the emerging threat of AI-powered social engineering?

A. AI improving social skills through virtual communication across computing environments
B. Using AI for convincing phishing at scale, deepfake impersonation, and personalized attacks harder to detect
C. AI creating automated social media accounts for marketing across computing environments
D. AI managing social media accounts for content scheduling across computing environments

Answer: B

Q1121. An organization discovers that an employee has been exfiltrating data for months undetected. Which security principle failure is MOST directly responsible?

A. Failure in conducting regular penetration testing against external perimeters
B. Failure in deploying sufficient network bandwidth for threat detection systems
C. Failure in implementing proper security monitoring and audit logging controls
D. Failure in applying timely software patches to all organizational endpoints

Answer: C

Q1122. A company implements multiple overlapping security controls. Which cyber security concept does this BEST demonstrate?

A. Defense in depth using layered protections across multiple levels
B. Least privilege limiting individual user permissions and access
C. Security through obscurity relying on hidden system implementations
D. Single point of failure with centralized management of controls

Answer: A

Q1123. During a risk assessment, the team identifies a threat with low probability but catastrophic impact. How should this risk be classified?

A. Medium risk since probability and impact partially offset each other
B. Low risk because the probability of occurrence is minimal
C. High risk because catastrophic impact outweighs the low probability
D. Negligible risk as low probability events should be safely ignored

Answer: C

Q1124. An attacker exploits a zero-day vulnerability before the vendor releases a patch. Which response strategy is MOST effective immediately?

A. Waiting for the vendor to release an official patch before taking action
B. Completely disconnecting all systems from every network until fully resolved
C. Implementing compensating controls like network segmentation and monitoring
D. Reinstalling the operating system on every affected endpoint in the network

Answer: C

Q1125. A security team must justify budget for new security tools to executive leadership. Which approach is MOST effective?

A. Presenting the total number of blocked attacks from the previous fiscal year
B. Highlighting technical specifications and vendor certifications of new tools
C. Quantifying risk reduction in financial terms using established risk frameworks
D. Comparing the organization's tool count with those of industry competitors

Answer: C

Q1126. In a mature security program, how should threat intelligence be integrated into operations?

A. Shared exclusively with executive management during annual board review meetings
B. Only used for generating quarterly reports for compliance and audit purposes
C. Stored in offline archives for reference during post-incident forensic investigations
D. Fed into SIEM, vulnerability management, and incident response processes continuously

Answer: D

Q1127. A nation-state actor targets critical infrastructure using advanced persistent threats. What classification does this attacker fall under?

A. Opportunistic criminal seeking quick financial gain from random targets
B. Hacktivist motivated primarily by political or social activist causes
C. Script kiddie with limited technical skill and basic attack toolkits
D. Advanced Persistent Threat actor with significant resources and funding

Answer: D

Q1128. When implementing a security program, why is it critical to align security objectives with business goals?

A. To reduce the overall complexity of network architecture within the organization systems
B. To guarantee full compliance with every international security regulation and standard
C. To ensure security spending directly supports organizational risk tolerance and priorities
D. To minimize the total number of security staff required across all business departments

Answer: C

Q1129. A company wants to measure the effectiveness of its security program. Which metric is MOST meaningful?

A. Mean time to detect and respond to confirmed security incidents over time
B. Number of security certifications held by individual team members on staff
C. Total count of firewall rules currently configured across all network devices
D. Total annual budget allocated to the information security department budget

Answer: A

Q1130. An organization adopts a risk transfer strategy for a specific cyber threat. What does this typically involve?

A. Purchasing cyber insurance to shift the financial burden of a potential breach
B. Implementing additional technical controls to fully eliminate the identified risk
C. Accepting the risk without any changes to current operations and security posture
D. Ignoring the identified risk entirely because the likelihood is considered minimal

Answer: A

Q1131. An organization implements RBAC but discovers that a junior analyst can access executive financial reports. What is the MOST likely cause?

A. The analyst discovered a zero-day exploit in the access control subsystem
B. The RBAC system has a software bug that randomly grants elevated permissions
C. Network segmentation failure allows unauthorized traffic to reach the server
D. Role definitions are too broad and include permissions beyond job requirements

Answer: D

Q1132. A security architect must choose between preventive and detective controls for a limited budget. What is the BEST strategy?

A. Invest entirely in preventive controls since prevention eliminates the need for detection
B. Defer all investment until the budget allows for implementing both control types fully
C. Balance both control types since prevention reduces incidents and detection catches gaps
D. Invest entirely in detective controls since detection is always cheaper than prevention

Answer: C

Q1133. When applying the Clark-Wilson integrity model, what mechanism ensures data consistency?

A. Periodic deletion of old data items to maintain storage efficiency across servers
B. Well-formed transactions through constrained data items and transformation procedures
C. Unrestricted access to data items by any authenticated user in the system
D. Mandatory encryption of all data items at rest and in transit across all systems

Answer: B

Q1134. An organization finds that employees share credentials to bypass access restrictions. Which combination of controls BEST addresses this?

A. Increasing the maximum number of concurrent sessions allowed for each user account
B. Multi-factor authentication combined with behavioral analytics and session monitoring
C. Stronger password complexity rules combined with more frequent password rotation policies
D. Implementing longer password expiration periods with reduced login attempt thresholds

Answer: B

Q1135. In the Bell-LaPadula model, what does the 'no write down' rule prevent?

A. Users from reading data at a higher classification level than their clearance
B. Applications from creating temporary files on shared network storage volumes
C. Users from writing data to a lower classification level causing data leakage
D. Administrators from deleting files that are marked as system-critical assets

Answer: C

Q1136. A company merges with another organization that uses different security standards. What is the FIRST step for security integration?

A. Merging all user accounts into one directory without modifying access permissions
B. Immediately applying the stricter security standards across both organizations
C. Conducting a gap analysis to identify differences in security controls and policies
D. Replacing all security tools in both organizations with a single vendor solution

Answer: C

Q1137. Which scenario BEST illustrates a violation of the separation of duties principle?

A. A security analyst monitors alerts while an incident responder handles confirmed breaches
B. A developer writes code while a separate quality team reviews and approves the deployment
C. A project manager assigns tasks while team leads independently track milestone progress
D. A single administrator both creates user accounts and approves their own access requests

Answer: D

Q1138. An organization's quantitative risk analysis calculates an ALE of $500,000 for a specific threat. The proposed countermeasure costs $600,000 annually. What is the BEST decision?

A. Defer the decision until the annualized loss expectancy increases above the threshold
B. Implement the countermeasure and increase the security budget to cover the difference
C. Implement the countermeasure because any protection is worth the investment overall
D. Reject the countermeasure because its cost exceeds the annualized loss expectancy

Answer: D

Q1139. What is the primary advantage of using attribute-based access control over role-based access control?

A. ABAC provides finer-grained access decisions based on multiple contextual attributes
B. ABAC is simpler to implement and requires significantly less administrative overhead
C. ABAC requires fewer computing resources and scales better on minimal hardware
D. ABAC eliminates the need for any user authentication before granting system access

Answer: A

Q1140. How does the Biba integrity model differ from the Bell-LaPadula confidentiality model?

A. Biba focuses on availability while Bell-LaPadula focuses on authentication mechanisms
B. Biba allows unrestricted access while Bell-LaPadula enforces mandatory access controls
C. Biba is only applicable to military systems while Bell-LaPadula is used commercially
D. Biba uses no read down and no write up to protect integrity of data classifications

Answer: D

Q1141. An organization must protect data against future quantum computing attacks. Which cryptographic approach should they adopt?

A. Switching from AES-256 to AES-128 for faster encryption processing speed
B. Implementing post-quantum cryptographic algorithms like lattice-based schemes
C. Increasing RSA key sizes to 4096 bits for stronger conventional encryption
D. Using triple DES instead of AES for backward compatibility with systems

Answer: B

Q1142. A developer uses ECB mode to encrypt user profile images. What vulnerability does this introduce?

A. ECB mode is too slow for image encryption causing application timeouts
B. ECB mode requires keys that are too long for practical image encryption use
C. ECB mode produces identical ciphertext for identical plaintext blocks revealing patterns
D. ECB mode cannot handle binary data formats like images and only works with text

Answer: C

Q1143. During a TLS handshake, what is the purpose of the server's digital certificate?

A. To establish the symmetric session key used for bulk data encryption directly
B. To authenticate the server's identity and provide its public key to the client
C. To encrypt all subsequent data transmitted between the client and the server
D. To verify the client's identity before allowing any connection to be established

Answer: B

Q1144. An attacker performs a birthday attack against a hash function. What is the attacker exploiting?

A. Side-channel information leaked through timing of the hash computation
B. Buffer overflow vulnerabilities in the hash function software implementation
C. Weak password policies that allow users to set easily guessable passwords
D. The probability that two different inputs produce the same hash output value

Answer: D

Q1145. Why is key stretching used in password-based key derivation functions like PBKDF2?

A. To reduce the length of the derived key for efficient storage in databases
B. To make brute-force attacks slower by increasing computational cost per attempt
C. To convert asymmetric keys into symmetric keys for hybrid encryption schemes
D. To enable multiple users to share the same derived key without coordination

Answer: B

Q1146. In a hybrid encryption scheme, how are symmetric and asymmetric encryption combined?

A. Symmetric encryption is used for authentication while asymmetric handles data integrity
B. Asymmetric encryption secures the symmetric key which then encrypts the bulk data
C. Both algorithms encrypt the same data independently for redundancy and verification
D. Asymmetric encryption protects the bulk data while symmetric encryption protects the keys

Answer: B

Q1147. What is homomorphic encryption and why is it significant for cloud computing?

A. Encryption that allows computations on ciphertext producing results matching plaintext operations
B. Encryption that only works within a single cloud provider's proprietary infrastructure
C. Encryption that uses identical keys across all cloud servers for simplified key management
D. Encryption that automatically scales key sizes based on the current computational workload

Answer: A

Q1148. A security team discovers that their certificate authority's private key has been compromised. What is the MOST critical immediate action?

A. Notifying end users to temporarily ignore certificate warnings in their browsers
B. Revoking all certificates issued by the compromised CA and reissuing from a new CA
C. Generating new public keys for all end-user certificates across the organization
D. Increasing the key length of the compromised CA certificate to strengthen security

Answer: B

Q1149. What is the primary security concern with using MD5 for integrity verification today?

A. MD5 is vulnerable to collision attacks making it unreliable for integrity checks
B. MD5 requires excessive computational resources compared to newer hash algorithms
C. MD5 can only hash text data and cannot process binary files or media content
D. MD5 produces output that is too long for efficient storage in modern databases

Answer: A

Q1150. How does a hardware security module (HSM) enhance cryptographic key management?

A. By converting all asymmetric keys to symmetric keys for faster processing speeds
B. By automatically distributing encryption keys to all devices on the local network
C. By compressing encryption keys to reduce the required storage space significantly
D. By storing keys in tamper-resistant hardware that prevents unauthorized key extraction

Answer: D

Q1151. An organization detects lateral movement within their network after an initial breach. Which network control would MOST effectively limit this?

A. Implementing micro-segmentation with strict inter-segment access control policies
B. Upgrading the external firewall to a newer model with higher throughput capacity
C. Deploying additional wireless access points throughout the building for coverage
D. Increasing the bandwidth of the core network switches to handle more traffic loads

Answer: A

Q1152. During a DDoS attack, the security team notices traffic from thousands of spoofed source IPs. Which mitigation is MOST effective?

A. Disabling all network interfaces until the attack subsides and traffic normalizes
B. Increasing server hardware resources to absorb the additional malicious traffic load
C. Using upstream provider scrubbing services with BGP flowspec to filter attack traffic
D. Blocking each individual spoofed IP address manually in the perimeter firewall rules

Answer: C

Q1153. A penetration tester discovers that VLAN hopping is possible on the network. What misconfiguration is MOST likely responsible?

A. Spanning tree protocol enabled with default priority values on all switch devices
B. Trunk ports configured with native VLAN matching user access VLAN assignments
C. DHCP snooping disabled on trunk ports connecting distribution and core switches
D. Access ports configured with the correct VLAN but incorrect speed auto-negotiation

Answer: B

Q1154. What is the primary advantage of implementing a zero trust network architecture?

A. Eliminating the need for any network firewalls or intrusion prevention systems
B. Reducing network complexity by consolidating all traffic through a single gateway
C. Automatically encrypting all data at rest without requiring application-level changes
D. Verifying every access request regardless of whether it originates inside the network

Answer: D

Q1155. An analyst notices DNS tunneling in network logs. What is the attacker MOST likely trying to achieve?

A. Improving network performance by bypassing the organization's proxy server
B. Speeding up DNS resolution by caching responses on the local DNS server
C. Testing the resilience of the DNS infrastructure against denial of service
D. Exfiltrating data or establishing command-and-control channels via DNS queries

Answer: D

Q1156. A company implements network detection and response (NDR). What capability does NDR primarily add beyond traditional IDS?

A. NDR replaces the need for endpoint detection and response tools on workstations
B. NDR provides faster packet forwarding speeds than traditional IDS appliances can
C. NDR uses behavioral analytics and machine learning to detect unknown threat patterns
D. NDR eliminates false positive alerts entirely through deterministic rule matching

Answer: C

Q1157. What is BGP hijacking and why is it dangerous?

A. Exploiting BGP to advertise false routes, redirecting internet traffic through attacker-controlled networks
B. Attacking the BGP daemon process to crash border routers and cause widespread network service outages
C. Intercepting BGP keepalive messages to prevent routers from maintaining their established peer sessions
D. Using BGP messages to flood internal routing tables causing memory exhaustion on core switch devices

Answer: A

Q1158. An organization uses deep packet inspection (DPI) but encrypted traffic is increasing. What is the BEST approach to maintain visibility?

A. Deploying TLS inspection proxies that decrypt, inspect, and re-encrypt the traffic
B. Downgrading encryption standards to weaker ciphers that are easier to inspect
C. Banning all encrypted traffic on the corporate network to maintain full inspection
D. Switching entirely to metadata analysis and abandoning payload inspection efforts

Answer: A

Q1159. What is the security risk of running network services on default ports?

A. Default ports cannot be protected by firewalls due to protocol specification limits
B. Attackers can easily identify and target services running on well-known default ports
C. Default ports consume more bandwidth than non-standard ports on network devices
D. Default ports are inherently less secure than non-standard ports at the protocol level

Answer: B

Q1160. How does software-defined networking (SDN) improve network security management?

A. SDN centralizes control enabling dynamic, programmable security policy enforcement
B. SDN automatically encrypts all traffic without requiring any additional configuration
C. SDN replaces all traditional security tools including firewalls and IDS solutions
D. SDN eliminates the need for physical network infrastructure entirely in all cases

Answer: A

Q1161. A Linux server is compromised via a kernel exploit that bypasses all userspace security controls. Which hardening mechanism would have BEST mitigated this?

A. Enabling Kernel Address Space Layout Randomization and Secure Boot with signed kernels
B. Installing additional antivirus software with real-time scanning enabled on the server
C. Configuring iptables with strict ingress and egress filtering rules on all interfaces
D. Implementing disk quotas to limit the amount of storage each user account can consume

Answer: A

Q1162. An attacker uses a return-oriented programming (ROP) attack. Which OS security mechanisms specifically counter this technique?

A. Disk encryption and secure boot processes that verify operating system integrity
B. File permission checks and user account control prompts before executing programs
C. Network firewall rules that block incoming connections from suspicious IP addresses
D. Control Flow Integrity and Shadow Stack implementations in the processor and compiler

Answer: D

Q1163. A containerized application escapes its container and gains host access. What is the MOST effective prevention mechanism?

A. Using rootless containers with user namespaces and mandatory access control policies
B. Running containers with root privileges to ensure all security modules are accessible
C. Disabling all container networking to prevent communication with the host system
D. Allocating more CPU and memory resources to the container for improved isolation

Answer: A

Q1164. An organization discovers a rootkit embedded in their server OS. What makes rootkits particularly dangerous compared to other malware?

A. Rootkits only target mobile operating systems and cannot infect desktop computers
B. Rootkits spread faster than worms across networks using standard network protocols
C. Rootkits modify the OS kernel or firmware to hide their presence from security tools
D. Rootkits are larger in file size than other malware making them consume more disk space

Answer: C

Q1165. What is the security advantage of using immutable infrastructure for OS deployments?

A. Immutable systems are faster because they do not need to load any security modules
B. Immutable systems never require updates because they are inherently secure by design
C. Immutable systems are replaced entirely rather than patched, preventing persistent compromise
D. Immutable systems allow administrators to modify configurations at any time without risk

Answer: C

Q1166. A system administrator needs to detect fileless malware that operates entirely in memory. Which approach is MOST effective?

A. Scanning network traffic logs for unusual DNS queries originating from external servers
B. Using endpoint detection and response tools with memory analysis and behavioral monitoring
C. Checking file integrity using checksums against a known-good baseline of all system files
D. Running traditional signature-based antivirus scans on all files stored on disk

Answer: B

Q1167. What is the security risk of symlink race conditions in Unix-like operating systems?

A. They consume excessive disk space by duplicating files across multiple directory paths
B. They prevent legitimate users from accessing their home directories during peak usage
C. They allow attackers to redirect privileged operations to unintended files via symbolic links
D. They cause system slowdowns by creating circular references in the filesystem structure

Answer: C

Q1168. How does Windows Credential Guard protect authentication credentials?

A. By storing credentials in an encrypted file on the system drive protected by BitLocker
B. By requiring all users to change their passwords every seven days automatically
C. By isolating credential processes in a virtualization-based security container from the OS
D. By disabling all remote authentication protocols to prevent credential interception

Answer: C

Q1169. A security team must secure a system running legacy software that cannot be patched. What is the BEST compensating strategy?

A. Replacing all other systems on the network with the same legacy software for consistency
B. Isolating the system with strict network segmentation, monitoring, and application whitelisting
C. Ignoring the risk since the legacy software has been stable for many years without issues
D. Granting administrator access to all users so they can manually address security concerns

Answer: B

Q1170. What is the security significance of Trusted Platform Module (TPM) in OS security?

A. TPM increases CPU processing speed to enable faster encryption and decryption operations
B. TPM automatically installs operating system updates without requiring administrator input
C. TPM replaces the need for software-based firewalls by filtering traffic in hardware only
D. TPM provides a hardware root of trust for secure boot, key storage, and platform integrity

Answer: D

Q1171. A web application uses JWT tokens for authentication. An attacker changes the algorithm header to 'none'. What vulnerability does this exploit?

A. Insecure session management allowing unlimited concurrent sessions for each user account
B. Cross-site request forgery enabling unauthorized actions on behalf of authenticated users
C. JWT algorithm confusion attack bypassing signature verification when none is accepted
D. Server-side template injection allowing arbitrary code execution on the web application

Answer: C

Q1172. A penetration tester discovers a blind SQL injection vulnerability. How does blind SQL injection differ from standard SQL injection?

A. Blind SQL injection requires physical access to the database server for exploitation
B. Blind SQL injection infers data from application behavior rather than direct query output
C. Blind SQL injection cannot extract any data from the database regardless of technique
D. Blind SQL injection only works against NoSQL databases and not relational databases

Answer: B

Q1173. An application is vulnerable to server-side template injection (SSTI). What is the primary risk?

A. Attackers can execute arbitrary code on the server through template engine exploitation
B. Users can modify the visual layout and CSS styling of the application pages
C. The application performance degrades because templates are rendered on every request
D. Template files are exposed to search engines causing information disclosure publicly

Answer: A

Q1174. A security team discovers that their web application's deserialization process is vulnerable. What is the MOST severe potential impact?

A. Remote code execution through crafted serialized objects processed by the application
B. Loss of CSS styling information causing visual degradation on mobile device browsers
C. Slightly increased response times when processing large serialized data payloads
D. The application displays incorrect date formats in the user interface components

Answer: A

Q1175. How does a race condition vulnerability manifest in web applications?

A. Two concurrent requests exploit timing gaps to bypass validation or duplicate operations
B. Page loading speed varies based on the number of concurrent users on the platform
C. The application crashes when multiple users attempt to log in at the same exact time
D. Database queries return incorrect results when executed during high traffic periods

Answer: A

Q1176. A web application uses OAuth 2.0 for authentication. What is the primary risk of the 'open redirect' vulnerability in this context?

A. It allows attackers to steal authorization codes by redirecting to attacker-controlled URLs
B. It causes the OAuth server to crash when processing redirect URLs with special characters
C. It exposes the client secret in the URL parameters visible in the browser address bar
D. It prevents legitimate users from completing the authentication flow on mobile browsers

Answer: A

Q1177. What is a prototype pollution vulnerability in JavaScript web applications?

A. An attack that modifies the Object prototype to inject properties affecting all objects
B. An issue where deprecated JavaScript functions cause compatibility errors in browsers
C. A vulnerability where JavaScript files are served without proper content type headers
D. A memory leak caused by creating too many JavaScript objects without cleanup routines

Answer: A

Q1178. A web application allows file uploads. Which combination of controls BEST prevents malicious file upload attacks?

A. Limiting file size to one megabyte and allowing only uploads during business hours daily
B. Validating file type, scanning content, storing outside webroot, and renaming uploaded files
C. Only checking the file extension on the client side before allowing the upload to proceed
D. Compressing all uploaded files into ZIP archives and storing them on a shared network drive

Answer: B

Q1179. What is the security impact of HTTP request smuggling?

A. It exploits discrepancies between frontend and backend HTTP parsing to inject requests
B. It downgrades HTTPS connections to HTTP by modifying the request protocol header field
C. It causes web pages to load slower because requests are processed in an incorrect order
D. It prevents the server from processing legitimate user requests during peak traffic hours

Answer: A

Q1180. How does Subresource Integrity (SRI) protect web applications that use CDN-hosted scripts?

A. By caching CDN resources locally so they load faster regardless of CDN server status
B. By verifying that fetched resources match expected cryptographic hashes before execution
C. By automatically updating CDN-hosted scripts when new versions become available online
D. By encrypting the communication channel between the browser and CDN server endpoints

Answer: B

Q1181. An organization is hit by ransomware that also exfiltrates data before encryption. What is this attack technique called?

A. Crypto-jacking where computing resources are hijacked to mine cryptocurrency secretly
B. Triple extortion where customers of the victim are also contacted for ransom payments
C. Double extortion where data is stolen and encrypted to pressure victims into paying
D. Single extortion where data is encrypted and a ransom is demanded for decryption

Answer: C

Q1182. A threat actor uses living-off-the-land techniques (LOLBins) during an attack. Why is this approach effective?

A. Because using legitimate system tools avoids triggering signature-based security detections
B. Because system binaries can be modified without administrator privileges on any system
C. Because custom malware tools are faster than legitimate system binaries for attacks
D. Because legitimate tools provide encryption capabilities not available in custom malware

Answer: A

Q1183. An APT group maintains persistence on a compromised system for months. Which technique is MOST commonly used for long-term persistence?

A. Physically accessing the server room weekly to reinstall their malware on the server
B. Continuously running brute force attacks against the same system to maintain access
C. Creating scheduled tasks and modifying registry run keys to survive system reboots
D. Sending daily phishing emails to the same users to re-establish compromised access

Answer: C

Q1184. During malware analysis, a sample is identified as metamorphic. How does metamorphic malware differ from polymorphic malware?

A. Metamorphic malware only changes file names while polymorphic malware changes the entire file structure
B. Metamorphic malware is exclusive to mobile devices while polymorphic malware targets desktop systems
C. Metamorphic malware spreads faster than polymorphic malware across networks due to its smaller size
D. Metamorphic malware completely rewrites its own code while polymorphic malware only encrypts its payload

Answer: D

Q1185. A company discovers that attackers used a compromised software update mechanism to distribute malware. What type of attack is this?

A. Man-in-the-middle attack intercepting downloads between the vendor and customer networks
B. Supply chain attack leveraging trusted software distribution channels for malware delivery
C. Watering hole attack targeting employees who visit the software vendor's support website
D. Brute force attack against the software vendor's authentication system and user accounts

Answer: B

Q1186. An incident responder identifies that malware communicates using DNS TXT records for command and control. Why is this technique effective?

A. DNS TXT records can carry arbitrary data and DNS traffic is often allowed through firewalls
B. DNS TXT records are not logged by any DNS server making forensic investigation impossible
C. DNS TXT records travel faster than other DNS record types due to priority routing protocols
D. DNS TXT records are encrypted by default making them invisible to all security monitoring tools

Answer: A

Q1187. What is the MITRE ATT&CK framework and how does it help in understanding malware attacks?

A. A vulnerability scanner that automatically detects and patches malware on infected systems
B. A firewall configuration standard that blocks all known malware communication protocols
C. An encryption standard used by government agencies to protect classified communications
D. A knowledge base of adversary tactics and techniques based on real-world attack observations

Answer: D

Q1188. An organization's EDR detects PowerShell executing encoded commands at 3 AM. What type of attack behavior does this MOST likely indicate?

A. A scheduled system maintenance script running automated update and cleanup operations
B. A developer testing deployment scripts in the production environment during quiet hours
C. Malicious activity using encoded PowerShell for obfuscation during low-monitoring periods
D. An automated backup process that requires elevated PowerShell execution permissions

Answer: C

Q1189. What is process injection and why do attackers use it?

A. Injecting malicious code into a legitimate running process to evade detection and gain its privileges
B. Creating new malicious processes with random names to confuse system administrators during analysis
C. Modifying the process scheduler to give malware higher priority than legitimate system applications
D. Injecting monitoring code into malware processes to observe their behavior for research purposes

Answer: A

Q1190. A threat intelligence report describes malware that uses domain generation algorithms (DGA). What is the purpose of DGA?

A. Creating legitimate websites that appear in search engine results to attract potential victims
B. Generating secure domain names for the attacker's personal websites and email services
C. Automatically registering domain names that are about to expire for resale profit purposes
D. Generating random domain names for C2 communication making it difficult to block all domains

Answer: D

Q1191. An organization implements a zero trust model. How should authentication change compared to traditional perimeter-based security?

A. Authentication is only required once at the network perimeter and then trusted throughout
B. Authentication is only required for external users while internal users are auto-trusted
C. Authentication is eliminated entirely because the zero trust model makes it unnecessary
D. Continuous authentication and verification is required for every resource access request

Answer: D

Q1192. A company discovers that an attacker used a golden ticket attack in Active Directory. What does this attack achieve?

A. It disables all group policies allowing unrestricted software installation on endpoints
B. It modifies DNS records to redirect all domain traffic to attacker-controlled servers
C. It resets all user passwords in the domain forcing everyone to create new credentials
D. It creates a forged Kerberos TGT granting unrestricted access to any domain resource

Answer: D

Q1193. What is the security risk of using bearer tokens without additional binding in OAuth 2.0?

A. Bearer tokens cannot be revoked once issued requiring server restarts to invalidate
B. Bearer tokens expire too quickly making them impractical for long-running sessions
C. Bearer tokens are too large in size causing performance issues in network requests
D. Anyone possessing the token can use it, making stolen tokens immediately exploitable

Answer: D

Q1194. An attacker performs a pass-the-hash attack. What makes this attack possible?

A. LDAP queries return password hashes to any authenticated user who requests directory data
B. NTLM authentication allows authentication using the password hash without the actual password
C. DNS service records expose password hashes when queried with specific malformed requests
D. Kerberos tickets are stored in plaintext on the domain controller's hard drive permanently

Answer: B

Q1195. How does risk-based adaptive authentication improve security?

A. It eliminates all authentication requirements to improve user experience and speed
B. It dynamically adjusts authentication requirements based on contextual risk signals
C. It uses the same authentication method regardless of the risk level of the access
D. It requires maximum authentication strength for all access requests at all times

Answer: B

Q1196. An organization deploys FIDO2 hardware keys for authentication. What is the primary attack vector this eliminates?

A. Physical theft attacks because FIDO2 keys cannot be used by anyone other than the owner
B. Phishing attacks because FIDO2 keys are bound to specific origins and resist credential theft
C. Malware attacks because FIDO2 keys include built-in antivirus scanning for connected devices
D. Denial of service attacks because FIDO2 keys provide faster authentication to all services

Answer: B

Q1197. What is the security challenge of implementing SSO across an organization?

A. SSO cannot work with cloud applications and is limited to on-premises systems only
B. A compromised SSO credential grants access to all connected applications simultaneously
C. SSO does not support multi-factor authentication and relies only on password access
D. SSO requires separate passwords for each application making it complex to manage

Answer: B

Q1198. How does certificate-based authentication provide stronger security than password-based authentication?

A. Certificates are shorter than passwords making them faster to process during authentication
B. Certificates use asymmetric cryptography and cannot be phished or replayed like passwords
C. Certificates work without any network connection making them suitable for offline access
D. Certificates do not expire so they never need to be renewed or rotated by administrators

Answer: B

Q1199. An organization needs to implement step-up authentication. In what scenario is this MOST appropriate?

A. When a system administrator performs routine maintenance on non-critical services
B. When a user initially logs in to access their basic email and calendar application
C. When a new employee creates their initial account during the onboarding process
D. When an already authenticated user attempts to access a highly sensitive resource

Answer: D

Q1200. What is Kerberoasting and how does it exploit Active Directory authentication?

A. Modifying Kerberos configuration files to disable ticket encryption on the domain controllers
B. Intercepting Kerberos tickets in transit by performing ARP spoofing on the network segment
C. Requesting service tickets for service accounts and cracking them offline to obtain passwords
D. Flooding the Key Distribution Center with ticket requests to cause a denial of service

Answer: C

Q1201. A development team discovers a critical vulnerability in a third-party library used across all their applications. What is the MOST effective response?

A. Rewriting all applications from scratch without using any third-party library dependencies
B. Assessing impact, applying patches or mitigations, and implementing SCA in the CI/CD pipeline
C. Removing the library immediately without considering functionality impact on applications
D. Ignoring the vulnerability because third-party libraries are the vendor's sole responsibility

Answer: B

Q1202. How does interactive application security testing (IAST) combine benefits of SAST and DAST?

A. IAST only works on interpreted languages while SAST and DAST work on compiled languages
B. IAST replaces both SAST and DAST entirely by using artificial intelligence for scanning
C. IAST runs SAST and DAST tools simultaneously in separate processes for speed improvement
D. IAST instruments the application to analyze code execution during runtime testing activities

Answer: D

Q1203. A CI/CD pipeline has no security gates. What risks does this introduce and what should be implemented?

A. Vulnerable code reaches production; implement SAST, DAST, SCA, and secret scanning gates
B. No risk since CI/CD automation inherently eliminates all security vulnerabilities in code
C. Only compliance risks exist; implement audit logging at the deployment stage exclusively
D. Only performance risks exist; implement load testing gates to validate application speed

Answer: A

Q1204. What is the security risk of hardcoded secrets in source code?

A. Hardcoded secrets only pose a risk if the application is written in interpreted languages
B. Hardcoded secrets make the code run slower because encryption is computed at every startup
C. Secrets in code are exposed in version control history even after removal from current files
D. Secrets in code are automatically protected by the compiler during the build optimization

Answer: C

Q1205. How does runtime application self-protection (RASP) provide security?

A. RASP scans source code before compilation to identify potential security vulnerabilities early
B. RASP monitors network traffic outside the application to filter malicious request patterns
C. RASP instruments the application to detect and block attacks from within the running application
D. RASP encrypts all application data at rest to prevent unauthorized access to stored files

Answer: C

Q1206. A development team uses microservices architecture. What unique security challenges does this introduce?

A. No unique challenges since microservices security is identical to monolithic application security
B. Only performance challenges exist since microservices do not introduce any new security concerns
C. Increased attack surface from inter-service communications requiring mutual authentication and encryption
D. Reduced attack surface because microservices are inherently more secure than monolithic applications

Answer: C

Q1207. What is the security significance of Software Bill of Materials (SBOM)?

A. SBOM is a financial document listing the costs of all software licenses for budget management
B. SBOM provides a complete inventory of software components enabling vulnerability tracking and response
C. SBOM is a testing report showing the results of all security scans performed on the software
D. SBOM is a deployment guide listing the steps required to install software on production servers

Answer: B

Q1208. A penetration tester finds that the application is vulnerable to mass assignment. What is this vulnerability?

A. An attacker modifies object properties by injecting unexpected parameters into API requests
B. An attacker assigns administrator roles to all users by exploiting a database trigger flaw
C. An attacker overwhelms the server by sending thousands of simultaneous assignment operations
D. An attacker copies large amounts of data by exploiting a flaw in the file download feature

Answer: A

Q1209. What is the purpose of security regression testing?

A. Verifying that previously fixed security vulnerabilities are not reintroduced by new code changes
B. Scanning the production environment for new zero-day vulnerabilities not found during development
C. Testing the application performance under heavy load to identify potential denial of service risks
D. Reviewing the application source code for compliance with organizational coding style guidelines

Answer: A

Q1210. How does a security-focused infrastructure as code (IaC) scanning tool improve deployment security?

A. It encrypts all infrastructure configuration files to prevent unauthorized access to server settings
B. It detects misconfigurations and security policy violations in infrastructure definitions before deployment
C. It replaces the need for network firewalls by implementing security rules within the code itself
D. It automatically fixes all application code vulnerabilities found during the build compilation process

Answer: B

Q1211. An organization discovers that employees' mobile devices are connecting to an evil twin access point in their parking lot. What is the MOST comprehensive solution?

A. Simply changing the corporate WiFi password and notifying employees via company-wide email
B. Banning all wireless device usage on the company premises to eliminate wireless attack surface
C. Deploying WIPS with rogue AP detection, enforcing VPN usage, and implementing 802.1X authentication
D. Installing signal jammers in the parking lot to prevent all wireless connections from working

Answer: C

Q1212. A mobile application stores sensitive data in shared preferences without encryption. What is the primary attack vector this enables?

A. Data extraction from the device's unencrypted shared preferences via backup or root access
B. Credential theft through man-in-the-middle attacks on the application's API communications
C. Denial of service against the application by filling shared preferences with random data
D. Remote exploitation of the application through the mobile operating system's network stack

Answer: A

Q1213. What is the security implication of 5G network slicing from a cyber security perspective?

A. 5G slicing reduces bandwidth making traditional wireless attacks completely ineffective
B. 5G slicing eliminates all wireless security concerns by design through quantum encryption
C. 5G slicing is only relevant for consumer devices and has no enterprise security implications
D. Compromise of one slice could potentially affect other slices if isolation controls are insufficient

Answer: D

Q1214. An attacker uses a Stingray device near a corporate office. What type of attack is this?

A. A Bluetooth sniffing attack that captures data from nearby paired mobile device connections
B. An IMSI catcher attack that intercepts mobile communications by impersonating a cell tower
C. A WiFi jamming attack that disrupts all wireless network signals within a building area
D. A GPS spoofing attack that provides false location data to mobile navigation applications

Answer: B

Q1215. A company implements a zero trust approach for mobile devices. What is the MOST critical component?

A. Allowing unrestricted access once the device passes an initial security check at enrollment
B. Trusting all devices on the corporate WiFi network and blocking only external connections
C. Requiring biometric authentication only for the initial device unlock at the start of day
D. Continuous device posture assessment and risk-based conditional access for every request

Answer: D

Q1216. What is the security risk of mobile deep links and how can they be exploited?

A. Deep links expose the application source code to reverse engineering through URL scheme analysis
B. Deep links increase application size making mobile devices slower and consuming excessive storage
C. Attackers craft malicious deep links to redirect users to phishing pages or trigger unauthorized actions
D. Deep links prevent the application from receiving push notifications from the backend server

Answer: C

Q1217. How does a Wi-Fi pineapple device facilitate wireless attacks?

A. It generates random WiFi networks to confuse nearby devices and prevent them from connecting
B. It automates evil twin, deauth, and man-in-the-middle attacks on wireless networks for penetration testing
C. It increases WiFi signal range allowing attackers to connect to distant corporate wireless networks
D. It blocks all wireless signals in an area creating a denial of service for all wireless devices

Answer: B

Q1218. An enterprise deploys EMM (Enterprise Mobility Management). How does EMM differ from basic MDM?

A. EMM only manages device hardware while MDM manages both hardware and installed applications
B. EMM replaces all security controls while MDM supplements existing security infrastructure
C. EMM includes MDM plus mobile application management, content management, and identity management
D. EMM is exclusively for iOS devices while MDM supports only Android mobile operating systems

Answer: C

Q1219. What is the security concern with wireless mesh networks in IoT deployments?

A. Each mesh node is a potential attack point and compromise can propagate through the entire network
B. Mesh networks provide too much bandwidth making it easy for attackers to exfiltrate large data
C. Mesh networks cannot be encrypted because the routing protocol requires plaintext communication
D. Mesh networks are immune to all wireless attacks because they use frequency hopping technology

Answer: A

Q1220. A mobile app development team implements runtime application self-protection. How does this specifically benefit mobile security?

A. RASP detects and prevents tampering, debugging, and exploitation attempts within the running app
B. RASP automatically updates the mobile application without requiring app store review approval
C. RASP replaces the need for encryption by preventing all unauthorized access at the OS level
D. RASP eliminates the need for any server-side security controls by handling everything on device

Answer: A

Q1221. An organization discovers that an attacker accessed their cloud environment using stolen API keys from a public GitHub repository. What series of actions is MOST appropriate?

A. Banning all developers from using version control systems to prevent future key exposure
B. Migrating all workloads to a different cloud provider to prevent similar future incidents
C. Immediately rotating compromised keys, auditing access logs, implementing secret scanning, and reviewing damage
D. Only deleting the exposed keys from the GitHub repository and continuing normal operations

Answer: C

Q1222. How does a cloud-native SIEM differ from a traditional on-premises SIEM?

A. Cloud SIEM is identical to traditional SIEM except it runs on virtual machines in the cloud
B. Cloud SIEM provides less security visibility because it cannot access on-premises network traffic
C. Cloud SIEM only works with a single cloud provider and cannot ingest logs from other sources
D. Cloud SIEM scales elastically, integrates with cloud APIs, and reduces infrastructure management overhead

Answer: D

Q1223. What is the primary security risk of cross-account access in multi-account cloud environments?

A. Cross-account access always requires physical network connections between cloud data centers
B. Cross-account access is inherently secure because cloud providers enforce strict isolation
C. Cross-account access eliminates all identity management because users share a single identity
D. Overly permissive trust policies between accounts can enable lateral movement across the organization

Answer: D

Q1224. A company uses Kubernetes in production. What is the MOST critical security concern for the cluster?

A. Disabling all logging to improve cluster performance and reduce storage costs for log files
B. Allowing all pods to run as root to simplify application deployment and avoid permission issues
C. Ensuring the cluster uses the maximum number of nodes to handle any distributed denial of service
D. Securing the API server, implementing RBAC, network policies, and scanning container images for vulnerabilities

Answer: D

Q1225. What is the confused deputy problem in cloud security?

A. A network routing issue where traffic intended for one VPC is accidentally sent to a different one
B. A vulnerability where a trusted service is tricked into performing unauthorized actions on behalf of an attacker
C. A bug in cloud billing systems that charges the wrong customer account for resource consumption
D. A situation where multiple cloud administrators have conflicting security policies applied simultaneously

Answer: B

Q1226. How does infrastructure as code (IaC) introduce security risks in cloud deployments?

A. IaC only affects development environments and has no impact on production security posture
B. IaC templates can codify misconfigurations that are then consistently deployed across all environments
C. IaC templates are automatically scanned by cloud providers preventing any security misconfigurations
D. IaC eliminates all security risks because automated deployments are inherently more secure

Answer: B

Q1227. An organization implements a multi-cloud strategy. What is the PRIMARY security challenge this introduces?

A. Reducing the total cost of cloud services by negotiating volume discounts with providers
B. Synchronizing time zones between different cloud provider regions for consistent logging
C. Maintaining consistent security policies and visibility across different cloud provider environments
D. Ensuring all cloud providers use identical hardware specifications in their data centers

Answer: C

Q1228. What is the security implication of instance metadata services (IMDS) in cloud environments?

A. IMDS is only accessible from the cloud provider's management console and not from instances
B. SSRF attacks can access IMDS to retrieve instance credentials and escalate privileges in the cloud
C. IMDS automatically rotates all credentials making them useless even if they are intercepted
D. IMDS provides no security-relevant information and is only used for instance performance metrics

Answer: B

Q1229. What is the purpose of cloud security benchmarks like CIS Benchmarks for cloud providers?

A. Comparing the pricing and cost structures of competing cloud service provider offerings
B. Providing prescriptive security configuration guidelines specific to each cloud provider's services
C. Measuring the network performance and latency of different cloud provider data center regions
D. Rating the customer support quality of different cloud providers based on user surveys

Answer: B

Q1230. A cloud architect needs to protect sensitive workloads from the cloud provider's own administrators. What technology BEST addresses this?

A. Cloud provider managed keys which give the provider full access to encrypted data
B. Standard server-side encryption which protects data at rest from external attackers only
C. Confidential computing using hardware-based trusted execution environments for data in use
D. Network encryption using TLS for all data in transit between cloud services and users

Answer: C

Q1231. A forensic investigator encounters full disk encryption on a suspect's device. What is the MOST effective approach to access the data?

A. Ignoring the encrypted drive and relying solely on other unencrypted evidence sources
B. Capturing memory while the device is running to extract encryption keys before shutdown
C. Using brute force to crack the encryption key which is guaranteed to succeed quickly
D. Contacting the encryption software vendor to request a master decryption backdoor key

Answer: B

Q1232. During a forensic investigation, anti-forensic techniques are discovered. Which technique makes timestamp analysis unreliable?

A. Timestomping which modifies file timestamps to mislead investigators about event timing
B. Disk wiping which securely overwrites all data making recovery completely impossible
C. File encryption which prevents investigators from reading the content of seized files
D. Steganography which hides data within image files to prevent content-based detection

Answer: A

Q1233. A forensic team must analyze a cloud-based system. What unique challenge does cloud forensics present compared to traditional forensics?

A. Cloud forensics requires no specialized tools because standard disk imaging tools always work
B. Limited physical access to infrastructure, multi-tenancy, and jurisdiction complexities across regions
C. Cloud systems always store data in plaintext making the analysis process significantly faster
D. Cloud providers automatically preserve all forensic evidence eliminating the need for imaging

Answer: B

Q1234. An investigator analyzes Windows registry hives. What type of forensic evidence can be found in the NTUSER.DAT file?

A. System-wide network configuration settings including IP addresses and DNS server addresses
B. User-specific data including recent documents, typed URLs, mounted devices, and application history
C. Operating system installation date, service pack level, and licensed software product keys
D. Hardware inventory data including processor model, memory capacity, and disk serial numbers

Answer: B

Q1235. How does memory forensics help in analyzing fileless malware attacks?

A. Memory analysis only works on Linux systems and cannot be applied to Windows-based attacks
B. Memory forensics is unnecessary for fileless malware since it leaves traces on the hard drive
C. Memory analysis can reveal injected code, suspicious processes, and network connections invisible on disk
D. Memory forensics requires the suspect device to be powered off before analysis can begin

Answer: C

Q1236. A forensic investigation involves analyzing a compromised Docker container. What specific challenges does container forensics present?

A. Container ephemeral nature means evidence is lost when containers are destroyed or recreated
B. Containers cannot be compromised because they run in completely isolated security sandboxes
C. Containers always persist their complete state to disk making forensic imaging straightforward
D. Container forensics is identical to virtual machine forensics with no additional complexity

Answer: A

Q1237. What is the forensic significance of the Windows Event Log entry ID 4624?

A. It records successful logon events including logon type, source address, and authentication details
B. It records when new user accounts are created by administrators in the domain directory
C. It records when a user's account is locked out after exceeding maximum login attempt limits
D. It records failed logon attempts with the incorrect password that was entered by the user

Answer: A

Q1238. An investigator uses the Volatility framework for memory analysis. What primary capability does this tool provide?

A. Creating forensic images of hard drives using bit-level copying with hash verification
B. Generating automated forensic reports from evidence files without any manual analysis
C. Analyzing memory dumps to extract processes, network connections, registry hives, and malware artifacts
D. Scanning network traffic captures for signatures of known malware communication patterns

Answer: C

Q1239. How does browser forensics help in investigating cyber crimes?

A. Browser data is automatically deleted when the browser is closed making forensics impossible
B. Browser forensics requires the user's cooperation to provide their browsing history voluntarily
C. Browser artifacts reveal browsing history, cached pages, cookies, downloaded files, and stored credentials
D. Browser forensics can only recover the URLs of websites visited within the last twenty-four hours

Answer: C

Q1240. What is the Locard's Exchange Principle and how does it apply to digital forensics?

A. All digital evidence must be exchanged between prosecution and defense before trial begins
B. Evidence can only be collected from the suspect's primary device and not from any other source
C. Every digital interaction leaves traces on both systems, providing evidence of contact and activity
D. Digital evidence loses its value over time and must be analyzed within seventy-two hours

Answer: C

Q1241. During a major breach, the IR team discovers the attacker has compromised Active Directory. What is the MOST critical containment action?

A. Resetting the KRBTGT account password twice and all privileged account passwords immediately
B. Disconnecting the domain controller from the network and waiting for the vendor's support
C. Simply changing the domain administrator password and continuing the ongoing investigation
D. Rebuilding all workstations from scratch before addressing the domain controller compromise

Answer: A

Q1242. An organization experiences a supply chain compromise affecting a widely used library. How should the IR team prioritize their response?

A. Waiting for the library vendor to release a patch before taking any response actions at all
B. Only investigating systems that have already shown signs of compromise and ignoring others
C. Immediately removing the library from all systems regardless of the impact on business operations
D. Identifying all systems using the compromised library, assessing exposure, and implementing mitigations

Answer: D

Q1243. During incident response, the team suspects the attacker is monitoring their communications. What is the BEST approach?

A. Switching to out-of-band communication channels not accessible to the attacker for coordination
B. Broadcasting false information through compromised channels to mislead and confuse the attacker
C. Stopping all communication until the attacker has been fully removed from all systems
D. Continuing to use normal email and chat systems while being careful about what is discussed

Answer: A

Q1244. How should an IR team handle a situation where the attacker has deployed multiple backdoors across the network?

A. Removing backdoors one at a time over several weeks to minimize disruption to operations
B. Mapping all identified backdoors, planning simultaneous removal, and monitoring for re-establishment
C. Negotiating with the attacker to voluntarily remove the backdoors from compromised systems
D. Ignoring the backdoors and focusing solely on strengthening perimeter firewall rule sets

Answer: B

Q1245. An organization faces a data breach requiring notification under GDPR. What is the maximum timeframe for notifying the supervisory authority?

A. Within 30 calendar days of discovering the personal data breach event
B. Within 72 hours of becoming aware of the personal data breach event
C. Within 7 business days of completing the full investigation of the breach
D. Within 24 hours of the breach occurring regardless of discovery timing

Answer: B

Q1246. What is the primary benefit of implementing SOAR (Security Orchestration, Automation, and Response) in IR?

A. Replacing all human analysts with automated systems that handle every type of incident alone
B. Providing unlimited storage for security event logs without any cost or capacity limitations
C. Eliminating the need for incident response plans because automation handles everything directly
D. Automating repetitive response tasks and orchestrating tools to reduce response time and errors

Answer: D

Q1247. An IR team must decide whether to monitor an attacker or immediately contain the breach. What factors should guide this decision?

A. Ongoing risk to data, attacker's current activity level, legal obligations, and intelligence value
B. Only the cost of the monitoring equipment needed to track the attacker's network activities
C. Whether the attack is occurring during business hours or after regular working time periods
D. The personal preferences of the incident response team lead regarding investigation approach

Answer: A

Q1248. How does a threat hunting program complement traditional incident response?

A. Replacing incident response entirely with continuous proactive threat elimination processes
B. Proactively searching for threats that evade automated detection before they cause incidents
C. Only hunting for threats after an incident has been detected and reported by monitoring
D. Focusing exclusively on external threats while ignoring all potential insider threat actors

Answer: B

Q1249. During a breach investigation, the IR team finds the initial access occurred six months ago. What does this indicate about the organization's detection capabilities?

A. Six months of undetected access is normal and expected for all organizations of similar size
B. Significant detection gaps exist since the attacker maintained undetected access for an extended period
C. The detection systems were working correctly but were intentionally configured to delay alerts
D. The organization's detection capabilities are excellent because they eventually found the breach

Answer: B

Q1250. An organization's IR plan includes both technical and executive response procedures. Why is executive involvement critical during major incidents?

A. Executives perform the technical analysis because they have the deepest technical expertise
B. Executives authorize resource allocation, make business decisions, and manage external communications
C. Executives are only needed to sign off on the final incident report after full resolution
D. Executives should not be involved because their involvement slows down the response process

Answer: B

Q1251. A SOC team needs to reduce mean time to detect (MTTD) threats. Which approach is MOST effective?

A. Increasing the alert threshold to generate fewer alerts so analysts can review each one carefully
B. Hiring more analysts to manually review every single log entry generated across all systems
C. Implementing automated detection with tuned correlation rules, ML models, and threat intelligence integration
D. Reducing the number of monitored data sources to focus only on firewall logs for simplicity

Answer: C

Q1252. How does deception technology enhance security monitoring beyond traditional honeypots?

A. Encrypting all network traffic to prevent attackers from understanding the network architecture
B. Blocking all network traffic from unknown sources before it reaches any internal network system
C. Replacing all production systems with decoy systems to eliminate the real attack surface completely
D. Deploying decoy assets throughout the network that generate high-fidelity alerts on any interaction

Answer: D

Q1253. A SIEM generates thousands of alerts daily but only a small fraction are true positives. What is the BEST approach to improve alert quality?

A. Tuning detection rules, implementing alert scoring, and using contextual enrichment to prioritize alerts
B. Increasing the alert volume by adding more detection rules without evaluating existing ones
C. Disabling all alert rules and relying entirely on manual log review by security analysts
D. Forwarding all alerts directly to management without any analyst review or prioritization

Answer: A

Q1254. What is the primary challenge of monitoring encrypted traffic in a SOC?

A. Encrypted traffic cannot be captured by any network monitoring tools available on the market today
B. Encrypted traffic hides payload content requiring alternative approaches like metadata analysis or decryption
C. Encrypted traffic is identical to unencrypted traffic from a monitoring perspective in all cases
D. Encrypted traffic always indicates malicious activity and should be blocked by default at all times

Answer: B

Q1255. How should a SOC measure the effectiveness of its detection capabilities?

A. Counting the total number of alerts generated per day regardless of their quality or accuracy
B. Measuring only the number of incidents that resulted in data loss across the entire organization
C. Tracking the number of security tools deployed without evaluating their actual effectiveness
D. Using metrics like MTTD, MTTR, detection coverage mapped to ATT&CK, and false positive rates

Answer: D

Q1256. An organization implements a data lake for security analytics. What advantage does this provide over traditional SIEM?

A. Eliminating the need for any structured queries because data lakes organize data automatically
B. Providing real-time alerting capabilities that are not possible with any traditional SIEM tools
C. Storing massive volumes of raw data at lower cost enabling long-term analysis and threat hunting
D. Replacing all security analysts with automated systems that process data without human input

Answer: C

Q1257. What is the concept of 'purple teaming' and how does it improve security monitoring?

A. Collaboration between red and blue teams to improve detection rules and response procedures together
B. A compliance framework that requires organizations to conduct biannual security assessments only
C. A third-party team that replaces both offensive and defensive teams with automated testing tools
D. A training program exclusively for security operations center analysts to improve their soft skills

Answer: A

Q1258. A SOC analyst notices beaconing behavior in network traffic. What does this MOST likely indicate?

A. A legitimate application checking for software updates from the vendor's update server
B. Malware communicating with a command-and-control server at regular intervals for instructions
C. Network equipment sending heartbeat messages to confirm device connectivity and status
D. A user streaming video content which creates periodic network traffic burst patterns

Answer: B

Q1259. How does security monitoring need to adapt for serverless and containerized environments?

A. Monitoring must shift to application-level telemetry, API calls, and runtime behavior analysis
B. Serverless environments require no monitoring because cloud providers handle all security aspects
C. Traditional host-based monitoring tools work identically in serverless and container environments
D. Container monitoring only needs to check container image signatures at deployment time only

Answer: A

Q1260. What is the role of AI and machine learning in modern security monitoring?

A. Completely replacing all human security analysts with fully autonomous threat response systems
B. Detecting complex patterns and anomalies at scale that human analysts and rules cannot identify
C. Only generating marketing reports about security posture for executive board presentations
D. Slowing down threat detection because ML models require extensive computation time always

Answer: B

Q1261. An organization operates across multiple countries with different data protection laws. What is the MOST effective approach to compliance?

A. Storing all data in a single country to avoid dealing with multiple legal jurisdictions entirely
B. Ignoring all data protection laws because it is impossible to comply with all of them simultaneously
C. Implementing the strictest applicable standard as a baseline and adding jurisdiction-specific requirements
D. Complying only with the laws of the country where the organization's headquarters is located

Answer: C

Q1262. A security researcher discovers a critical vulnerability in widely-used software. Under what circumstances could disclosure become legally problematic?

A. If the researcher is employed by a competing software company in the same industry sector
B. If the vulnerability affects more than one hundred users across multiple different countries
C. If the researcher uses automated scanning tools rather than performing manual code review only
D. If disclosure occurs without vendor notification, outside a bug bounty scope, or violates CFAA provisions

Answer: D

Q1263. How does the concept of 'privacy by design' differ from traditional approaches to data privacy?

A. Privacy by design embeds privacy into systems from the start rather than adding it after development
B. Privacy by design only applies to mobile applications while traditional approaches cover all systems
C. Privacy by design eliminates the need for privacy policies by making systems inherently compliant
D. Privacy by design requires hiring a dedicated privacy team while traditional approaches do not

Answer: A

Q1264. An organization faces a conflict between a government's lawful data access request and GDPR data protection requirements. How should this be handled?

A. Deleting all requested data to prevent both the government and regulators from accessing it
B. Automatically complying with the government request and ignoring all data protection requirements
C. Refusing all government requests regardless of their legal basis or jurisdictional authority
D. Engaging legal counsel to evaluate the request, applying appropriate legal frameworks, and documenting decisions

Answer: D

Q1265. What is the legal significance of the Schrems II ruling for international data transfers?

A. It created a new encryption standard that must be used for all international data transfers
B. It permanently banned all data transfers between the European Union and the United States
C. It established that cloud providers are solely responsible for all international data compliance
D. It invalidated Privacy Shield and requires additional safeguards for EU-US personal data transfers

Answer: D

Q1266. How do whistleblower protection laws intersect with cyber security?

A. They mandate that all security incidents be reported to the media for public transparency
B. They require whistleblowers to have formal cyber security certifications before making reports
C. They protect individuals who report security violations or illegal activities from employer retaliation
D. They only protect whistleblowers in government organizations and not in private sector companies

Answer: C

Q1267. What legal challenges does the use of AI in cyber security decision-making present?

A. AI in cyber security is universally prohibited by international law across all jurisdictions globally
B. AI decisions may lack transparency, create liability issues, and potentially introduce discriminatory bias
C. AI decisions are always legally defensible because they are based on objective data processing only
D. AI decision-making eliminates all legal liability because responsibility shifts to the algorithm vendor

Answer: B

Q1268. An employee uses company resources to conduct unauthorized security testing on a third party. What legal liability does the organization face?

A. The organization is only liable if the testing successfully finds vulnerabilities in the third party
B. The organization may be vicariously liable for the employee's unauthorized actions using company resources
C. The organization is automatically protected by its acceptable use policy regardless of circumstances
D. The organization has no liability because unauthorized actions are solely the employee's responsibility

Answer: B

Q1269. How does the concept of 'digital sovereignty' affect cloud computing and data storage decisions?

A. Digital sovereignty eliminates the need for data encryption because national borders provide protection
B. Digital sovereignty only applies to government data and has no impact on commercial organizations
C. Digital sovereignty is a theoretical concept with no practical legal implications for organizations
D. Countries require data to be stored within their borders, affecting cloud architecture and provider selection

Answer: D

Q1270. What is the legal framework for active cyber defense measures and 'hack back' by private organizations?

A. Hack-back is legal as long as the organization documents the attacker's IP address beforehand
B. Private sector hack-back is generally illegal under most jurisdictions, with very limited exceptions
C. International law provides blanket immunity for all defensive cyber operations by organizations
D. Organizations have unrestricted legal authority to attack systems used to breach their networks

Answer: B

Q1271. How does quantum key distribution (QKD) fundamentally change secure communication?

A. QKD eliminates the need for key management because quantum keys never expire or need rotation
B. QKD replaces all existing encryption algorithms with faster quantum-based alternatives for performance
C. QKD only works over distances shorter than one meter making it impractical for any real deployment
D. QKD uses quantum mechanics to detect any eavesdropping attempt making interception theoretically detectable

Answer: D

Q1272. An organization considers implementing confidential computing. What specific security problem does this technology solve?

A. Improving network transmission security by implementing quantum-resistant encryption protocols everywhere
B. Protecting data during processing in hardware-isolated enclaves even from privileged system administrators
C. Encrypting data at rest using stronger algorithms than currently available standard encryption methods
D. Preventing physical theft of servers by implementing advanced biometric access controls on hardware

Answer: B

Q1273. How does the concept of 'shift everywhere' extend beyond traditional 'shift left' in DevSecOps?

A. Security responsibility shifts entirely to developers with no involvement from security teams
B. Security is applied at every stage including design, development, deployment, and runtime operations
C. All security testing is moved to the earliest possible development stage and never done elsewhere
D. Security testing shifts to production only because that is where real threats actually manifest

Answer: B

Q1274. What is the security implication of neuromorphic computing for future cyber threats?

A. Neuromorphic computing has no relevance to cyber security and only affects medical applications
B. Neuromorphic computers cannot be programmed for malicious purposes due to hardware constraints
C. Brain-inspired computing could enable more sophisticated AI attacks that mimic human decision patterns
D. Neuromorphic computing eliminates all cyber threats by processing data like a biological brain

Answer: C

Q1275. How does the concept of software-defined perimeter (SDP) improve upon traditional VPN security?

A. SDP hides infrastructure from unauthorized users entirely and provides least-privilege application access
B. SDP replaces all firewalls and IDS systems with a single unified network security appliance
C. SDP provides faster network speeds than VPN by eliminating all encryption overhead completely
D. SDP is only applicable to on-premises networks and cannot be used with cloud environments

Answer: A

Q1276. What are the security challenges of Web3 and decentralized applications?

A. Decentralized applications are inherently secure because they have no single point of failure
B. Web3 security is identical to Web2 security with no new threat models or attack surfaces
C. Smart contract vulnerabilities, private key management, and irreversible transactions create unique risks
D. Web3 eliminates all security risks through decentralization making traditional attacks impossible

Answer: C

Q1277. How does adversarial machine learning pose a threat to AI-powered security systems?

A. Adversarial ML only affects image recognition systems and has no impact on security applications
B. Adversarial ML improves security by training models to be more robust against future attacks
C. Attackers craft inputs that deceive ML models into misclassifying malicious activity as benign traffic
D. ML models are immune to adversarial inputs because they learn from millions of training examples

Answer: C

Q1278. What is the 'harvest now, decrypt later' threat in the context of quantum computing?

A. Organizations harvest threat intelligence now to decrypt future attack patterns using AI analysis
B. Security teams collect malware samples now for decryption and analysis at a later scheduled date
C. Adversaries collect encrypted data now planning to decrypt it when quantum computers become available
D. Cloud providers harvest encryption keys now to simplify key management processes in the future

Answer: C

Q1279. How does the concept of cyber threat intelligence platforms evolve with emerging technologies?

A. Platforms only focus on historical threat data and cannot incorporate real-time intelligence feeds
B. Platforms integrate AI for automated analysis, predict attack trends, and enable proactive defense strategies
C. Platforms become obsolete because automated security tools eliminate the need for threat intelligence
D. Platforms are replaced entirely by blockchain-based solutions that distribute intelligence automatically

Answer: B

Q1280. What is the emerging concept of cyber insurance and how does it impact organizational security posture?

A. Cyber insurance only covers physical damage to hardware and does not cover data breach expenses
B. Cyber insurance premiums are identical regardless of the organization's security maturity level
C. Cyber insurance transfers financial risk but requires demonstrating minimum security controls for coverage
D. Cyber insurance eliminates the need for security controls because all losses are financially covered

Answer: C

Q1281. An organization implements a risk-based approach to cyber security. How should residual risk be handled after applying security controls?

A. Residual risk should be completely eliminated before proceeding
B. Residual risk should be documented, accepted by management, and continuously monitored
C. Residual risk does not exist if proper controls are applied
D. Residual risk is only relevant during the initial risk assessment

Answer: B

Q1282. How does the Diamond Model of intrusion analysis differ from the Cyber Kill Chain?

A. The Diamond Model focuses only on malware classification
B. The Diamond Model analyzes intrusions using four core features (adversary, infrastructure, capability, victim) while the Kill Chain describes attack phases sequentially
C. The Cyber Kill Chain is only applicable to insider threats
D. The Diamond Model is a compliance framework

Answer: B

Q1283. What is the primary challenge of implementing a cyber security governance framework in a multinational organization?

A. Multinational organizations are too small for governance frameworks
B. Balancing global security standards with varying local regulations, cultural differences, and regional threat landscapes
C. Governance frameworks are only designed for single-country operations
D. The only challenge is language translation of policies

Answer: B

Q1284. In cyber security risk quantification, what does the FAIR (Factor Analysis of Information Risk) model provide that qualitative approaches do not?

A. FAIR eliminates the need for risk assessments entirely
B. FAIR provides a quantitative framework for measuring risk in financial terms using probability and loss magnitude
C. FAIR only measures physical security risks
D. FAIR replaces all other security frameworks

Answer: B

Q1285. An organization's CISO must present the return on security investment (ROSI) to the board. Which approach BEST demonstrates security value?

A. Listing all security tools purchased
B. Correlating security spending with reduction in incident frequency, severity, and potential financial losses avoided
C. Comparing the number of employees in the security team to other departments
D. Only showing compliance checkbox completions

Answer: B

Q1286. What is the key difference between cyber security and cyber resilience?

A. They are identical concepts with different names
B. Cyber security focuses on preventing and protecting against attacks, while cyber resilience encompasses the ability to continue operating during and recover quickly after an attack
C. Cyber resilience only applies to cloud systems
D. Cyber security is outdated and replaced by cyber resilience

Answer: B

Q1287. When conducting a cyber security gap analysis, what should be the primary benchmark?

A. The security budget of competing organizations
B. Industry-specific frameworks and regulatory requirements mapped against current security posture
C. The number of security tools deployed
D. Employee satisfaction surveys about security policies

Answer: B

Q1288. How does the concept of 'security debt' parallel 'technical debt' in software development?

A. Security debt only affects open-source projects
B. Deferred security fixes and shortcuts accumulate over time, increasing the cost and complexity of future remediation, similar to technical debt
C. Security debt refers to financial debts from purchasing security tools
D. Security debt is only relevant during audits

Answer: B

Q1289. What challenge does the convergence of Information Technology (IT) and Operational Technology (OT) create for cyber security programs?

A. IT and OT systems have identical security requirements
B. OT systems often have different lifecycles, patching constraints, and availability requirements than IT systems, requiring tailored security approaches
C. Convergence eliminates all security risks
D. OT systems are inherently more secure than IT systems

Answer: B

Q1290. A board of directors asks for a cyber risk appetite statement. What should this statement primarily define?

A. The exact number of acceptable security incidents per year
B. The level and types of cyber risk the organization is willing to accept in pursuit of its strategic objectives
C. A list of all security tools the organization uses
D. The cyber security team's annual training schedule

Answer: B

Q1291. An organization performs a quantitative risk analysis and calculates an SLE of $200,000 and an ARO of 0.5. What is the Annual Loss Expectancy (ALE) and how should it guide security investment?

A. ALE is $400,000 and any control costing less should be implemented
B. ALE is $100,000 and security controls costing less than this amount may be justified
C. ALE is $200,000 because ARO is irrelevant
D. ALE cannot be calculated from SLE and ARO alone

Answer: B

Q1292. How does the Brewer-Nash (Chinese Wall) model address conflicts of interest in access control?

A. It prevents users from reading any data
B. It dynamically restricts access based on a user's previous access history to prevent conflicts of interest
C. It only applies to financial institutions
D. It uses mandatory access control labels exclusively

Answer: B

Q1293. What is the security principle of 'open design' and why is it considered stronger than security through obscurity?

A. Open design means making all passwords public
B. Open design means a system's security should not depend on the secrecy of its implementation, as peer review strengthens security
C. Open design prohibits the use of encryption
D. Open design means using only open-source operating systems

Answer: B

Q1294. When implementing a defense-in-depth strategy, why is diversity of controls important across layers?

A. Diverse controls are cheaper to implement
B. Using different types of controls at each layer ensures that a single vulnerability or exploit technique cannot bypass multiple layers simultaneously
C. Diverse controls are easier to manage
D. Using identical controls at each layer provides better consistency

Answer: B

Q1295. An organization must choose between risk avoidance, risk mitigation, risk transfer, and risk acceptance. Under what circumstances is risk acceptance the most appropriate strategy?

A. When the cost of mitigation exceeds the potential impact and the risk falls within the organization's risk appetite
B. Risk acceptance is never appropriate in cyber security
C. When regulatory requirements mandate specific controls
D. When the risk involves critical infrastructure systems

Answer: A

Q1296. How does the Graham-Denning model address the secure creation and deletion of objects and subjects in access control?

A. It only defines read and write permissions
B. It defines eight protection rules governing how subjects and objects can be securely created, deleted, and how access rights can be transferred
C. It is limited to network access control only
D. It replaces the need for authentication mechanisms

Answer: B

Q1297. A security architect must evaluate the trade-off between usability and security. Which approach BEST balances these competing requirements?

A. Always maximize security regardless of usability impact
B. Implement risk-based controls that apply stronger security to higher-risk activities while minimizing friction for low-risk operations
C. Always maximize usability regardless of security impact
D. Apply the same level of security to all operations regardless of risk

Answer: B

Q1298. What is the Harrison-Ruzzo-Ullman (HRU) model's contribution to access control theory?

A. It only addresses network segmentation
B. It provides a formal framework for analyzing whether a given access control system can reach an unsafe state, proving that the general safety problem is undecidable
C. It replaces all other access control models
D. It only applies to physical access control systems

Answer: B

Q1299. Why is the concept of 'trust but verify' being replaced by 'never trust, always verify' in modern security architectures?

A. Because trust but verify is easier to implement
B. Because the traditional perimeter-based model assumed internal network trust, which modern threats like insider attacks and lateral movement have proven inadequate
C. Because never trust always verify is less expensive
D. Because trust but verify only applies to physical security

Answer: B

Q1300. An organization discovers that its security controls address individual risks but fail to account for compound or cascading risks. What concept addresses this gap?

A. Single point of failure analysis
B. Systemic risk analysis, which evaluates how individual risks can combine and cascade to create larger, emergent risks across interconnected systems
C. Simple vulnerability scanning
D. Individual risk acceptance for each identified risk

Answer: B

Q1301. A security architect must choose between RSA-2048 and ECC P-256 for a resource-constrained IoT deployment. Which is more suitable and why?

A. RSA-2048 because it uses larger keys
B. ECC P-256 because it provides equivalent security to RSA-2048 with much smaller keys and lower computational overhead
C. Neither can be used in IoT devices
D. RSA-2048 because it is newer than ECC

Answer: B

Q1302. What is the security vulnerability of using AES in GCM mode with a reused nonce?

A. It has no effect on security
B. Nonce reuse in AES-GCM can reveal the authentication key and allow forgery of ciphertexts, catastrophically breaking both confidentiality and authenticity
C. It only affects performance, not security
D. It causes the encryption to become stronger

Answer: B

Q1303. How does lattice-based cryptography provide resistance against quantum computing attacks?

A. It uses longer RSA keys
B. Lattice-based problems like Learning With Errors (LWE) are believed to be hard for both classical and quantum computers to solve
C. It relies on the same mathematical problems as RSA
D. It only works on quantum computers

Answer: B

Q1304. What is the primary security risk when using CBC mode encryption without a MAC (encrypt-only)?

A. CBC mode cannot encrypt data properly
B. It is vulnerable to padding oracle attacks, where an attacker can decrypt ciphertext by manipulating padding and observing error responses
C. CBC mode without MAC uses too much bandwidth
D. There is no security risk with encrypt-only CBC

Answer: B

Q1305. Why is the Dual_EC_DRBG random number generator considered compromised, and what broader lesson does it teach?

A. It generates numbers that are too random
B. It contained suspected NSA backdoor constants that could allow prediction of output, teaching that cryptographic standards must be transparent and verifiable
C. It was too slow for practical use
D. It only worked on specific hardware

Answer: B

Q1306. In a TLS 1.3 handshake, what fundamental change was made compared to TLS 1.2 regarding cipher suites?

A. TLS 1.3 no longer uses encryption
B. TLS 1.3 removed support for static RSA key exchange and non-AEAD ciphers, mandating forward secrecy and authenticated encryption
C. TLS 1.3 only supports symmetric encryption
D. TLS 1.3 increased the handshake from two to four round trips

Answer: B

Q1307. What is the security implication of Shor's algorithm for current public key cryptographic systems?

A. It makes symmetric encryption obsolete
B. It can efficiently factor large numbers and compute discrete logarithms on a quantum computer, breaking RSA and ECC
C. It only affects hash functions
D. It strengthens existing public key systems

Answer: B

Q1308. What is the difference between deterministic and probabilistic encryption, and why does it matter for security?

A. They produce identical outputs
B. Deterministic encryption always produces the same ciphertext for the same plaintext and key, while probabilistic encryption includes randomness producing different ciphertexts, which prevents pattern leakage
C. Deterministic encryption is always more secure
D. Probabilistic encryption cannot be decrypted

Answer: B

Q1309. What is the security purpose of key commitment in authenticated encryption, and what attacks does its absence enable?

A. Key commitment is only about key storage efficiency
B. Without key commitment, an attacker can craft a ciphertext that decrypts to valid but different plaintexts under different keys, enabling invisible salamander attacks
C. Key commitment prevents brute force attacks
D. Key commitment is required only for symmetric ciphers

Answer: B

Q1310. A cryptographic implementation passes all functional tests but is found vulnerable to a timing side-channel attack. What is the root cause and mitigation?

A. The algorithm itself is broken and must be replaced
B. The implementation takes different amounts of time for different inputs, leaking information. Mitigation requires constant-time implementation of cryptographic operations
C. Timing attacks only affect hardware, not software
D. Using a faster processor eliminates timing attacks

Answer: B

Q1311. An attacker performs a VLAN hopping attack using double tagging. What network misconfiguration enables this attack?

A. Using encrypted VLANs
B. Having the native VLAN of trunk ports be the same as a user VLAN, allowing double-tagged frames to traverse VLAN boundaries
C. Using too many VLANs on the network
D. Having DHCP enabled on the network

Answer: B

Q1312. How does a network detection and response (NDR) solution differ from traditional IDS/IPS systems?

A. NDR only monitors email traffic
B. NDR uses behavioral analytics and machine learning to detect unknown threats based on network behavior patterns, while traditional IDS/IPS primarily relies on signatures
C. NDR replaces firewalls entirely
D. Traditional IDS/IPS is always more effective than NDR

Answer: B

Q1313. What is the security risk of running recursive DNS resolvers open to the internet?

A. Recursive DNS resolvers cannot be accessed from the internet
B. Open recursive resolvers can be abused for DNS amplification DDoS attacks and DNS cache poisoning, and may leak information about internal queries
C. Open resolvers improve DNS performance globally
D. Recursive DNS resolvers are inherently secure

Answer: B

Q1314. A company implements TLS inspection (SSL decryption) on their network firewall. What privacy and security trade-offs must be considered?

A. TLS inspection has no trade-offs
B. TLS inspection enables detection of encrypted threats but breaks end-to-end encryption, requires careful certificate management, and raises privacy concerns for employee communications
C. TLS inspection improves end-to-end encryption
D. TLS inspection eliminates the need for endpoint security

Answer: B

Q1315. What makes a Slowloris attack effective against web servers, and how does it differ from volumetric DDoS attacks?

A. Slowloris uses high bandwidth to overwhelm servers
B. Slowloris keeps many connections open by sending partial HTTP requests slowly, exhausting the server's connection pool with minimal bandwidth, unlike volumetric attacks that flood with traffic
C. Slowloris only targets DNS servers
D. Slowloris attacks are always detectable by firewalls

Answer: B

Q1316. How does the QUIC protocol change the traditional network security monitoring approach?

A. QUIC uses unencrypted UDP packets that are easier to monitor
B. QUIC encrypts transport metadata that was previously visible in TCP+TLS, reducing the effectiveness of traditional network monitoring that relied on inspecting TCP headers and TLS handshake details
C. QUIC only works on IPv4 networks
D. QUIC eliminates the need for any encryption

Answer: B

Q1317. What is the security implication of IPv6 dual-stack network configurations if IPv6 security controls are not properly implemented?

A. IPv6 is inherently secure and needs no additional controls
B. Attackers can use IPv6 to bypass IPv4 security controls if the network has IPv6 enabled but not properly monitored or firewalled, creating a shadow network path
C. Dual-stack configurations always improve security
D. IPv6 cannot coexist with IPv4 on the same network

Answer: B

Q1318. What is a network covert channel and how can DNS be used to create one?

A. A covert channel is an encrypted VPN tunnel
B. A covert channel uses legitimate network protocols in unintended ways to secretly communicate. DNS tunneling encodes data within DNS queries and responses to bypass network controls
C. Covert channels require dedicated hardware
D. DNS cannot be used for covert communication

Answer: B

Q1319. An organization implements a software-defined perimeter (SDP). How does this differ from traditional VPN-based remote access?

A. SDP and VPN are identical technologies
B. SDP authenticates users before granting network visibility and creates individual, encrypted connections to specific resources, while VPNs grant broad network access after authentication
C. SDP requires no authentication
D. VPNs provide more granular access control than SDP

Answer: B

Q1320. What is the security risk of protocol downgrade attacks in network communications?

A. Downgrade attacks improve security by using older, more tested protocols
B. Attackers force communications to use weaker, older protocol versions with known vulnerabilities, bypassing the security of newer protocols even when both endpoints support them
C. Downgrade attacks only affect physical layer protocols
D. Modern protocols are immune to downgrade attacks

Answer: B

Q1321. In a padding oracle attack against CBC mode encryption, what information does the attacker exploit?

A. The encryption key leaked through side channels
B. The server's response indicating whether decrypted padding is valid or invalid
C. The predictability of the initialization vector
D. The weakness of the block cipher itself

Answer: B

Q1322. What is the security advantage of X25519 over traditional ECDH for key exchange?

A. X25519 uses a larger key size
B. X25519 is resistant to timing attacks by design and avoids common implementation pitfalls
C. X25519 uses symmetric encryption internally
D. X25519 does not require any computation

Answer: B

Q1323. What is the primary challenge of implementing threshold cryptography in a distributed system?

A. It requires quantum computers
B. The need to securely distribute key shares while ensuring no single party can reconstruct the full key alone
C. It only works with RSA encryption
D. It doubles the key length required

Answer: B

Q1324. How does a commitment scheme work in cryptographic protocols, and what two properties must it satisfy?

A. Speed and efficiency
B. Hiding (the committed value is secret) and binding (the committer cannot change the value after committing)
C. Encryption and decryption
D. Authentication and authorization

Answer: B

Q1325. What is the security risk of using AES-CBC with a MAC computed over the ciphertext versus over the plaintext?

A. There is no difference between the two approaches
B. MAC-then-encrypt can be vulnerable to padding oracle attacks, while encrypt-then-MAC is generally secure
C. MAC over ciphertext is always insecure
D. Both approaches are equally vulnerable

Answer: B

Q1326. What is the significance of the discrete logarithm problem in modern cryptography?

A. It is only used in hash functions
B. It is easily solvable with modern computers
C. It provides the mathematical hardness underlying Diffie-Hellman, DSA, and elliptic curve cryptography
D. It has been proven to be unsolvable

Answer: C

Q1327. A system uses ECDSA for digital signatures. What catastrophic failure occurs if the same random nonce k is used for two different signatures with the same private key?

A. The signatures become too large to verify
B. Nothing happens as the nonce does not affect security
C. The private key can be mathematically recovered from the two signatures
D. The public key becomes invalid

Answer: C

Q1328. What is the fundamental difference between zero-knowledge proofs and traditional authentication mechanisms?

A. Zero-knowledge proofs are faster than password authentication
B. Zero-knowledge proofs allow a prover to demonstrate knowledge of a secret without revealing any information about the secret itself
C. Zero-knowledge proofs require biometric data
D. Zero-knowledge proofs eliminate the need for cryptographic keys

Answer: B

Q1329. In post-quantum cryptography, why are lattice-based schemes considered promising candidates for standardization?

A. They use simple XOR operations only
B. They offer strong security proofs from worst-case hardness assumptions and support diverse functionalities including encryption, signatures, and FHE
C. They require no computational resources
D. They are identical to RSA but with larger keys

Answer: B

Q1330. What is format-preserving encryption (FPE) and in what scenario is it particularly useful?

A. Encryption that always produces the same output format as the input, useful for encrypting data that must retain its format such as credit card numbers in legacy databases
B. Encryption that compresses data before encrypting
C. Encryption that formats output as JSON
D. Encryption that preserves file extensions

Answer: A

Q1331. How does Kernel Address Space Layout Randomization (KASLR) differ from standard ASLR, and what are its limitations?

A. KASLR and ASLR are identical with no differences
B. KASLR randomizes kernel memory addresses but can be bypassed through information disclosure vulnerabilities that leak kernel pointers
C. KASLR only applies to user-space programs
D. KASLR provides perfect protection against all kernel attacks

Answer: B

Q1332. What is a TOCTOU (Time of Check to Time of Use) race condition, and how can it be exploited in OS security?

A. A type of brute-force attack on passwords
B. A vulnerability where the state of a resource changes between checking its properties and using it, allowing privilege escalation through symlink attacks
C. A network timing attack on encryption
D. A denial-of-service attack using timestamps

Answer: B

Q1333. A security team must harden a Linux server. What is the security benefit of implementing seccomp-bpf?

A. It encrypts network traffic
B. It filters system calls available to processes, reducing the kernel attack surface by restricting which syscalls a program can make
C. It manages user passwords
D. It monitors disk usage

Answer: B

Q1334. What is the Dirty COW vulnerability and what class of OS security issue does it represent?

A. A malware variant targeting IoT devices
B. A race condition in the Linux kernel's copy-on-write mechanism that allowed unprivileged users to write to read-only memory mappings for privilege escalation
C. A Windows registry corruption bug
D. A DNS spoofing technique

Answer: B

Q1335. How does hardware-based memory tagging (like ARM MTE) improve OS security compared to software-only solutions?

A. It replaces the need for an operating system
B. It assigns tags to memory regions and pointers, detecting use-after-free and buffer overflow at hardware speed with minimal performance overhead
C. It only protects GPU memory
D. It eliminates the need for encryption

Answer: B

Q1336. What is the security architecture of a microkernel-based OS and why is it considered more secure than a monolithic kernel?

A. Microkernels are faster and thus more secure
B. Microkernels run minimal code in kernel mode with drivers and services in user space, reducing the trusted computing base and limiting the impact of vulnerabilities
C. Microkernels use more encryption
D. Microkernels eliminate all vulnerabilities

Answer: B

Q1337. An organization detects a sophisticated rootkit using Direct Kernel Object Manipulation (DKOM). What makes this technique particularly dangerous?

A. It corrupts the bootloader permanently
B. DKOM modifies kernel data structures directly in memory to hide processes and connections without modifying files on disk, evading traditional detection methods
C. It only affects network interfaces
D. It can be detected easily by antivirus software

Answer: B

Q1338. What is the security purpose of Intel SGX (Software Guard Extensions) and what attacks has it proven vulnerable to?

A. SGX accelerates encryption with no known weaknesses
B. SGX creates hardware-encrypted enclaves for sensitive computation but has been shown vulnerable to side-channel attacks like Spectre, Foreshadow, and power analysis
C. SGX is a network security protocol
D. SGX only protects data at rest

Answer: B

Q1339. How does mandatory integrity control (MIC) in Windows protect against privilege escalation?

A. It encrypts all system files
B. It assigns integrity levels to processes and objects, preventing lower-integrity processes from writing to higher-integrity objects even with appropriate DACLs
C. It disables all non-Microsoft software
D. It monitors network traffic

Answer: B

Q1340. What is a Spectre-class vulnerability and why is it fundamentally difficult to mitigate at the OS level?

A. It is a simple buffer overflow fixed by input validation
B. Spectre exploits speculative execution in modern CPUs to leak data across security boundaries, and full mitigation requires microcode updates and significant performance trade-offs because the vulnerability is in hardware design
C. It only affects 32-bit operating systems
D. It is a type of malware that can be removed by antivirus

Answer: B

Q1341. What is a deserialization gadget chain and how is it used in insecure deserialization attacks?

A. A blockchain verification mechanism
B. A sequence of existing classes in an application whose methods can be chained together during deserialization to achieve arbitrary code execution
C. A series of database queries optimized for performance
D. A method of encrypting serialized objects

Answer: B

Q1342. How can a web cache poisoning attack be executed, and what makes it particularly dangerous?

A. By deleting the server's cache files
B. By manipulating unkeyed HTTP headers or parameters to store malicious responses in the cache, which are then served to all subsequent users
C. By overloading the cache with too many requests
D. By encrypting cached content

Answer: B

Q1343. What is a second-order SQL injection and why is it harder to detect than standard SQL injection?

A. SQL injection performed by two attackers simultaneously
B. Malicious input stored in the database and later executed when retrieved and used in another SQL query without sanitization
C. SQL injection that only works on the second attempt
D. A SQL injection that targets backup databases

Answer: B

Q1344. A web application implements CSP with 'unsafe-inline' for scripts. What attack vectors does this leave open and how can nonce-based CSP improve security?

A. It has no impact on security
B. 'unsafe-inline' allows any inline scripts to execute, defeating XSS protection. Nonce-based CSP allows only scripts with a matching server-generated nonce, blocking injected scripts
C. Nonce-based CSP is less secure than unsafe-inline
D. unsafe-inline only affects CSS, not scripts

Answer: B

Q1345. What is a Server-Side Request Forgery (SSRF) attack through DNS rebinding, and how does it bypass common SSRF mitigations?

A. It exploits DNS caching to speed up the server
B. The attacker controls a domain that first resolves to an allowed IP, passes validation, then resolves to an internal IP on the actual request, bypassing allowlist/blocklist checks
C. It only works against DNS servers themselves
D. It replaces the server's DNS configuration

Answer: B

Q1346. How does a prototype pollution vulnerability in JavaScript enable remote code execution in server-side applications?

A. By crashing the JavaScript engine
B. By modifying Object.prototype to inject properties that alter application logic, which in template engines or child process spawning can lead to command injection
C. By changing the JavaScript language syntax
D. By corrupting the package.json file

Answer: B

Q1347. What is HTTP request smuggling via CL.TE desync and what infrastructure conditions make it possible?

A. It is a type of DDoS attack
B. It occurs when a front-end server uses Content-Length and a back-end uses Transfer-Encoding, causing them to disagree on request boundaries, allowing an attacker to smuggle requests
C. It requires the attacker to have server access
D. It only affects HTTP/2 connections

Answer: B

Q1348. What is the security implication of GraphQL introspection being enabled in production and how can it be exploited?

A. GraphQL introspection improves security by documenting the API
B. Introspection reveals the entire API schema including types, fields, mutations, and relationships, giving attackers a complete map for targeted attacks on sensitive operations
C. Introspection only affects performance
D. GraphQL does not support introspection

Answer: B

Q1349. A security researcher finds a web application vulnerable to blind XSS. How does blind XSS differ from reflected XSS and why is it particularly dangerous?

A. Blind XSS is less dangerous than reflected XSS
B. Blind XSS payloads are stored and execute in a different application context (like an admin panel) that the attacker cannot directly access, potentially compromising privileged accounts
C. Blind XSS only works in Internet Explorer
D. Blind XSS requires physical access to the server

Answer: B

Q1350. What is a WebSocket hijacking attack and how does the lack of same-origin policy enforcement for WebSockets create a vulnerability?

A. WebSockets cannot be hijacked due to built-in encryption
B. Cross-site WebSocket hijacking occurs because WebSocket connections do not enforce same-origin policy; a malicious page can initiate a WebSocket connection to a vulnerable server using the victim's cookies
C. WebSocket hijacking requires modifying network hardware
D. WebSockets automatically validate all origins

Answer: B

Q1351. How does the WebAuthn protocol provide phishing-resistant authentication?

A. By using longer passwords
B. By binding credentials to the origin (domain) so that credentials created for one site cannot be used on a phishing site with a different domain
C. By requiring users to type the URL manually
D. By encrypting the login page

Answer: B

Q1352. What is a token binding and how does it prevent token theft attacks?

A. Binding tokens to a physical location
B. Cryptographically binding security tokens to the TLS connection so that stolen tokens cannot be used from a different TLS session
C. Using stronger passwords for token generation
D. Limiting the number of tokens a user can have

Answer: B

Q1353. An organization implements a zero trust architecture. How should the authentication model change from traditional perimeter-based security?

A. Authentication is only needed at the perimeter
B. Every access request must be authenticated, authorized, and continuously validated regardless of network location, assuming no implicit trust
C. Internal users should not need authentication
D. Authentication frequency should be reduced for convenience

Answer: B

Q1354. What is a silver ticket attack in Active Directory and how does it differ from a golden ticket attack?

A. Silver tickets are less harmful versions of golden tickets
B. A silver ticket forges a service ticket for a specific service using the service account's hash, while a golden ticket forges a TGT using the KRBTGT hash granting access to all services
C. Silver tickets target Linux systems while golden tickets target Windows
D. Silver tickets expire faster but golden tickets never expire

Answer: B

Q1355. How does continuous adaptive risk and trust assessment (CARTA) improve access control beyond static policies?

A. By removing all access controls
B. By continuously evaluating risk signals during sessions and dynamically adjusting access levels based on changing context and behavior, not just at the point of initial authentication
C. By requiring re-authentication every minute
D. By using only biometric authentication

Answer: B

Q1356. What are the security implications of the OAuth 2.0 implicit flow and why was it deprecated for SPAs?

A. Implicit flow is the most secure OAuth flow
B. The implicit flow returns tokens in the URL fragment, exposing them to browser history, referrer headers, and potential token leakage; PKCE-enhanced authorization code flow is now recommended for SPAs
C. Implicit flow was deprecated because it is too slow
D. SPAs cannot use OAuth at all

Answer: B

Q1357. What is the security risk of JWT algorithm confusion attacks and how do they work?

A. They slow down JWT verification
B. An attacker changes the JWT header algorithm from RS256 to HS256, causing the server to verify the signature using the RSA public key as the HMAC secret, allowing token forgery
C. They only affect expired tokens
D. They require access to the private key

Answer: B

Q1358. How does decentralized identity (DID) change the traditional identity management paradigm?

A. By centralizing all identity data in one database
B. By giving individuals control over their own identity credentials through self-sovereign identity, eliminating dependence on centralized identity providers
C. By removing the need for authentication entirely
D. By using only username and password

Answer: B

Q1359. What is a relay attack on NFC-based authentication and how does it bypass physical proximity requirements?

A. It blocks all NFC signals within an area
B. An attacker uses two devices to relay the NFC communication between a legitimate token and reader over a distance, making the reader believe the token is nearby when it is not
C. It speeds up NFC communication
D. It only works against Bluetooth devices

Answer: B

Q1360. What is the principle behind passwordless authentication using FIDO2 and why is it considered more secure than traditional passwords?

A. It uses simpler passwords that are easier to remember
B. FIDO2 replaces passwords with public-key cryptography where the private key never leaves the device, eliminating password databases, phishing, replay attacks, and credential stuffing
C. It stores passwords in the cloud instead of locally
D. It only works on specific operating systems

Answer: B

Q1361. What is a supply chain attack through a compromised build pipeline, and how does code signing mitigate it?

A. An attack on physical supply logistics
B. An attacker compromises the CI/CD pipeline to inject malicious code into builds; code signing creates a cryptographic proof of build integrity, allowing consumers to verify the software was not tampered with
C. Code signing prevents all supply chain attacks completely
D. Build pipelines cannot be compromised

Answer: B

Q1362. How does taint tracking analysis work in identifying security vulnerabilities?

A. It tracks paint colors in the UI
B. It marks user-controlled data as 'tainted' and traces its flow through the application to detect if it reaches security-sensitive operations (sinks) without proper sanitization
C. It monitors CPU temperature
D. It tracks changes in version control

Answer: B

Q1363. What is the SLSA (Supply-chain Levels for Software Artifacts) framework and what problem does it address?

A. A programming language specification
B. A framework defining increasing levels of supply chain security for software artifacts, addressing integrity and provenance from source to build to distribution
C. A type of encryption standard
D. A software testing methodology

Answer: B

Q1364. A development team discovers a deserialization vulnerability in their Java application. What makes Java deserialization attacks particularly dangerous?

A. Java deserialization is slower than other languages
B. Java's classpath often contains libraries with exploitable gadget chains that allow arbitrary code execution when crafted objects are deserialized
C. Java does not support serialization
D. Deserialization only affects database operations

Answer: B

Q1365. What is the security significance of reproducible builds and how do they protect the software supply chain?

A. Reproducible builds make software faster
B. Reproducible builds ensure that compiling the same source code always produces identical binary output, allowing independent verification that distributed binaries match the source and have not been tampered with
C. Reproducible builds only work for open-source software
D. They are identical to version control

Answer: B

Q1366. How does mutation testing evaluate the effectiveness of a security test suite?

A. By testing the application with random inputs
B. By introducing small changes (mutations) to the source code and checking whether the test suite detects them; surviving mutants indicate gaps in test coverage
C. By mutating the database schema
D. By changing the programming language

Answer: B

Q1367. What is a confused deputy vulnerability in application development and how can capability-based security prevent it?

A. When a developer is confused about requirements
B. A privilege escalation where a trusted program (deputy) is tricked into misusing its authority; capability-based security prevents it by requiring explicit unforgeable tokens for each resource access
C. A type of race condition
D. A denial-of-service attack on the development server

Answer: B

Q1368. What is the security impact of improper certificate validation in mobile and desktop applications?

A. It only affects loading speed
B. Improper certificate validation can allow man-in-the-middle attacks by accepting invalid, expired, or self-signed certificates, enabling interception of encrypted communications
C. It improves security by accepting more certificates
D. It only affects web browsers

Answer: B

Q1369. What are the security implications of using WebAssembly (WASM) in web applications and what unique threats does it introduce?

A. WASM has no security implications
B. WASM can be used to obfuscate malicious code, perform cryptomining, bypass traditional JavaScript security analysis, and introduce memory safety vulnerabilities from languages like C/C++
C. WASM is inherently more secure than JavaScript
D. WASM cannot interact with web APIs

Answer: B

Q1370. How does a security-focused chaos engineering approach differ from traditional chaos engineering?

A. They are identical practices
B. Security chaos engineering deliberately introduces security-relevant failures (certificate expiration, credential leaks, firewall rule removal) to verify that security controls respond correctly under adverse conditions
C. Security chaos engineering only tests network outages
D. It replaces the need for penetration testing

Answer: B

Q1371. How does the KRACK (Key Reinstallation Attack) exploit the WPA2 four-way handshake, and what specifically is compromised?

A. It cracks the WiFi password directly
B. It forces reinstallation of an already-in-use key by manipulating handshake messages, causing nonce reuse that allows decryption of packets and potential injection in TKIP and GCMP modes
C. It disables the access point's encryption hardware
D. It only works against WEP encryption

Answer: B

Q1372. What is the FragAttacks vulnerability class in WiFi security and why does it affect virtually all WiFi devices?

A. It only affects devices manufactured before 2010
B. FragAttacks comprises design flaws in WiFi's frame aggregation and fragmentation features present in the IEEE 802.11 standard since 1997, along with widespread implementation flaws, affecting nearly all WiFi devices
C. It is specific to one router manufacturer
D. It only works when WiFi encryption is disabled

Answer: B

Q1373. How do Stingray/IMSI catcher devices operate, and what defense mechanisms exist against them?

A. They simply block cell signals
B. They impersonate legitimate cell towers to force phones to connect, intercepting calls, texts, and tracking location; 5G standalone networks with SUPI concealment help mitigate identification attacks
C. They only work within 1 meter range
D. They are only used for WiFi attacks

Answer: B

Q1374. What is the security risk of Bluetooth Low Energy (BLE) tracking and how have recent attacks like BLESA exploited BLE reconnection?

A. BLE is too short-range to pose security risks
B. BLESA (BLE Spoofing Attacks) exploits the reconnection process where authentication is optional, allowing an attacker to impersonate a previously paired device and send spoofed data
C. BLE attacks require physical contact with the device
D. BLE tracking only works indoors

Answer: B

Q1375. What are the unique security challenges of eSIM compared to traditional physical SIM cards?

A. eSIMs are identical to physical SIMs in security
B. eSIMs introduce risks of remote provisioning attacks, profile manipulation, and remove the physical possession requirement, but also eliminate SIM swapping at carrier stores
C. eSIMs cannot be used for authentication
D. eSIMs are less secure in every aspect

Answer: B

Q1376. How does the Dragonblood attack affect WPA3-SAE (Simultaneous Authentication of Equals) security?

A. WPA3 is completely immune to all attacks
B. Dragonblood reveals side-channel vulnerabilities in WPA3-SAE's dragonfly handshake including timing-based and cache-based attacks that can recover the WiFi password, plus downgrade attacks to WPA2
C. Dragonblood only affects WPA2 networks
D. Dragonblood is a physical attack on routers

Answer: B

Q1377. What is a man-in-the-disk attack on Android and why is it effective despite Android's sandboxing?

A. An attack that fills up the device storage
B. An attack exploiting Android apps that use external storage (shared by all apps) for receiving data, allowing a malicious app to modify files before the target app processes them
C. It bypasses device encryption
D. It only works on rooted devices

Answer: B

Q1378. What security mechanisms does 5G introduce to address the vulnerabilities found in 4G LTE networks?

A. 5G has no security improvements over 4G
B. 5G introduces subscriber identity encryption (SUCI), enhanced key hierarchy, network slicing isolation, and edge computing security, addressing IMSI catching, false base stations, and subscriber tracking
C. 5G only improves speed without security changes
D. 5G uses the same security as WiFi

Answer: B

Q1379. What is a baseband processor attack and why is it considered one of the most severe mobile security threats?

A. It is a type of app-level malware that can be removed easily
B. Baseband attacks target the separate processor handling cellular communications, which runs its own RTOS with high privileges, potentially allowing call interception, SMS theft, and persistent access that survives factory resets
C. It only affects WiFi connectivity
D. It requires the attacker to have physical access to the device

Answer: B

Q1380. How does a WiFi direct connection present security risks different from traditional WiFi, and what attack scenarios are unique to WiFi Direct?

A. WiFi Direct is more secure than traditional WiFi in all cases
B. WiFi Direct creates peer-to-peer connections that bypass network security controls; attacks include rogue group owner impersonation, unauthorized device discovery, and exploiting WPS vulnerabilities in the setup process
C. WiFi Direct cannot transfer data
D. WiFi Direct uses wired connections

Answer: B

Q1381. What is a cloud instance metadata service (IMDS) attack and how did it contribute to the Capital One breach?

A. IMDS attacks target cloud provider's headquarters
B. An attacker exploited an SSRF vulnerability to query the instance metadata service at 169.254.169.254, obtaining temporary IAM credentials that gave access to S3 buckets containing customer data
C. IMDS only contains non-sensitive information
D. The Capital One breach was caused by a phishing attack

Answer: B

Q1382. How does a cross-account confused deputy attack work in cloud environments?

A. It confuses cloud administrators about their account credentials
B. A malicious customer tricks a cloud service (deputy) into using the service's cross-account permissions to access resources in a victim's account by providing the victim's account ID as the target
C. It only affects personal cloud accounts
D. It is a type of DDoS attack

Answer: B

Q1383. What is the security challenge of Kubernetes RBAC in multi-tenant cloud environments?

A. Kubernetes does not support RBAC
B. Kubernetes RBAC can be complex to configure correctly for multi-tenancy, with risks of overly permissive ClusterRoles, insecure default service accounts, and namespace escape through cluster-wide resources
C. Kubernetes RBAC is identical to OS-level access control
D. Multi-tenancy is not possible in Kubernetes

Answer: B

Q1384. What is the security purpose of confidential computing in cloud environments and how does it differ from traditional encryption?

A. It is the same as encrypting data at rest
B. Confidential computing protects data during processing (in use) using hardware-based trusted execution environments, ensuring not even the cloud provider can access data during computation
C. It only encrypts network traffic
D. It provides encryption for backup data only

Answer: B

Q1385. How does cloud infrastructure entitlements management (CIEM) address the permissions gap problem?

A. CIEM manages cloud infrastructure hardware
B. CIEM continuously analyzes actual permission usage versus granted permissions, identifying overly permissive access and recommending least-privilege policies based on real behavior patterns
C. CIEM replaces IAM entirely
D. CIEM only manages storage permissions

Answer: B

Q1386. What are the security risks of serverless function event injection and how does it differ from traditional injection attacks?

A. Serverless functions cannot be attacked
B. Serverless event injection exploits the various event sources (API Gateway, S3, SNS, DynamoDB) that trigger functions; each source can carry malicious payloads in different formats, expanding the attack surface beyond traditional HTTP input
C. Serverless injection is identical to web injection
D. Only API Gateway events can be exploited

Answer: B

Q1387. What is the security significance of cloud provider control plane versus data plane, and how should monitoring differ for each?

A. Control plane and data plane are the same in cloud environments
B. The control plane manages cloud resources (API calls, configuration) while the data plane handles actual data traffic; monitoring must cover both: control plane for unauthorized changes and data plane for exfiltration and anomalies
C. Only the data plane needs monitoring
D. The control plane is automatically secure

Answer: B

Q1388. How can an attacker exploit insecure cloud function dependencies to achieve persistent access in a serverless environment?

A. Serverless environments prevent all dependency attacks
B. An attacker can compromise a dependency in the function's package or inject a malicious layer, gaining code execution each time the function is invoked, achieving persistence without maintaining infrastructure
C. Dependencies do not affect function security
D. Only first-party code can be compromised

Answer: B

Q1389. What is a cloud-native application protection platform (CNAPP) and how does it unify previously separate security tools?

A. CNAPP is a new cloud provider service
B. CNAPP combines CSPM, CWPP, CIEM, and IaC scanning into a unified platform, providing end-to-end visibility across the application lifecycle from code to cloud runtime, reducing tool sprawl and alert correlation gaps
C. CNAPP only provides antivirus for cloud
D. CNAPP replaces the need for IAM

Answer: B

Q1390. What security challenges arise from cloud provider managed keys versus customer managed keys (CMK) for encryption?

A. There is no difference between managed and customer keys
B. Provider-managed keys simplify operations but give the provider access to key material; CMKs give customers control but require managing key rotation, access policies, and disaster recovery, with the risk of permanent data loss if keys are lost
C. Customer keys are always less secure
D. Provider keys cannot be used for compliance

Answer: B

Q1391. How does SSD wear leveling and TRIM complicate traditional forensic data recovery?

A. SSDs are easier to forensically analyze than HDDs
B. TRIM instructs the SSD to erase deleted data blocks for performance, while wear leveling moves data across cells, making traditional recovery of deleted files unreliable as data may be erased or relocated without notice
C. SSDs store data identically to traditional hard drives
D. TRIM and wear leveling only affect SSD performance, not forensics

Answer: B

Q1392. What are the forensic challenges of investigating incidents in containerized environments?

A. Containers are identical to virtual machines for forensics
B. Containers are ephemeral with short lifespans, share the host kernel, use layered filesystems, and may be automatically destroyed and replaced, making traditional disk imaging impractical and requiring real-time log collection and orchestrator-level evidence
C. Container forensics uses the same tools as disk forensics
D. Containers always preserve all evidence

Answer: B

Q1393. How does memory forensics using tools like Volatility detect rootkits that hide from traditional analysis?

A. Memory forensics cannot detect rootkits
B. Volatility analyzes RAM dumps to find discrepancies between OS-reported process lists and actual memory structures, detect hidden processes, injected code, and hooks that rootkits use to hide from live system tools
C. Memory forensics only finds cached passwords
D. Volatility is a network analysis tool

Answer: B

Q1394. What is the forensic significance of Windows Prefetch files and how do they aid in malware analysis?

A. Prefetch files only speed up application loading
B. Prefetch files record which executables were run, when they were last executed, run count, and which DLLs and files were loaded, providing evidence of malware execution even after the malware binary is deleted
C. Prefetch files are encrypted and cannot be analyzed
D. Prefetch files exist only on Linux systems

Answer: B

Q1395. What are the legal and technical challenges of performing forensics on encrypted devices with full disk encryption?

A. Encryption has no impact on forensic investigation
B. Full disk encryption prevents traditional dead-box forensic imaging of readable data, requiring either live acquisition while the device is running and unlocked, key recovery from memory or key escrow, or legal compulsion to provide the decryption key
C. Encrypted devices can always be easily decrypted by forensic tools
D. Encryption only protects deleted files

Answer: B

Q1396. How does NTFS journal forensics ($UsnJrnl and $LogFile) provide evidence that regular file analysis cannot?

A. NTFS journals contain no useful forensic data
B. The USN Journal records all file system changes (creation, modification, deletion, rename) with timestamps, and $LogFile records transactional metadata, providing evidence of file operations even after files are deleted and overwritten
C. NTFS journals only exist on Linux systems
D. Journal analysis requires access to the original user account

Answer: B

Q1397. What is the role of digital forensics in investigating Advanced Persistent Threat (APT) campaigns?

A. Digital forensics cannot help with APT investigations
B. Forensics must trace lateral movement across multiple systems, identify initial access vectors, recover C2 communications, analyze custom malware through reverse engineering, and build a comprehensive timeline spanning months of activity
C. APT investigations only require network monitoring
D. APTs leave no forensic evidence

Answer: B

Q1398. What is the forensic approach to analyzing fileless malware that operates entirely in memory?

A. Fileless malware cannot be detected or analyzed
B. Analysis requires memory acquisition from the live system, examining PowerShell logs, WMI event subscriptions, registry-resident payloads, and system event logs since traditional disk-based forensics finds no malware files
C. Fileless malware always leaves files on disk
D. Simply scanning the hard drive is sufficient

Answer: B

Q1399. How does anti-forensic timestamp manipulation (timestomping) work, and what techniques can detect it?

A. Timestamps cannot be manipulated
B. Timestomping modifies file timestamps to blend in with legitimate files; detection involves comparing $STANDARD_INFORMATION timestamps with $FILE_NAME timestamps in NTFS MFT, analyzing USN Journal entries, and checking for timestamp inconsistencies
C. Only law enforcement can detect timestamp manipulation
D. Timestomping permanently destroys all timestamp evidence

Answer: B

Q1400. What are the unique challenges of cloud forensics compared to traditional on-premises forensics?

A. Cloud forensics is simpler than traditional forensics
B. Cloud forensics faces challenges including limited physical access, multi-tenant data isolation, jurisdiction across regions, volatile/ephemeral resources, dependency on provider cooperation, and ensuring forensic soundness without hardware control
C. Cloud environments provide better forensic capabilities
D. There are no differences between cloud and traditional forensics

Answer: B

Q1401. During a major incident, the IR team suspects the attacker is monitoring their Slack and email. What should the team do?

A. Continue using Slack and email to avoid tipping off the attacker
B. Switch to pre-established out-of-band communication channels such as a separate system, encrypted phone calls, or in-person meetings that the attacker has no access to
C. Post misleading information on Slack to confuse the attacker
D. Shut down all communication and work independently

Answer: B

Q1402. How should an IR team handle the discovery that a supply chain partner's software update was the initial attack vector?

A. Immediately remove all partner software from the network
B. Coordinate with the partner for joint investigation, isolate affected systems without breaking critical dependencies, analyze the compromised update for IoCs, and notify relevant stakeholders and potentially CISA or sector ISACs
C. Ignore the supply chain aspect and focus only on internal systems
D. Publicly blame the supply chain partner

Answer: B

Q1403. An organization detects ransomware but the attacker also exfiltrated data before encryption. How does this dual-threat change the incident response approach?

A. Focus only on decrypting the ransomware
B. The response must address both the ransomware (restoration from backups, containment) and the data breach (regulatory notification, determining what data was stolen, monitoring for data publication), treating it as a data breach with ransomware
C. Data exfiltration is not a concern if data is encrypted on the attacker's end
D. Only law enforcement can handle this type of incident

Answer: B

Q1404. What is the 'dwell time' metric in incident response and what does a high dwell time indicate about an organization's detection capabilities?

A. Dwell time measures how long it takes to deploy patches
B. Dwell time is the duration between initial compromise and detection; high dwell time indicates poor detection capabilities, allowing attackers to deeply entrench, move laterally, and accomplish objectives before being discovered
C. Dwell time measures the time between incidents
D. Dwell time is only relevant for insider threats

Answer: B

Q1405. How should an IR team determine whether to rebuild compromised systems from scratch versus cleaning and restoring them?

A. Always clean and restore to save time
B. Rebuilding is preferred for high-severity compromises where the attacker had deep access (admin/root), persistence mechanisms may be hidden, or the full extent of compromise is uncertain; cleaning is acceptable for low-severity, well-understood incidents
C. Always rebuild every system regardless of the incident
D. The decision should be made by the legal department only

Answer: B

Q1406. What is the role of deception technology during active incident response?

A. Deception has no place in incident response
B. Deploying decoys and honeypots during active response can detect attacker lateral movement, misdirect the attacker, gather intelligence on TTPs, and confirm when the attacker has been fully removed from the environment
C. Deception technology only works before an incident occurs
D. Deception technology replaces the need for containment

Answer: B

Q1407. What are the legal considerations when an IR team discovers evidence of criminal activity by an insider during a routine security investigation?

A. Legal considerations do not apply during incident response
B. The team must immediately involve legal counsel, ensure evidence is collected in a legally defensible manner, consider employee privacy rights, determine whether to involve law enforcement, and separate the HR process from the technical investigation
C. The IR team should confront the employee directly
D. The team should delete the evidence to avoid complications

Answer: B

Q1408. How does the MITRE ATT&CK framework enhance incident response activities?

A. MITRE ATT&CK is only useful for threat intelligence, not incident response
B. ATT&CK provides a common language for describing attacker techniques, helps map observed activity to known threat groups, identifies gaps in detection coverage, guides investigation by predicting likely next steps, and structures post-incident reporting
C. ATT&CK replaces the need for an incident response plan
D. ATT&CK only works for nation-state attacks

Answer: B

Q1409. An IR team has contained a breach but the attacker had access for 6 months. What specific challenges does this extended dwell time create for the response?

A. Extended dwell time does not create additional challenges
B. Extended access means the attacker likely established multiple persistence mechanisms, moved laterally across many systems, exfiltrated significant data, potentially tampered with logs and backups, and created credentials that must all be identified and remediated
C. After 6 months the threat is no longer active
D. Only the initially compromised system needs attention

Answer: B

Q1410. What is the strategic difference between tactical incident response and strategic incident response during a major breach?

A. There is no difference between tactical and strategic response
B. Tactical response focuses on immediate technical actions (containment, eradication, recovery) while strategic response addresses business continuity, stakeholder communication, regulatory compliance, reputation management, and long-term security improvements
C. Tactical response is done by management and strategic by engineers
D. Strategic response only happens after the incident is resolved

Answer: B

Q1411. How can an attacker evade security monitoring through living-off-the-land techniques, and what detection strategies are effective?

A. Living-off-the-land techniques are easily detected by antivirus
B. Attackers use legitimate system tools (PowerShell, WMI, certutil) for malicious purposes, evading signature-based detection; effective detection requires behavioral analysis, command-line logging, and baselining normal administrative tool usage
C. These techniques only work on Linux systems
D. Standard SIEM rules detect all living-off-the-land activity

Answer: B

Q1412. What is the detection challenge of encrypted C2 (command and control) traffic, and what network-level indicators can still reveal it?

A. Encrypted C2 traffic cannot be detected at all
B. While content is hidden, encrypted C2 traffic can be detected through JA3/JA3S fingerprinting, certificate analysis, beacon interval patterns, traffic volume anomalies, SNI field inspection, and unusual destination characteristics
C. Simply decrypting all traffic is the only solution
D. C2 traffic always uses unencrypted protocols

Answer: B

Q1413. How should security monitoring architecture be designed for a hybrid cloud environment?

A. Use only on-premises monitoring tools for all environments
B. Implement unified monitoring that aggregates logs from on-premises, cloud provider native logs, and SaaS audit logs into a centralized SIEM with normalized data formats, cloud-specific detection rules, and cross-environment correlation
C. Cloud environments do not need monitoring
D. Use separate, unconnected monitoring for each environment

Answer: B

Q1414. What is the OODA loop (Observe, Orient, Decide, Act) and how does it apply to SOC operations?

A. OODA is a software development methodology
B. The OODA loop provides a decision-making framework for SOC analysts: Observe (collect data), Orient (analyze context and threat intelligence), Decide (determine response), Act (execute response); faster OODA loops lead to better security outcomes
C. OODA only applies to military operations
D. OODA replaces SIEM technology

Answer: B

Q1415. What are the key metrics for measuring SOC effectiveness, and what do they indicate?

A. Only the number of alerts matters
B. Key metrics include MTTD (Mean Time To Detect), MTTR (Mean Time To Respond), false positive rate, alert-to-incident ratio, coverage against ATT&CK techniques, and analyst workload; together they measure detection capability, response efficiency, and operational health
C. SOC effectiveness cannot be measured
D. Only compliance audit results matter

Answer: B

Q1416. How does security orchestration, automation, and response (SOAR) reduce mean time to respond?

A. SOAR replaces all human analysts
B. SOAR automates repetitive investigation steps (enrichment, correlation), orchestrates actions across security tools, and executes predefined playbooks for common alert types, freeing analysts for complex decisions while reducing response time for routine incidents
C. SOAR only generates reports
D. SOAR increases response time due to complexity

Answer: B

Q1417. What is the challenge of monitoring east-west traffic in modern data center and cloud environments?

A. East-west traffic does not exist in modern networks
B. East-west (lateral) traffic between servers often bypasses traditional perimeter monitoring; detecting threats requires micro-segmentation with inline monitoring, agent-based endpoint telemetry, or network detection and response (NDR) solutions within the data center
C. East-west traffic is automatically monitored by firewalls
D. Only north-south traffic matters for security

Answer: B

Q1418. What is the role of machine learning anomaly detection in security monitoring, and what are its limitations?

A. ML anomaly detection perfectly detects all threats with no false positives
B. ML anomaly detection identifies deviations from learned baseline behavior, useful for detecting novel threats without signatures; limitations include high false positive rates during baseline changes, susceptibility to adversarial evasion, and need for quality training data
C. ML makes all other detection methods obsolete
D. ML anomaly detection only works for network traffic

Answer: B

Q1419. How should a SOC handle monitoring during a zero-day vulnerability disclosure before patches are available?

A. Zero-day monitoring is impossible
B. The SOC should implement compensating detection rules based on known exploitation indicators, increase monitoring of likely target systems, deploy virtual patches through WAF/IPS, monitor for proof-of-concept exploit code releases, and coordinate with threat intelligence for IoCs
C. Simply wait for the vendor patch
D. Disconnect all vulnerable systems from the network

Answer: B

Q1420. What is the concept of detection-as-code and how does it improve security monitoring operations?

A. Detection-as-code means writing detection rules in any programming language
B. Detection-as-code applies software engineering practices (version control, testing, peer review, CI/CD) to detection rule development, enabling systematic rule management, automated testing for false positives, and collaborative detection engineering
C. Detection-as-code replaces SIEM platforms
D. It only applies to cloud-native environments

Answer: B

Q1421. How does the CLOUD Act affect international data access for law enforcement, and what tensions does it create with GDPR?

A. The CLOUD Act has no impact on international data access
B. The CLOUD Act allows US authorities to compel US-based technology companies to provide data regardless of where it is stored; this creates conflicts with GDPR's data transfer restrictions and other countries' sovereignty concerns over their citizens' data
C. The CLOUD Act only applies to cloud storage companies
D. GDPR and the CLOUD Act are fully compatible

Answer: B

Q1422. What are the legal and ethical considerations of 'hack back' or active cyber defense measures by private organizations?

A. Hack back is legal and encouraged for all organizations
B. Active cyber defense by private entities raises complex legal issues: most jurisdictions prohibit unauthorized access regardless of motive, there are attribution challenges, risks of escalation, potential collateral damage, and limited legal frameworks distinguishing defensive from offensive actions
C. Hack back is universally illegal with no exceptions
D. Private organizations have unlimited rights to defend their networks through offensive measures

Answer: B

Q1423. How does the Budapest Convention on Cybercrime facilitate international cooperation, and what are its limitations?

A. The Budapest Convention is no longer relevant
B. The Convention provides a framework for mutual legal assistance, harmonizing cybercrime definitions and procedures; limitations include non-participation by major cyber powers (Russia, China), slow MLAT processes, and challenges adapting to emerging technologies
C. The Convention automatically resolves all jurisdictional disputes
D. All countries are members of the Budapest Convention

Answer: B

Q1424. What legal framework governs the use of artificial intelligence in cybersecurity decision-making, and what liability issues arise?

A. AI in cybersecurity has no legal implications
B. The legal framework is evolving: AI-powered security decisions raise questions of liability when automated systems cause false positives blocking legitimate users, algorithmic bias in threat detection, accountability for AI errors, and regulatory requirements for explainable AI
C. AI decisions are always legally defensible
D. Only developers of AI are liable, not the organizations using it

Answer: B

Q1425. What are the legal challenges of prosecuting state-sponsored cyber attacks under international law?

A. International law clearly addresses all state-sponsored cyber attacks
B. State-sponsored attacks face challenges including attribution difficulty, sovereign immunity, lack of binding international cyber norms, the Tallinn Manual's non-binding status, and debates about whether cyber attacks constitute 'armed attacks' triggering self-defense rights
C. All state-sponsored attacks are considered acts of war
D. International courts have jurisdiction over all cyber attacks

Answer: B

Q1426. How does the right to encryption conflict with government demands for lawful access, and what are the implications of encryption backdoors?

A. There is no conflict between encryption and lawful access
B. The tension lies between individuals' right to privacy through encryption and governments' need for lawful access to investigate crimes; mandated backdoors weaken security for all users and cannot be limited to authorized access only
C. Encryption backdoors are perfectly secure
D. Governments do not seek access to encrypted communications

Answer: B

Q1427. What is the legal significance of Pakistan's Prevention of Electronic Crimes Act (PECA) 2016 Section 10 regarding cyber terrorism?

A. Section 10 only addresses spam emails
B. Section 10 criminalizes cyber terrorism including using information systems to create fear, panic, or insecurity, interfering with critical infrastructure, or threatening national security, with severe penalties including imprisonment up to fourteen years
C. PECA 2016 does not address terrorism
D. Section 10 is about copyright protection

Answer: B

Q1428. What are the legal implications of cross-border data transfers following the Schrems II ruling, and how do organizations ensure compliance?

A. Schrems II has no practical impact on data transfers
B. Schrems II invalidated the EU-US Privacy Shield and requires organizations to conduct transfer impact assessments when using Standard Contractual Clauses, implement supplementary measures, and ensure the destination country's surveillance laws do not undermine EU-level data protection
C. Organizations can freely transfer data between any countries
D. Only EU organizations are affected by Schrems II

Answer: B

Q1429. How do cybersecurity regulations for critical infrastructure differ from general data protection laws, and what additional obligations do they impose?

A. Critical infrastructure has fewer regulations than regular businesses
B. Critical infrastructure regulations impose additional obligations including mandatory incident reporting with shorter deadlines, minimum security standards, regular security assessments, supply chain security requirements, and potential government oversight or certification
C. Critical infrastructure only needs to follow GDPR
D. There are no specific regulations for critical infrastructure

Answer: B

Q1430. What is the legal and ethical framework around vulnerability disclosure, and how do coordinated vulnerability disclosure policies reduce legal risk for researchers?

A. Vulnerability disclosure has no legal framework
B. Coordinated vulnerability disclosure (CVD) policies provide a legal safe harbor by defining how researchers should report vulnerabilities, establishing timelines for patches, and protecting researchers from prosecution under computer crime laws when they act in good faith within the policy's scope
C. All vulnerability disclosure is illegal
D. Only government researchers can disclose vulnerabilities

Answer: B

Q1431. How does the convergence of AI and cybersecurity create an arms race between attackers and defenders?

A. AI only benefits defenders, not attackers
B. Both attackers and defenders use AI: defenders for threat detection, anomaly analysis, and automated response; attackers for evading detection, generating polymorphic malware, automating social engineering, and discovering vulnerabilities, creating a continuous escalation cycle
C. AI has no impact on the attacker-defender dynamic
D. The arms race is only theoretical and has not materialized

Answer: B

Q1432. What is the concept of security chaos engineering and how does it proactively improve security posture?

A. Chaos engineering makes security systems more chaotic
B. Security chaos engineering deliberately introduces controlled security failures (expired certificates, disabled controls, simulated breaches) to verify that detection, alerting, and response mechanisms function correctly, identifying weaknesses before attackers exploit them
C. It is identical to penetration testing
D. Chaos engineering only tests system availability

Answer: B

Q1433. What are the unique security challenges of Web3 and decentralized applications (dApps)?

A. Web3 applications are inherently more secure than Web2
B. Web3 introduces unique challenges including smart contract vulnerabilities, irreversible transactions on blockchain, private key management, bridge protocol exploits, flash loan attacks, governance token manipulation, and the tension between immutability and the need to patch vulnerabilities
C. Web3 has no security challenges
D. Web3 uses the same security model as traditional web applications

Answer: B

Q1434. How does quantum key distribution (QKD) fundamentally differ from post-quantum cryptography (PQC), and what are the practical deployment challenges of each?

A. QKD and PQC are the same technology
B. QKD uses quantum physics to distribute keys with information-theoretic security but requires dedicated fiber/satellite links; PQC uses classical algorithms resistant to quantum attacks that work on existing infrastructure; QKD faces distance and cost limitations while PQC faces algorithm maturity and standardization challenges
C. QKD is software-based while PQC requires hardware
D. Neither technology addresses quantum threats

Answer: B

Q1435. What is the security significance of software-defined perimeter (SDP) and how does it implement zero trust principles?

A. SDP is identical to a traditional VPN
B. SDP creates dynamic, identity-based perimeters by making application infrastructure invisible to unauthorized users through single-packet authorization, mutual TLS, and need-to-know access, implementing zero trust by eliminating the concept of a trusted network
C. SDP only works for physical security
D. SDP replaces firewalls entirely

Answer: B

Q1436. What is the emerging threat of adversarial machine learning and how can it compromise AI-based security systems?

A. Adversarial ML only affects image recognition
B. Adversarial ML attacks manipulate AI models through techniques like evasion attacks (crafting inputs to bypass detection), poisoning attacks (corrupting training data), model stealing (extracting model parameters), and inversion attacks (extracting training data from model outputs)
C. AI security systems cannot be manipulated
D. Adversarial attacks require access to the model's source code

Answer: B

Q1437. How does the concept of cyber-physical systems security extend traditional cybersecurity to address safety-critical environments?

A. Cyber-physical security is identical to IT security
B. Cyber-physical security must address the intersection of digital and physical systems where cyber attacks can cause physical harm (e.g., industrial control systems, medical devices, autonomous vehicles), requiring safety engineering integration, real-time constraints, and consequence-based risk assessment
C. Cyber-physical systems cannot be hacked
D. Only military systems are cyber-physical

Answer: B

Q1438. What is the concept of digital sovereignty in cybersecurity and how does it influence technology and policy decisions?

A. Digital sovereignty only means hosting websites domestically
B. Digital sovereignty encompasses a nation's ability to control its digital infrastructure, data, and technology supply chains, influencing decisions on data localization, domestic technology development, trusted vendor requirements, and resistance to foreign surveillance
C. Digital sovereignty has no impact on cybersecurity
D. Only large countries can achieve digital sovereignty

Answer: B

Q1439. What is the security implication of neuromorphic computing and how might it change the cybersecurity landscape?

A. Neuromorphic computing only affects battery life
B. Neuromorphic computing mimics brain neural networks in hardware, potentially enabling real-time AI-powered threat detection with extremely low power consumption, but also poses risks of creating more sophisticated AI-driven attacks and may require new security paradigms for protecting brain-inspired architectures
C. Neuromorphic computing is identical to quantum computing
D. Neuromorphic computing has no security implications

Answer: B

Q1440. How does the concept of cyber resilience fundamentally differ from traditional cybersecurity, and why is it becoming more important?

A. Cyber resilience and cybersecurity are identical concepts
B. Cyber resilience accepts that breaches are inevitable and focuses on an organization's ability to anticipate, withstand, recover from, and adapt to adverse cyber events while maintaining critical operations, whereas traditional cybersecurity primarily focuses on prevention; resilience is critical as attack sophistication outpaces pure prevention
C. Cyber resilience means giving up on security
D. Traditional cybersecurity is always sufficient

Answer: B