CSE 4380 Information Security
Spring 2025

Final Exam Review

1. A nonce is
    A. A random number
    B. A one-time password
    C. A single use-token
    D. A challenge negation

Solution: A random number

2. How long would it take to break 128-bit AES assuming 10^6 (1 million) decryptions per microsecond on average?
    A. 5.4×10^{18}seconds
    B. 5.4×10^{18}days
    C. 5.4×10^{18}years
    D. 5.4×10^{18}millennia

Solution: 5.4×10^{18} years

3. Which is not true about DES?
    A. It is a symmetric key algorithm
    B. It is an asymmetric key algorithm
    C. It is no longer secure
    D. It is no longer the current NIST recommended standard

Solution: It is an asymmetric key algorithm

4. Ensuring timely and reliable access to and use of information.
    A. Contigency planning
    B. Integrity
    C. Disaster recovery plan
    D. Availability

Solution: Availability

5. Which of the following is a not a phase in the virus lifetime
    A. Infection Phase
    B. Dormant Phase
    C. Triggering Phase
    D. Execution Phase

Solution: Infection Phase

6. The security mechanisms should not interfere unduly with the work of users, while at the same time meeting the needs of those who authorize access.
    A. Least priviledge
    B. Isolation
    C. Psychological acceptability
    D. Least astonishment

Solution: Psychological acceptability

7. Shoulder surfing is a type of what attack?
    A. Replay
    B. Eavesdropping
    C. Reconnaisance
    D. Cross-site scripting

Solution: Eavesdropping

8. What is an example of a moderate impact loss of confidentiality?
    A. Student enrollment information is exposed
    B. Entries in an online discussion forum are falsified
    C. Access to an online telephone directory is blocked
    D. A personal health record is exposed

Solution: A personal health record is exposed

9. How much more security do you get against brute force when you go from a 64-bit key to an 80-bit key?
   A. 25% more
   B. 16 times as much
   C. $2^8 = 256$ times as much
   D. $2^{16} = 65,536$ times as much

Solution: $2^{16} = 65,536$ times as much

10. What property does Alices signature on a message NOT provide?
    A. Authentication: The message came from Alice
    B. Non-repudiation: The receiver can prove that Alice signed it
    C. Data integrity: The message has not been altered since it left Alice
    D. Confidentiality: The message has not been read by anyone except Alice

Solution: Confidentiality: The message has not been read by anyone except Alice

11. A secure hash function has which of these properties?
    A. It is impossible to undo the hash to find original input X
    B. It is computationally infeasible to compute the hash of X
    C. It is impossible to find inputs X and Y with the same hash value
    D. It is computationally infeasible to find inputs X and Y with the same hash value

Solution: It is computationally infeasible to find inputs X and Y with the same hash value

12. A program or user interface should always respond in the way that is least likely to surprise the user.
    A. Least priviledge
    B. Isolation
    C. Psychological acceptability
    D. Least astonishment

Solution: Least astonishment

13. Which security principle dictates that you should use multiple, diverse, and complementary defense mechanisms?
    A. Least privilege
    B. Accountability
    C. Defense in Depth
    D. Minimize the variety, size, and complexity of trusted components (KISS)

Solution: Defense in Depth

14. What is the purpose of a certificate?
    A. To encrypt the secret key
    B. To keep the private key secret
    C. To prove that an identity and a public key are linked
    D. To prove that a certificate authority trusts a given user

Solution: To prove that an identity and a public key are linked

15. A brute force attack on a hash function with n-bit outputs requires about how many hash operations?
    A. 2^n
    B. $(2^n)^{1/2} (the square root of 2^n)$
    C. n
    D. n^2

Solution: $(2^n)^{1/2} (the square root of 2^n)$

16. Which is true about AES?
    A. It is a symmetric key algorithm
    B. It is an asymmetric key algorithm
    C. It is no longer secure
    D. It replaced the MD5 algorithm

Solution: It is a symmetric key algorithm

17. This is the original message or data that is fed into the algorithm as input.
    A. Plaintext
    B. Ciphertext
    C. Plain key
    D. Message digest

Solution: Plaintext

18. Which of the following terms isn't equivalent
    A. Policy
    B. Rights
    C. Authorizations
    D. Privileges
    E. Entitlements

Solution: Policy

19. When checking the digital signature of Bobs message, how is a hash function used?
    A. It is used to hash the input to the encryption function
    B. It is used to hash the output of the decryption function
    C. It is used to hash Bobs public key before decryption; the key is long otherwise
    D. It is used to hash the message; the hash is compared with the decrypted hash value

Solution: It is used to hash the message; the hash is compared with the decrypted hash value

20. APT
    A. Advanced Persistant Threat
    B. Advanced Persistant Trojan
    C. Asynchronous Partition Table
    D. Advanced Persistant Thread

Solution: Advanced Persistant Threat

21. A downside to the Access Control Matrix
    A. It's sparse
    B. Its one to one relationship
    C. Its one to many relationship
    D. It follows the rule of least privilege

Solution: It's sparse

22. This is an attack on system availability
    A. Incapacitation
    B. Corruption
    C. Misappropriation
    D. Usurpation

Solution: Incapacitation

23. The design of security measures embodied in both hardware and software should be as simple and small as possible.
    A. KISS method
    B. Encapsulation
    C. Economy of mechanism
    D. Complete mediation

Solution: KISS method

24. Role-Based Access Control
    A. Controls access based on the identity of the requestor and on access rules (authorizations) stating what requestors are (or are not) allowed to do.
    B. Controls access based on comparing security labels (which indicate how sensitive or critical system resources are) with security clearances (which indicate system entities are eligible to access certain resources).
    C. Controls access based on the roles that users have within the system and on rules stating what accesses are allowed to users in given roles.

D. Controls access based on characteristics of the user, the resource to be accessed, and current environmental conditions.

Solution: Controls access based on the roles that users have within the system and on rules stating what accesses are allowed to users in given roles.

25. Which of these is NOT a requirement for secure use of symmetric encryption?
    A. Sender and receiver keep the key secure
    B. Hiding the details of the encryption algorithm from the attacker
    C. Sender and receiver have obtained the secret key in a secure fashion
    D. Keys are long and random enough to prevent brute force attacks

Solution: Hiding the details of the encryption algorithm from the attacker

26. Measures and controls that ensure confidentiality, integrity, and availability of information system assets including hardware, software, firmware, and information being processed, stored, and communicated
    A. Computer Security
    B. Information Systems
    C. Auditing
    D. Security controls

Solution: Security controls

27. Cryptanalysis is
    A. The study of cryptography
    B. A symmetric encryption attack
    C. The analysis of a cryptographic algorithm
    D. The study of codes

Solution: The analysis of a cryptographic algorithm

28. Which of these is considered a secure cryptographic hash function?
    A. MD5

B. SHA (the Secure Hash Algorithm)

C. SHA-384

D. SHA-1024

Solution: SHA-384

29. Which of these systems has a high availability requirement (just choose the best answer)?

    A. A university Website

    B. A system to process financial transactions

    C. An online telephone directory

    D. Anti-virus software running on a PC

Solution: A system to process financial transactions

30. What type of plaintext is hardest to perform brute force on (starting from the ciphertext)?

    A. English text

    B. Chinese text

    C. A Windows 7 executable

    D. A compressed spreadsheet of numerical data

Solution: A compressed spreadsheet of numerical data

31. A branching, hierarchical data structure that represents a set of potential techniques for exploiting security vulnerabilities

    A. Attack surface

    B. Attack vector

    C. Attack tree

    D. Attack pattern

Solution: Attack tree

32. What verifies the user can access what they are requesting?

A. Authentication
B. Authorization
C. Audit
D. Access control

Solution: Authorization

33. Keeping the trusted code base very small in trusted computing is an example of which security property?
    A. Least privilege
    B. Default Security
    C. Defense in Depth
    D. Minimize the variety, size, and complexity of trusted components (KISS)

Solution: Minimize the variety, size, and complexity of trusted components (KISS)

34. An attempt by an unauthorized user to gain access to a system by posing as an authorized user
    A. Deauthentication
    B. Masquerading
    C. Repudiation
    D. Man-in-the-middle

Solution: Masquerading

35. Traffic analysis is what type of attack?
    A. Inference
    B. Interference
    C. Interception
    D. Intrusion

Solution: Interception

36. Using a public encryption scheme which key would Alice use to send an ecrypted message to Bob?

A. Alice's private key
B. Bob's private key
C. Alice's public key
D. Bob's public key

Solution: Bob's public key

37. What is the BEST reason to be concerned about the insider threat?
    A. Insiders can plant malware on the system
    B. Insiders have some degree of authorized access to the system
    C. Insiders like disgruntled employees have greater motivation to cause harm
    D. Insiders are harder to prosecute than external hackers

Solution: Insiders have some degree of authorized access to the system

38. Which virus creates copies during replication that are functionally equivalent but have distinctly different bit patterns, in order to vary its signature
    A. Metamorphic virus
    B. Polymorphic virus
    C. Stealth virus
    D. Cryptographic virus

Solution: Metamorphic virus

39. What is the first step in devising security services and mechanisms?
    A. Developing a security policy
    B. Deciding between prevention and detection/reaction
    C. Designing assurance metrics
    D. Locking down unnecessary services

Solution: Developing a security policy

40. In which application area is integrity typically valued higher than confidentiality?
    A. Military documents
    B. Financial transactions
    C. Health care records
    D. Video rental records

Solution: Financial transactions

41. A practice in which multiple privilege attributes are required to achieve access to a restricted resource.
    A. Least priviledge
    B. Separation of priveledge
    C. Authorization
    D. Least common mechanism

Solution: Separation of priveledge

42. Random numbers for cryptography should have which of these features?
    A. Uniform distribution, Independence, and Unbreakability
    B. Uniform distribution, Independence, and Unpredictability
    C. Non-uniform distribution, Independence, and Unbreakability
    D. Non-uniform distribution, Independence, and Unpredictability

Solution: Uniform distribution, Independence, and Unpredictability

43. Creating a digital envelope includes which of these steps?
    A. Encrypt the symmetric key with the senders public key
    B. Encrypt the symmetric key with the receivers public key
    C. Encrypt the senders private key with the receivers public key
    D. Encrypt the receivers private key with the senders public key

Solution: Encrypt the symmetric key with the receivers public key

44. Why do attackers have a significant advantage over defenders?

    A. Security mechanisms are complex and it is not obvious that such measures are needed

    B. Computer security has complex requirements that are hard to describe

    C. The attacker only needs to find one hole; defenders must attempt to close all holes

    D. Finding successful attacks is straightforward exercise once the system is understood

Solution: The attacker only needs to find one hole; defenders must attempt to close all holes

45. Attribute-based Access Control

    A. Controls access based on the identity of the requestor and on access rules (authorizations) stating what requestors are (or are not) allowed to do.

    B. Controls access based on comparing security labels (which indicate how sensitive or critical system resources are) with security clearances (which indicate system entities are eligible to access certain resources).

    C. Controls access based on the roles that users have within the system and on rules stating what accesses are allowed to users in given roles.

    D. Controls access based on characteristics of the user, the resource to be accessed, and current environmental conditions.

Solution: Controls access based on characteristics of the user, the resource to be accessed, and current environmental conditions.

46. Why is security a weak-link property?

    A. One weakness in the system leads to more weaknesses later

    B. The security of the whole system is only as good as the security of each (exposed) part

    C. The link between typical users and the system security goals is weak

    D. Weak links in a defense can be overcome with stronger links through security design

Solution: The security of the whole system is only as good as the security of each (exposed) part

47. Role Based Access Control

    A. Is based on the roles that users assume in a system rather than the users identity

    B. Is based on the roles the resources assume in a system rather than the resources type

    C. Is based on the roles the processes assumes in a system rather than the user's identity

D. Is based on the roles the access conrtol matrix assumes in a system rather than the role's identity

Solution: Is based on the roles that users assume in a system rather than the users identity

48. An attempt to learn or make use of information from the system that does not affect system resources.
    A. Passive Attack
    B. Port Scanning
    C. nmap
    D. Exfiltration

Solution: Passive Attack

49. Why is it difficult to simply ban the use of mobile code in a strictly controlled environment (e.g. military)?
    A. Mobile code makes Flash animations possible
    B. Mobile code runs more efficiently than static code
    C. Virus scanners use mobile code to distribute and install patches
    D. Virus scanners would fail to detect the use of mobile code, making enforcement hard

Solution: Virus scanners use mobile code to distribute and install patches

50. Encryption of a plaintext using ones private key is .
    A. insecure, because anyone with the public key can decrypt it
    B. useful for providing authentication but not confidentiality
    C. useful for providing confidentiality but not authentication
    D. useful for providing both authentication and confidentiality

Solution: useful for providing authentication but not confidentiality

51. Establish, maintain, and implement plans for emergency response, backup operations, and postdisaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

A. Risk Management
B. Risk Management Framework
C. Incident Response
D. Contingency Planning

Solution: Contingency Planning

52. Which is not an example of mult-factor authentication?
    A. A key and a PIN
    B. Your eyeball and a key
    C. Credit card and an authenticator app
    D. The way you walk and a password

Solution: Credit card and an authenticator app

53. Assures that information is not made available or disclosed to unauthorized individuals.
    A. Data integrity
    B. Confidentiality
    C. Encryption
    D. Authentication

Solution: Confidentiality

54. Why do people use 3DES?
    A. AES is not yet a federal standard
    B. It is three times as secure as DES
    C. It is almost three times faster than DES
    D. It retains the security of DES against cryptanalysis

Solution: It retains the security of DES against cryptanalysis

55. What is the advantage of a digital envelope over encrypting the message with the public key?

A. The digital envelope method uses less bandwidth

B. Public key encryption is less secure than symmetric key encryption

C. Public key encryption is slow, so it saves computation time in most cases

D. Public key encryption can only be made to work on small amounts of data at a time

Solution: Public key encryption is slow, so it saves computation time in most cases

56. Discretionary Access Control

    A. Controls access based on the identity of the requestor and on access rules (authorizations) stating what requestors are (or are not) allowed to do.

    B. Controls access based on comparing security labels (which indicate how sensitive or critical system resources are) with security clearances (which indicate system entities are eligible to access certain resources).

    C. Controls access based on the roles that users have within the system and on rules stating what accesses are allowed to users in given roles.

    D. Controls access based on characteristics of the user, the resource to be accessed, and current environmental conditions.

Solution: Controls access based on the identity of the requestor and on access rules (authorizations) stating what requestors are (or are not) allowed to do.

57. What verifies the use is who they say they are?

    A. Authentication

    B. Authorization

    C. Audit

    D. Access control

Solution: Authentication

58. Lowering the decision threshold on a biometric measure results in

    A. More false positives

    B. More false negatives

Solution: More false negatives

59. Authentication, authorization, and audit (AAA) are all part of which security property?
    A. Least privilege
    B. Accountability
    C. Default security
    D. Minimize the variety, size, and complexity of trusted components (KISS)

Solution: Accountability

60. A potential for violation of security, which exists when there is a circumstance, capability, action, or event, that could breach security and cause harm.
    A. Weakness
    B. Threat
    C. Vulnerability
    D. Breach

Solution: Threat

61. A misconfigured rule enforced by a firewall is an example of which of these?
    A. Risk
    B. Threat
    C. Attack
    D. Vulnerability

Solution: Vulnerability

62. Why is the DES algorithm considered unacceptable today?
    A. It is too slow
    B. It is vulnerable to brute force
    C. It is vulnerable to cryptanalysis
    D. It is vulnerable to rainbow tables

Solution: It is vulnerable to brute force

63. A flaw or weakness in a systems design, implementation, or operation and management that could be exploited to violate the systems security policy.
    A. Weakness
    B. Threat
    C. Vulnerability
    D. Breach

Solution: Vulnerability

64. Which of these involves backup systems?
    A. Prevention
    B. Detection
    C. Response
    D. Recovery

Solution: Recovery

65. Which of these statements is true?
    A. Public key encryption is commonly used to share secret keys
    B. Public key encryption is likely to supplant symmetric key encryption in the next decade
    C. Public key encryption is more secure against brute force than symmetric key encryption
    D. Public key encryption is more secure against cryptanalysis than symmetric key encryption

Solution: Public key encryption is commonly used to share secret keys

66. Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.
    A. Access Control
    B. Identity Management
    C. Authentication

D. Service Acquisition

Solution: Access Control

67. Which of the following biometric schemes is the most accurate?
    A. Retina
    B. Iris
    C. Hand
    D. Finger

Solution: Iris

68. Mandatory Access Control
    A. Controls access based on the identity of the requestor and on access rules (authorizations) stating what requestors are (or are not) allowed to do.
    B. Controls access based on comparing security labels (which indicate how sensitive or critical system resources are) with security clearances (which indicate system entities are eligible to access certain resources).
    C. Controls access based on the roles that users have within the system and on rules stating what accesses are allowed to users in given roles.
    D. Controls access based on characteristics of the user, the resource to be accessed, and current environmental conditions.

Solution: Controls access based on comparing security labels (which indicate how sensitive or critical system resources are) with security clearances (which indicate system entities are eligible to access certain resources).

69. What doesn't a digital signature provide?
    A. Integrity
    B. Confidentiality
    C. Non-repudiation
    D. Authenticity

Solution: Confidentiality

70. Which of these is NOT a part of what needs to be considered when developing a security policy?
    A. The value of the assets being protected
    B. The effect on ease of use of the system of various decisions
    C. The degree to which the security system implementation meets its specifications
    D. The cost of failure and recovery

Solution: The degree to which the security system implementation meets its specifications

71. An attempt to alter system resources or affect their operation.
    A. Breach
    B. Exploit
    C. Active Attack
    D. Denial of Service

Solution: Active Attack

72. Which of these is the best for encrypting secret keys when speed is critical?
    A. RSA
    B. Diffie-Hellman
    C. DSS
    D. ECC

Solution: ECC

73. What is the main advantage of risk management over risk avoidance?
    A. It leads to greater focus on defending against more dangerous threats
    B. It leads to removal of a greater number of vulnerabilities from the system
    C. It leads to defending against a larger variety of threats
    D. It is more effective against insider threats

Solution: It leads to defending against a larger variety of threats

74. What is an attack against hashed passwords?
    A. Dictionary attack
    B. Rainbow Table
    C. Salting
    D. Reactive password checking

Solution: Rainbow Table

75. Asymmetric encryption requires
    A. Alice and Bob have the same key
    B. Alice has 1 key and Bob has 2
    C. Alice has two keys and Bob has two keys
    D. A way to securely transmit keys

Solution: Alice has two keys and Bob has two keys

76. Attribute-Based Access Control
    A. Defines authorizations that express conditions on properties of both the resource and the subject
    B. Defines authorizations that express conditions on properties of both the user and the subject
    C. Defines authorizations that express conditions on properties of both the resource and the system
    D. Defines authorizations that express conditions on properties of both the system and the subject

Solution: Defines authorizations that express conditions on properties of both the resource and the subject

77. Symmetric encryption provides
    A. Confidentiality
    B. Integrity
    C. Availability

Solution: Confidentiality

78. The degree of confidence one has that the security measures, both technical and operational, work as intended to protect the system and the information it processes
    A. Level of assurance
    B. Assurance
    C. Risk level
    D. Mitigation factor

Solution: Assurance

79. Trying every possible combination is what type of attack?
    A. Brute-force attack
    B. Man-in-the-middle
    C. Monte Carlo
    D. Combo attack

Solution: Brute-force attack

80. Manufacturers setting a strong password on wireless routers is an example of which security property?
    A. Least privilege
    B. Accountability
    C. Default security
    D. Minimize the variety, size, and complexity of trusted components (KISS)

Solution: Default security

81. Any means taken to deal with a security attack.
    A. Countermeasure
    B. Mitigation
    C. Risk
    D. Patch

Solution: Countermeasure

82. Multi-factor authentication doesn't involve
    A. Something you have
    B. Something you are
    C. Something you know
    D. Something you prove

Solution: Something you prove

83. Which of these crypto tools does a certificate NOT need?
    A. Hashing
    B. Symmetric key encryption
    C. Decryption using the public key
    D. Encryption using the private key

Solution: Symmetric key encryption

84. A threat that is carried out (threat action) and, if successful, leads to an undesirable violation of security, or threat consequence.
    A. Attack
    B. Exploit
    C. Threat
    D. Vulnerability

Solution: Attack

85. Which of these is the best example of why administration of systems is so important to security?
    A. Administrators have more privilege than other users
    B. Administrators are responsible for password creation
    C. The bulk of attacks can be blocked by a properly administered firewall
    D. The bulk of attacks are against vulnerabilities for which there are patches available

Solution: The bulk of attacks are against vulnerabilities for which there are patches available

86. For a bank website, what kind of checking of identity should the certificate authority do (ideally)?
    A. Go to the banks website to validate their information
    B. Make a phone call to the head of the banks Website division
    C. Go to a bank branch in person and get bank details from a manager
    D. Go to the bank headquarters and verify details in person with the CEO and the top Website people

Solution: Go to the bank headquarters and verify details in person with the CEO and the top Website people

87. A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources.
    A. System security plan
    B. Security policy
    C. Rules based enforcement
    D. Authentication and Authorization

Solution: Security policy

88. If our main concern is confidentiality of data from a hostile countrys hackers, we should be most concerned about what type of attack?
    A. Active insider attack
    B. Passive insider attack
    C. Active outsider attack
    D. Passive outsider attack

Solution: Active outsider attack

89. Asymmetric encryption does not provide
    A. Confidentiality
    B. Integrity

C. Availability

Solution: Availability

90. (1 point) What is the primary goal of an intrusion detection system (IDS)?
    A. To detect and respond to unauthorized access attempts
    B. To monitor and log all network activity continuously
    C. To identify and log only high-severity attacks on systems
    D. To block all forms of unauthorized access automatically

Solution: To detect and respond to unauthorized access attempts

91. (1 point) Which feature best distinguishes a network-based IDS?
    A. It monitors packets for suspicious patterns
    B. It analyzes both host activity and system logs
    C. It evaluates encrypted traffic without decryption
    D. It identifies internal host configuration vulnerabilities

Solution: It monitors packets for suspicious patterns

92. (1 point) What kind of attack is most likely to evade detection by signature-based IDS?
    A. A known attack with slight variations in payload delivery
    B. A previously unseen exploit targeting a novel vulnerability
    C. A phishing campaign targeting system administrators
    D. A brute-force attack on administrative passwords

Solution: A previously unseen exploit targeting a novel vulnerability

93. (1 point) What is a significant limitation of anomaly-based IDS detection?

A. It requires extensive historical data for accurate profiling
B. It can only detect insider threats based on signature analysis
C. It operates effectively only on isolated host machines
D. It lacks support for network-level intrusion detection

Solution: It requires extensive historical data for accurate profiling

94. (1 point) What is the primary function of the Cyber Kill Chain framework?
A. To classify adversary behaviors during different phases of an attack
B. To optimize cryptographic key exchange during active threats
C. To create a database of zero-day vulnerabilities for future analysis
D. To reduce system vulnerabilities through automated patch management

Solution: To classify adversary behaviors during different phases of an attack

95. (1 point) How does threshold detection enhance anomaly-based intrusion detection systems?
A. By identifying abnormal user behaviors over extended time periods
B. By limiting the number of false negatives through signature comparison
C. By flagging excessive occurrences of defined system events
D. By detecting encrypted traffic that deviates from baseline patterns

Solution: By flagging excessive occurrences of defined system events

96. (1 point) Why is signature-based IDS unsuitable for detecting unknown attacks?
A. It cannot adapt to changes in encrypted payloads dynamically
B. It requires frequent updates to its signature database
C. It relies on predefined patterns for attack identification
D. It only analyzes event sequences within network traffic

Solution: It relies on predefined patterns for attack identification

97. (1 point) Which scenario represents a masquerader intrusion?
    A. A valid user intentionally misusing their privileges
    B. An outsider gaining system access through stolen credentials
    C. A user escalating their permissions through privilege escalation
    D. An attacker modifying system logs to hide evidence of activity

Solution: An outsider gaining system access through stolen credentials

98. (1 point) What differentiates a distributed IDS from other intrusion detection systems?
    A. It aggregates and analyzes data from multiple sensors
    B. It focuses solely on host-based event monitoring
    C. It operates independently without requiring configuration
    D. It monitors only encrypted and unencrypted traffic signatures

Solution: It aggregates and analyzes data from multiple sensors

99. (1 point) How does an IDS typically respond to detecting suspicious behavior?
    A. By sending real-time alerts or recording the activity in logs
    B. By terminating all active connections within the network
    C. By dynamically blocking the source IP of the detected attack
    D. By isolating the affected host from the network automatically

Solution: By sending real-time alerts or recording the activity in logs

100. (1 point) Which characteristic best describes a clandestine intruder?

A. A user exploiting vulnerabilities for privilege escalation

B. An outsider conducting brute-force attacks on login credentials

C. An attacker seizing unauthorized administrative control

D. A hacker defacing public-facing web servers

Solution: An attacker seizing unauthorized administrative control

101. (1 point) What is a critical advantage of host-based intrusion detection systems (HIDS)?

A. Monitoring individual system logs and resource usage

B. Capturing real-time network traffic anomalies

C. Detecting vulnerabilities in encrypted system backups

D. Tracking interactions between distributed systems

Solution: Monitoring individual system logs and resource usage

102. (1 point) What is the primary goal of cryptography?

A. To protect data by making it unreadable without proper credentials

B. To secure communication by encrypting and authenticating data

C. To ensure information confidentiality, integrity, and non-repudiation

D. To enable safe storage of sensitive information across devices

Solution: To ensure information confidentiality, integrity, and non-repudiation

103. (1 point) Which of the following best describes a transposition cipher?

A. A cipher that rearranges the order of plaintext characters

B. A cipher that substitutes plaintext letters with encoded ones

C. A cipher that uses multiple keys for data encryption

D. A cipher that combines substitution and transposition techniques

Solution: A cipher that rearranges the order of plaintext characters

104. (1 point) What is a key weakness of the Electronic Codebook (ECB) encryption mode?
    A. It encrypts data in fixed-size blocks, revealing patterns in identical plaintext blocks
    B. It relies on a static key, making it susceptible to brute-force attacks
    C. It requires synchronization between sender and receiver
    D. It uses multiple initialization vectors, complicating decryption

Solution: It encrypts data in fixed-size blocks, revealing patterns in identical plaintext blocks

105. (1 point) What makes asymmetric encryption distinct from symmetric encryption?

A. It uses a pair of keys for encryption and decryption

B. It encrypts data without requiring shared key distribution

C. It enables secure data transfer using a public-private key pair

D. It provides enhanced confidentiality compared to symmetric encryption

Solution: It uses a pair of keys for encryption and decryption

106. (1 point) How does Cipher Block Chaining (CBC) improve encryption security?

A. By using initialization vectors to introduce randomness in ciphertext

B. By XORing each plaintext block with the previous ciphertext block

C. By ensuring all blocks are encrypted independently of others

D. By using dynamic keys to enhance the encryption process

Solution: By XORing each plaintext block with the previous ciphertext block

107. (1 point) What is the most significant challenge associated with symmetric encryption?

A. Difficulty in sharing and managing keys securely

B. Vulnerability to brute-force attacks on short keys

C. Requirement for pre-distributed secret keys between users

D. Dependency on the randomness of initialization vectors

Solution: Difficulty in sharing and managing keys securely

108. (1 point) Why was DES replaced with AES as a standard encryption method?

A. DES could not handle data larger than 56 bits securely

B. AES provides stronger security and supports larger key sizes

C. AES is more efficient in hardware than DES

D. DES required complex key management processes

Solution: AES provides stronger security and supports larger key sizes

109. (1 point) What distinguishes a polymorphic virus in cryptographic contexts?
    A. It changes its encryption signature dynamically to evade detection
    B. It infects multiple files simultaneously using unique payloads
    C. It encrypts data using self-generated keys for every host
    D. It uses symmetric encryption to spread across network systems

Solution: It changes its encryption signature dynamically to evade detection

110. (1 point) Why is key exchange critical in cryptographic systems?
    A. To establish a secure channel for encryption before communication begins
    B. To synchronize encryption parameters for efficient data transfer
    C. To negotiate stronger encryption algorithms between communicating parties
    D. To authenticate the identity of the recipient before sending data

Solution: To establish a secure channel for encryption before communication begins

111. (1 point) What is the primary characteristic of malware?
    A. It disrupts system functionality or compromises data integrity
    B. It modifies operating system files to enhance performance
    C. It infects software to prevent unauthorized access
    D. It creates redundant processes to improve resource utilization

Solution: It disrupts system functionality or compromises data integrity

112. (1 point) How does a worm differ from a virus?

A. A worm propagates without needing a host program

B. A worm spreads slower than a virus due to limited functionality

C. A worm relies on user interaction to execute malicious code

D. A worm encrypts its payload to evade detection

Solution: A worm propagates without needing a host program

113. (1 point) Which scenario best describes the behavior of a Trojan horse?

A. It disguises itself as legitimate software to trick users into execution

B. It replicates itself across systems to exploit vulnerabilities

C. It encrypts files to demand a ransom for decryption

D. It scans network ports to find unpatched services

Solution: It disguises itself as legitimate software to trick users into execution

114. (1 point) What is the purpose of a logic bomb in malware?

A. To trigger malicious activity when specific conditions are met

B. To deliver a payload only during scheduled intervals

C. To encrypt data silently before initiating a ransom request

D. To scan for open network ports before exploitation

Solution: To trigger malicious activity when specific conditions are met

115. (1 point) What is the primary goal of Advanced Persistent Threats (APTs)?

A. To remain undetected while accessing sensitive information over time

B. To exploit vulnerabilities for immediate financial gain

C. To disrupt critical infrastructure with rapid attacks

D. To overwhelm systems through massive distributed denial-of-service (DDoS) attacks

Solution: To remain undetected while accessing sensitive information over time

116. (1 point) What defines the payload of malware?

A. The actions the malware performs after activation

B. The method by which malware spreads between systems

C. The encryption algorithm used to protect its code

D. The triggers used to determine when malware executes

Solution: The actions the malware performs after activation

117. (1 point) Which characteristic is typical of polymorphic malware?

A. It changes its code signature to evade detection

B. It encrypts files to prevent access without a decryption key

C. It disables antivirus software during execution

D. It replicates across systems using network vulnerabilities

Solution: It changes its code signature to evade detection

118. (1 point) What makes a rootkit particularly dangerous?

A. It grants attackers privileged access to compromised systems

B. It encrypts system logs to cover tracks after an attack

C. It replicates rapidly across all connected devices

D. It targets critical infrastructure with denial-of-service attacks

Solution: It grants attackers privileged access to compromised systems

119. (1 point) What is the role of a bot in a botnet?
    A. To execute commands issued by a centralized controller
    B. To distribute spam emails using harvested credentials
    C. To encrypt data on infected systems for financial extortion
    D. To identify vulnerabilities in connected devices

Solution: To execute commands issued by a centralized controller

120. (1 point) What distinguishes a distributed denial-of-service (DDoS) attack?

A. It uses multiple compromised systems to target a single resource

B. It encrypts traffic between attackers and targets to evade detection

C. It relies on phishing emails to compromise end-user systems

D. It exploits zero-day vulnerabilities in network hardware

Solution: It uses multiple compromised systems to target a single resource

121. (1 point) What makes zero-day attacks particularly difficult to defend against?

A. They exploit vulnerabilities that have not been publicly disclosed

B. They use encryption to bypass traditional network defenses

C. They replicate across systems faster than known malware

D. They are distributed through advanced phishing techniques

Solution: They exploit vulnerabilities that have not been publicly disclosed

122. (1 point) How does a stealth virus evade detection?

A. By hiding its presence during file scans or system checks

B. By encrypting itself and storing the decryption key on a remote server

C. By disabling active antivirus software before executing its payload

D. By corrupting system logs to prevent forensic analysis

Solution: By hiding its presence during file scans or system checks

123. (1 point) Which of the following best describes a ransomware delivery mechanism?

A. Phishing emails with malicious attachments

B. Network scans for unpatched vulnerabilities

C. System exploits leveraging privilege escalation techniques

D. Remote access trojans with keylogging functionality

Solution: Phishing emails with malicious attachments

124. (1 point) What is the primary function of antivirus software's heuristic detection?
    A. To identify new malware based on behavior patterns
    B. To isolate known malicious files using signature databases
    C. To prevent unauthorized software installation on endpoints
    D. To monitor real-time traffic for encrypted payloads

Solution: To identify new malware based on behavior patterns

125. (1 point) What is the primary role of security controls in IT security management?
    A. To reduce vulnerabilities and mitigate risks to acceptable levels
    B. To detect unauthorized access attempts and log them
    C. To ensure compliance with organizational policies and standards
    D. To enforce user authentication and system integrity protocols

Solution: To reduce vulnerabilities and mitigate risks to acceptable levels

126. (1 point) Which of the following best describes a technical security control?
    A. A mechanism that enforces system-level protection measures
    B. A policy outlining user access rights and privileges
    C. A process for reviewing and updating risk assessments
    D. A training program designed to improve employee security awareness

Solution: A mechanism that enforces system-level protection measures

127. (1 point) Which of the following is an example of a preventative technical control?

A. Intrusion detection systems (IDS) monitoring network traffic
B. Firewalls configured to block unauthorized access
C. Encryption applied to sensitive data in transit
D. Access logs reviewed for suspicious activities

Solution: Firewalls configured to block unauthorized access

128. (1 point) What is the primary focus of detection and recovery controls?
A. Identifying and responding to security breaches promptly
B. Preventing unauthorized access through technical safeguards
C. Mitigating potential vulnerabilities in system configurations
D. Ensuring compliance with organizational risk assessments

Solution: Identifying and responding to security breaches promptly

129. (1 point) What is the primary purpose of a risk assessment in IT security management?
A. To evaluate threats and vulnerabilities to determine appropriate controls
B. To ensure technical and operational measures meet compliance standards
C. To establish a framework for monitoring and auditing controls
D. To prioritize security policies based on business requirements

Solution: To evaluate threats and vulnerabilities to determine appropriate controls

130. (1 point) What is the significance of cost-benefit analysis in selecting security controls?

A. It ensures the chosen controls provide optimal risk reduction within budget

B. It justifies the allocation of resources for technical safeguards

C. It evaluates the impact of control implementation on user productivity

D. It determines the return on investment for proposed security measures

Solution: It ensures the chosen controls provide optimal risk reduction within budget

131. (1 point) Which of the following is an example of a residual risk?

A. A vulnerability that remains after implementing security controls

B. A new threat identified during the latest risk assessment

C. A system misconfiguration caused by incomplete updates

D. A technical control failing to mitigate a known vulnerability

Solution: A vulnerability that remains after implementing security controls

132. (1 point) What is the purpose of an IT security plan?

A. To outline risks, controls, and actions for mitigating threats

B. To enforce compliance with industry and regulatory standards

C. To document security incidents and their resolutions

D. To establish monitoring protocols for security control effectiveness

Solution: To outline risks, controls, and actions for mitigating threats

133. (1 point) How does a contingency plan contribute to IT security?

A. By providing guidance on recovering from unexpected disruptions

B. By identifying vulnerabilities in system configurations

C. By preventing unauthorized physical access to facilities

D. By monitoring user activities and logging access attempts

Solution: By providing guidance on recovering from unexpected disruptions

134. (1 point) Which of the following is an essential element of security compliance?
    A. Auditing security controls for adherence to policies
    B. Updating encryption algorithms to meet new standards
    C. Conducting penetration tests on critical infrastructure
    D. Implementing user training programs for security awareness

Solution: Auditing security controls for adherence to policies

135. (1 point) Which example represents a corrective security control?

A. Restoring data from backups after a ransomware attack

B. Configuring multi-factor authentication for user accounts

C. Encrypting sensitive files stored on the network

D. Reviewing system logs to identify unauthorized activities

Solution: Restoring data from backups after a ransomware attack

136. (1 point) What is the purpose of a baseline approach in risk management?

A. To implement common safeguards against widely known threats

B. To establish benchmarks for evaluating security control effectiveness

C. To analyze organizational risk using informal assessments

D. To identify critical risks for formal evaluation

Solution: To implement common safeguards against widely known threats

137. (1 point) What distinguishes formal risk analysis from informal approaches?

A. Formal risk analysis uses structured methods to assess risks and controls

B. Formal risk analysis focuses on common vulnerabilities across systems

C. Formal risk analysis emphasizes rapid evaluations for small organizations

D. Formal risk analysis integrates operational and technical controls

Solution: Formal risk analysis uses structured methods to assess risks and controls

138. (1 point) Which task is essential for maintaining the effectiveness of implemented controls?

A. Periodically reviewing and updating controls based on new threats

B. Documenting control specifications in the organizational security policy

C. Restricting control updates to align with system downtime

D. Enforcing strict access controls for updating system settings

Solution: Periodically reviewing and updating controls based on new threats

139. (1 point) What is the primary role of incident handling procedures?
    A. To provide a structured approach for responding to security incidents
    B. To document vulnerabilities identified in system audits
    C. To monitor real-time activities for early threat detection
    D. To ensure compliance with post-incident reporting regulations

Solution: To provide a structured approach for responding to security incidents

140. (1 point) What is the primary objective of risk assessment in security management?

A. To identify vulnerabilities and recommend appropriate countermeasures

B. To evaluate potential threats and their likelihood of occurrence

C. To prioritize risks and allocate resources for mitigation efforts

D. To reduce organizational exposure by implementing technical controls

Solution: To identify vulnerabilities and recommend appropriate countermeasures

141. (1 point) Which element is NOT a part of the risk assessment process?

A. Identification of assets and their value to the organization

B. Development of security policies for user access control

C. Analysis of potential threats and vulnerabilities

D. Evaluation of existing controls and residual risks

Solution: Development of security policies for user access control

142. (1 point) What is the primary function of a security policy?

A. To define organizational guidelines for protecting assets

B. To enforce user compliance with technical safeguards

C. To detect and mitigate active threats in real-time

D. To evaluate system configurations for compliance with standards

Solution: To define organizational guidelines for protecting assets

143. (1 point) Which component of a risk management plan focuses on residual risks?

A. Risk acceptance strategy for handling low-priority risks

B. Risk mitigation strategies to address identified vulnerabilities

C. Risk transference measures for minimizing financial exposure

D. Risk monitoring protocols for tracking ongoing threats

Solution: Risk acceptance strategy for handling low-priority risks

144. (1 point) What is the main advantage of conducting a Business Impact Analysis (BIA)?
    A. It identifies critical business processes and their dependencies
    B. It prioritizes technical safeguards for high-value systems
    C. It defines the scope of compliance monitoring programs
    D. It improves disaster recovery plans by simulating failure scenarios

Solution: It identifies critical business processes and their dependencies

145. (1 point) What is the purpose of a risk register in security management?

A. To document identified risks, their analysis, and mitigation plans

B. To track compliance with regulatory and legal requirements

C. To store incident response details and post-event analyses

D. To consolidate data from threat monitoring tools for reporting

Solution: To document identified risks, their analysis, and mitigation plans

146. (1 point) What is the primary goal of security governance?

A. To align security efforts with organizational goals and objectives

B. To enforce compliance with technical security standards

C. To ensure consistent application of encryption and access control

D. To minimize operational disruptions caused by security breaches

Solution: To align security efforts with organizational goals and objectives

147. (1 point) How does risk transference differ from risk mitigation?

A. Risk transference shifts potential losses to third parties, such as insurers

B. Risk transference reduces the likelihood of vulnerabilities being exploited

C. Risk transference focuses on eliminating the root cause of threats

D. Risk transference ensures compliance with security regulations

Solution: Risk transference shifts potential losses to third parties, such as insurers

148. (1 point) What is the role of continuous monitoring in risk management?

A. To detect changes in risk exposure and adjust controls as needed

B. To enforce compliance with established risk assessment policies

C. To evaluate the effectiveness of disaster recovery plans regularly

D. To identify vulnerabilities introduced by hardware and software updates

Solution: To detect changes in risk exposure and adjust controls as needed

149. (1 point) Which approach is most effective for managing high-priority risks?
    A. Implementing advanced technical controls to reduce their likelihood
    B. Developing robust contingency plans for worst-case scenarios
    C. Allocating resources to mitigate or eliminate vulnerabilities directly
    D. Outsourcing security operations to external service providers

Solution: Allocating resources to mitigate or eliminate vulnerabilities directly

150. (1 point) What distinguishes strategic controls from operational controls in security management?

A. Strategic controls align security policies with organizational objectives

B. Strategic controls ensure compliance with technical standards

C. Strategic controls focus on immediate mitigation of active threats

D. Strategic controls implement technical safeguards for critical systems

Solution: Strategic controls align security policies with organizational objectives

151. (1 point) Which factor is most critical when prioritizing risks during assessment?

A. The potential impact of the risk on organizational objectives

B. The likelihood of the risk materializing based on historical data

C. The cost of mitigating the risk versus its potential consequences

D. The availability of technical controls to address identified threats

Solution: The potential impact of the risk on organizational objectives

152. (1 point) How does an incident response plan support risk management?

A. By providing a structured process for handling security incidents

B. By documenting lessons learned to prevent future occurrences

C. By ensuring rapid recovery from security breaches or disruptions

D. By validating the effectiveness of existing technical controls

Solution: By providing a structured process for handling security incidents

153. (1 point) What is the primary benefit of risk aggregation?

A. It provides a consolidated view of all risks across the organization

B. It reduces the likelihood of overlapping risk mitigation strategies

C. It improves decision-making by ranking risks based on priority

D. It ensures compliance with regulatory requirements for reporting

Solution: It provides a consolidated view of all risks across the organization

154. (1 point) What is the role of the Trusted Platform Module (TPM) in Trusted Computing?
    A. To provide secure hardware storage for cryptographic keys
    B. To enforce system policies through remote attestation
    C. To validate user credentials before granting access
    D. To encrypt all data stored on the device by default

Solution: To provide secure hardware storage for cryptographic keys

155. (1 point) Which Trusted Computing component ensures software integrity during execution?

A. Code signing ensures that software has not been tampered with

B. Encrypted memory prevents unauthorized data access

C. Secure hardware tokens validate user identities

D. Remote attestation verifies runtime system configurations

Solution: Code signing ensures that software has not been tampered with

156. (1 point) Which Trusted Computing feature ensures unauthorized code cannot run?

A. Secure Boot prevents the execution of unsigned software

B. Code Signing restricts access to unverified processes

C. Encrypted memory blocks unauthorized read operations

D. Remote Attestation validates software authenticity remotely

Solution: Secure Boot prevents the execution of unsigned software

157. (1 point) What is the purpose of cryptographic keys stored in a TPM?

A. To encrypt sensitive data and authenticate system components

B. To enforce role-based access controls for critical resources

C. To validate firmware updates before they are applied

D. To provide multi-factor authentication for user logins

Solution: To encrypt sensitive data and authenticate system components

158. (1 point) How does TPM-backed encryption enhance security?

A. By ensuring encryption keys never leave secure hardware storage

B. By enabling faster key generation and distribution for large datasets

C. By authenticating users with hardware-level credentials

D. By encrypting network traffic without affecting latency

Solution: By ensuring encryption keys never leave secure hardware storage

question[1] What is the primary purpose of user authentication in a security context?

A. To verify the identity of users accessing systems or resources

B. To enforce access control policies and manage user permissions

C. To detect unauthorized access attempts through activity logs

D. To prevent malicious software from executing on user devices

Solution: To verify the identity of users accessing systems or resources

159. (1 point) Which of the following best defines multifactor authentication (MFA)?

A. Authentication requiring multiple pieces of evidence from different categories

B. A process involving the use of at least two passwords for system access

C. A security mechanism combining biometrics and token-based verification

D. A method ensuring network-level encryption during authentication attempts

Solution: Authentication requiring multiple pieces of evidence from different categories

160. (1 point) What distinguishes biometric authentication from other methods?

A. It uses unique physiological or behavioral traits for identity verification

B. It relies on hardware-based tokens or smart cards for authentication

C. It combines a user ID with a secret passphrase for access control

D. It validates the identity of users through location-based parameters

Solution: It uses unique physiological or behavioral traits for identity verification

161. (1 point) Which factor is NOT typically considered in two-factor authentication (2FA)?

A. Something the user knows, like a password

B. Something the user has, like a hardware token

C. Something the user does, like their typing pattern

D. Something the user is, like a fingerprint or iris scan

Solution: Something the user does, like their typing pattern

162. (1 point) Which vulnerability is most effectively mitigated by password hashing?

A. Password database breaches exposing plain-text credentials

B. Brute-force attacks targeting encrypted authentication tokens

C. Replay attacks using intercepted session credentials

D. Phishing attempts to obtain user account information

Solution: Password database breaches exposing plain-text credentials

163. (1 point) What is the purpose of an authentication token?

A. To provide a temporary, secure credential for accessing systems

B. To validate the encryption algorithm used during authentication

C. To store user credentials securely on a hardware device

D. To encrypt session data for secure network communication

Solution: To provide a temporary, secure credential for accessing systems

164. (1 point) What is the key difference between authorization and authentication?

A. Authentication verifies identity, while authorization grants access rights

B. Authentication enforces compliance, while authorization audits user actions

C. Authentication protects credentials, while authorization validates tokens

D. Authentication encrypts data, while authorization restricts permissions

Solution: Authentication verifies identity, while authorization grants access rights

165. (1 point) What is a primary limitation of password-based authentication systems?

A. They are vulnerable to phishing and brute-force attacks

B. They cannot encrypt sensitive data during transmission

C. They do not support multifactor authentication mechanisms

D. They lack compatibility with single sign-on protocols

Solution: They are vulnerable to phishing and brute-force attacks

166. (1 point) What defines cybercrime in the context of computer security?

A. Criminal activity where computers serve as tools, targets, or environments for illegal actions

B. Unauthorized access to private systems for financial gain

C. Exploitation of vulnerabilities in network protocols for malicious purposes

D. Theft of intellectual property using advanced computer algorithms

Solution: Criminal activity where computers serve as tools, targets, or environments for illegal actions

167. (1 point) What exclusive right is granted to patent holders?

A. To prevent others from making, using, or selling the patented invention

B. To claim royalties from any similar invention globally

C. To limit competition in markets where the invention is used

D. To register additional patents derived from the original invention

Solution: To prevent others from making, using, or selling the patented invention

168. (1 point) What is a key provision of the U.S. Digital Millennium Copyright Act (DMCA)?

A. Prohibition of circumvention of technological copyright protection measures

B. Mandated use of digital rights management (DRM) for copyrighted works

C. Universal registration of all digital content for legal protection

D. Requirement for encryption of copyrighted digital media

Solution: Prohibition of circumvention of technological copyright protection measures

169. (1 point) How does the European Union Data Protection Directive address privacy?

A. By requiring member states to safeguard personal data while ensuring free data flow

B. By enforcing strict penalties for breaches of individual privacy

C. By centralizing data protection laws under a unified regulatory framework

D. By mandating encryption for all personal data processed within the EU

Solution: By requiring member states to safeguard personal data while ensuring free data flow

170. (1 point) What is a critical concern regarding the use of digital rights management (DRM)?

A. Potential inhibition of legitimate security and cryptographic research

B. Excessive cost of implementing DRM solutions for small businesses

C. Limited support for cross-platform content use

D. Increased risk of data breaches due to DRM vulnerabilities

Solution: Potential inhibition of legitimate security and cryptographic research

171. (1 point) Which action exemplifies a copyright infringement?

A. Distributing unauthorized copies of a software program

B. Modifying the code of open-source software without consent

C. Developing similar software functionality using different algorithms

D. Using unlicensed fonts in a personal project

Solution: Distributing unauthorized copies of a software program

172. (1 point) What is a key ethical issue in computer security?

A. Balancing professional responsibilities with ethical duties to protect privacy

B. Protecting intellectual property at the expense of public knowledge

C. Prioritizing organizational security over individual user freedoms

D. Enforcing stricter access controls to mitigate human errors

Solution: Balancing professional responsibilities with ethical duties to protect privacy

173. (1 point) What is the purpose of a privacy policy in an organization?
    A. To define procedures for handling and protecting personal data in compliance with laws
    B. To prevent data breaches by implementing technical safeguards
    C. To standardize data collection methods across all departments
    D. To restrict access to sensitive information to authorized users only

Solution: To define procedures for handling and protecting personal data in compliance with laws

174. (1 point) What is a fundamental ethical principle in information security?

A. Ensuring actions benefit society while minimizing harm

B. Maximizing profits while maintaining minimal compliance

C. Prioritizing technical efficiency over ethical considerations

D. Protecting corporate interests against external scrutiny

Solution: Ensuring actions benefit society while minimizing harm

175. (1 point) What distinguishes privacy laws in the United States from those in the EU?

A. U.S. privacy laws are sector-specific, while EU laws emphasize uniform data protection

B. U.S. privacy laws mandate encryption, while EU laws focus on consent

C. EU privacy laws prioritize corporate accountability, while U.S. laws prioritize user control

D. EU laws centralize data storage, while U.S. laws require distributed systems

Solution: U.S. privacy laws are sector-specific, while EU laws emphasize uniform data protection

176. (1 point) Which action violates the principles of the Privacy Act of 1974?

A. Using personal data for purposes not disclosed to the individual

B. Denying individuals access to records containing their information

C. Collecting personal data without individual consent or notification

D. Sharing anonymized data for research without explicit permission

Solution: Using personal data for purposes not disclosed to the individual

177. (1 point) What is the primary purpose of a security audit?

A. To evaluate the effectiveness of security controls and identify vulnerabilities

B. To enforce compliance with organizational security policies and standards

C. To detect and respond to ongoing security incidents in real-time

D. To implement advanced security measures for critical assets

Solution: To evaluate the effectiveness of security controls and identify vulnerabilities

178. (1 point) Which type of audit focuses on verifying compliance with external regulations?
    A. Regulatory audit ensuring adherence to legal and industry requirements
    B. Internal audit reviewing organizational security policies
    C. Penetration audit testing the effectiveness of technical safeguards
    D. Operational audit assessing day-to-day security practices

Solution: Regulatory audit ensuring adherence to legal and industry requirements

179. (1 point) What distinguishes an internal audit from an external audit?
    A. Internal audits are conducted by an organizations staff, while external audits involve independent third parties
    B. Internal audits focus on technical controls, while external audits prioritize compliance
    C. Internal audits are voluntary, while external audits are legally mandated
    D. Internal audits assess operational risks, while external audits review financial risks

Solution: Internal audits are conducted by an organizations staff, while external audits involve independent third parties

180. (1 point) Which phase of a security audit involves defining its scope and objectives?
    A. Planning phase where the audit framework is established
    B. Execution phase where data collection and testing occur
    C. Reporting phase where findings and recommendations are documented
    D. Follow-up phase where remediations are verified

Solution: Planning phase where the audit framework is established

181. (1 point) What is the role of audit trails in security auditing?

A. To provide a chronological record of system activities for investigation

B. To enforce real-time monitoring of access controls and permissions

C. To document compliance with security and privacy standards

D. To evaluate the performance of implemented security controls

Solution: To provide a chronological record of system activities for investigation

182. (1 point) Which type of audit specifically tests an organization's response to simulated threats?

A. Penetration testing that evaluates technical vulnerabilities

B. Operational audit analyzing incident response effectiveness

C. Forensic audit investigating historical breaches and impacts

D. Compliance audit reviewing adherence to legal frameworks

Solution: Penetration testing that evaluates technical vulnerabilities

183. (1 point) What is the significance of a risk-based audit approach?

A. It prioritizes auditing efforts based on the potential impact of identified risks

B. It ensures audits are conducted at regular intervals for consistency

C. It focuses exclusively on financial and operational risks in security systems

D. It minimizes auditing costs by limiting the scope to critical areas

Solution: It prioritizes auditing efforts based on the potential impact of identified risks

184. (1 point) What is a primary goal of continuous auditing?

A. To provide real-time insights into security posture and compliance

B. To document audit findings for regulatory submissions

C. To ensure periodic review of access logs and security configurations

D. To support disaster recovery plans by maintaining updated records

Solution: To provide real-time insights into security posture and compliance

185. (1 point) What is the purpose of a security audit checklist?

A. To ensure all critical areas are evaluated consistently during the audit

B. To provide a detailed guide for implementing corrective actions

C. To streamline the reporting process for audit findings

D. To monitor system activities continuously for policy violations

Solution: To ensure all critical areas are evaluated consistently during the audit

186. (1 point) Which of the following is a limitation of manual security audits?

A. They are time-intensive and prone to human error

B. They fail to detect vulnerabilities in real-time systems

C. They rely exclusively on predefined compliance frameworks

D. They cannot incorporate feedback from automated tools

Solution: They are time-intensive and prone to human error

187. (1 point) Which phase of a security audit involves assessing vulnerabilities and controls?

A. Execution phase where testing and data collection are performed

B. Planning phase where objectives and scope are defined

C. Reporting phase where findings are documented for stakeholders

D. Follow-up phase where implemented controls are reviewed

Solution: Execution phase where testing and data collection are performed

188. (1 point) What is the primary focus of a compliance audit?
    A. Ensuring adherence to legal, regulatory, and organizational standards
    B. Detecting technical vulnerabilities in current systems
    C. Evaluating the incident response readiness of an organization
    D. Analyzing the effectiveness of existing risk management strategies

Solution: Ensuring adherence to legal, regulatory, and organizational standards

189. (1 point) What is the purpose of an audit report?

A. To summarize findings and recommend actions for addressing identified risks

B. To document system configurations and user activity for reference

C. To validate compliance with technical standards during inspections

D. To enforce security policies through detailed risk assessments

Solution: To summarize findings and recommend actions for addressing identified risks