C4N

1. Account lockout is a mitigation strategy used by Jane, the administrator, to combat which of the following attacks? (Choose two.)
A. Spoofing
B. Man-in-the-middle
C. Dictionary
D. Brute force
E. Privilege escalation

2. A recent audit has discovered that at the time of password expiration clients are able to recycle the previous credentials for authentication. Which of the following controls should be used together to prevent this from occurring? (Choose two.)
A. Password age
B. Password hashing
C. Password complexity
D. Password history
E. Password length

3. A password history value of three means which of the following?
A. Three different passwords are used before one can be reused.
B. A password cannot be reused once changed for three years.
C. After three hours a password must be re-entered to continue.
D. The server stores passwords in the database for three days.

4. An administrator discovers that many users have used their same passwords for years even though the network requires that the passwords be changed every six weeks. Which of the following, when used together, would BEST prevent users from reusing their existing password? (Choose two.)
A. Length of password
B. Password history
C. Minimum password age
D. Password expiration
E. Password complexity
F. Non-dictionary words

5. A system administrator has noticed that users change their password many times to cycle back to the original password when their passwords expire. Which of the following would BEST prevent this behavior?
A. Assign users passwords based upon job role.
B. Enforce a minimum password age policy.
C. Prevent users from choosing their own passwords.
D. Increase the password expiration time frame.

6. Which of the following is an important implementation consideration when deploying a wireless network that uses a shared password?
A. Authentication server
B. Server certificate
C. Key length
D. EAP method

7. A security administrator is reviewing the below output from a password auditing tool:
P@ss.
@pW1.
S3cU4

Which of the following additional policies should be implemented based on the tool's output?
A. Password age
B. Password history
C. Password length
D. Password complexity

8. Several employee accounts appear to have been cracked by an attacker. Which of the following should the security administrator implement to mitigate password cracking attacks? (Choose two.)
AF
A. Increase password complexity
B. Deploy an IDS to capture suspicious logins
C. Implement password history
D. Implement monitoring of logins
E. Implement password expiration

F. Increase password length

9. Human Resources suspects an employee is accessing the employee salary database. The administrator is asked to find out who it is. In order to complete this task, which of the following is a security control that should be in place?
A. Shared accounts should be prohibited.
B. Account lockout should be enabled
C. Privileges should be assigned to groups rather than individuals
D. Time of day restrictions should be in use

10. A network administrator is configuring access control for the sales department which has high employee turnover. Which of the following is BEST suited when assigning user rights to individuals in the sales department?
A. Time of day restrictions
B. Group based privileges
C. User assigned privileges
D. Domain admin restrictions

11. A new network administrator is setting up a new file server for the company. Which of the following would be the BEST way to manage folder security?
A. Assign users manually and perform regular user access reviews
B. Allow read only access to all folders and require users to request permission
C. Assign data owners to each folder and allow them to add individual users to each folder
D. Create security groups for each folder and assign appropriate users to each group

12. A new intern was assigned to the system engineering department, which consists of the system architect and system software developer's teams. These two teams have separate privileges. The intern requires privileges to view the system architectural drawings and comment on some software development projects. Which of the following methods should the system administrator implement?
A. Group based privileges
B. Generic account prohibition
C. User access review
D. Credential management

13. A system administrator needs to ensure that certain departments have more restrictive controls to their shared folders than other departments. Which of the following security controls would be implemented to restrict those departments?
A. User assigned privileges
B. Password disablement
C. Multiple account creation
D. Group based privileges

14. Which of the following practices reduces the management burden of access management?
A. Password complexity policies
B. User account audit
C. Log analysis and review
D. Group based privileges

15. A supervisor in the human resources department has been given additional job duties in the accounting department. Part of their new duties will be to check the daily balance sheet calculations on spreadsheets that are restricted to the accounting group. In which of the following ways should the account be handled?
A. The supervisor should be allowed to have access to the spreadsheet files, and their membership in the human resources group should be terminated.
B. The supervisor should be removed from the human resources group and added to the accounting group.
C. The supervisor should be added to the accounting group while maintaining their membership in the human resources group.
D. The supervisor should only maintain membership in the human resources group.

16. A security analyst implemented group-based privileges within the company active directory. Which of the following account management techniques should be undertaken regularly to ensure least privilege principles?
A. Leverage role-based access controls.
B. Perform user group clean-up.
C. Verify smart card access controls.
D. Verify SHA-256 for password hashes.

17. Privilege creep among long-term employees can be mitigated by which of the following procedures?
A. User permission reviews
B. Mandatory vacations
C. Separation of duties
D. Job function rotation

18. A recent audit of a company's identity management system shows that 30% of active accounts belong to people no longer with the firm. Which of the following should be performed to help avoid this scenario? (Choose two.)
A. Automatically disable accounts that have not been utilized for at least 10 days.
B. Utilize automated provisioning and de-provisioning processes where possible.
C. Request that employees provide a list of systems that they have access to prior to leaving the firm.
D. Perform regular user account review / revalidation process.
E. Implement a process where new account creations require management approval.

19. In order for network monitoring to work properly, you need a PC and a network card running in what mode?
A. Launch
B. Exposed
C. Promiscuous
D. Sweep

20. Which of the following techniques enables a highly secured organization to assess security weaknesses in real time?
A. Access control lists
B. Continuous monitoring
C. Video surveillance
D. Baseline reporting

21. A customer has provided an email address and password to a website as part of the login process. Which of the following BEST describes the email address?
A. Identification
B. Authorization
C. Access control
D. Authentication

22. A company has 5 users. Users 1, 2 and 3 need access to payroll and users 3, 4 and 5 need access to sales. Which of the following should be implemented to give the appropriate access while enforcing least privilege?
A. Assign individual permissions to users 1 and 2 for payroll. Assign individual permissions to users 4 and 5 for sales. Make user 3 an administrator.
B. Make all users administrators and then restrict users 1 and 2 from sales. Then restrict users 4 and 5 from payroll.
C. Create two additional generic accounts, one for payroll and one for sales that users utilize.
D. Create a sales group with users 3, 4 and 5. Create a payroll group with users 1, 2 and 3.

23. An administrator implements SELinux on a production web server. After implementing this, the web server no longer serves up files from users' home directories. To rectify this, the administrator creates a new policy as the root user. This is an example of which of the following? (Choose two.)
A. Enforcing SELinux in the OS kernel is role-based access control
B. Enforcing SELinux in the OS kernel is rule-based access control
C. The policy added by the root user is mandatory access control
D. Enforcing SELinux in the OS kernel is mandatory access control
E. The policy added by the root user is role-based access control
F. The policy added by the root user is rule-based access control

24. A security administrator has deployed all laptops with Self Encrypting Drives (SED) and enforces key encryption. Which of the following represents the greatest threat to maintaining data confidentiality with these devices?
A. Full data access can be obtained by connecting the drive to a SATA or USB adapter bypassing the SED hardware.
B. A malicious employee can gain the SED encryption keys through software extraction allowing access to other laptops.

C. If the laptop does not use a Secure Boot BIOS, the SED hardware is not enabled allowing full data access.
D. Laptops that are placed in a sleep mode allow full data access when powered back on.

25. A recent review of accounts on various systems has found that after employees' passwords are required to change they are recycling the same password as before. Which of the following policies should be enforced to prevent this from happening? (Choose two.)
A. Reverse encryption
B. Minimum password age
C. Password complexity
D. Account lockouts
E. Password history
F. Password expiration

26. An organizations' security policy requires that users change passwords every 30 days. After a security audit, it was determined thatusers were recycling previously used passwords. Which of the following password enforcement policies would have mitigated thisissue?
A. Password history
B. Password complexity
C. Password length
D. Password expiration

27. A security administrator must implement a system that will support and enforce the following file system access control model:
FILE NAME -- SECURITY LABEL
Employees.doc -- Confidential
Salary.xls -- Confidential
OfficePhones.xls -- Unclassified
PersonalPhones.xls -- Restricted

Which of the following should the security administrator implement?
A. White and black listing
B. SCADA system
C. Trusted OS
D. Version control

28. Which of the following is the BEST reason for placing a password lock on a mobile device?
A. Prevents an unauthorized user from accessing owner's data
B. Enables remote wipe capabilities
C. Stops an unauthorized user from using the device again
D. Prevents an unauthorized user from making phone calls

29. Ann is the data owner of financial records for a company. She has requested that she have the ability to assign read and write privileges to her folders. The network administrator is tasked with setting up the initial access control system and handing Ann's administrative capabilities. Which of the following systems should be deployed?
A. Role-based
B. Mandatory
C. Discretionary
D. Rule-based

30. Ann was reviewing her company's event logs and observed several instances of GUEST accessing the company print server, file server, and archive database. As she continued to investigate, Ann noticed that it seemed to happen at random intervals throughout the day, but mostly after the weekly automated patching and often logging in at the same time. Which of the following would BEST mitigate this issue?
A. Enabling time of day restrictions
B. Disabling unnecessary services
C. Disabling unnecessary accounts
D. Rogue machine detection

31. Ann is a member of the Sales group. She needs to collaborate with Joe, a member of the IT group, to edit a file. Currently, the file has the following permissions:
Ann:read/write
Sales Group:read
IT Group:no access

If a discretionary access control list is in place for the files owned by Ann, which of the following would be the BEST way to share the file with Joe?
A. Add Joe to the Sales group.
B. Have the system administrator give Joe full access to the file.
C. Give Joe the appropriate access to the file directly.
D. Remove Joe from the IT group and add him to the Sales group.

32. A network administrator, Joe, arrives at his new job to find that none of the users have changed their network passwords since they were initially hired. Joe wants to have everyone change their passwords immediately. Which of the following policies should be enforced to initiate a password change?
A. Password expiration
B. Password reuse
C. Password recovery
D. Password disablement

33. Ann, a security administrator at a call center, has been experiencing problems with users intentionally installing unapproved and occasionally malicious software on their computers. Due to the nature of their jobs, Ann cannot change their permissions. Which of the following would BEST alleviate her concerns?
A. Deploy a HIDS suite on the users' computers to prevent application installation.
B. Maintain the baseline posture at the highest OS patch level.
C. Enable the pop-up blockers on the users' browsers to prevent malware.
D. Create an approved application list and block anything not on it.

34. Which of the following should be used to authenticate and log connections from wireless users connecting with EAP-TLS?
A. Kerberos
B. LDAP
C. SAML
D. RADIUS

35. Ann has recently transferred from the payroll department to engineering. While browsing file shares, Ann notices she can access the payroll status and pay rates of her new coworkers. Which of the following could prevent this scenario from occurring?
A. Credential management
B. Continuous monitoring
C. Separation of duties
D. User access reviews

36. An organization's security policy states that users must authenticate using something you do. Which of the following would meet the objectives of the security policy?
A. Fingerprint analysis
B. Signature analysis
C. Swipe a badge
D. Password

37. Which of the following protocols is MOST likely to be leveraged by users who need additional information about another user?
A. LDAP
B. RADIUS
C. Kerberos
D. TACACS+

38. The security manager wants to unify the storage of credential, phone numbers, office numbers, and address information into one system. Which of the following is a system that will support the requirement on its own?
A. LDAP
B. SAML
C. TACACS
D. RADIUS

39. Joe, a network administrator, is able to manage the backup software console by using his network login credentials. Which of the following authentication services is the MOST likely using?
A. SAML
B. LDAP

C. iSCSI
D. Two-factor authentication

40. An organization is implementing a password management application which requires that all local administrator passwords be stored and automatically managed. Auditors will be responsible for monitoring activities in the application by reviewing the logs. Which of the following security controls is the BEST option to prevent auditors from accessing or modifying passwords in the application?
A. Time of day restrictions
B. Create user accounts for the auditors and assign read-only access
C. Mandatory access control
D. Role-based access with read-only

41. A security administrator is tackling issues related to authenticating users at a remote site. There have been a large number of security incidents that resulted from either tailgating or impersonation of authorized users with valid credentials. The security administrator has been told to implement multifactor authentication in order to control facility access. To secure access to the remote facility, which of the following could be implemented without increasing the amount of space required at the entrance? Message of the Day
A. MOTD challenge and PIN pad
B. Retina scanner and fingerprint reader
C. Voice recognition and one-time PIN token
D. One-time PIN token and proximity reader

42. The security administrator notices a user logging into a corporate Unix server remotely as root. Which of the following actions should the administrator take?
A. Create a firewall rule to block SSH
B. Delete the root account
C. Disable remote root logins
D. Ensure the root account has a strong password

43. A company plans to expand by hiring new engineers who work in highly specialized areas. Each engineer will have very different job requirements and use unique tools and applications in their job. Which of the following is MOST appropriate to use?
A. Role-based privileges
B. Credential management
C. User assigned privileges
D. User access

44. A file on a Linux server has default permissions of rw-rw-r--. The system administrator has verified that Ann, a user, is not a member of the group owner of the file. Which of the following should be modified to assure that Ann has read access to the file?
A. User ownership information for the file in question
B. Directory permissions on the parent directory of the file in question
C. Group memberships for the group owner of the file in question
D. The file system access control list (FACL) for the file in question

45. Which of the following protocols uses an asymmetric key to open a session and then establishes a symmetric key for the remainder of the session?
A. SFTP
B. HTTPS
C. TFTP
D. TLS

46. A company uses PGP to ensure that sensitive email is protected. Which of the following types of cryptography is being used here for the key exchange?
A. Symmetric
B. Session-based
C. Hashing
D. Asymmetric

Ans: A

47. Which of the following is true about asymmetric encryption?
A. A message encrypted with the private key can be decrypted by the same key
B. A message encrypted with the public key can be decrypted with a shared key.
C. A message encrypted with a shared key, can be decrypted by the same key.
D. A message encrypted with the public key can be decrypted with the private key.

48. Encryption used by RADIUS is BEST described as:
A. Quantum
B. Elliptical curve
C. Asymmetric
D. Symmetric

49. Symmetric encryption utilizes _____, while asymmetric encryption utilizes _____.
A. Public keys, one time
B. Shared keys, private keys
C. Private keys, session keys
D. Private keys, public keys

50. Users need to exchange a shared secret to begin communicating securely. Which of the following is another name for this symmetric key?
A. Session Key
B. Public Key
C. Private Key
D. Digital Signature

51. In order to securely communicate using PGP, the sender of an email must do which of the following when sending an email to a recipient for the first time?
A. Import the recipient's public key
B. Import the recipient's private key
C. Export the sender's private key
D. Export the sender's public key

52. A network stream needs to be encrypted. Sara, the network administrator, has selected a cipher which will encrypt 8 bits at a time before sending the data across the network. Which of the following has Sara selected?
A. Block cipher
B. Stream cipher
C. CRC
D. Hashing algorithm

53. The concept of rendering data passing between two points over an IP based network impervious to all but the most sophisticated advanced persistent threats is BEST categorized as which of the following?
A. Stream ciphers
B. Transport encryption
C. Key escrow
D. Block ciphers

54. Which of the following transportation encryption protocols should be used to ensure maximum security between a web browser and a web server?
A. SSLv2
B. SSHv1
C. RSA
D. TLS

55. When employing PKI to send signed and encrypted data the individual sending the data must have: (Choose two.)
A. The receiver's private key
B. The root certificate
C. The sender's private key
D. The sender's public key
E. The receiver's public key

56. Which of the following concepts is enforced by certifying that email communications have been sent by who the message says it has been sent by?
A. Key escrow
B. Non-repudiation
C. Multifactor authentication
D. Hashing

57. All of the following are valid cryptographic hash functions EXCEPT:
A. RIPEMD.
B. RC4.
C. SHA-512.

D. MD4.

58. Which of the following concepts is used by digital signatures to ensure integrity of the data?
A. Non-repudiation
B. Hashing
C. Transport encryption
D. Key escrow

59. A security administrator discovers an image file that has several plain text documents hidden in the file. Which of the following security goals is met by camouflaging data inside of other files?
A. Integrity
B. Confidentiality
C. Steganography
D. Availability

60. A security analyst discovered data such as images and word documents hidden within different types of files. Which of the following cryptographic concepts describes what was discovered?
A. Symmetric encryption
B. Non-repudiation
C. Steganography
D. Hashing

61. Which of the following can hide confidential or malicious data in the whitespace of other files (e.g. JPEGs)?
A. Hashing
B. Transport encryption
C. Digital signatures
D. Steganography

62. Which of the following must a user implement if they want to send a secret message to a coworker by embedding it within an image?
A. Transport encryption
B. Steganography
C. Hashing
D. Digital signature

63. Digital Signatures provide which of the following?
A. Confidentiality
B. Authorization
C. Integrity
D. Authentication
E. Availability

64. Matt, a security analyst, needs to select an asymmetric encryption method that allows for the same level of encryption strength with a lower key length than is typically necessary. Which of the following encryption methods offers this capability?
A. Twofish
B. Diffie-Hellman
C. ECC
D. RSA

65. Which of the following types of cryptography should be used when minimal overhead is necessary for a mobile device?
A. Block cipher
B. Elliptical curve cryptography
C. Diffie-Hellman algorithm
D. Stream cipher

66. A security technician is attempting to access a wireless network protected with WEP. The technician does not know any information about the network. Which of the following should the technician do to gather information about the configuration of the wireless network?
A. Spoof the MAC address of an observed wireless network client
B. Ping the access point to discover the SSID of the network
C. Perform a dictionary attack on the access point to enumerate the WEP key
D. Capture client to access point disassociation packets to replay on the local PC's

loopback

67. The IT department has installed new wireless access points but discovers that the signal extends far into the parking lot. Which of the following actions should be taken to this?
A. Disable the SSID broadcasting
B. Configure the access points so that MAC filtering is not used
C. Implement WEP encryption on the access points
D. Lower the power for office coverage only

68. Joe, the systems administrator, is setting up a wireless network for his team's laptops only and needs to prevent other employees from accessing it. Which of the following would BEST address this?
A. Disable default SSID broadcasting.
B. Use WPA instead of WEP encryption.
C. Lower the access point's power settings.
D. Implement MAC filtering on the access point.

69. Which of the following provides the strongest authentication security on a wireless network?
A. MAC filter
B. WPA2
C. WEP
D. Disable SSID broadcast

70. Which of the following is a concern when encrypting wireless data with WEP?
A. WEP displays the plain text entire key when wireless packet captures are reassembled
B. WEP implements weak initialization vectors for key transmission
C. WEP uses a very weak encryption algorithm
D. WEP allows for only four pre-shared keys to be configured

71. Which of the following provides the HIGHEST level of confidentiality on a wireless network?
A. Disabling SSID broadcast
B. MAC filtering
C. WPA2
D. Packet switching

72. While setting up a secure wireless corporate network, which of the following should Pete, an administrator, avoid implementing?
A. EAP-TLS
B. PEAP
C. WEP
D. WPA

73. Joe, an employee, was escorted from the company premises due to suspicion of revealing trade secrets to a competitor. Joe had already been working for two hours before leaving the premises. A security technician was asked to prepare a report of files that had changed since last night's integrity scan. Which of the following could the technician use to prepare the report? (Choose two.)
A. PGP
B. MD5
C. ECC
D. AES
E. Blowfish
F. HMAC

74. Users report that after downloading several applications, their systems' performance has noticeably decreased. Which of the following would be used to validate programs prior to installing them?
A. Whole disk encryption
B. SSH
C. Telnet
D. MD5

75. Which of the following is used to verify data integrity?
A. SHA
B. 3DES
C. AES

D. RSA

76. Which of the following can be implemented with multiple bit strength?
A. AES
B. DES
C. SHA-1
D. MD5
E. MD4

77. To ensure compatibility with their flagship product, the security engineer is tasked to recommend an encryption cipher that will be compatible with the majority of third party software and hardware vendors. Which of the following should be recommended?
A. SHA
B. MD5
C. Blowfish
D. AES

78. Which of the following provides additional encryption strength by repeating the encryption process with additional keys?
A. AES
B. 3DES
C. TwoFish
D. Blowfish

79. Which of the following are restricted to 64-bit block sizes? (Choose two.)
A. PGP
B. DES
C. AES256
D. RSA
E. 3DES
F. AES

80. A bank has a fleet of aging payment terminals used by merchants for transactional processing. The terminals currently support single DES but require an upgrade in order to be compliant with security standards. Which of the following is likely to be the simplest upgrade to the aging terminals which will improve in-transit protection of transactional data?
A. AES
B. 3DES
C. RC4
D. WPA2

81. Which of the following would Matt, a security administrator, use to encrypt transmissions from an internal database to an internal server, keeping in mind that the encryption process must add as little latency to the process as possible?
A. ECC
B. RSA
C. SHA
D. 3DES

82. Which of the following MUST Matt, a security administrator, implement to verify both the integrity and authenticity of a message while requiring a shared secret?
A. RIPEMD
B. MD5
C. SHA
D. HMAC

83. Which of the following cryptographic algorithms is MOST often used with IPSec?
A. Blowfish
B. Twofish
C. RC4
D. HMAC

84. When creating a public / private key pair, for which of the following ciphers would a user need to specify the key strength?
A. SHA
B. AES
C. DES
D. RSA

85. Which of the following uses both a public and private key?
A. RSA
B. AES
C. MD5
D. SHA

86. Which of the following ciphers would be BEST used to encrypt streaming video?
A. RSA
B. RC
C. SHA1
D. 3DES

87. Due to hardware limitation, a technician must implement a wireless encryption algorithm that uses the RC4 protocol. Which of the following is a wireless encryption solution that the technician should implement while ensuring the STRONGEST level of security?
A. WPA2-AES
B. 802.11ac C
C. WPA-TKIP
D. WEP

88. A security administrator must implement a wireless encryption system to secure mobile devices' communication. Some users have mobile devices which only support 56-bit encryption. Which of the following wireless encryption methods should be implemented?
A. RC4 Streaming cipher
B. AES
C. MD5
D. TKIP

89. Which of the following can use RC4 for encryption? (Choose two.)
A. CHAP
B. SSL
C. WEP
D. AES
E. 3DES

90. Which of the following would provide the STRONGEST encryption?
A. Random one-time pad
B. DES with a 56-bit key
C. AES with a 256-bit key
D. RSA with a 1024-bit key

91. Which of the following symmetric key algorithms are examples of block ciphers? (Choose three.)
A. RC4
B. 3DES
C. AES
D. MD5
E. PGP
F. Blowfish

92. Which of the following should be used when a business needs a block cipher with minimal key size for internal encryption?
A. AES 128 192. 256
B. Blowfish 64 bit block size 32 - 448 bit
C. RC5 32. 64. 128 block size.
D. 3DES 163 112 56

93. Sara, a security engineer, is testing encryption ciphers for performance. Which of the following ciphers offers strong encryption with the FASTEST speed?
A. 3DES
B. Blowfish
C. Serpent
D. AES256

94. Jane, a VPN administrator, was asked to implement an encryption cipher with a MINIMUM effective security of 128-bits. Which of the following should Jane select for the tunnel encryption?

A. Blowfish
B. DES
C. SHA256
D. HMAC

95. When using PGP, which of the following should the end user protect from compromise? (Choose two.)
A. Private key
B. CRL details
C. Public key
D. Key password
E. Key escrow
F. Recovery agent

96. A security administrator must implement a system to allow clients to securely negotiate encryption keys with the company's server over a public unencrypted communication channel. Which of the following implements the required secure key negotiation? (Choose two.)
A. PBKDF2
B. Symmetric encryption
C. Steganography
D. ECDHE
E. Diffie-Hellman

97. An administrator has two servers and wants them to communicate with each other using a secure algorithm. Which of the following choose to provide both CRC integrity checks and RCA encryption?
A. NTLM
B. RSA
C. CHAP
D. ECDHE

98. Connections using point-to-point protocol authenticate using which of the following? (Choose two.)
A. RIPEMD
B. PAP
C. CHAP
D. RC4
E. Kerberos

99. Which of the following offers the LEAST secure encryption capabilities?
A. TwoFish
B. PAP
C. NTLM
D. CHAP

100. Which of the following algorithms has well documented collisions? (Choose two.)
A. AES
B. MD5
C. SHA
D. SHA-256
E. RSA