C3N (with Explaination)

1. Which of the following protocols is the security administrator observing in this packet capture?
12:33:43, SRC 192.168.4.3:3389, DST 10.67.33.20:8080, SYN/ACK
A. HTTPS
B. RDP
C. HTTP
D. SFTP

2. Which of the following cryptographic related browser settings allows an organization to communicate securely?
A. SSL 3.0/TLS 1.0
B. 3DES
C. Trusted Sites
D. HMAC

3. Recent data loss on financial servers due to security breaches forced the system administrator to harden their systems. Which of the following algorithms with transport encryption would be implemented to provide the MOST secure web connections to manage and access these servers?
A. SSL
B. TLS
C. HTTP
D. FTP

4. A security administrator has been tasked with setting up a new internal wireless network that must use end to end TLS. Which of the following may be used to meet this objective?
A. WPA
B. HTTPS
C. WEP
D. WPA 2

5. Which of the following protocols encapsulates an IP packet with an additional IP header?
A. SFTP
B. IPSec
C. HTTPS
D. SSL

6. A new MPLS network link has been established between a company and its business partner. The link provides logical isolation in order to prevent access from other business partners. Which of the following should be applied in order to achieve confidentiality and integrity of all data across the link?
A. MPLS should be run in IPVPN mode.
B. SSL/TLS for all application flows.
C. IPSec VPN tunnels on top of the MPLS link.
D. HTTPS and SSH for all application flows.

7. Which of the following would be used as a secure substitute for Telnet?
A. SSH
B. SFTP
C. SSL
D. HTTPS

8. Which of the following protocols provides transport security for virtual terminal emulation?
A. TLS
B. SSH
C. SCP
D. S/MIME

9. A security engineer is asked by the company's development team to recommend the most secure method for password storage. Which of the following provide the BEST protection against brute forcing stored passwords? (Choose two.)
A. PBKDF2
B. MD5
C. SHA2
D. Bcrypt
E. AES

F. CHAP

10. Deploying a wildcard certificate is one strategy to:
A. Secure the certificate's private key.
B. Increase the certificate's encryption key length.
C. Extend the renewal date of the certificate.
D. Reduce the certificate management burden.

11. A certificate authority takes which of the following actions in PKI?
A. Signs and verifies all infrastructure messages
B. Issues and signs all private keys
C. Publishes key escrow lists to CRLs
D. Issues and signs all root certificates

12. Which of the following is used to certify intermediate authorities in a large PKI deployment?
A. Root CA
B. Recovery agent
C. Root user
D. Key escrow

13. Which of the following components MUST be trusted by all parties in PKI?
A. Key escrow
B. CA
C. Private key
D. Recovery key

14. Company employees are required to have workstation client certificates to access a bank website. These certificates were backed upas a precautionary step before the new computer upgrade. After the upgrade and restoration, users state they can access the bank'swebsite, but not login.Which is the following is MOST likely the issue?
A. The IP addresses of the clients have change
B. The client certificate passwords have expired on the server
C. The certificates have not been installed on the workstations
D. The certificates have been installed on the CA

15. A company's security administrator wants to manage PKI for internal systems to help reduce costs. Which of the following is the FIRST step the security administrator should take?
A. Install a registration server.
B. Generate shared public and private keys.
C. Install a CA
D. Establish a key escrow policy.

16. Pete, an employee, needs a certificate to encrypt data. Which of the following would issue Pete a certificate?
A. Certification authority
B. Key escrow
C. Certificate revocation list
D. Registration authority

17. When reviewing a digital certificate for accuracy, which of the following would Matt, a security administrator, focus on to determine who affirms the identity of the certificate owner?
A. Trust models
B. CRL
C. CA
D. Recovery agent

218. Joe, a user, reports to the system administrator that he is receiving an error stating his certificate has been revoked. Which of the following is the name of the database repository for these certificates?
A. CSR
B. OCSP
C. CA
D. CRL

19. A systems administrator has implemented PKI on a classified government network. In the event that a disconnect occurs from the primary CA, which of the following should

be accessible locally from every site to ensure users with bad certificates cannot gain access to the network?
A. A CRL
B. Make the RA available
C. A verification authority
D. A redundant CA

20. A CRL is comprised of.
A. Malicious IP addresses.
B. Trusted CA's.
C. Untrusted private keys.
D. Public keys.

21. Which of the following MUST be updated immediately when an employee is terminated to prevent unauthorized access?
A. Registration
B. CA
C. CRL
D. Recovery agent

22. Which of the following provides a static record of all certificates that are no longer valid?
A. Private key
B. Recovery agent
C. CRLs
D. CA

23. A CA is compromised and attacks start distributing maliciously signed software updates. Which of the following can be used to warn users about the malicious activity?
A. Key escrow
B. Private key verification
C. Public key verification
D. Certificate revocation list

24. The finance department works with a bank which has recently had a number of cyber attacks. The finance department is concerned that the banking website certificates have been compromised. Which of the following can the finance department check to see if any of the bank's certificates are still valid?
A. Bank's CRL
B. Bank's private key
C. Bank's key escrow
D. Bank's recovery agent

25. A security administrator needs a locally stored record to remove the certificates of a terminated employee. Which of the following describes a service that could meet these requirements?
A. OCSP
B. PKI
C. CA
D. CRL

26. Public key certificates and keys that are compromised or were issued fraudulently are listed on which of the following?
A. PKI
B. ACL
C. CA
D. CRL

27. Which of the following identifies certificates that have been compromised or suspected of being compromised?
A. Certificate revocation list
B. Access control list
C. Key escrow registry
D. Certificate authority

28. When employees that use certificates leave the company they should be added to which of the following?
A. PKI
B. CA

C. CRL
D. TKIP

29. Which of the following should a security technician implement to identify untrusted certificates?
A. CA
B. PKI
C. CRL
D. Recovery agent

30. Which of the following is true about the CRL?
A. It should be kept public
B. It signs other keys
C. It must be kept secret
D. It must be encrypted

31. A system administrator is notified by a staff member that their laptop has been lost. The laptop contains the user's digital certificate. Which of the following will help resolve the issue? (Choose two.)
A. Revoke the digital certificate
B. Mark the key as private and import it
C. Restore the certificate using a CRL
D. Issue a new digital certificate
E. Restore the certificate using a recovery agent

32. Which of the following protocols is used to validate whether trust is in place and accurate by returning responses of either "good", "unknown", or "revoked"?
A. CRL
B. PKI
C. OCSP
D. RA

33. An administrator needs to renew a certificate for a web server. Which of the following should be submitted to a CA?
A. CSR
B. Recovery agent
C. Private key
D. CRL

34. An administrator needs to submit a new CSR to a CA. Which of the following is a valid FIRST step?
A. Generate a new private key based on AES.
B. Generate a new public key based on RSA.
C. Generate a new public key based on AES.
D. Generate a new private key based on RSA.

35. In which of the following scenarios is PKI LEAST hardened?
A. The CRL is posted to a publicly accessible location.
B. The recorded time offsets are developed with symmetric keys.
C. A malicious CA certificate is loaded on all the clients.
D. All public keys are accessed by an unauthorized user.

36. Which of the following BEST describes part of the PKI process?
A. User1 decrypts data with User2's private key
B. User1 hashes data with User2's public key
C. User1 hashes data with User2's private key
D. User1 encrypts data with User2's public key

37. A software development company wants to implement a digital rights management solution to protect its intellectual property. Which of the following should the company implement to enforce software digital rights?
A. Transport encryption
B. IPsec
C. Non-repudiation
D. Public key infrastructure

38. Which of the following is the MOST likely cause of users being unable to verify a single user's email signature and that user being unable to decrypt sent messages?
A. Unmatched key pairs

B. Corrupt key escrow
C. Weak public key
D. Weak private key

39. In PKI, a key pair consists of: (Choose two.)
A. A key ring
B. A public key
C. A private key
D. Key escrow
E. A passphrase

40. Which of the following is true about PKI? (Choose two.)
A. When encrypting a message with the public key, only the public key can decrypt it.
B. When encrypting a message with the private key, only the private key can decrypt it.
C. When encrypting a message with the public key, only the CA can decrypt it.
D. When encrypting a message with the public key, only the private key can decrypt it.
E. When encrypting a message with the private key, only the public key can decrypt it.

41. Which of the following allows a company to maintain access to encrypted resources when employee turnover is high?
A. Recovery agent
B. Certificate authority
C. Trust model
D. Key escrow

42. Pete, an employee, is terminated from the company and the legal department needs documents from his encrypted hard drive. Which of the following should be used to accomplish this task? (Choose two.)
A. Private hash
B. Recovery agent
C. Public key
D. Key escrow
E. CRL

43. After encrypting all laptop hard drives, an executive officer's laptop has trouble booting to the operating system. Now that it is successfully encrypted the helpdesk cannot retrieve the data. Which of the following can be used to decrypt the information for retrieval?
A. Recovery agent
B. Private key
C. Trust models
D. Public key

44. Which of the following is true about the recovery agent?
A. It can decrypt messages of users who lost their private key.
B. It can recover both the private and public key of federated users.
C. It can recover and provide users with their lost or private key.
D. It can recover and provide users with their lost public key.

45. The recovery agent is used to recover the:
A. Root certificate
B. Key in escrow
C. Public key
D. Private key

46. Which of the following is synonymous with a server's certificate?
A. Public key
B. CRL
C. Private key
D. Recovery agent

47. The security administrator installed a newly generated SSL certificate onto the company web server. Due to a misconfiguration of the website, a downloadable file containing one of the pieces of the key was available to the public. It was verified that the disclosure did not require a reissue of the certificate. Which of the following was MOST likely compromised?
A. The file containing the recovery agent's keys.
B. The file containing the public key.
C. The file containing the private key.

D. The file containing the server's encrypted passwords.

48. The public key is used to perform which of the following? (Choose three.)
A. Validate the CRL
B. Validate the identity of an email sender
C. Encrypt messages
D. Perform key recovery
E. Decrypt messages
F. Perform key escrow

49. Public keys are used for which of the following?
A. Decrypting wireless messages
B. Decrypting the hash of an electronic signature
C. Bulk encryption of IP based email traffic
D. Encrypting web browser traffic

50. Which of the following explains the difference between a public key and a private key?
A. The public key is only used by the client while the private key is available to all.Both keys are mathematically related.
B. The private key only decrypts the data while the public key only encrypts the data.Both keys are mathematically related.
C. The private key is commonly used in symmetric key decryption while the public key is used in asymmetric key decryption.
D. The private key is only used by the client and kept secret while the public key is available to all.

51. Ann wants to send a file to Joe using PKI. Which of the following should Ann use in order to sign the file?
A. Joe's public key
B. Joe's private key
C. Ann's public key
D. Ann's private key

52. Which of the following devices is BEST suited for servers that need to store private keys?
A. Hardware security module
B. Hardened network firewall
C. Solid state disk drive
D. Hardened host firewall

53. Company A sends a PGP encrypted file to company B. If company A used company B's public key to encrypt the file, which of the following should be used to decrypt data at company B?
A. Registration
B. Public key
C. CRLs
D. Private key

54. Which of the following is true about an email that was signed by User A and sent to User B?
A. User A signed with User B's private key and User B verified with their own public key.
B. User A signed with their own private key and User B verified with User A's public key.
C. User A signed with User B's public key and User B verified with their own private key.
D. User A signed with their own public key and User B verified with User A's private key.

55. Which of the following must be kept secret for a public key infrastructure to remain secure?
A. Certificate Authority
B. Certificate revocation list
C. Public key ring
D. Private key

56. Which of the following allows an organization to store a sensitive PKI component with a trusted third party?
A. Trust model
B. Public Key Infrastructure
C. Private key
D. Key escrow

57. Which of the following is a requirement when implementing PKI if data loss is unacceptable?
A. Web of trust
B. Non-repudiation
C. Key escrow
D. Certificate revocation list

58. Which of the following allows lower level domains to access resources in a separate Public Key Infrastructure?
A. Trust Model
B. Recovery Agent
C. Public Key
D. Private Key

59. A network administrator is looking for a way to automatically update company browsers so they import a list of root certificates from an online source. This online source will then be responsible for tracking which certificates are to be trusted or not trusted. Which of the following BEST describes the service that should be implemented to meet these requirements?
A. Trust model
B. Key escrow
C. OCSP
D. PKI

60. In order to use a two-way trust model the security administrator MUST implement which of the following?
A. DAC
B. PKI
C. HTTPS
D. TPM

61. Which of the following types of trust models is used by a PKI?
A. Transitive
B. Open source
C. Decentralized
D. Centralized

62. RC4 is a strong encryption protocol that is generally used with which of the following?
A. WPA2 CCMP
B. PEAP
C. WEP WEP & WPA encryption
D. EAP-TLS

63. A security administrator must implement a secure key exchange protocol that will allow company clients to autonomously exchange symmetric encryption keys over an unencrypted channel. Which of the following MUST be implemented?
A. SHA-256
B. AES
C. Diffie-Hellman
D. 3DES

64. A security administrator at a company which implements key escrow and symmetric encryption only, needs to decrypt an employee's file. The employee refuses to provide the decryption key to the file. Which of the following can the administrator do to decrypt the file?
A. Use the employee's private key
B. Use the CA private key
C. Retrieve the encryption key
D. Use the recovery agent

65. A system administrator is setting up a file transfer server. The goal is to encrypt the user authentication and the files the user is sending using only a user ID and a key pair. Which of the following methods would achieve this goal?
A. AES
B. IPSec
C. PGP
D. SSH

66. Joe, a user, wants to protect sensitive information stored on his hard drive. He uses a program that encrypted the whole hard drive. Once the hard drive is fully encrypted, he uses the same program to create a hidden volume within the encrypted hard drive and stores the sensitive information within the hidden volume. This is an example of which of the following? (Choose two.)
A. Multi-pass encryption
B. Transport encryption
C. Plausible deniability
D. Steganography
E. Transitive encryption
F. Trust models

67. A company is concerned that a compromised certificate may result in a man-in-the-middle attack against backend financial servers. In order to minimize the amount of time a compromised certificate would be accepted by other servers, the company decides to add another validation step to SSL/TLS connections. Which of the following technologies provides the FASTEST revocation capability?
A. Online Certificate Status Protocol (OCSP)
B. Public Key Cryptography (PKI)
C. Certificate Revocation Lists (CRL)
D. Intermediate Certificate Authority (CA)

68. A technician wants to verify the authenticity of the system files of a potentially compromised system. Which of the following can the technician use to verify if a system file was compromised? (Choose two.)
A. AES
B. PGP
C. SHA
D. MD5
E. ECDHE

69. When confidentiality is the primary concern, and a secure channel for key exchange is not available, which of the following should be used for transmitting company documents?
A. Digital Signature
B. Symmetric
C. Asymmetric
D. Hashing

70. A small company wants to employ PKI. The company wants a cost effective solution that must be simple and trusted. They are considering two options: X.509 and PGP. Which of the following would be the BEST option?
A. PGP, because it employs a web-of-trust that is the most trusted form of PKI.
B. PGP, because it is simple to incorporate into a small environment.
C. 509, because it uses a hierarchical design that is the most trusted form of PKI.
E. 509, because it is simple to incorporate into a small environment.

71. Which of the following represents a cryptographic solution where the encrypted stream cannot be captured by a sniffer without the integrity of the stream being compromised?
A. Elliptic curve cryptography.
B. Perfect forward secrecy.
C. Steganography.
D. Quantum cryptography.

72. A new client application developer wants to ensure that the encrypted passwords that are stored in their database are secure from cracking attempts. To implement this, the developer implements a function on the client application that hashes passwords thousands of times prior to being sent to the database. Which of the following did the developer MOST likely implement?
A. RIPEMD
B. PBKDF2 Password-based key Derivation Function 2
C. HMAC H
D. ECDHE

73. Joe must send Ann a message and provide Ann with assurance that he was the actual sender. Which of the following will Joe need to use to BEST accomplish the objective?
A. A pre-shared private key

B. His private key
C. Ann's public key
D. His public key

74. A system administrator wants to confidentially send a user name and password list to an individual outside the company without the information being detected by security controls. Which of the following would BEST meet this security goal?
A. Digital signatures
B. Hashing
C. Full-disk encryption
D. Steganography

75. Protecting the confidentiality of a message is accomplished by encrypting the message with which of the following?
A. Sender's private key
B. Recipient's public key
C. Sender's public key
D. Recipient's private key

76. A software developer utilizes cryptographic functions to generate codes that verify message integrity. Due to the nature if the data that is being sent back and forth from the client application to the server, the developer would like to change the cryptographic function to one that verities both authentication and message integrity. Which of the following algorithms should the software developer utilize?
A. HMAC
B. SHA
C. Two Fish
D. RIPEMD

77. When designing a corporate NAC solution, which of the following is the MOST relevant integration issue?
A. Infrastructure time sync
B. End user mobility
C. 802.1X supplicant compatibility
D. Network Latency
E. Network Zoning

78. Which of the following access methods uses radio frequency waves for authentication?
A. Video surveillance
B. Mantraps
C. Proximity readers
D. Biometrics

79. Which of the following authentication methods can use the SCTP and TLS protocols for reliable packet transmissions?
A. TACACS+
B. SAML
C. Diameter
D. Kerberos

80. Which of the following authentication protocols makes use of UDP for its services?
A. RADIUS
B. TACACS+
C. LDAP
D. XTACACS

81. Which of the following is considered a risk management BEST practice of succession planning?
A. Reducing risk of critical information being known to an individual person who may leave the organization
B. Implementing company-wide disaster recovery and business continuity plans
C. Providing career advancement opportunities to junior staff which reduces the possibility of insider threats
D. Considering departmental risk management practices in place of company-wide practices

82. Which of the following is the BEST technology for the sender to use in order to secure the in-band exchange of a shared key?
A. Steganography
B. Hashing algorithm

C. Asymmetric cryptography
D. Stream cipher

83. Which of the following design components is used to isolate network devices such as web servers?
A. VLAN
B. VPN
C. NAT
D. DMZ

84. Which of the following is MOST critical in protecting control systems that cannot be regularly patched?
A. Asset inventory
B. Full disk encryption
C. Vulnerability scanning
D. Network segmentation

85. Identifying residual is MOST important to which of the following concepts?
A. Risk deterrence
B. Risk acceptance
C. Risk mitigation
D. Risk avoidance

86. Which of the following is replayed during wireless authentication to exploit a weak key infrastructure?
A. Preshared keys
B. Ticket exchange
C. Initialization vectors
D. Certificate exchange

87. Which of the following steps of incident response does a team analyze the incident and determine steps to prevent a future occurrence?
A. Mitigation
B. Identification
C. Preparation
D. Lessons learned

88. A technician wants to secure communication to the corporate web portal, which is currently using HTTP. Which of the following is the FIRST step the technician should take?
A. Send the server's public key to the CA
B. Install the CA certificate on the server
C. Import the certificate revocation list into the server
D. Generate a certificate request from the server

89. An organization has a need for security control that identifies when an organizational system has been unplugged and a rouge system has been plugged in. The security control must also provide the ability to supply automated notifications. Which of the following would allow the organization to BEST meet this business requirement?
A. MAC filtering
B. ACL
C. SNMP
D. Port security

90. Internet banking customers currently use an account number and password to access their online accounts. The bank wants to improve security on high value transfers by implementing a system which call users back on a mobile phone to authenticate the transaction with voice verification. Which of the following authentication factors are being used by the bank?
A. Something you know, something you do, and something you have
B. Something you do, somewhere you are, and something you have
C. Something you are, something you do and something you know
D. Something you have, something you are, and something you know

91. A security administrator has concerns that employees are installing unapproved applications on their company provide smartphones. Which of the following would BEST mitigate this?
A. Implement remote wiping user acceptance policies
B. Disable removable storage capabilities

C. Implement an application whitelist
D. Disable the built-in web browsers

92. The security manager must store a copy of a sensitive document and needs to verify at a later point that the document has not been altered. Which of the following will accomplish the security manager's objective?
A. RSA
B. AES
C. MD5
D. RC4

Should be SHA

93. A security Operations Center was scanning a subnet for infections and found a contaminated machine. One of the administrators disabled the switch port that the machine was connected to, and informed a local technician of the infection. Which of the following steps did the administrator perform?
A. Escalation
B. Identification
C. Notification
D. Quarantine
E. Preparation

94. A security administrator wants to block unauthorized access to a web server using a locally installed software program. Which of the following should the administrator deploy?
A. NIDS
B. HIPS
C. NIPS
D. HIDS

95. A network administrator has identified port 21 being open and the lack of an IDS as a potential risk to the company. Due to budget constraints, FTP is the only option that the company can is to transfer data and network equipment cannot be purchased. Which of the following is this known as?
A. Risk transference
B. Risk deterrence
C. Risk acceptance
D. Risk avoidance

96. A security administrator is investigating a recent server breach. The breach occurred as a result of a zero-day attack against a user program running on the server. Which of the following logs should the administrator search for information regarding the breach?
A. Application log
B. Setup log
C. Authentication log
D. System log

97. A user attempts to install new and relatively unknown software recommended by a colleague. The user is unable to install the program, despite having successfully installed other programs previously. Which of the following is MOST likely the cause for the user's inability to complete the installation?
A. Application black listing
B. Network Intrusion Prevention System
C. Group policy
D. Application white listing

98. A system administrator is configuring shared secrets on servers and clients. Which of the following authentication services is being deployed by the administrator? (Choose two.)
A. Kerberos
B. RADIUS
C. TACACS+
D. LDAP
E. Secure LDAP

99. Joe a technician is tasked with finding a way to test operating system patches for a wide variety of servers before deployment to the production environment while utilizing a limited amount of hardware resources. Which of the following would provide the BEST environment for performing this testing?

A. OS hardening
B. Application control
C. Virtualization
D. Sandboxing

100. After an audit, it was discovered that an account was not disabled in a timely manner after an employee has departed from the organization. Which of the following did the organization fail to properly implement?
A. Routine account audits
B. Account management processes
C. Change management processes
D. User rights and permission review