1. The ability to permit or deny the use of an information asset, resource or facility is referred to as .....
   a. Integrity
   b. Authentication
   c. Authorisation
   d. Access

2. The procedure of implementing more than one authentication mechanism is known as .....
   a. The principle of least privilege
   b. The principle of separation of duties
   c. Defence in depth
   d. Multifactor authentication

3. ..... defines the rights and permissions on a system
   a. Integrity
   b. Authentication
   c. Authorization
   d. Access

4. ..... controls use software and data to monitor and control access to information and computing systems
   a. Logical (technical)
   b. Administrative
   c. Physical
   d. Socio-economic

5. ..... requires that an individual, program or system process is not granted any more access privileges that are necessary to perform his work.
   a. The principle of least privilege
   b. The principle of separation of duties
   c. Defence in depth
   d. Multifactor authentication

6. An important physical control that ensures that an individual cannot complete a critical task by himself is known as .....
   a. The principle of least privilege
   b. The principle of separation of duties
   c. Defence in depth
   d. Multifactor authentication

7. ..... is the act of gathering proprietary data from private companies or the government for the purpose of aiding another company or companies
   a. Industrial espionage
   b. Foreign industrial espionage
   c. Industrial spying
   d. Corporate spying

8. ..... controls consist of written down policies, procedure, guidelines and standards which form the framework for running the business and managing people
   a. Logical
   b. Administrative
   c. Physical
   d. Socio-economic

9. The assurance that information has not been corrupted, degraded or undergone unauthorized modification is referred to as .....
   a. Confidentiality
   b. Integrity
   c. Availability
   d. Authentication

10. The process of verifying an identity is known as .....
   a. Confidentiality
   b. Integrity
   c. Nonrepudiation
   d. Authentication

11. ..... is a way to guarantee that the sender of a message cannot later deny having sent the message and the recipient cannot deny having received the message
   a. Confidentiality
   b. Integrity
   c. Nonrepudiation
   d. Authentication

12. The ability to positively identify an individual responsible for an action is known as .....
   a. Accountability
   b. Responsibility
   c. Audit trail
   d. SSH

13. A code segment that replicates by attaching copies of itself to executable programs is likely to be a .....
    a. Logic bomb
    b. Trojan horse
    c. Virus
    d. Worm

14. A self-replicating program that is self contained and which requires no host program is likely to be a .....
    a. Logic bomb
    b. Trojan horse
    c. Virus
    d. Worm

15. Which of the following is an independent malicious code?
    a. Zombie
    b. Trojan horse
    c. Virus
    d. Back door

16. ..... provide immediate access to a system bypassing employed authentication
    a. Zombie
    b. Trojan horse
    c. Virus
    d. Back door

17. A ..... is a code embedded in some legitimate program that execute when certain predefined events occurs.
    a. Logic bomb
    b. Trojan horse
    c. Virus
    d. Worm

18. A ..... virus create copies of itself that re functionally equivalent but have different bit patterns
    a. Stealth
    b. Macro
    c. Polymorphic
    d. Binary code

19. A ..... is a format virus that is explicitly design to hide itself from detection by antivirus software.
    a. Stealth
    b. Macro
    c. Polymorphic
    d. Binary code

20. The type of denial of service attack that employs the use of an amplification network to increase the severity of the attack is known as .....
    a. DoS
    b. DDoS
    c. DRDoS
    d. IPsec

21. A type of DoS attack which is characterized by a dramatic increase in the number of spam mails received is considered a .....
    a. Brute force attack
    b. Social engineering
    c. Denial of service
    d. Spamming

22. Which of the following is considered a back door?
    a. An active workstation whose user has walked away
    b. The COM port on the back of a router
    c. An entry ate with a broken lock
    d. A weak password

23. What is the common name for a program that has no useful purpose, but attempts to spread itself to other systems and often damages resources on the systems where it is found?
    a. Windows messenger
    b. Virus
    c. Java applet
    d. Trojan horse

24. What is the most common means of virus distribution?
    a. Applets
    b. Scripts
    c. Errors
    d. Email

25. Which of the following cryptographic methods serves as a means to provide access control?
    a. Shared private key
    b. Digital envelope
    c. Hashing value
    d. Digital signature

26. Which of the following tools can be used to bypass a firewall that blocks FTP traffic?
    a. NAT
    b. IPsec
    c. Anti Firewall
    d. Smurf

27. A ..... checks the address of incoming traffic and turns away anything that doesn't match the list of trusted addresses.
    a. Packet filter firewall
    b. Application level proxy server
    c. Stateful packet inspection firewall
    d. Demilitarized zone firewall

28. Which of the below firewall is likely to determine all part of an IP packet to determine whether to accept or reject the request communication?
    a. Packet filter firewall
    b. Application level proxy server
    c. Stateful packet inspection firewall
    d. Demilitarized zone firewall

29. Which feature of a firewall will you deploy to prevent employees from accessing a particular website?
    a. Packet filtering
    b. Demilitarized zone firewalls
    c. Content filtering
    d. VPNs

30. Which of the firewall is effective for companies that invite customers to contact their network from external sources – through the internet or any other route?
    a. Packet filtering
    b. Demilitarized zone firewalls
    c. Content filtering
    d. VPNs

31. Which of the following cryptographic methods serves as a means to provide access control?
    a. Shared private key
    b. Digital envelope
    c. Hashing value
    d. Digital signate

32. Which of the following is not true in a centralized key management scheme?
    a. Users retain full control over their private key
    b. The CA generates both the public and private keys
    c. A centralized mechanism requires significant infrastructure
    d. A centralized mechanism supports a high level of control

33. Which of the following is not a countermeasure against dictionary attacks?
    a. Avoiding common words
    b. Using short passwords
    c. Using three or four different keyboard character types (i.e. lowercase, uppercase, numerals, & symbols)
    d. Avoiding industry acronyms

34. Which type of password attack employs a list of predefined passwords that it tries against a login attempt or a local copy of a security accounts database?
    a. Asynchronous
    b. Salami
    c. Brute force
    d. Dictionary

35. Which of the following is the single best rule to enforce when designing complex passwords?
    a. Maximum password age
    b. Computer generated passwords
    c. Longer passwords
    d. Force use of all fur types of characters (i.e. lowercase, uppercase, numerals, & symbols)

36. Which of the following is the strongest password?
    a. PASSWORD#
    b. PAssW$90^0rd
    c. Password1
    d. PaSsWoRd43

37. Which of the following is considered a back door?
    a. An active workstation whose user has walked away
    b. The COM port on the back of a router
    c. An entry gate with a broken lock
    d. A weak password

38. Capturing packets as they travel from one host to another with the intent of altering the contents of the packets is a from of which security concern?
    a. Distributed denial of service
    b. Spamming
    c. Man-in-the-middle attack
    d. Passive logging

39. Integrity is the protection of data from all the following except …….
    a. Unauthorized changes
    b. Accidental changes
    c. Data analysis
    d. Intentional manipulation

40. Data classification can assist an organization in …….
    a. Eliminating regulatory mandates
    b. Lowering accountability
    c. Reducing cost for protecting data
    d. Normalization of databases

41. One main objective of an awareness training is …….
    a. Provide understanding of responsibilities
    b. Entertaining the user through creative programs
    c. Overcoming all resistance to security
    d. To be repetitive to ensure accountability

42. What is the primary target of a person employing social engineering?
    a. An individual
    b. A policy
    c. Government
    d. An information system

43. Social engineering can take many forms except
    a. Dumpster diving
    b. Coercion
    c. Sympathy
    d. Eavesdropping

44. Which of the following is not a characteristic of a virus?
    a. Its primary effect is to consume system resources
    b. It may or may not carry a payload
    c. It spreads through user action
    d. It attaches itself to executable code

45. Audit logs should record all of the following except
    a. Successful attempts
    b. System performance measurements
    c. Failed access attempts
    d. Changes to user permissions

46. What is one of the differences between a virus and a worm?
    a. Only the virus is distributed through email attachments
    b. Only the worm is capable of executing without user interaction
    c. Only the worm is capable of attaching to an application and creating its own macro programming infection
    d. Only the virus is a standalone file that can be executed by an interpreter

47. In following the concept of separation of duties during software production which of the following would not occur?
    a. Separation between programmers
    b. Separation between programmers and system
    c. Separation between programmers and quality assurance personnel
    d. Separation between programmers and staff

48. When an employee transfers within an organization:
    a. They must undergo a new security review
    b. All old system Ids must be disabled
    c. All access permissions should be reviewed
    d. The employee must turn in all remote access devices

49. Digital signatures do not allow for:
    a. Unauthorized modification to a message
    b. Authentication of the signatory
    c. Third-party verification of sender
    d. Confidentiality of a document

50. Site location should consider the following except ……
    a. Lightening
    b. Crime
    c. Natural disaster
    d. Emergency response facilities

51. The primary function of risk management is to ……
    a. Identify vulnerabilities
    b. Identify threats
    c. Measure risk
    d. Mitigate risk

52. Authentication that is based on "what you are" is known as ……
    a. *Biometrics*
    b. Token
    c. User ID and password
    d. Threat

53. The absence of a safeguard constitutes a ……
    a. Weakness
    b. Vulnerability
    c. *Threat*
    d. Risk

54. Which feature of a firewall will you deploy to prevent employees from accessing a particular website?
    a. Packet filtering firewall
    b. Demilitarized zone firewalls
    c. *Content filtering*
    d. VPNs

55. Which feature of a firewall is effective for companies that invite customers to contact their network from external source – through the internet or any other route?
    a. Packet filtering firewall
    b. *Demilitarized zone firewalls*
    c. Content filtering
    d. VPNs

56. Which of the following cryptographic methods serve as a means to provide access control?
    a. Shared private key
    b. *Digital envelope*
    c. Hashing value
    d. Digital signature

57. Which of the following is not true in a centralized key management scheme?
    a. *Users retain full control over their private key*
    b. The CA generates both the public and private keys
    c. A centralized mechanism requires significant infrastructure
    d. A centralized mechanism supports a high level of control

58. Which of the following is not a countermeasure against dictionary attacks?
    a. Avoiding common words
    b. *Using short passwords*
    c. Using three or four different keyboard character types (i.e. lowercase, uppercase, numerals, & symbols)
    d. Avoiding industry acronyms

59. Which type of password attack employs a list of pre-defined passwords that it tries against a logon prompt or local copy of a security accounts database?
    a. Asynchronous
    b. Salami
    c. Brute force
    d. Dictionary

60. Which of the following is the single best rule to enforce when designing complex passwords?
    a. Maximum password age
    b. Computer generated passwords
    c. Longer passwords
    d. Force use of all four types of characters (i.e. lowercase, uppercase, numerals, & symbols)