Unit-VI

1. **What is the primary purpose of a firewall in a computer system?**
   a. Data storage
   b. Network connectivity
   c. Access control
   d. File encryption

2. **What does the term 'phishing' refer to in the context of cybersecurity?**
   a. Protecting sensitive information
   b. Sending malicious emails to trick users
   c. Enhancing network speed
   d. Encrypting files for security

3. **Which cryptographic key is kept secret and known only to the owner?**
   a. Public key
   b. Private key
   c. Symmetric key
   d. Session key

4. **What does the acronym 'SSL' stand for?**
   a. Secure Socket Layer
   b. System Security Language
   c. Simple Security Layer
   d. Strong System Lock

5. **Which of the following is a common biometric authentication method?**
   a. Passwords
   b. PINs
   c. Fingerprint scanning
   d. Security tokens

6. **What is the purpose of antivirus software?**
   a. Secure network connections
   b. Prevent unauthorised access
   c. Detect and remove malicious software
   d. Encrypt files for privacy

7. **What is a Denial of Service (DoS) attack?**
   a. Unauthorised access to a system
   b. Stealing sensitive information
   c. Flooding a network or server to make it unavailable
   d. Intercepting communication between devices

8. **Which of the following is an example of a strong password?**
   a. 'password1230'
   b. 'SecurePwd!2022'
   c. '123456'
   d. 'admin'

9. **What is the purpose of a Virtual Private Network (VPN)?**
   a. Securely connect two devices on the same network
   b. Encrypt data for secure transmission over the internet
   c. Block unauthorised access to a website
   d. Scan for malware on a computer

10. **What is the principle behind Two-Factor Authentication (2FA)?**
    a. Using two different encryption algorithms
    b. Verifying identity using two independent methods
    c. Creating two separate user accounts
    d. Encrypting data with two different keys

11. **What is the primary goal of an intruder in the context of cybersecurity?**
    a. Enhance system performance
    b. Ensure data integrity
    c. Gain unauthorised access or disrupt operations
    d. Improve network connectivity

12. **Which of the following is a common method used by intruders to gain unauthorised access to a system?**
    a. Encryption
    b. Authentication
    c. Phishing
    d. Firewalls

13. **What is the term for a malicious program that disguises itself as a legitimate software?**
    a. Firewall
    b. Trojan horse
    c. Antivirus
    d. VPN

14. **What does the acronym 'IDS' stand for in the context of cybersecurity?**
    a. Internet Data Service
    b. Intrusion Detection System
    c. Internal Data Security
    d. Internet Defense Strategy

15. **Which type of intrusion detection system operates by comparing current network activity to a baseline?**
    a. Anomaly-based
    b. Signature-based
    c. Behaviour-based
    d. Pattern-based

16. **What is a 'zero-day exploit'?**
    a. An attack that occurs at midnight
    b. An attack that targets zero users
    c. An exploit targeting a vulnerability before it is known or patched
    d. An exploit with zero impact on the system

17. **What is the primary purpose of a honeypot in cybersecurity?**
    a. Detecting and attracting intruders
    b. Enhancing network speed
    c. Encrypting sensitive data
    d. Blocking malicious websites

18. **Which of the following is a social engineering technique commonly used by intruders?**
    a. Encryption
    b. Two-factor authentication
    c. Shoulder surfing
    d. Firewall

19. **What does the term 'penetration testing' involve in the context of cybersecurity?**
    a. Testing the speed of the internet connection
    b. Testing the strength of physical security
    c. Simulating a cyber attack to identify vulnerabilities
    d. Testing the performance of antivirus software

20. **In the context of network security, what is a 'man-in-the-middle' attack?**
    a. Gaining unauthorised access to a system
    b. Intercepting and altering communication between two parties
    c. Using social engineering to trick users
    d. Flooding a network with traffic

21. **What is a computer virus?**
    a. A type of malware that steals personal information
    b. Software designed to protect against cyber threats
    c. Malicious code that attaches itself to legitimate programs
    d. A hardware component used for data storage

22. **How does a worm differ from a virus?**
    a. Worms are always benign, while viruses are malicious
    b. Viruses spread through networks, while worms can spread independently
    c. Viruses primarily target hardware, while worms target software
    d. Worms require user interaction, while viruses spread automatically

23. What is the purpose of a 'Trojan horse' in the context of cybersecurity?
a. To encrypt data for security
b. To provide remote access to a computer
c. To detect and remove malware
d. To enhance system performance

24. Which of the following is an example of ransomware?
a. Adware
b. Spyware
c. Cryptolocker
d. Rootkit

25. What is the term for a security technique that involves disguising sensitive information within innocent-looking data?
a. Encryption
b. Steganography
c. Authentication
d. Intrusion detection

26. What does the acronym 'DDoS' stand for in the context of cyber threats?
a. Data Disruption over Security
b. Direct Detection of System Vulnerabilities
c. Distributed Denial of Service
d. Digital Defense against Software

27. Which of the following statements about phishing is true?
a. Phishing only occurs through email
b. Phishing involves physically stealing computers
c. Phishing relies on tricking individuals to reveal sensitive information
d. Phishing is a type of antivirus software

28. What is the primary purpose of antivirus software?
a. Encrypting data for security
b. Detecting and removing malicious software
c. Enhancing network connectivity
d. Blocking phishing emails

29. What is a 'zero-day vulnerability'?
a. A security hole that is always present
b. A vulnerability that has existed for zero days
c. A flaw that is exploited before a patch is available
d. A type of antivirus definition

30. Which type of malware is designed to hide its presence on a system?
a. Virus
b. Worm
c. Spyware
d. Ransomware

31. What is the primary purpose of a firewall in a network?
a. Encrypting data
b. Controlling network traffic
c. Enhancing internet speed
d. Managing hardware resources

32. What is the difference between a stateful and a stateless firewall?
a. Stateful firewalls analyse the content of packets, while stateless firewalls only examine packet headers
b. Stateless firewalls inspect the application layer, while stateful firewalls focus on the network layer
c. Stateful firewalls only allow outgoing traffic, while stateless firewalls only filter incoming traffic
d. Stateless firewalls use complex rule sets, while stateful firewalls rely on simple rule-based filtering

33. What is the purpose of an application layer firewall (proxy firewall)?
a. To filter traffic based on IP addresses
b. To examine and control traffic at the application layer
c. To encrypt all incoming and outgoing data
d. To manage network hardware

34. Which type of firewall operates at both the network and application layers of the OSI model?
a. Packet-filtering firewall
b. Stateful firewall
c. Proxy firewall
d. Circuit-level gateway firewall

35. What is the purpose of Network Address Translation (NAT) in a firewall?
a. Encrypting data for secure transmission
b. Translating private IP addresses to a public IP address
c. Blocking all incoming traffic
d. Managing network hardware resources

36. Which of the following is a benefit of using a DMZ (Demilitarised Zone) in firewall design?
a. Faster internet speed
b. Enhanced security by isolating public-facing services
c. Increased network capacity
d. Simplified firewall configuration

37. **What is the purpose of ingress and egress filtering in firewall rules?**
a. Allowing or blocking traffic based on the source and destination IP addresses
b. Encrypting incoming and outgoing data
c. Managing network hardware
d. Controlling the speed of internet connections

38. **Which firewall rule would allow outbound traffic from the internal network while blocking all incoming traffic?**
a. Ingress rule
b. Egress rule
c. Outbound rule
d. Inbound rule

39. **What is the purpose of a VPN (Virtual Private Network) in the context of firewall design?**
a. Blocking malicious websites
b. Encrypting data for secure transmission over the internet
c. Managing hardware resources
d. Filtering traffic based on IP addresses

40. **In the context of firewall design, what is a 'default-deny' rule?**
a. All traffic is allowed by default
b. All traffic is denied by default
c. Ingress and egress rules are combined
d. Stateful inspection is disabled

41. **Which of the following case tools is commonly used for Unified Modeling Language (UML) diagrams?**
a. Microsoft Excel
b. Rational Rose
c. Adobe Photoshop
d. Eclipse IDE

42. **Which software platform is often used for version control and collaboration in software development?**
a. Microsoft Word
b. Git
c. Adobe Illustrator
d. IntelliJ IDEA

43. **In software development, which tool is commonly used for continuous integration and automated build processes?**
a. JIRA
b. Jenkins
c. Microsoft PowerPoint
d. Visual Studio Code

44. **Which case tool is designed for requirements management, test management and project management?**
a. MATLAB
b. Selenium
c. IBM Engineering Requirements Management DOORS
d. Android Studio

45. **Which software platform is widely used for developing android applications?**
a. Xcode
b. Android Studio
c. Eclipse
d. NetBeans

46. **What is the purpose of a tool like SonarQube in software development?**
a. Graphic design
b. Code quality analysis and continuous inspection
c. Project management
d. Requirements gathering

47. **Which of the following is a popular agile project management tool used for tracking tasks and managing sprints?**
a. Trello
b. Adobe Premiere Pro
c. Autodesk Maya
d. Blender

48. **In web development, which software platform is commonly used for frontend development and design?**
a. MongoDB
b. React.js
c. Django
d. Node.js

49. **Which case tool facilitates the modeling of business processes and workflows?**
a. Apache Maven
b. Bizagi
c. JUnit
d. Sublime Text

50. **Which software platform is widely used for container orchestration and management in cloud environments?**
a. Kubernetes
b. Docker
c. Amazon Web Services (AWS)
d. Heroku

51. What is the primary goal of configuration management in software development?
a. Enhancing system performance
b. Managing project timelines
c. Controlling and tracking changes to software and system components
d. Optimising network speed

52. Which of the following is a key benefit of configuration management?
a. Faster code compilation
b. Easier hardware installation
c. Improved collaboration among team members
d. Enhanced user interface design

53. What is the purpose of a version control system in configuration management?
a. Managing hardware resources
b. Tracking changes to source code and documents
c. Accelerating software testing
d. Controlling network access

54. In version control systems, what does 'commit' refer to?
a. Submitting code changes to the project manager
b. Storing changes permanently in the version control system
c. Testing the latest version of the software
d. Reverting to a previous software version

55. Which configuration management process involves identifying and documenting the characteristics of system components?
a. Change management
b. Release management
c. Identification
d. Verification and audit

56. What is the purpose of a baseline in configuration management?
a. Establishing a reference point for tracking changes
b. Implementing the latest software updates
c. Performing system backups
d. Managing user authentication

57. Which tool is commonly used for continuous integration and configuration management in software development?
a. JIRA
b. Git
c. Jenkins
d. Docker

58. What is the role of a Configuration Management Database (CMDB) in configuration management?
a. Storing passwords for system access
b. Managing hardware inventory
c. Documenting and tracking configuration items
d. Controlling network firewalls

59. Which term describes the process of ensuring that the actual configuration matches the desired configuration?
a. Configuration control
b. Configuration identification
c. Configuration audit
d. Configuration baseline

60. What does the term 'rollback' mean in the context of configuration management?
a. Implementing the latest software updates
b. Reverting to a previous version of the software
c. Submitting code changes to the version control system
d. Testing the latest version of the code