First 50

1. B) Securing information that is in a digital format
2. C) Accessibility
3. C) Allowing unauthorized access to sensitive information
4. B) Data is accurate and reliable
5. B) Ensuring systems are accessible to authorized users
6. C) Availability
7. B) Worm
8. B) Scrambling virus code and placing parts randomly in host programs
9. B) Employee computers used for cash transfer systems
10. C) SQL Injection
11. B) User actions, such as opening an email attachment
12. A) Constantly changing encryption techniques to avoid detection
13. B) Change their internal code without altering the functionality
14. B) Overwriting files like JPEGs and MP3s
15. A) A type of malware that hides its presence from detection tools
16. B) Individuals who use automated tools for attacks
17. A) Sell vulnerabilities to the highest bidder
18. C) Mitigation
19. B) Perform penetration tests to find vulnerabilities
20. B) Long-term, undetected access to sensitive data
21. C) Availability
22. B) The confidentiality of data
23. B) Document files like Word or Excel
24. C) Foundation-level security skills
25. B) Unauthorized users accessing sensitive information
26. B) Integrity
27. D) Antivirus developers
28. B) Using multiple levels of security controls
29. C) Human users through deception
30. D) Fragmentation
31. A) Access to the system without the user’s knowledge
32. B) Demands payment to restore access to files
33. B) Newly discovered vulnerabilities that haven’t been patched yet
34. B) Deny legitimate users access to services
35. A) Hiding internal system details from attackers
36. B) Rootkit
37. C) Spying on traffic between two parties
38. B) Social engineering through email
39. A) Remotely viewing and controlling infected systems
40. B) Manipulating people into giving up sensitive information
41. B) Embedding malicious code in Word or Excel documents
42. B) Filter traffic based on security rules
43. B) DDoS attacks using IoT devices
44. B) The intended actions of an object before it executes
45. A) Comparing file content to known virus signatures
46. B) Record keystrokes on a system
47. B) Spyware
48. B) Confidentiality, Integrity, Availability
49. A) Restricting user access to only what they need
50. B) Long-term access to sensitive information

Second 50

**Correct Answers:**

1. B) Obscurity
2. B) Using different types of defense mechanisms in different layers
3. B) Appears as legitimate software but has malicious intent
4. C) Encrypt files and demand payment for decryption
5. A) Worms do not need user interaction to spread
6. B) Hide the existence of malicious processes from detection
7. A) Multiple types of defenses are in place
8. A) Monitor user activity and steal sensitive information
9. B) Database systems
10. B) Exploiting improperly handled memory in software
11. B) Trickery to make users divulge personal information
12. B) Sending a phishing email to employees
13. A) Political and strategic goals
14. A) Block unauthorized incoming and outgoing traffic
15. C) Making a service unavailable to legitimate users
16. A) Phishing
17. A) Guessing passwords by trying every possible combination
18. A) Verifying that a user is who they claim to be
19. A) Confidentiality
20. A) Unpatched vulnerabilities
21. B) Confidentiality, Integrity, Availability
22. B) Long-term, undetected access to systems
23. B) Files and programs on a system
24. A) Capturing passwords and sensitive information
25. A) Monitor user activities without their knowledge
26. A) Displays unwanted advertisements to users
27. B) Trick users into providing personal information
28. A) Hide malicious processes from detection
29. B) Unsolicited and often irrelevant emails sent to large numbers of users
30. A) Block unauthorized access to or from the network
31. B) Manipulating people into giving up confidential information
32. C) Ideological reasons
33. D) Firewall
34. B) Provide stronger security by requiring multiple forms of verification
35. B) Increase security by requiring two forms of verification
36. B) Conducting large-scale attacks like DDoS
37. A) Communications between two parties
38. A) Exploit vulnerabilities in web applications
39. A) Sending excessive traffic to overwhelm systems
40. A) Capture and record keystrokes made by a user
41. A) Change its code to avoid detection
42. A) Human behavior and decision-making
43. A) Systems designed to attract and trap attackers
44. A) Passwords and sensitive information
45. A) Self-replicating malware that requires user intervention
46. A) They do not need user action to spread
47. A) Monitor and block unauthorized traffic
48. A) Financial gain or malicious intent
49. B) Exposing vulnerabilities for security improvement
50. A) Breaking into systems without permission but not for malicious purposes