**First 50**

**1. Which of the following best defines Information Security?**

* A) Preventing physical access to data
* B) Securing information that is in a digital format
* C) Creating backups of all files
* D) Restricting access to social media accounts

**2. Which of the following is not a part of the CIA triad?**

* A) Confidentiality
* B) Integrity
* C) Accessibility
* D) Availability

**3. Which of the following is a violation of confidentiality?**

* A) Encrypting sensitive data
* B) Deleting critical files
* C) Allowing unauthorized access to sensitive information
* D) Correcting errors in data

**4. Integrity ensures that:**

* A) Data is protected from unauthorized access
* B) Data is accurate and reliable
* C) Data is available when needed
* D) Data is encrypted in transit

**5. The availability aspect of the CIA triad focuses on:**

* A) Preventing unauthorized access to systems
* B) Ensuring systems are accessible to authorized users
* C) Encrypting sensitive data in transit
* D) Detecting unauthorized modifications to files

**6. A DDoS attack affects which aspect of the CIA triad?**

* A) Confidentiality
* B) Integrity
* C) Availability
* D) Accessibility

**7. Which malware type spreads without user intervention?**

* A) Virus
* B) Worm
* C) Trojan horse
* D) Rootkit

**8. Swiss cheese infection refers to:**

* A) Infecting system files
* B) Scrambling virus code and placing parts randomly in host programs
* C) Encrypting the virus payload
* D) Infecting multiple devices simultaneously

**9. The Carbanak malware used in bank attacks provided access to:**

* A) The bank’s database systems
* B) Employee computers used for cash transfer systems
* C) Bank customer accounts
* D) ATM systems directly

**10. What attack was used in the Sony data breach of 2011?**

* A) Malware infection
* B) DDoS attack
* C) SQL Injection
* D) Phishing attack

**11. Viruses cannot spread automatically and rely on:**

* A) Internet connections
* B) User actions, such as opening an email attachment
* C) Exploiting network vulnerabilities
* D) Using admin privileges to copy themselves

**12. Polymorphic malware uses:**

* A) Constantly changing encryption techniques to avoid detection
* B) Only one method of attack
* C) Hardware vulnerabilities to gain access
* D) System memory to store data

**13. Metamorphic viruses differ from polymorphic ones because they:**

* A) Use the same code structure for every attack
* B) Change their internal code without altering the functionality
* C) Cannot replicate on their own
* D) Only attack executable files

**14. The ILOVEYOU virus caused damage by:**

* A) Infecting databases
* B) Overwriting files like JPEGs and MP3s
* C) Sending ransomware demands
* D) Destroying operating system files

**15. Which of the following best describes a rootkit?**

* A) A type of malware that hides its presence from detection tools
* B) A virus that spreads through emails
* C) A Trojan horse that steals login credentials
* D) An exploit that corrupts hardware components

**16. Script kiddies are typically:**

* A) Highly skilled hackers with in-depth system knowledge
* B) Individuals who use automated tools for attacks
* C) Hackers who work for governments
* D) Programmers who develop malware

**17. Brokers are attackers who:**

* A) Sell vulnerabilities to the highest bidder
* B) Write malicious software for personal use
* C) Protect systems from hackers
* D) Launch denial-of-service attacks

**18. The Cyber Kill Chain includes all of the following steps except:**

* A) Reconnaissance
* B) Weaponization
* C) Mitigation
* D) Delivery

**19. White hat hackers:**

* A) Violate systems for financial gain
* B) Perform penetration tests to find vulnerabilities
* C) Cause malicious damage to systems
* D) Sell exploits on the black market

**20. Advanced Persistent Threats (APTs) are primarily characterized by:**

* A) Immediate disruption of services
* B) Long-term, undetected access to sensitive data
* C) Frequent password attacks
* D) Use of ransomware

**21. Which of the following security principles ensures that information is available to authorized users at all times?**

* A) Confidentiality
* B) Integrity
* C) Availability
* D) Authenticity

**22. Encryption is primarily used to protect:**

* A) The availability of data
* B) The confidentiality of data
* C) The integrity of hardware
* D) The functionality of software

**23. A macro virus typically infects:**

* A) Executable files
* B) Document files like Word or Excel
* C) Network configurations
* D) Web browsers

**24. The CompTIA Security+ certification focuses on:**

* A) Ethical hacking
* B) Physical security
* C) Foundation-level security skills
* D) Cloud-based security

**25. Confidentiality breaches can result from:**

* A) Deleting files accidentally
* B) Unauthorized users accessing sensitive information
* C) Failing to back up data
* D) Hardware failures

**26. Hashing is a technique used to ensure:**

* A) Confidentiality
* B) Integrity
* C) Availability
* D) Authenticity

**27. Which of the following is not a category of attackers?**

* A) Hactivists
* B) Insiders
* C) Brokers
* D) Antivirus developers

**28. Layering as a security principle refers to:**

* A) Restricting access based on job roles
* B) Using multiple levels of security controls
* C) Encrypting data at rest and in transit
* D) Monitoring network traffic continuously

**29. Phishing attacks primarily target:**

* A) System vulnerabilities
* B) Data encryption methods
* C) Human users through deception
* D) Wireless networks

**30. Which of the following is not a defense principle in cybersecurity?**

* A) Layering
* B) Diversity
* C) Limiting
* D) Fragmentation

**31. A backdoor in malware allows:**

* A) Access to the system without the user’s knowledge
* B) Infection of other systems automatically
* C) The virus to reproduce itself
* D) Protection from antivirus software

**32. Ransomware is a type of malware that:**

* A) Spies on user activity
* B) Demands payment to restore access to files
* C) Infects system boot sectors
* D) Corrupts network traffic

**33. Zero-day vulnerabilities refer to:**

* A) Vulnerabilities that have been publicly known for a long time
* B) Newly discovered vulnerabilities that haven’t been patched yet
* C) Vulnerabilities caused by outdated software
* D) Network-related vulnerabilities only

**34. A DoS (Denial of Service) attack is designed to:**

* A) Steal confidential information
* B) Deny legitimate users access to services
* C) Corrupt system files
* D) Install spyware on a system

**35. Obscurity as a defense strategy means:**

* A) Hiding internal system details from attackers
* B) Limiting the number of security layers
* C) Using encryption for all data transmission
* D) Simplifying system architecture

**36. Which malware hides its activities by modifying the operating system?**

* A) Spyware
* B) Rootkit
* C) Adware
* D) Worm

**37. Man-in-the-middle attacks involve:**

* A) Redirecting traffic to an unauthorized server
* B) Crashing systems by overloading them
* C) Spying on traffic between two parties
* D) Infecting a system via email attachments

**38. Phishing is often carried out via:**

* A) Phone calls
* B) Social engineering through email
* C) In-person attacks
* D) Keylogging software

**39. VNC (Virtual Network Computing) malware capabilities include:**

* A) Remotely viewing and controlling infected systems
* B) Stealing passwords only
* C) Disabling antivirus software
* D) Encrypting files for ransom

**40. Social engineering attacks rely on:**

* A) Exploiting software vulnerabilities
* B) Manipulating people into giving up sensitive information
* C) Infecting files with a virus
* D) DDoS attacks on servers

**41. A macro virus typically spreads by:**

* A) Attaching itself to system files
* B) Embedding malicious code in Word or Excel documents
* C) Infecting the system boot sector
* D) Spreading via email spam

**42. Firewalls are primarily used to:**

* A) Encrypt data at rest
* B) Filter traffic based on security rules
* C) Monitor user activity
* D) Detect malware infections

**43. The Mirai botnet was used in:**

* A) Ransomware attacks
* B) DDoS attacks using IoT devices
* C) Phishing campaigns
* D) Spyware installation

**44. Behavior-based detection evaluates:**

* A) The source code of malware
* B) The intended actions of an object before it executes
* C) The network traffic for anomalies
* D) The type of encryption used

**45. Signature-based detection relies on:**

* A) Comparing file content to known virus signatures
* B) Monitoring for unusual system behavior
* C) Blocking encrypted data transmissions
* D) Evaluating system configurations

**46. Keylogging malware is designed to:**

* A) Log network traffic
* B) Record keystrokes on a system
* C) Block access to websites
* D) Monitor email attachments

**47. Which type of malware is designed to steal personal information from a system?**

* A) Adware
* B) Spyware
* C) Ransomware
* D) Worm

**48. The CIA triad in information security stands for:**

* A) Cybersecurity, Integrity, Access
* B) Confidentiality, Integrity, Availability
* C) Control, Innovation, Access
* D) Cryptography, Identity, Authorization

**49. Limiting as a security principle means:**

* A) Restricting user access to only what they need
* B) Using a single layer of security
* C) Encrypting all system data
* D) Using the same passwords for all accounts

**50. APT attacks usually focus on:**

* A) Quick financial gain
* B) Long-term access to sensitive information
* C) Spreading ransomware
* D) Creating network outages

**Second 50**

**1. Which security principle involves hiding internal system details from attackers?**

* A) Limiting
* B) Obscurity
* C) Diversity
* D) Layering

**2. Diversity in security means:**

* A) Using multiple layers of the same type of defense
* B) Using different types of defense mechanisms in different layers
* C) Encrypting all data
* D) Restricting access to certain files

**3. A Trojan horse is a type of malware that:**

* A) Replicates itself automatically
* B) Appears as legitimate software but has malicious intent
* C) Infects the boot sector of the system
* D) Crashes systems by overloading memory

**4. Ransomware attacks primarily aim to:**

* A) Spy on user activity
* B) Steal sensitive information
* C) Encrypt files and demand payment for decryption
* D) Hijack browsers for click fraud

**5. The primary difference between viruses and worms is:**

* A) Worms do not need user interaction to spread
* B) Worms always cause system crashes
* C) Viruses cannot cause system damage
* D) Worms cannot replicate themselves

**6. Rootkits are designed to:**

* A) Replicate across systems
* B) Hide the existence of malicious processes from detection
* C) Lock users out of their systems
* D) Slow down network performance

**7. Layering as a defense mechanism ensures that:**

* A) Multiple types of defenses are in place
* B) Only the simplest defense is used
* C) Systems are less vulnerable to zero-day exploits
* D) Users have access to all resources

**8. Spyware is designed to:**

* A) Monitor user activity and steal sensitive information
* B) Encrypt system files
* C) Replicate through email attachments
* D) Shut down the system when activated

**9. SQL injection is an attack that targets:**

* A) Web server vulnerabilities
* B) Database systems
* C) Network infrastructure
* D) Authentication mechanisms

**10. A buffer overflow attack involves:**

* A) Overloading a system with traffic
* B) Exploiting improperly handled memory in software
* C) Sending phishing emails to multiple users
* D) Spreading malware through USB drives

**11. Phishing attacks rely on:**

* A) Exploiting system vulnerabilities
* B) Trickery to make users divulge personal information
* C) Hijacking user sessions
* D) Injecting malicious code into websites

**12. Which of the following is an example of social engineering?**

* A) A brute force attack on passwords
* B) Sending a phishing email to employees
* C) Injecting malware into a database
* D) DDoS attacks on servers

**13. State-sponsored attackers are generally motivated by:**

* A) Political and strategic goals
* B) Financial gain only
* C) Disruption of small businesses
* D) Crashing network infrastructure

**14. The primary role of a firewall is to:**

* A) Block unauthorized incoming and outgoing traffic
* B) Encrypt all traffic over a network
* C) Detect viruses on the system
* D) Analyze software vulnerabilities

**15. A denial-of-service (DoS) attack is primarily aimed at:**

* A) Disabling antivirus software
* B) Stealing user credentials
* C) Making a service unavailable to legitimate users
* D) Spreading ransomware

**16. Which attack is most commonly associated with data breaches?**

* A) Phishing
* B) Denial of Service
* C) Man-in-the-middle
* D) Malware injection

**17. Brute force attacks focus on:**

* A) Guessing passwords by trying every possible combination
* B) Sending a large amount of data to a server
* C) Injecting malicious code into software
* D) Gaining access to databases

**18. Authentication is the process of:**

* A) Verifying that a user is who they claim to be
* B) Assigning user permissions to data
* C) Encrypting sensitive information
* D) Monitoring user activities on the network

**19. Encryption ensures the following for data in transit:**

* A) Confidentiality
* B) Availability
* C) Integrity
* D) Usability

**20. Zero-day attacks target:**

* A) Unpatched vulnerabilities
* B) Network traffic
* C) Encrypted data
* D) Updated software

**21. The CIA triad consists of:**

* A) Cryptography, Integrity, Availability
* B) Confidentiality, Integrity, Availability
* C) Control, Identity, Access
* D) Confidentiality, Identity, Authorization

**22. APT attacks are most often associated with:**

* A) Immediate financial gain
* B) Long-term, undetected access to systems
* C) Disrupting internet services
* D) Corrupting hardware components

**23. A virus attaches itself to:**

* A) Network connections
* B) Files and programs on a system
* C) System firmware
* D) User login credentials

**24. Which of the following is a common use of keyloggers?**

* A) Capturing passwords and sensitive information
* B) Spreading ransomware
* C) Locking users out of their systems
* D) Infecting web servers

**25. Spyware is often used to:**

* A) Monitor user activities without their knowledge
* B) Encrypt files for ransom
* C) Destroy data on hard drives
* D) Execute commands on a remote system

**26. Adware typically:**

* A) Displays unwanted advertisements to users
* B) Encrypts system files
* C) Locks users out of their devices
* D) Corrupts network traffic

**27. The primary goal of phishing is to:**

* A) Infect systems with ransomware
* B) Trick users into providing personal information
* C) Disable firewalls and security systems
* D) Steal system resources for cryptocurrency mining

**28. Rootkits are commonly used to:**

* A) Hide malicious processes from detection
* B) Encrypt files and demand payment for decryption
* C) Destroy system files
* D) Spread malware through email attachments

**29. Spam refers to:**

* A) Malicious software that replicates itself
* B) Unsolicited and often irrelevant emails sent to large numbers of users
* C) Emails containing malicious attachments
* D) Software designed to steal information

**30. Firewall rules are primarily designed to:**

* A) Block unauthorized access to or from the network
* B) Prevent hardware failures
* C) Encrypt data at rest
* D) Identify zero-day vulnerabilities

**31. Social engineering relies on:**

* A) Technical vulnerabilities
* B) Manipulating people into giving up confidential information
* C) Exploiting weak encryption
* D) Injecting malware into databases

**32. Hactivists typically attack for:**

* A) Financial gain
* B) Personal vendettas
* C) Ideological reasons
* D) State-sponsored activities

**33. Which of the following is not an example of malware?**

* A) Trojan horse
* B) Spyware
* C) Keylogger
* D) Firewall

**34. Multi-factor authentication (MFA) is designed to:**

* A) Speed up the login process
* B) Provide stronger security by requiring multiple forms of verification
* C) Replace passwords with PINs
* D) Prevent malware from infecting a system

**35. The primary purpose of two-factor authentication (2FA) is to:**

* A) Simplify the login process
* B) Increase security by requiring two forms of verification
* C) Replace passwords with encryption keys
* D) Encrypt all data at rest

**36. Botnets are primarily used for:**

* A) Spreading malware
* B) Conducting large-scale attacks like DDoS
* C) Encrypting system files
* D) Crashing operating systems

**37. Man-in-the-middle attacks intercept:**

* A) Communications between two parties
* B) Malicious code in files
* C) Phishing emails
* D) System logs

**38. SQL injection is primarily used to:**

* A) Exploit vulnerabilities in web applications
* B) Attack email servers
* C) Corrupt network traffic
* D) Infect system files

**39. DDoS attacks typically involve:**

* A) Sending excessive traffic to overwhelm systems
* B) Spying on user activity
* C) Infecting files with malware
* D) Hijacking web servers

**40. Keyloggers are used to:**

* A) Capture and record keystrokes made by a user
* B) Encrypt data at rest
* C) Inject malware into system files
* D) Block access to network resources

**41. Polymorphic malware is designed to:**

* A) Change its code to avoid detection
* B) Disable firewalls and antivirus software
* C) Encrypt user data for ransom
* D) Spread through email attachments

**42. Social engineering attacks target:**

* A) Human behavior and decision-making
* B) System vulnerabilities in software
* C) Wireless networks
* D) Backup systems

**43. Honeypots are:**

* A) Systems designed to attract and trap attackers
* B) Antivirus programs that scan for malware
* C) Password management tools
* D) Backup solutions for sensitive data

**44. Keyloggers often target:**

* A) Passwords and sensitive information
* B) Network infrastructure
* C) Encrypted files
* D) Backup systems

**45. A virus can be classified as:**

* A) Self-replicating malware that requires user intervention
* B) Malware that spreads automatically
* C) A type of spyware
* D) A hidden backdoor in systems

**46. Worms differ from viruses in that:**

* A) They do not need user action to spread
* B) They only infect executable files
* C) They hide in system root directories
* D) They cannot spread across networks

**47. Firewalls are primarily used to:**

* A) Monitor and block unauthorized traffic
* B) Encrypt network traffic
* C) Store sensitive data
* D) Detect keyloggers

**48. Black hat hackers are motivated by:**

* A) Financial gain or malicious intent
* B) Exposing vulnerabilities for ethical reasons
* C) Protecting corporate data
* D) Conducting legal penetration tests

**49. White hat hackers are typically involved in:**

* A) Developing malware
* B) Exposing vulnerabilities for security improvement
* C) Selling exploits to governments
* D) Disabling corporate firewalls

**50. Gray hat hackers are characterized by:**

* A) Breaking into systems without permission but not for malicious purposes
* B) Developing viruses and Trojans
* C) Only attacking government institutions
* D) Working directly for state-sponsored groups