? EASY (Q1–Q10)

Q1. A computer virus requires which condition to spread?
A. Network connectivity
B. User interaction or host file execution
C. Internet access
D. Administrative privilege

Q2. A worm differs from a virus because a worm:
A. Requires a host file
B. Is manually executed
C. Self-propagates over networks
D. Cannot spread

Q3. Boot sector viruses infect:
A. Application files
B. Operating system kernel
C. Boot records of storage media
D. Network packets

Q4. Macro viruses primarily target:
A. Operating systems
B. Firmware
C. Document files
D. Network services

Q5. Antivirus software primarily aims to:
A. Create malware
B. Detect and remove malicious code
C. Encrypt files
D. Optimize systems

Q6. Signature-based detection works by:
A. Monitoring behavior
B. Matching known malware patterns
C. Encrypting files
D. Blocking ports

Q7. Worms mainly affect which security objective?
A. Confidentiality
B. Integrity
C. Availability
D. Authentication

Q8. Stealth viruses attempt to:
A. Destroy hardware
B. Hide their presence
C. Encrypt networks
D. Improve performance

Q9. Antivirus updates are required to:
A. Improve UI
B. Detect new malware
C. Increase speed
D. Reduce disk usage

Q10. File-infector viruses attach to:
A. Boot sectors
B. Executable files
C. Network packets
D. Databases

□ MEDIUM (Q11–Q25)

Q11. Worm propagation is faster because worms:
A. Need user execution
B. Exploit network vulnerabilities
C. Depend on documents
D. Use encryption

Q12. Polymorphic viruses evade detection by:
A. Changing file size only
B. Modifying code signatures
C. Avoiding execution
D. Deleting themselves

Q13. Antivirus evasion techniques aim to:
A. Improve detection
B. Bypass security defenses
C. Increase transparency
D. Encrypt user data

Q14. Heuristic detection identifies malware based on:
A. Exact signatures
B. Suspicious characteristics
C. File size
D. Hash values

Q15. Behavioral detection focuses on:
A. Code syntax
B. Runtime actions
C. File headers
D. Hash databases

Q16. Macro viruses became popular because:
A. Operating systems were insecure
B. Office macros were trusted
C. Networks were slow
D. Encryption was weak

Q17. Metamorphic viruses are harder to detect because they:
A. Do not execute
B. Rewrite their own code
C. Use encryption only
D. Avoid files

Q18. Antivirus sandboxing works by:
A. Blocking traffic
B. Executing malware in isolation
C. Encrypting files
D. Logging events

Q19. Worms often cause:
A. Data theft only
B. Network congestion
C. Hardware damage
D. Authentication bypass

Q20. Virus infection may result in:
A. Performance degradation
B. Data corruption
C. System instability
D. All of the above

Q21. Signature-based detection fails against:
A. Known malware
B. Polymorphic malware
C. Static malware
D. Old viruses

Q22. Antivirus evasion using packing involves:
A. Compressing malware code
B. Encrypting network traffic
C. Blocking ports
D. Deleting signatures

Q23. Fileless malware detection relies more on:
A. Disk scanning
B. Memory and behavior analysis
C. Hash checking
D. File permissions

Q24. Worm outbreaks are difficult to control because they:
A. Require user execution
B. Spread automatically
C. Are easily detected
D. Use weak protocols

Q25. Antivirus software effectiveness improves with:
A. No updates
B. Regular updates and heuristics
C. Reduced scanning
D. Disabled sandboxing

🟥 HARD (Q26–Q40)

Q26. Virus vs worm distinction is critical for defense because:
A. Viruses are harmless
B. Worms spread without user interaction
C. Worms require documents
D. Viruses spread faster

Q27. Advanced antivirus evasion combines:
A. Encryption and obfuscation
B. Packing and polymorphism
C. Anti-debugging techniques
D. All of the above

Q28. Behavioral detection false positives occur when:
A. Legitimate software behaves unusually
B. Malware is static
C. Hash matches exactly
D. Signatures are updated

Q29. Rootkits assist viruses by:
A. Increasing speed
B. Hiding malware components
C. Encrypting networks
D. Blocking antivirus

Q30. Worm containment strategies include:
A. Signature updates only
B. Network segmentation and patching
C. User training only
D. Encryption

Q31. Antivirus sandboxing is limited because:
A. Malware may detect sandbox environments
B. It is too fast
C. It blocks all malware
D. It requires no resources

Q32. Metamorphic malware differs from polymorphic because it:
A. Encrypts payload only
B. Rewrites entire code structure
C. Uses fixed signatures
D. Avoids execution

Q33. Signature databases grow rapidly due to:
A. Hardware changes
B. New malware variants
C. Network upgrades
D. Software patches

Q34. Antivirus evasion via timing delays aims to:
A. Speed up execution
B. Bypass sandbox time limits
C. Improve stealth
D. Encrypt payload

Q35. Effective malware defense requires:
A. Antivirus alone
B. Defense-in-depth approach
C. Password policies only
D. Firewalls only

Q36. Worm traffic can be identified by:
A. Random scanning patterns
B. Normal user behavior
C. Encrypted packets
D. Low bandwidth usage

Q37. Behavioral detection complements signature detection by:
A. Replacing it completely
B. Detecting unknown malware
C. Increasing false positives only
D. Slowing systems

Q38. Malware detection accuracy improves when combining:
A. Signature and heuristic methods
B. Antivirus and firewalls only
C. IDS only
D. Encryption

Q39. Virus detection fails if malware:
A. Uses known signatures
B. Is polymorphic or metamorphic
C. Is file-based
D. Is executable

Q40. The ultimate goal of virus detection is to:
A. Increase scan speed
B. Prevent system compromise
C. Generate logs
D. Consume fewer resources