? EASY (Q1–Q10)

Q1. Malware reverse engineering primarily involves:
A. Writing malware
B. Analyzing malicious code behavior
C. Encrypting malware
D. Distributing malware

Q2. The main purpose of malware analysis is to:
A. Improve malware performance
B. Understand functionality and mitigate threats
C. Spread malware
D. Hide malware

Q3. A virus differs from a worm because a virus:
A. Self-propagates without interaction
B. Requires a host file or user action
C. Uses only networks
D. Is harmless

Q4. Ransomware primarily targets:
A. Network bandwidth
B. Data availability
C. Physical security
D. Authentication

Q5. Spyware is designed to:
A. Encrypt files
B. Monitor user activity secretly
C. Crash systems
D. Block network access

Q6. Botnets are mainly used for:
A. File backups
B. Coordinated attacks
C. System optimization
D. Encryption

Q7. Static malware analysis does NOT involve:
A. File hashes
B. String analysis
C. Executing malware
D. Header inspection

Q8. Dynamic malware analysis requires:
A. Source code
B. Execution in a controlled environment
C. No isolation
D. Production systems

Q9. Indicators of Compromise (IOCs) include:
A. File hashes and IP addresses
B. Password policies
C. Network speed
D. System uptime

Q10. Rootkits primarily aim to:
A. Encrypt data
B. Hide malicious presence
C. Improve performance
D. Patch vulnerabilities

□ MEDIUM (Q11–Q25)

Q11. Fileless malware primarily resides in:
A. Disk files
B. Memory
C. Boot sector
D. BIOS

Q12. Polymorphic malware evades detection by:
A. Changing functionality
B. Changing code appearance
C. Disabling antivirus
D. Avoiding execution

Q13. Metamorphic malware is harder to detect because it:
A. Encrypts payload
B. Rewrites its own code
C. Uses fixed signatures
D. Avoids files

Q14. Logic bombs are triggered by:
A. Network traffic
B. Specific conditions or events
C. User login
D. Antivirus scans

Q15. Ransomware-as-a-Service (RaaS) allows:
A. Free encryption
B. Malware distribution as a service
C. Antivirus testing
D. Secure backups

Q16. Advanced Persistent Threats (APTs) are characterized by:
A. Short-term attacks
B. Long-term targeted campaigns
C. Random scanning
D. No persistence

Q17. Static analysis tools help identify:
A. Runtime behavior
B. Embedded strings and imports
C. Network traffic
D. Registry changes

Q18. Dynamic analysis reveals:
A. Code syntax
B. Actual runtime behavior
C. File headers only
D. Hash values

Q19. Memory analysis is useful for detecting:
A. File permissions
B. In-memory malware artifacts
C. Disk usage
D. Network latency

Q20. Network traffic analysis helps identify:
A. CPU usage
B. Command and Control communication
C. File integrity
D. BIOS changes

Q21. Disassembly converts binaries into:
A. Source code
B. Assembly instructions
C. High-level language
D. Pseudocode only

Q22. Decompilation attempts to produce:
A. Assembly code
B. High-level source code
C. Machine code
D. Hex dumps

Q23. Packers are used by malware to:
A. Compress files for storage
B. Obfuscate malicious code
C. Improve execution speed
D. Patch vulnerabilities

Q24. Anti-debugging techniques aim to:
A. Improve performance
B. Prevent analysis
C. Encrypt traffic
D. Block execution

Q25. Anti-VM techniques detect:
A. User behavior
B. Virtualized environments
C. Encryption keys
D. Network latency

🟥 HARD (Q26–Q40)

Q26. Fileless malware increases detection difficulty because it:
A. Leaves no disk artifacts
B. Uses encryption only
C. Is slower
D. Requires reboot

Q27. Behavioral analysis is effective against:
A. Known malware only
B. Zero-day malware
C. Static malware only
D. Signed binaries

Q28. Polymorphic malware defeats which detection method most effectively?
A. Behavioral
B. Signature-based
C. Heuristic
D. Network-based

Q29. Metamorphic malware increases analysis complexity by:
A. Changing execution order
B. Altering code structure each generation
C. Using encryption only
D. Avoiding execution

Q30. APT malware typically prioritizes:
A. Speed
B. Stealth and persistence
C. Immediate impact
D. Visibility

Q31. Memory forensics can reveal:
A. Deleted registry keys only
B. Injected processes and hooks
C. Disk partitions
D. BIOS updates

Q32. Network-based IOCs include:
A. File hashes
B. IPs, domains, and URLs
C. File permissions
D. Registry paths

Q33. Sandboxing limitations arise when malware:
A. Is encrypted
B. Detects sandbox environments
C. Uses files
D. Is static

Q34. Reverse engineering malware assists defenders by:
A. Creating exploits
B. Developing detection signatures
C. Spreading malware
D. Improving malware

Q35. Malware targeting IoT is dangerous because IoT devices:
A. Are well-patched
B. Have limited security controls
C. Use strong encryption
D. Are rarely connected

Q36. AI-assisted malware increases threat because it:
A. Is easier to detect
B. Adapts to defenses dynamically
C. Is slower
D. Uses static logic

Q37. Malware lifecycle persistence is achieved through:
A. Temporary files only
B. Startup entries and scheduled tasks
C. Network packets
D. Encryption

Q38. Signature-based detection fails when malware:
A. Is well known
B. Is heavily obfuscated
C. Has fixed hashes
D. Is static

Q39. Effective malware mitigation requires:
A. Malware removal only
B. Detection, containment, and remediation
C. Antivirus updates only
D. Firewall rules only

Q40. The primary ethical requirement in malware analysis labs is:
A. Speed
B. Isolation and authorization
C. Public execution
D. Internet connectivity