? EASY (Q1–Q10)

Q1. Wrapping in malware refers to:
A. Encrypting network traffic
B. Hiding malicious code inside legitimate files
C. Compressing data
D. Signing executables

Q2. Trojan construction kits are used to:
A. Detect malware
B. Automate Trojan creation
C. Encrypt databases
D. Patch vulnerabilities

Q3. System file verification ensures:
A. Faster boot time
B. Integrity of system files
C. Higher bandwidth
D. Better UI

Q4. Hashing is primarily used for:
A. Encryption
B. Integrity checking
C. Authentication only
D. Compression

Q5. Trojan prevention focuses mainly on:
A. Speed
B. Detection and blocking
C. Exploitation
D. Obfuscation

Q6. Malware evasion techniques aim to:
A. Improve performance
B. Avoid detection
C. Encrypt databases
D. Patch systems

Q7. Polymorphic malware changes its:
A. Functionality
B. Code appearance
C. Target system
D. Payload intent

Q8. Metamorphic malware differs because it:
A. Uses encryption only
B. Rewrites its own code
C. Is fileless
D. Uses signatures

Q9. Anti-VM techniques help malware to:
A. Run faster
B. Detect sandbox environments
C. Encrypt files
D. Patch OS

Q10. System file changes without authorization indicate:
A. Normal updates
B. Possible compromise
C. Improved security
D. Optimization

□ MEDIUM (Q11–Q25)

Q11. Wrapping is dangerous because it:
A. Increases file size
B. Bypasses user suspicion
C. Slows execution
D. Improves encryption

Q12. Trojan kits reduce attack complexity by:
A. Manual coding
B. Automating malware creation
C. Detecting vulnerabilities
D. Encrypting payloads

Q13. Automated Trojan creation increases risk because:
A. It improves security
B. Low-skilled attackers can create malware
C. It is easily detected
D. It reduces attack surface

Q14. Host-based Trojan countermeasures include:
A. Network firewalls only
B. Antivirus and endpoint security
C. IDS only
D. VPN usage

Q15. Network-based Trojan prevention includes:
A. Strong passwords
B. Traffic inspection and IDS
C. File hashing
D. User training only

Q16. Obfuscation helps malware by:
A. Encrypting network traffic
B. Making code analysis difficult
C. Improving performance
D. Reducing size

Q17. Encryption in malware primarily protects:
A. Users
B. Malware payload
C. System files
D. Logs

Q18. Anti-debugging techniques prevent:
A. Network monitoring
B. Reverse engineering
C. Encryption
D. File access

Q19. Hash-based integrity checking works by:
A. Comparing file sizes
B. Comparing hash values
C. Checking timestamps
D. Checking permissions

Q20. System file verification is important after:
A. Software updates
B. Malware incidents
C. Power failures
D. Network outages

Q21. Trojan evasion techniques increase:
A. Detectability
B. Malware persistence
C. Security awareness
D. Encryption strength

Q22. Signature-based defenses struggle against:
A. Static malware
B. Polymorphic malware
C. Known threats
D. Unchanged code

Q23. Trojan kits often include:
A. Antivirus engines
B. Payload customization options
C. OS patches
D. IDS rules

Q24. Integrity monitoring tools alert when:
A. Network traffic spikes
B. Unauthorized file changes occur
C. Passwords expire
D. Users log in

Q25. User awareness helps prevent Trojans by:
A. Blocking traffic
B. Avoiding malicious downloads
C. Encrypting data
D. Updating OS

🟥 HARD (Q26–Q40)

Q26. Wrapping combined with social engineering increases success because:
A. Users ignore security
B. Malicious payload appears legitimate
C. Files are encrypted
D. IDS is bypassed

Q27. Trojan construction kits are a threat because they:
A. Require high expertise
B. Enable mass malware production
C. Improve detection
D. Limit payloads

Q28. Polymorphic malware evades detection by:
A. Changing signatures
B. Encrypting traffic
C. Disabling antivirus
D. Avoiding execution

Q29. Metamorphic malware is harder to detect because:
A. It rewrites code logic
B. It uses encryption only
C. It avoids files
D. It uses proxies

Q30. Anti-VM detection triggers malware to:
A. Execute payload
B. Stay dormant
C. Encrypt disk
D. Delete files

Q31. Integrity verification failure indicates:
A. Network attack
B. Unauthorized modification
C. Normal operation
D. Encryption success

Q32. Host-based integrity monitoring complements:
A. Antivirus alone
B. Defense-in-depth strategy
C. Firewalls only
D. Encryption

Q33. Trojan evasion techniques reduce effectiveness of:
A. Behavioral detection
B. Signature-based detection
C. Network IDS
D. All security controls

Q34. File verification tools rely heavily on:
A. File permissions
B. Cryptographic hashes
C. Encryption keys
D. Logs

Q35. Automated malware kits increase threat landscape by:
A. Reducing attacks
B. Lowering skill barrier
C. Increasing detection
D. Improving defenses

Q36. Anti-debugging checks include detecting:
A. CPU speed
B. Debugger presence
C. Network latency
D. File permissions

Q37. System file verification is ineffective if:
A. Hashes are protected
B. Baseline is compromised
C. Monitoring is continuous
D. Alerts are enabled

Q38. Defense against advanced Trojans requires:
A. Antivirus only
B. Layered security controls
C. Password changes
D. Firewalls only

Q39. Malware obfuscation increases analysis cost by:
A. Simplifying code
B. Increasing reverse engineering effort
C. Improving readability
D. Reducing execution

Q40. The best mitigation against Trojan kits is:
A. Network isolation only
B. Endpoint security + user awareness
C. Encryption only
D. Disabling internet