? EASY (Q1–Q10)

Q1. Password-cracking countermeasures primarily aim to:
A. Speed up login
B. Prevent unauthorized access
C. Simplify authentication
D. Remove encryption

Q2. Online password attacks require:
A. Physical access
B. Network connectivity
C. Malware installation
D. Disk access

Q3. Offline password attacks target:
A. Live authentication systems
B. Stored password hashes
C. Network traffic
D. Browser cookies

Q4. Keyloggers are used to:
A. Encrypt keystrokes
B. Capture user input
C. Block keyboards
D. Improve typing speed

Q5. Trojans differ from viruses because Trojans:
A. Self-replicate
B. Require user execution
C. Infect boot sectors
D. Spread automatically

Q6. A backdoor provides attackers with:
A. Encryption
B. Persistent unauthorized access
C. Network monitoring
D. Authentication

Q7. Overt channels are:
A. Hidden communications
B. Legitimate visible channels
C. Encrypted tunnels
D. Malware-only paths

Q8. Spyware primarily compromises:
A. Availability
B. Confidentiality
C. Integrity
D. Performance

Q9. Reverse-connecting Trojans initiate connections from:
A. Attacker to victim
B. Victim to attacker
C. Server to server
D. Client to client

Q10. Netcat can be used legitimately for:
A. Malware creation only
B. Network troubleshooting
C. Password cracking
D. OS exploitation

□ MEDIUM (Q11–Q25)

Q11. Strong password policies include:
A. Short passwords
B. Predictable patterns
C. Complexity and length
D. Reuse across systems

Q12. Salting passwords helps prevent:
A. Brute-force attacks
B. Rainbow table attacks
C. DoS attacks
D. Phishing

Q13. Multi-factor authentication improves security by:
A. Replacing passwords
B. Adding additional verification layers
C. Encrypting traffic
D. Blocking malware

Q14. Passive online attacks involve:
A. Intercepting authentication data
B. Sending login requests
C. Locking accounts
D. Modifying passwords

Q15. Active online attacks include:
A. Sniffing
B. Brute-force login attempts
C. Traffic analysis
D. Packet capture

Q16. Offline attacks are faster because they:
A. Use encryption
B. Avoid account lockouts
C. Require user interaction
D. Are detected by IDS

Q17. Hardware keyloggers are dangerous because they:
A. Are easy to detect
B. Bypass OS-level security
C. Require admin access
D. Encrypt data

Q18. Software keyloggers typically operate at:
A. Hardware layer
B. Application or OS level
C. Network layer
D. BIOS level

Q19. Persistence mechanisms ensure malware:
A. Executes only once
B. Survives reboots
C. Self-deletes
D. Avoids detection

Q20. Covert channels are difficult to detect because they:
A. Use standard protocols
B. Hide data within normal traffic
C. Use encryption only
D. Flood networks

Q21. Banking Trojans are designed to:
A. Improve transactions
B. Steal financial credentials
C. Encrypt files
D. Monitor performance

Q22. Downloader Trojans mainly:
A. Steal passwords
B. Install additional malware
C. Perform DDoS
D. Encrypt disks

Q23. Reverse-connecting Trojans evade firewalls because they:
A. Use UDP only
B. Initiate outbound connections
C. Disable firewalls
D. Use proxy servers

Q24. Indicators of Trojan infection include:
A. Faster system performance
B. Unexpected network connections
C. Improved stability
D. Reduced traffic

Q25. Netcat becomes malicious when used to:
A. Test connectivity
B. Open unauthorized shells
C. Transfer files legally
D. Monitor ports

🟥 HARD (Q26–Q40)

Q26. Password cracking countermeasures should combine:
A. Policies only
B. Technical and administrative controls
C. Encryption only
D. User training only

Q27. Online attacks are easier to detect because they:
A. Are encrypted
B. Generate authentication logs
C. Use offline tools
D. Avoid IDS

Q28. Offline attacks pose higher risk when:
A. Password hashes are leaked
B. MFA is enabled
C. Accounts are locked
D. Encryption is strong

Q29. Behavioral spyware detection focuses on:
A. Signatures only
B. Runtime activity patterns
C. Hash values
D. File size

Q30. Trojans often rely on social engineering to:
A. Self-replicate
B. Trick users into execution
C. Bypass encryption
D. Patch systems

Q31. Covert channels violate security by:
A. Blocking traffic
B. Bypassing policy controls
C. Encrypting data
D. Authenticating users

Q32. Polymorphic Trojans evade detection by:
A. Using fixed signatures
B. Changing code appearance
C. Disabling antivirus
D. Using plaintext

Q33. Reverse-connecting Trojans are especially effective against:
A. Air-gapped systems
B. NAT and firewall-protected networks
C. Offline machines
D. IDS systems

Q34. Netcat misuse is dangerous because it:
A. Encrypts traffic
B. Enables backdoor shells
C. Blocks ports
D. Detects malware

Q35. Trojan indicators may be missed because attackers use:
A. No persistence
B. Legitimate system processes
C. Visible pop-ups
D. High CPU usage

Q36. Effective Trojan defense requires:
A. Antivirus only
B. Defense-in-depth strategy
C. Password changes only
D. Disabling internet

Q37. Offline password cracking effectiveness depends on:
A. Network latency
B. Hash algorithm strength
C. IDS rules
D. Firewall policies

Q38. Spyware compromises privacy primarily by:
A. Encrypting files
B. Exfiltrating personal data
C. Blocking applications
D. Crashing systems

Q39. Trojan backdoors differ from worms because they:
A. Spread automatically
B. Require user assistance
C. Exploit network vulnerabilities
D. Self-replicate

Q40. The most reliable indicator of compromise is:
A. Antivirus alerts alone
B. Correlated system and network anomalies
C. User complaints
D. File size increase