◇ EASY (Q1–Q10)

Q1. Authentication is the process of:
A. Granting permissions
B. Verifying identity
C. Encrypting data
D. Auditing access

Q2. Which is an example of a single-factor authentication method?
A. Password only
B. Password + OTP
C. Smart card + PIN
D. Biometrics + OTP

Q3. Multi-factor authentication (MFA) combines factors from:
A. Same category only
B. At least two different categories
C. Passwords only
D. Tokens only

Q4. Which factor category does a fingerprint belong to?
A. Something you know
B. Something you have
C. Something you are
D. Somewhere you are

Q5. Single Sign-On (SSO) allows users to:
A. Use multiple passwords
B. Authenticate once and access multiple services
C. Bypass authentication
D. Encrypt sessions automatically

Q6. OAuth is primarily used for:
A. User authentication
B. Password storage
C. Delegated authorization
D. File encryption

Q7. OpenID is mainly used for:
A. Authorization
B. Authentication
C. Encryption
D. Key exchange

Q8. Which authentication method is MOST vulnerable to shoulder surfing?
A. OTP

B. Graphical password
C. Hardware token
D. Biometric fingerprint

Q9. Which factor BEST improves security against password compromise?
A. Longer usernames
B. MFA
C. Password hints
D. Encryption only

Q10. Which protocol is commonly used to implement enterprise SSO?
A. FTP
B. SMTP
C. SAML
D. ICMP

◇ MEDIUM (Q11–Q25)

Q11. Which authentication factor is represented by a smart card?
A. Something you know
B. Something you have
C. Something you are
D. Something you do

Q12. Which MFA combination is STRONGEST?
A. Password + security question
B. Password + OTP
C. OTP + CAPTCHA
D. Fingerprint + smart card

Q13. Which SSO benefit MOST improves user productivity?
A. Strong encryption
B. Reduced password fatigue
C. Hardware acceleration
D. Centralized logging

Q14. Which risk is MOST associated with poorly implemented SSO?
A. Network latency
B. Single point of failure
C. Weak hashing
D. Key reuse

Q15. Which statement BEST differentiates OpenID from OAuth?
A. OpenID is for authorization; OAuth is for authentication

B. OpenID is for authentication; OAuth is for authorization
C. Both are encryption protocols
D. Both replace MFA

Q16. Which OAuth role owns the protected resource?
A. Authorization server
B. Client
C. Resource owner
D. Resource server

Q17. Which OAuth token is used to access protected APIs?
A. Refresh token
B. ID token
C. Access token
D. Session cookie

Q18. Which attack targets reuse of stolen session identifiers?
A. Brute force
B. Session fixation
C. SQL injection
D. Replay attack

Q19. Which authentication approach reduces password storage risks on servers?
A. Plain password auth
B. OAuth-based login
C. Static passwords
D. Local accounts

Q20. Which graphical password weakness affects usability?
A. High entropy
B. Memorability issues
C. Cryptographic strength
D. Key length

Q21. Which MFA factor is MOST resistant to phishing?
A. Password
B. OTP via SMS
C. Hardware security key
D. Knowledge-based questions

Q22. Which SSO protocol uses XML-based assertions?
A. OAuth
B. OpenID Connect
C. SAML
D. Kerberos

Q23. Which OpenID Connect token contains user identity claims?
A. Access token
B. Refresh token
C. ID token
D. CSRF token

Q24. Which threat is MOST mitigated by MFA?
A. Insider misuse
B. Credential stuffing
C. DoS attacks
D. Traffic analysis

Q25. Which authentication system is MOST suitable for cloud-native applications?
A. Local OS accounts
B. LDAP only
C. OAuth 2.0 / OpenID Connect
D. BIOS authentication

◇ HARD (Q26–Q40)

Q26. Which scenario BEST demonstrates delegated authorization using OAuth?
A. User logs into email
B. App accesses user’s cloud storage without password
C. Password reset flow
D. Biometric login

Q27. Which MFA deployment risk arises if backup codes are poorly managed?
A. Increased latency
B. Authentication bypass
C. Hash collision
D. Token expiration

Q28. Which authentication failure MOST threatens SSO environments?
A. Password expiry
B. Central identity provider compromise
C. User logout
D. Network congestion

Q29. Which OAuth grant type is MOST appropriate for server-to-server communication?
A. Authorization code
B. Implicit
C. Client credentials
D. Resource owner password

Q30. Which graphical password attack exploits observation of login behavior?
A. Brute force
B. Shoulder surfing
C. Replay attack
D. Dictionary attack

Q31. Which OpenID Connect improvement MOST enhances security over legacy OpenID?
A. XML assertions
B. JSON-based tokens with signatures
C. Plain HTTP usage
D. Password sharing

Q32. Which MFA factor combination BEST aligns with Zero Trust principles?
A. Password only
B. Password + CAPTCHA
C. Device certificate + biometrics
D. Username + security question

Q33. Which attack is MOST effective against SMS-based OTP?
A. Collision attack
B. SIM-swap attack
C. Hash preimage attack
D. Padding oracle

Q34. Which identity system risk arises from long-lived access tokens?
A. Token leakage impact
B. Faster authentication
C. Reduced storage
D. Improved availability

Q35. Which authentication mechanism BEST supports passwordless login?
A. Static passwords
B. Security questions
C. FIDO2 / WebAuthn
D. Graphical passwords

Q36. Which OAuth security best practice mitigates token theft?
A. Long-lived tokens
B. Token binding / PKCE
C. Plain redirects
D. Client secrets in URLs

Q37. Which SSO protocol natively integrates with Windows Active Directory?
A. OAuth
B. OpenID

C. Kerberos
D. RADIUS

Q38. Which MFA usability issue MOST affects user adoption?
A. Strong cryptography
B. Additional login steps
C. Hardware security
D. Audit logging

Q39. Which authentication design mistake MOST undermines security?
A. Using open standards
B. Implementing custom authentication logic
C. Using MFA
D. Centralized identity

Q40. Which statement BEST summarizes modern authentication systems?
A. Passwords alone are sufficient
B. MFA + federated identity improves security and usability
C. Encryption replaces authentication
D. SSO eliminates all risks