◇ EASY (Q1–Q10)

Q1. Authentication protocols are primarily designed to:
A. Encrypt data
B. Verify identity securely
C. Store passwords
D. Manage networks

Q2. Which protocol is commonly used for centralized authentication in enterprise networks?
A. FTP
B. Kerberos
C. HTTP
D. SMTP

Q3. FIDO authentication aims to eliminate:
A. Encryption
B. Certificates
C. Passwords
D. Tokens

Q4. Zero Trust Architecture is based on which core principle?
A. Trust internal networks
B. Trust but verify
C. Never trust, always verify
D. Trust certificates only

Q5. Which authentication factor is primarily used in FIDO?
A. Password
B. Biometric or hardware-based
C. Knowledge-based questions
D. CAPTCHA

Q6. Which protocol uses tickets for authentication?
A. OAuth
B. Kerberos
C. LDAP
D. RADIUS

Q7. Which Zero Trust component continuously evaluates access requests?
A. Firewall
B. Policy engine
C. IDS
D. VPN

Q8. Which FIDO standard supports web-based authentication?
A. FIDO UAF

B. FIDO U2F
C. WebAuthn
D. SAML

Q9. Which protocol commonly works with Kerberos for directory authentication?
A. FTP
B. SMTP
C. LDAP
D. ICMP

Q10. Zero Trust focuses MOST on protecting:
A. Perimeter only
B. Endpoints only
C. Data and identities
D. Network devices

◇ MEDIUM (Q11–Q25)

Q11. Which authentication protocol provides mutual authentication by default?
A. RADIUS
B. Kerberos
C. PAP
D. CHAP

Q12. Which attack does Kerberos MOST effectively mitigate?
A. Replay attack
B. Brute-force attack
C. Side-channel attack
D. Phishing attack

Q13. Which FIDO component securely stores private keys?
A. Server database
B. Authentication server
C. Authenticator device
D. Browser cache

Q14. Which Zero Trust concept replaces traditional network trust boundaries?
A. VPN
B. Micro-segmentation
C. NAT
D. DMZ

Q15. Which protocol supports passwordless authentication using public-key cryptography?
A. LDAP

B. RADIUS
C. FIDO2
D. PAP

Q16. Which Kerberos ticket allows access to specific services?
A. Authentication Service Ticket
B. Ticket Granting Ticket
C. Service Ticket
D. Session Key

Q17. Which Zero Trust pillar ensures users have only necessary access?
A. Visibility
B. Least privilege
C. Availability
D. Encryption

Q18. Which authentication protocol is MOST vulnerable to credential replay?
A. Kerberos
B. OAuth
C. PAP
D. FIDO

Q19. Which FIDO advantage MOST improves resistance to phishing?
A. Password complexity
B. Server-side key storage
C. Origin binding
D. Centralized identity

Q20. Which Zero Trust practice continuously verifies device posture?
A. Static ACLs
B. Continuous authentication
C. VLAN segmentation
D. NAT

Q21. Which authentication protocol uses shared secrets and challenge-response?
A. PAP
B. CHAP
C. Kerberos
D. OAuth

Q22. Which FIDO standard supports cross-platform authentication?
A. UAF
B. U2F
C. FIDO2
D. OTP

Q23. Which Zero Trust model assumes breach and limits blast radius?
A. Perimeter security
B. Defense in depth
C. Assume breach
D. Trust zones

Q24. Which authentication protocol is commonly used for network access control (Wi-Fi, VPN)?
A. RADIUS
B. Kerberos
C. OpenID
D. TLS

Q25. Which Zero Trust outcome MOST improves insider threat mitigation?
A. Strong encryption
B. Continuous monitoring and access re-evaluation
C. Firewalls
D. NAT

◇ HARD (Q26–Q40)

Q26. Which authentication failure MOST undermines Kerberos security?
A. Long passwords
B. Clock synchronization issues
C. Strong encryption
D. Ticket expiration

Q27. Which attack is MOST difficult against FIDO-based authentication?
A. Brute-force
B. Phishing
C. Replay
D. Shoulder surfing

Q28. Which Zero Trust component makes real-time access decisions?
A. Policy enforcement point
B. Policy engine
C. Firewall
D. Proxy

Q29. Which Kerberos weakness requires secure time synchronization?
A. Dictionary attacks
B. Replay attacks
C. MITM attacks
D. Side-channel attacks

Q30. Which FIDO implementation risk arises if authenticators are lost?
A. Loss of encryption
B. Account lockout without recovery
C. Hash collision
D. Network failure

Q31. Which Zero Trust architecture principle enforces segmentation at workload level?
A. Perimeter security
B. Macro-segmentation
C. Micro-segmentation
D. VLAN tagging

Q32. Which authentication protocol relies on a centralized Key Distribution Center (KDC)?
A. OAuth
B. Kerberos
C. RADIUS
D. LDAP

Q33. Which Zero Trust strategy MOST reduces lateral movement?
A. VPN tunneling
B. Micro-segmentation
C. Strong hashing
D. NAT

Q34. Which FIDO design choice prevents credential reuse across sites?
A. Long passwords
B. Origin-bound keys
C. Centralized authentication
D. Encryption

Q35. Which authentication protocol is MOST susceptible to offline password guessing?
A. Kerberos
B. FIDO
C. PAP
D. OAuth

Q36. Which Zero Trust telemetry source is MOST critical for adaptive access?
A. IP address only
B. User behavior and device posture
C. MAC address
D. Network bandwidth

Q37. Which Kerberos ticket compromise exposes ALL services in a session?
A. Service Ticket
B. Authentication Service Ticket

C. Ticket Granting Ticket
D. Session key

Q38. Which Zero Trust mistake MOST undermines its effectiveness?
A. Continuous verification
B. Static trust assumptions
C. Micro-segmentation
D. Strong identity

Q39. Which FIDO deployment BEST supports enterprise passwordless strategy?
A. Software-only OTP
B. Hardware-backed FIDO2 authenticators
C. SMS-based MFA
D. Graphical passwords

Q40. Which statement BEST summarizes Zero Trust and FIDO synergy?
A. They replace PKI
B. They reduce reliance on passwords and network trust
C. They eliminate encryption
D. They prevent all attacks