? EASY (Q1–Q10)

Q1. Web server hacking primarily targets:
A. Physical security
B. Server software and configurations
C. User passwords only
D. Network cables

Q2. A common web server vulnerability is:
A. SQL Injection
B. Weak file permissions
C. Physical theft
D. Power failure

Q3. Web-based password cracking typically exploits:
A. Hardware flaws
B. Weak authentication mechanisms
C. Disk errors
D. BIOS vulnerabilities

Q4. Wireless hacking targets:
A. Fiber optics
B. Radio frequency communication
C. Wired Ethernet only
D. Bluetooth only

Q5. SSID stands for:
A. Secure System Identifier
B. Service Set Identifier
C. System Security ID
D. Secure Session ID

Q6. WEP encryption is considered insecure because it:
A. Uses long keys
B. Uses weak initialization vectors
C. Uses AES
D. Is hardware-based

Q7. WPA improves security by using:
A. Static keys
B. TKIP or AES encryption
C. No authentication
D. Plaintext passwords

Q8. Wireless sniffers are used to:
A. Block signals
B. Capture wireless traffic
C. Encrypt packets
D. Authenticate users

Q9. MAC spoofing involves:
A. Encrypting MAC addresses
B. Changing MAC address identity
C. Blocking MAC traffic
D. Monitoring MAC tables

Q10. Default credentials on web servers lead to:
A. Better performance
B. Unauthorized access
C. Improved logging
D. Faster authentication

□ MEDIUM (Q11–Q25)

Q11. Web server attack surface includes:
A. OS, services, and applications
B. Network cables
C. Power supply
D. User devices

Q12. Directory traversal vulnerabilities allow attackers to:
A. Modify DNS records
B. Access restricted files
C. Crash servers
D. Encrypt data

Q13. Brute-force web password attacks exploit:
A. Firewall misconfigurations
B. Weak password policies
C. Strong encryption
D. Secure cookies

Q14. Wireless sniffing is easier when:
A. WPA3 is enabled
B. Traffic is unencrypted
C. MAC filtering is active
D. IDS is present

Q15. Hidden SSIDs:
A. Cannot be detected
B. Still appear in wireless traffic
C. Use strong encryption
D. Prevent attacks

Q16. WEP cracking is possible because:
A. Keys are long
B. IV reuse occurs
C. WPA is enabled
D. Traffic is encrypted

Q17. WPA-PSK security depends heavily on:
A. Hardware
B. Passphrase strength
C. SSID length
D. Channel number

Q18. Wireless hacking often begins with:
A. Exploitation
B. Reconnaissance and sniffing
C. Privilege escalation
D. Data exfiltration

Q19. MAC filtering is weak because:
A. MAC addresses can be spoofed
B. It encrypts traffic
C. It blocks traffic
D. It is hardware-based

Q20. Web application vulnerabilities differ from server vulnerabilities because they:
A. Affect only hardware
B. Exist in application logic
C. Are always network-based
D. Are physical

Q21. Web-based password cracking detection relies on:
A. File integrity checks
B. Login attempt monitoring
C. Encryption
D. Backups

Q22. Wireless attacks mainly affect:
A. Availability only
B. Confidentiality and integrity
C. Authentication only
D. Physical security

Q23. WPA handshake capture is used to:
A. Encrypt traffic
B. Attempt offline password attacks
C. Block wireless access
D. Hide SSID

Q24. Rogue access points are dangerous because they:
A. Improve connectivity
B. Perform MITM attacks
C. Encrypt traffic
D. Block networks

Q25. Secure wireless configuration includes:
A. WEP encryption
B. Strong WPA2/WPA3 passwords
C. Open networks
D. Hidden SSIDs only

🔴 HARD (Q26–Q40)

Q26. Web server hardening reduces attack surface by:
A. Adding services
B. Removing unnecessary services
C. Disabling firewalls
D. Using default settings

Q27. Web-based password attacks scale when:
A. CAPTCHA is enabled
B. Rate limiting is absent
C. MFA is enforced
D. HTTPS is enabled

Q28. Wireless sniffing combined with deauthentication enables:
A. Encryption
B. Forced handshake capture
C. IDS detection
D. Network isolation

Q29. WEP cracking uses statistical attacks because:
A. Keys are long
B. IVs are reused frequently
C. Traffic is encrypted
D. WPA is used

Q30. WPA2-Enterprise improves security by using:
A. Shared keys
B. Individual user authentication
C. Static passwords
D. MAC filtering

Q31. Web application password cracking is mitigated by:
A. Logging only
B. Account lockout and MFA
C. Encryption only
D. Hiding login pages

Q32. Wireless sniffers can detect hidden SSIDs because:
A. SSIDs are encrypted
B. Clients reveal SSIDs during association
C. AP hides traffic
D. Firewalls block signals

Q33. MAC spoofing bypasses security by:
A. Encrypting MACs
B. Imitating allowed devices
C. Blocking access points
D. Detecting traffic

Q34. Wireless attacks are harder to trace because:
A. Signals are invisible
B. Attackers can operate anonymously
C. Logs are perfect
D. Encryption blocks traffic

Q35. Web server exploitation often leads to:
A. Limited access
B. Full system compromise
C. No impact
D. Improved security

Q36. Wireless IDS helps defend by:
A. Blocking signals
B. Detecting rogue APs and attacks
C. Encrypting traffic
D. Spoofing MACs

Q37. WPA3 improves over WPA2 by adding:
A. WEP compatibility
B. Stronger handshake protection
C. Static keys
D. No encryption

Q38. Web application vulnerabilities persist because:
A. Hardware issues
B. Poor input validation and logic flaws
C. Network speed
D. Power failures

Q39. Wireless attack surface increases with:
A. Fewer APs
B. Poor configuration and open networks
C. Strong encryption
D. IDS deployment

Q40. Defense against web and wireless attacks requires:
A. Single control
B. Layered security controls
C. Antivirus only
D. Physical security only