# ? EASY (Q1–Q10)

**Q1. TCP flags are used to:**
A. Encrypt packets
B. Control TCP connection behavior
C. Authenticate users
D. Compress data

**Q2. Which TCP flag initiates a connection?**
A. ACK
B. FIN
C. SYN
D. RST

**Q3. Banner grabbing is used to identify:**
A. User passwords
B. Service and OS information
C. Encryption keys
D. Firewall rules

**Q4. Proxy servers help attackers by providing:**
A. Encryption
B. Anonymity
C. Authentication
D. Integrity

**Q5. Enumeration is the process of:**
A. Crashing services
B. Gathering detailed system information
C. Encrypting data
D. Blocking ports

**Q6. Password cracking attempts to:**
A. Encrypt passwords
B. Recover plaintext passwords
C. Reset user accounts
D. Disable authentication

**Q7. IP spoofing involves:**
A. Encrypting IP addresses
B. Forging source IP address
C. Blocking IP packets
D. Assigning new IPs

**Q8. SMB is mainly used for:**
A. Email transmission
B. File and printer sharing
C. Web browsing
D. DNS resolution

**Q9. DDoS attacks mainly target:**
A. Confidentiality
B. Integrity
C. Availability
D. Authentication

**Q10. NetBIOS attacks primarily affect:**
A. Linux systems
B. Windows networking
C. Mobile devices
D. Databases

---

# □ MEDIUM (Q11–Q25)

**Q11. ACK flag in TCP indicates:**
A. Connection termination
B. Acknowledgment of received data
C. Urgent data
D. Connection reset

**Q12. OS fingerprinting helps attackers to:**
A. Encrypt data
B. Choose appropriate exploits
C. Block services
D. Increase bandwidth

**Q13. HTTP tunneling allows attackers to:**
A. Bypass firewall restrictions
B. Encrypt traffic
C. Authenticate users
D. Compress data

**Q14. Enumeration usually follows which phase?**
A. Exploitation
B. Foot-printing
C. Scanning
D. Covering tracks

**Q15. Dictionary attacks rely on:**
A. All possible combinations
B. Predefined wordlists
C. Rainbow tables only
D. GPU acceleration

**Q16. Windows password hashes are often stored in:**
A. BIOS
B. SAM database
C. Registry backup
D. Page file

**Q17. SMB relay attacks exploit:**
A. Weak encryption
B. Trust relationships
C. Packet fragmentation
D. DNS spoofing

**Q18. NetBIOS DoS attacks typically flood:**
A. Port 80
B. Port 21
C. Port 137
D. Port 443

**Q19. Enumeration increases attack success because it:**
A. Reduces noise
B. Reveals user and service details
C. Encrypts traffic
D. Blocks defenses

**Q20. HTTP tunneling is often used to:**
A. Increase latency
B. Hide malicious traffic
C. Authenticate sessions
D. Patch vulnerabilities

**Q21. Brute-force attacks differ from dictionary attacks because they:**
A. Are faster
B. Try all combinations
C. Use wordlists
D. Use hashes only

**Q22. SMB logon redirection tricks victims into:**
A. Logging out
B. Sending credentials to attacker
C. Resetting passwords
D. Encrypting files

**Q23. FIN flag in TCP indicates:**
A. Data transfer
B. Connection termination
C. Urgent data
D. Reset request

**Q24. Banner grabbing can be performed using:**
A. Telnet or Netcat
B. Hashcat
C. Metasploit only
D. Wireshark only

**Q25. DDoS attacks differ from DoS because they:**
A. Use one source
B. Use multiple distributed sources
C. Are harmless
D. Use encryption

---

# 🟥 HARD (Q26–Q40)

**Q26. SYN flooding exploits TCP by:**
A. Completing handshakes
B. Leaving half-open connections
C. Closing connections quickly
D. Encrypting packets

**Q27. NULL and XMAS scans evade detection by:**
A. Using valid handshakes
B. Sending abnormal TCP flags
C. Encrypting payloads
D. Flooding traffic

**Q28. Idle scan requires:**
A. Proxy server
B. Zombie host with predictable IPID
C. VPN tunnel
D. DNS server

**Q29. SMB relay MITM attacks are mitigated by:**
A. Disabling SMB signing
B. Enabling SMB signing
C. Using HTTP only
D. Removing firewalls

**Q30. Enumeration is dangerous because it:**
A. Consumes bandwidth
B. Reveals attack surface details
C. Encrypts services
D. Blocks ports

**Q31. Password cracking success depends heavily on:**
A. Network speed
B. Password complexity
C. Firewall rules
D. IDS signatures

**Q32. HTTP tunneling traffic is difficult to detect because it:**
A. Uses standard ports
B. Mimics normal web traffic
C. Is encrypted
D. Is blocked by default

**Q33. IP spoofing is difficult over TCP because:**
A. TCP uses UDP
B. Three-way handshake validation
C. Encryption
D. Authentication headers

**Q34. Enumeration should be limited during ethical hacking because it:**
A. Is illegal
B. Can expose sensitive information
C. Requires encryption
D. Breaks hardware

**Q35. SMB attacks are more common in:**
A. Linux servers
B. Windows-based networks
C. Mobile networks
D. Cloud containers

**Q36. Password cracking countermeasures include:**
A. Weak passwords
B. Account lockout policies
C. Disabling logging
D. Plaintext storage

**Q37. DDoS botnets are controlled using:**
A. IDS
B. Command and Control servers
C. Firewalls
D. Proxies

**Q38. Banner information leakage increases risk by:**
A. Improving availability
B. Revealing exploitable versions
C. Encrypting traffic
D. Blocking attackers

**Q39. Enumeration without authorization is:**
A. Ethical
B. Legal
C. Illegal
D. Mandatory

**Q40. Effective defense against DDoS includes:**
A. Strong passwords
B. Traffic filtering and rate limiting
C. Code obfuscation
D. User training only