? EASY (Q1–Q10)

Q1. A hacker who works to improve security legally is called:
A. Black hat
B. Grey hat
C. White hat
D. Script kiddie

Q2. Hackers who use pre-written tools without deep knowledge are:
A. Ethical hackers
B. Script kiddies
C. Hacktivists
D. Insiders

Q3. Black hat hackers primarily aim for:
A. System hardening
B. Financial or malicious gain
C. Security audits
D. Compliance

Q4. Red Team focuses mainly on:
A. Defense strategies
B. Simulating attacks
C. Writing policies
D. User training

Q5. Blue Team is responsible for:
A. Launching attacks
B. Defending and monitoring systems
C. Developing exploits
D. Writing malware

Q6. Grey Team combines:
A. Legal and illegal actions
B. Attack and defense roles
C. Physical and cyber security
D. Policy and compliance

Q7. Ethical hackers must have:
A. Criminal intent
B. Authorization
C. Hidden identity
D. No documentation

Q8. Insider threats originate from:
A. External attackers
B. Internal trusted users
C. Hacktivists
D. Script kiddies

Q9. Hacktivists are motivated mainly by:
A. Curiosity
B. Political or social causes
C. Skill improvement
D. Financial gain

Q10. Which factor balances security and usability?
A. CIA Triad
B. Security-Functionality-Ease triangle
C. OSI model
D. TCP/IP stack

□ MEDIUM (Q11–Q25)

Q11. Ethical hackers differ from crackers mainly in:
A. Tools used
B. Legal authorization
C. Technical skills
D. Network access

Q12. Red Team exercises help organizations to:
A. Increase bandwidth
B. Identify real-world attack weaknesses
C. Replace firewalls
D. Train programmers

Q13. Blue Team activities include:
A. Exploitation
B. Incident response
C. Social engineering
D. Malware creation

Q14. Grey Team members primarily:
A. Attack only
B. Defend only
C. Observe and assess both sides
D. Write policies

Q15. Script kiddies are dangerous because they:
A. Write advanced malware
B. Use powerful tools irresponsibly
C. Have insider access
D. Bypass laws

Q16. Attacker goals often include:
A. Data theft
B. Financial gain
C. Service disruption
D. All of the above

Q17. Espionage-motivated attackers usually target:
A. Gaming servers
B. Government and enterprises
C. Home users
D. Open-source projects

Q18. Reputation damage attacks often involve:
A. DDoS or defacement
B. Password cracking
C. Encryption
D. Hardware theft

Q19. Security-Functionality-Ease triangle highlights:
A. Perfect security
B. Trade-offs between usability and protection
C. Network design
D. Malware analysis

Q20. Increasing security usually results in:
A. Higher usability
B. Reduced functionality
C. No impact
D. Better performance

Q21. Ethical hackers must document:
A. Only successful exploits
B. Vulnerabilities and remediation
C. User credentials
D. Malware code

Q22. Insider threats are difficult to detect because:
A. They use malware
B. They have legitimate access
C. They use encryption
D. They avoid networks

Q23. Which certification is widely known for ethical hacking?
A. CEH
B. CCNA
C. ITIL
D. PMP

Q24. Soft skills for ethical hackers include:
A. Programming only
B. Communication and reporting
C. Hardware repair
D. Marketing

Q25. Grey-hat hacking is risky because it:
A. Is fully legal
B. Operates in legal ambiguity
C. Requires permission
D. Is always ethical

🟥 HARD (Q26–Q40)

Q26. Red Team assessments are most effective when:
A. Conducted openly
B. Simulate real attacker behavior
C. Avoid documentation
D. Ignore defenses

Q27. Blue Team success depends heavily on:
A. Offensive tools
B. Monitoring and response capability
C. Exploit development
D. Social engineering

Q28. Hacktivist attacks often aim to:
A. Steal credentials
B. Spread ideology
C. Improve security
D. Test systems

Q29. Advanced persistent attackers focus on:
A. Short-term disruption
B. Long-term undetected access
C. Random attacks
D. Script-based exploits

Q30. Balancing security and usability requires:
A. Eliminating controls
B. Risk-based decisions
C. Maximum restrictions
D. No user input

Q31. Ethical hacking programs fail when organizations:
A. Allow testing
B. Ignore remediation
C. Document findings
D. Train staff

Q32. Skill progression for ethical hackers should include:
A. Only tools
B. Networking, OS, and programming
C. Social media skills only
D. Hardware design

Q33. Attacker sophistication is increasing due to:
A. Automation and toolkits
B. Strong laws
C. User awareness
D. Network upgrades

Q34. Red-Blue team collaboration improves:
A. Attack success
B. Overall security posture
C. Malware creation
D. Legal compliance only

Q35. Ethical hacking limitations include:
A. No detection
B. Scope restrictions
C. Unlimited access
D. Automatic fixes

Q36. Crackers typically ignore:
A. Laws and ethics
B. Vulnerabilities
C. Exploits
D. Targets

Q37. Security triangle imbalance often leads to:
A. User satisfaction
B. Increased attacks or misuse
C. Faster systems
D. Better UX

Q38. Skilled ethical hackers reduce organizational risk by:
A. Publishing exploits
B. Proactively identifying weaknesses
C. Hiding vulnerabilities
D. Bypassing policies

Q39. Attacker goals help defenders by:
A. Confusing strategy
B. Improving threat modeling
C. Reducing security
D. Eliminating attacks

Q40. Ethical hacking success is measured by:
A. Number of exploits
B. Improved security posture
C. System crashes
D. User lockouts