? EASY (Q1–Q10)

Q1. Cyber crime refers to crimes committed using:
A. Physical force
B. Computer systems and networks
C. Mechanical devices
D. Electrical circuits

Q2. Hacking is legally permitted when performed:
A. Without permission
B. For personal gain
C. With proper authorization
D. Secretly

Q3. Which cyber crime involves deceiving users to obtain credentials?
A. Sniffing
B. Phishing
C. DoS
D. Spoofing

Q4. Ethical hacking is conducted to:
A. Steal data
B. Test and improve security
C. Damage systems
D. Bypass laws

Q5. Which law in India addresses cyber crimes?
A. IPC only
B. IT Act, 2000
C. Contract Act
D. Evidence Act

Q6. Obscenity on the internet primarily affects:
A. Network performance
B. Social ethics and law
C. Encryption strength
D. Hardware reliability

Q7. Which hacker type operates with malicious intent?
A. White hat
B. Black hat
C. Grey hat
D. Ethical hacker

Q8. Malware creation is an example of:
A. Ethical hacking
B. Cyber crime
C. Security audit
D. Penetration testing

Q9. International cyber crime regulation is complex due to:
A. Hardware limitations
B. Cross-border jurisdiction
C. Encryption usage
D. Network speed

Q10. Ethical hacking follows:
A. Criminal intent
B. Legal and ethical standards
C. Hidden identity
D. Anonymous reporting

□ MEDIUM (Q11–Q25)

Q11. Cyber crimes commonly target:
A. Only individuals
B. Only organizations
C. Both individuals and organizations
D. Only governments

Q12. E-commerce fraud is an example of:
A. Physical crime
B. Cyber crime
C. Environmental crime
D. Administrative crime

Q13. Freedom of expression online must be balanced with:
A. Network performance
B. Legal regulation
C. Encryption strength
D. Hardware cost

Q14. Which IPC section deals with cheating and fraud?
A. Section 66
B. Section 420
C. Section 43
D. Section 65

Q15. International cyber law aims to:
A. Eliminate all cyber crimes
B. Enable cross-border cooperation
C. Replace national laws
D. Control the internet

Q16. Obscenity laws on the internet focus on:
A. Content distribution
B. Server security
C. Encryption protocols
D. Network topology

Q17. Ethical hackers are also known as:
A. Crackers
B. White-hat hackers
C. Script kiddies
D. Hacktivists

Q18. Vulnerability in ethical hacking refers to:
A. A threat actor
B. A system weakness
C. A legal loophole
D. A security policy

Q19. Exploit is best defined as:
A. Security patch
B. Technique to use a vulnerability
C. Malware type
D. Defense mechanism

Q20. Reconnaissance phase in ethical hacking involves:
A. Exploitation
B. Information gathering
C. Maintaining access
D. Reporting

Q21. Malware is often used to achieve:
A. Security auditing
B. Unauthorized access
C. Encryption
D. Compliance

Q22. Which cyber crime affects privacy the most?
A. Identity theft
B. DoS
C. Website defacement
D. Spamming

Q23. Ethical hacking reports must include:
A. Attack scripts only
B. Vulnerabilities and mitigation
C. Exploit code
D. User credentials

Q24. Hacking without permission is:
A. Legal
B. Ethical
C. Illegal
D. Auditable

Q25. Cyber law ensures:
A. Faster internet
B. Legal framework for digital activities
C. Better hardware
D. Strong passwords

🔴 HARD (Q26–Q40)

Q26. Cyber crimes in cloud environments increase due to:
A. Centralized storage
B. Shared responsibility model
C. Weak hardware
D. Slow networks

Q27. Cross-border cyber crimes are difficult to prosecute because:
A. Encryption blocks evidence
B. Different national laws apply
C. Hackers are anonymous
D. Networks are slow

Q28. Ethical hacking differs from malicious hacking mainly in:
A. Tools used
B. Intent and authorization
C. Skill level
D. Network access

Q29. Obscenity detection online faces challenges due to:
A. Volume of content
B. Cultural differences
C. Automated distribution
D. All of the above

Q30. Grey-hat hackers operate:
A. Fully legally
B. Fully illegally
C. Between ethical and illegal boundaries
D. Only for governments

Q31. Ethical hacking phases end with:
A. Exploitation
B. Maintaining access
C. Covering tracks
D. Reporting

Q32. Hacktivism is motivated by:
A. Financial gain
B. Political or ideological goals
C. Curiosity
D. Skill improvement

Q33. Malware distribution through email violates:
A. Civil law only
B. Cyber law
C. Traffic rules
D. Contract law

Q34. Cyber crime evidence must maintain:
A. Speed
B. Chain of custody
C. Encryption
D. Compression

Q35. Ethical hacking certifications emphasize:
A. Illegal techniques
B. Professional responsibility
C. Malware creation
D. Anonymity

Q36. Which act addresses unauthorized access to computer systems in India?
A. IPC
B. IT Act
C. Consumer Protection Act
D. Copyright Act

Q37. Digital forensics supports cyber law by:
A. Attacking systems
B. Collecting admissible evidence
C. Encrypting data
D. Monitoring networks

Q38. International conventions like Budapest Convention aim to:
A. Restrict internet usage
B. Harmonize cyber crime laws
C. Replace national laws
D. Ban encryption

Q39. Ethical hackers must follow which principle?
A. Secrecy
B. Accountability
C. Anonymity
D. Obfuscation

Q40. The greatest impact of cyber crimes is on:
A. Hardware performance
B. Trust in digital systems
C. Programming languages
D. Network speed