? EASY (Q1–Q10)

Q1. A Denial of Service (DoS) attack primarily affects:
A. Confidentiality
B. Integrity
C. Availability
D. Authentication

Q2. Which resource is commonly exhausted during a DoS attack?
A. CPU
B. Memory
C. Network bandwidth
D. All of the above

Q3. Buffer overflow occurs due to:
A. Excessive encryption
B. Improper input handling
C. Network congestion
D. Weak passwords

Q4. Which access control model assigns permissions based on roles?
A. DAC
B. MAC
C. RBAC
D. ABAC

Q5. Which attack sends excessive requests to overwhelm a server?
A. Phishing
B. DoS
C. SQL Injection
D. XSS

Q6. Stack-based buffer overflow affects:
A. Heap memory
B. Stack memory
C. Disk space
D. Network buffer

Q7. Which security objective is most impacted by buffer overflow?
A. Confidentiality
B. Integrity
C. Availability
D. Both B and C

Q8. Access control ensures:
A. Encryption
B. Authentication only
C. Authorized resource usage
D. Data backup

Q9. Which access control is discretionary in nature?
A. DAC
B. MAC
C. RBAC
D. ABAC

Q10. A system crash caused by malformed input indicates:
A. DoS
B. Buffer overflow
C. Spoofing
D. Phishing

□ MEDIUM (Q11–Q25)

Q11. Distributed Denial of Service (DDoS) differs from DoS because it:
A. Uses a single system
B. Targets databases only
C. Uses multiple attacking systems
D. Is always internal

Q12. Heap-based buffer overflow affects:
A. Static memory
B. Dynamic memory allocation
C. Stack frames
D. CPU registers

Q13. Improper bounds checking leads to:
A. SQL Injection
B. Buffer overflow
C. Sniffing
D. Phishing

Q14. Which access control model enforces strict security policies?
A. DAC
B. MAC
C. RBAC
D. ABAC

Q15. SYN flooding exploits which protocol?
A. UDP
B. ICMP
C. TCP
D. HTTP

Q16. Input validation failures can result in:
A. Buffer overflow
B. Injection attacks
C. System crashes
D. All of the above

Q17. Which CIA component is most affected by DDoS attacks?
A. Confidentiality
B. Integrity
C. Availability
D. Authentication

Q18. Which access control uses attributes such as time and location?
A. DAC
B. MAC
C. RBAC
D. ABAC

Q19. A buffer overflow can allow attackers to:
A. Encrypt data
B. Execute arbitrary code
C. Improve performance
D. Secure applications

Q20. Which defense limits request rates to prevent DoS?
A. Encryption
B. Input validation
C. Rate limiting
D. Logging

Q21. Mandatory Access Control is commonly used in:
A. Home systems
B. Military environments
C. Social media apps
D. Public websites

Q22. Improper authorization logic leads to:
A. Authentication bypass
B. Privilege escalation
C. Information disclosure
D. All of the above

Q23. Which attack overwrites return addresses in memory?
A. Heap overflow
B. Stack overflow
C. SQL Injection
D. CSRF

Q24. Which mechanism helps prevent buffer overflow?
A. ASLR
B. Weak typing
C. Hardcoded limits
D. Plaintext input

Q25. Which monitoring system detects DoS patterns?
A. Firewall
B. IDS/IPS
C. Antivirus
D. Proxy server

🟥 HARD (Q26–Q40)

Q26. Volumetric DDoS attacks primarily target:
A. Application logic
B. Network bandwidth
C. Authentication services
D. Databases

Q27. Which buffer overflow allows overwriting function pointers?
A. Stack-based
B. Heap-based
C. Integer overflow
D. Format string

Q28. Access control failure can result in:
A. Unauthorized access
B. Data manipulation
C. Privilege escalation
D. All of the above

Q29. Which technique randomizes memory locations to prevent exploitation?
A. DEP
B. ASLR
C. Firewall
D. IDS

Q30. SYN cookies are used to mitigate:
A. SQL Injection
B. XSS
C. SYN flood attacks
D. Phishing

Q31. Input validation should be performed at:
A. Client side only
B. Server side only
C. Both client and server side
D. Network layer

Q32. Role explosion is a challenge in:
A. DAC
B. MAC
C. RBAC
D. ABAC

Q33. Which access control model is most flexible?
A. MAC
B. DAC
C. RBAC
D. ABAC

Q34. A successful buffer overflow can compromise:
A. Confidentiality
B. Integrity
C. Availability
D. All of the above

Q35. Which DoS attack exploits incomplete TCP handshakes?
A. Smurf
B. SYN Flood
C. Ping of Death
D. Teardrop

Q36. Which principle minimizes damage from access control failure?
A. Least privilege
B. Defense-in-depth
C. Risk acceptance
D. Obfuscation

Q37. Which tool is commonly used to monitor DoS attacks?
A. Wireshark
B. Nmap
C. Nessus
D. Burp Suite

Q38. Improper access control is categorized under:
A. Availability attacks
B. Authorization flaws
C. Authentication flaws
D. Physical threats

Q39. Which secure coding practice prevents overflow?
A. Using unsafe functions
B. Bounds checking
C. Hardcoded values
D. Disabling ASLR

Q40. Access control decisions should be enforced at:
A. Client side
B. Network side
C. Server side
D. User interface only