? EASY (Q1–Q10)

Q1. A backdoor is primarily used to:
A. Encrypt data
B. Provide unauthorized persistent access
C. Improve authentication
D. Patch vulnerabilities

Q2. Hardware backdoors are dangerous because they:
A. Are easily removable
B. Operate below the OS level
C. Require admin access
D. Are software-based

Q3. DDoS attacks mainly target:
A. Confidentiality
B. Integrity
C. Availability
D. Authentication

Q4. Botnets are used in DDoS attacks to:
A. Reduce traffic
B. Distribute attack load
C. Improve bandwidth
D. Encrypt packets

Q5. Biometric spoofing attempts to:
A. Encrypt biometric data
B. Fool biometric authentication systems
C. Improve accuracy
D. Replace passwords

Q6. Fingerprint spoofing often uses:
A. Hashes
B. Fake fingerprints or molds
C. Encryption keys
D. Password lists

Q7. Linux hacking commonly exploits:
A. Hardware failures
B. Misconfigurations and weak permissions
C. BIOS bugs
D. Physical damage

Q8. A Linux backdoor ensures:
A. Temporary access
B. Persistence after reboot
C. Improved performance
D. Encryption

Q9. IDS stands for:
A. Integrated Defense System
B. Intrusion Detection System
C. Internal Detection Service
D. Internet Defense Software

Q10. Firewalls primarily control:
A. File integrity
B. Network traffic
C. User behavior
D. System logs

□ MEDIUM (Q11–Q25)

Q11. Software backdoors are often introduced via:
A. Hardware flaws
B. Malware or malicious code
C. Power failures
D. Network congestion

Q12. Botnet-based DDoS attacks are effective because:
A. Traffic comes from a single source
B. Traffic originates from many compromised hosts
C. Encryption is weak
D. Bandwidth is low

Q13. Amplification attacks increase DDoS impact by:
A. Reducing packets
B. Leveraging protocol responses
C. Blocking traffic
D. Encrypting data

Q14. Biometric systems are vulnerable because:
A. Biometrics change frequently
B. Biometrics cannot be revoked easily
C. Encryption is weak
D. Authentication is optional

Q15. Liveness detection helps prevent:
A. Password reuse
B. Biometric spoofing
C. Brute-force attacks
D. SQL injection

Q16. Linux privilege escalation occurs when attackers:
A. Lose permissions
B. Gain higher privileges
C. Encrypt files
D. Disable services

Q17. Cron jobs can be abused to:
A. Improve scheduling
B. Maintain persistence
C. Encrypt traffic
D. Detect malware

Q18. Host-based IDS monitors:
A. Network packets only
B. System logs and activities
C. Firewall rules
D. Routing tables

Q19. Network-based IDS focuses on:
A. File changes
B. Network traffic analysis
C. User authentication
D. OS updates

Q20. Honeypots are deployed to:
A. Block attacks
B. Detect and study attackers
C. Encrypt systems
D. Patch vulnerabilities

Q21. Low-interaction honeypots:
A. Fully emulate OS
B. Provide limited interaction
C. Are production servers
D. Block traffic

Q22. Stateful firewalls track:
A. User credentials
B. Connection state
C. File integrity
D. Logs

Q23. Application-layer firewalls protect against:
A. Physical attacks
B. Web-based attacks
C. Power failures
D. Hardware faults

Q24. Linux backdoors are difficult to detect because they:
A. Are visible
B. Mimic legitimate services
C. Use no persistence
D. Increase CPU usage

Q25. IDS alerts require:
A. Immediate shutdown always
B. Analysis and correlation
C. Ignoring events
D. Automatic blocking

🟥 HARD (Q26–Q40)

Q26. Hardware backdoors are especially risky because:
A. They are software removable
B. They bypass OS-level controls
C. They are easily detectable
D. They require admin credentials

Q27. DDoS mitigation often uses:
A. Password policies
B. Traffic scrubbing services
C. Disk encryption
D. Antivirus

Q28. Peer-to-peer botnets improve resilience by:
A. Using single C2
B. Eliminating central control
C. Increasing detection
D. Reducing traffic

Q29. Biometric spoofing impacts security because:
A. Biometrics are secret
B. Compromised biometrics cannot be changed
C. Encryption fails
D. MFA is disabled

Q30. Linux misconfiguration exploitation includes:
A. Strong permissions
B. SUID/SGID abuse
C. Secure cron jobs
D. Patched kernels

Q31. Persistence mechanisms in Linux backdoors include:
A. Temporary files only
B. Startup scripts and services
C. RAM-only execution
D. User logs

Q32. IDS vs IPS difference is that IPS:
A. Only detects
B. Can block attacks
C. Is passive
D. Logs only

Q33. Honeypots help defenders by:
A. Blocking attacks
B. Diverting and studying attackers
C. Encrypting traffic
D. Authenticating users

Q34. Firewalls alone are insufficient because:
A. They encrypt traffic
B. They cannot detect all attacks
C. They replace IDS
D. They block everything

Q35. Linux hardening reduces attack surface by:
A. Adding services
B. Removing unnecessary services
C. Disabling firewalls
D. Allowing root login

Q36. DDoS detection relies heavily on:
A. File integrity
B. Traffic baselining and anomaly detection
C. Antivirus alerts
D. User reports only

Q37. Biometric spoofing defenses include:
A. Strong passwords
B. Liveness detection and multi-factor auth
C. Encryption only
D. MAC filtering

Q38. IDS false positives occur when:
A. Attacks are blocked
B. Legitimate traffic triggers alerts
C. Logs are encrypted
D. Traffic is normal

Q39. Defense-in-depth is essential because:
A. Single controls are sufficient
B. Multiple layers compensate for failures
C. IDS replaces firewalls
D. Encryption replaces monitoring

Q40. The primary goal of defensive technologies is to:
A. Eliminate all attacks
B. Reduce risk and detect incidents
C. Stop user activity
D. Replace administrators