? EASY (Q1–Q10)

Q1. Service security primarily focuses on:
A. Improving UI performance
B. Preventing unauthorized access
C. Increasing disk capacity
D. Reducing boot time

Q2. Which principle limits users and services to minimum required permissions?
A. Maximum privilege
B. Least privilege
C. Open access
D. Anonymous access

Q3. Which Linux file stores general system logs?
A. /var/log/secure
B. /var/log/messages
C. /var/log/maillog
D. /var/log/boot.log

Q4. Which service is commonly used for system logging in Linux?
A. syslogd / rsyslog
B. cron
C. sshd
D. ntpd

Q5. NTP stands for:
A. Network Transfer Protocol
B. Network Time Protocol
C. Node Timing Process
D. Network Tuning Protocol

Q6. Which port does NTP use?
A. 22
B. 53
C. 123
D. 161

Q7. Which service provides DNS functionality in Linux?
A. httpd
B. named
C. sshd
D. postfix

Q8. Which DNS security extension signs DNS data?
A. TLS

B. IPsec
C. DNSSEC
D. Kerberos

Q9. Which command checks NTP synchronization status?
A. ntpdate
B. timedatectl
C. chronyc sources
D. Both B and C

Q10. Which log file records authentication events?
A. /var/log/messages
B. /var/log/syslog
C. /var/log/secure
D. /var/log/cron

□ MEDIUM (Q11–Q25)

Q11. Which service replaces ntpd in modern Linux distributions?
A. systemd-timesyncd
B. chronyd
C. time-sync
D. timedated

Q12. Which configuration file controls rsyslog behavior?
A. /etc/syslog.conf
B. /etc/rsyslog.conf
C. /etc/logrotate.conf
D. /etc/systemd/log.conf

Q13. Which command rotates and compresses log files automatically?
A. logrotate
B. rsyslog
C. journalctl
D. syslog

Q14. Which command queries DNS securely with validation?
A. nslookup
B. dig +dnssec
C. host
D. ping

Q15. Which BIND file is the main configuration file?
A. /etc/resolv.conf

B. /etc/named.conf
C. /etc/dns.conf
D. /etc/bind.conf

Q16. Which directive disables recursion on authoritative DNS servers?
A. recursion yes;
B. recursion no;
C. allow-query;
D. allow-transfer;

Q17. Which NTP best practice improves security?
A. Open NTP to all
B. Disable time sync
C. Restrict NTP queries
D. Use random servers

Q18. Which command controls the BIND daemon?
A. dig
B. rndc
C. named-checkconf
D. nslookup

Q19. Which logging mechanism stores logs in binary format?
A. rsyslog
B. syslog
C. journald
D. logrotate

Q20. Which file limits core dumps and system resources?
A. /etc/sysctl.conf
B. /etc/security/limits.conf
C. /etc/profile
D. /etc/fstab

Q21. Which attack targets time synchronization services?
A. DNS spoofing
B. NTP amplification
C. ARP poisoning
D. IP spoofing

Q22. Which DNS security measure prevents cache poisoning?
A. Open recursion
B. DNSSEC
C. Forwarders
D. Caching only

Q23. Which command views systemd journal logs?
A. tail
B. journalctl
C. less
D. grep

Q24. Which directive hides BIND version information?
A. recursion no;
B. allow-query any;
C. version "none";
D. forwarders;

Q25. Which logging practice improves forensic analysis?
A. Disable logs
B. Centralized logging
C. Short retention
D. Overwrite logs

🟥 HARD (Q26–Q40)

Q26. Why is accurate system time critical for security?
A. Improves GUI display
B. Ensures correct log correlation and authentication
C. Reduces disk usage
D. Speeds up DNS

Q27. Which DNS attack redirects traffic to malicious servers?
A. DoS
B. DNS cache poisoning
C. SYN flood
D. ARP spoofing

Q28. Which BIND configuration restricts who can query DNS server?
A. allow-query
B. allow-transfer
C. recursion
D. forwarders

Q29. Which NTP configuration mitigates amplification attacks?
A. Public NTP access
B. restrict default ignore
C. Open UDP ports
D. Disable authentication

Q30. Which logging strategy supports compliance requirements?
A. Local logs only
B. No rotation
C. Log retention and integrity
D. Disable auditing

Q31. Which DNS security feature ensures authenticity and integrity?
A. Forwarding
B. Caching
C. DNSSEC
D. ACL only

Q32. Which command validates BIND configuration syntax?
A. dig
B. nslookup
C. named-checkconf
D. rndc

Q33. Why should log files be protected from modification?
A. Improve performance
B. Prevent tampering and preserve evidence
C. Reduce size
D. Simplify reading

Q34. Which NTP alternative is recommended for modern systems?
A. ntpd
B. chrony
C. rdate
D. timedate

Q35. Which DNS best practice improves resilience?
A. Single DNS server
B. Disable caching
C. Secondary DNS servers
D. Open recursion

Q36. Which attack exploits open DNS resolvers?
A. SQL injection
B. DNS amplification
C. Brute force
D. XSS

Q37. Which service ensures time consistency across distributed systems?
A. DNS
B. LDAP

C. NTP
D. SMTP

Q38. Which command checks DNSSEC validation status?
A. dig +dnssec
B. nslookup
C. host
D. ping

Q39. Which security control monitors and records system events?
A. Firewall
B. Logging
C. Backup
D. RAID

Q40. Which overarching principle best secures services?
A. Open configuration
B. Default settings
C. Defense in depth
D. Anonymous access