

☑ EASY (Q1–Q10)

Q1. Performance tuning in Linux primarily aims to:

- A. Change the kernel version
- B. Improve system efficiency and responsiveness
- C. Reduce user accounts
- D. Disable services

Q2. Which command shows real-time CPU and memory usage?

- A. ps
- B. top
- C. free
- D. df

Q3. Which command displays free and used memory?

- A. top
- B. df
- C. free
- D. du

Q4. Which file system directory contains system log files?

- A. /etc
- B. /usr
- C. /var/log
- D. /boot

Q5. Which command shows system load averages?

- A. uptime
- B. free
- C. vmstat
- D. iostat

Q6. Which tool monitors disk I/O statistics?

- A. free
- B. vmstat
- C. iostat
- D. top

Q7. Which maintenance task helps recover from failures?

- A. Logging
- B. Backup
- C. Monitoring
- D. Patching

Q8. Which threat targets system availability?

- A. Spoofing

- B. Information disclosure
- C. Denial of Service
- D. Privilege escalation

Q9. Which command checks running processes?

- A. ls
- B. ps
- C. mount
- D. df

Q10. Which protection method restricts network access?

- A. Backup
 - B. Firewall
 - C. Logging
 - D. Monitoring
-

☐ **MEDIUM (Q11–Q25)**

Q11. Which command provides detailed memory, process, and CPU statistics?

- A. free
- B. top
- C. vmstat
- D. df

Q12. Which file contains kernel boot and runtime messages?

- A. /var/log/messages
- B. /var/log/secure
- C. /var/log/maillog
- D. /boot/grub/grub.cfg

Q13. Which command identifies disk space usage per directory?

- A. df
- B. du
- C. lsblk
- D. mount

Q14. Which tuning parameter controls maximum open files?

- A. fs.file-max
- B. net.ipv4.ip_forward
- C. kernel.shmmni
- D. vm.swappiness

Q15. Which tool shows CPU usage per process?

- A. free

- B. ps
- C. top
- D. df

Q16. Which maintenance activity reduces security vulnerabilities?

- A. Logging
- B. Monitoring
- C. Patching
- D. Backup

Q17. Which file defines system-wide kernel parameters?

- A. /etc/profile
- B. /etc/sysctl.conf
- C. /etc/fstab
- D. /etc/security/limits.conf

Q18. Which command reloads kernel parameters at runtime?

- A. sysctl
- B. modprobe
- C. insmod
- D. reboot

Q19. Which troubleshooting step should be performed first?

- A. Reinstall OS
- B. Identify the problem
- C. Apply random fixes
- D. Disable services

Q20. Which threat involves gaining unauthorized higher privileges?

- A. Spoofing
- B. DoS
- C. Privilege escalation
- D. Sniffing

Q21. Which tool helps analyze system boot performance?

- A. top
- B. htop
- C. systemd-analyze
- D. uptime

Q22. Which log helps troubleshoot authentication issues?

- A. /var/log/messages
- B. /var/log/secure
- C. /var/log/boot.log
- D. /var/log/dmesg

Q23. Which parameter controls swap usage tendency?

- A. `vm.dirty_ratio`
- B. `vm.swappiness`
- C. `fs.inotify.max_user_watches`
- D. `kernel.pid_max`

Q24. Which protection method detects suspicious activity?

- A. Firewall
- B. IDS/IPS
- C. Backup
- D. RAID

Q25. Which command displays network statistics?

- A. `ss`
 - B. `ip addr`
 - C. `route`
 - D. `ping`
-

HARD (Q26–Q40)

Q26. Why is load average analysis important in performance tuning?

- A. It measures disk size
- B. It reflects system scheduling pressure
- C. It shows memory leaks
- D. It displays network latency

Q27. Which `sysctl` parameter improves network performance under high load?

- A. `net.ipv4.tcp_tw_reuse`
- B. `vm.swappiness`
- C. `kernel.core_pattern`
- D. `fs.protected_symlinks`

Q28. Which scenario best justifies increasing `vm.swappiness`?

- A. Memory-rich database server
- B. Diskless system
- C. Memory-constrained system with swap
- D. CPU-bound workload

Q29. Which maintenance strategy minimizes downtime?

- A. Reactive maintenance
- B. Preventive maintenance
- C. Corrective maintenance
- D. Emergency maintenance

Q30. Which threat model category targets confidentiality?

- A. Denial of Service
- B. Information disclosure
- C. Tampering
- D. Repudiation

Q31. Which tool correlates logs for troubleshooting complex issues?

- A. grep
- B. journalctl
- C. awk
- D. sed

Q32. Which performance issue is indicated by high iowait?

- A. CPU bottleneck
- B. Memory leak
- C. Disk I/O bottleneck
- D. Network congestion

Q33. Which protection mechanism enforces mandatory access control?

- A. ACL
- B. SELinux
- C. chmod
- D. chown

Q34. Why should unused services be disabled?

- A. Improve GUI performance
- B. Reduce attack surface and resource usage
- C. Increase boot time
- D. Simplify updates

Q35. Which troubleshooting technique isolates components step by step?

- A. Guessing
- B. Divide and conquer
- C. Random testing
- D. Trial and error

Q36. Which metric best indicates memory pressure?

- A. CPU idle
- B. Swap usage
- C. Disk size
- D. Network throughput

Q37. Which threat involves altering system data?

- A. Spoofing
- B. Tampering

- C. Repudiation
- D. DoS

Q38. Which tool provides historical performance data?

- A. top
- B. uptime
- C. sar
- D. free

Q39. Which best practice improves long-term system stability?

- A. Ignore alerts
- B. Regular monitoring and tuning
- C. Disable logs
- D. One-time optimization

Q40. Which principle should guide performance and security decisions?

- A. Maximum utilization
- B. Convenience
- C. Balance between performance and security
- D. Disable controls