INFOSEC

1. Do not assume anything.
2. Nothing is secure.
3. Trust no-one, nothing.
4. Security is a trade-off with usability.
5. Paranoia is your friend.

Security Checklist - 1

1. Ensure Physical Security.
2. BIOS Protection.
3. Disable Booting from external media devices.
4. Boot Loader Protection.
5. Keep the OS updated (only from trusted sources).
6. Check the installed packages and remove the unnecessary ones.
7. Check for Open Ports and stop unnecessary services.
8. Enforce Password Policy.
9. Audit Passwords using John the Ripper.
10. Eliminate unused and well-known accounts that are not needed.
11. Give users limited administrative access.
12. Do not use the root account on a regular basis and do not allow direct root login.

Security Checklist - 2

13. Set limits using the *ulimit* command to avoid DoS attacks such as launching a fork bomb.
14. Set proper file permissions.
    a. Audit the Set User ID (SUID) and Set Group ID (SGID) binaries on the system.
    b. Do not mount remote filesystems with root read-write access. Read-only access would be enough.
    c. Set the sticky bit on any world-writable directories.
    d. harden /tmp – mount it on a separate partition (not to fill all the disk space), mount it with noexec,nosuid bits set.
15. Implement File Monitoring (Host IDS - AIDE).
16. Scan for Rootkits, Viruses, and Malware (Rootkit Hunter, chkrootkit, ClamAV).
17. Use Disk Encryption to protect your data. Don’t forget to encrypt your Backups as well.
18. Secure every Network Service especially SSHd.

Security Checklist - 3

19. Scan your Network and Hosts using Nmap.
20. Securing Your Linux System with a Firewall (Netfilter/Iptables).
21. Monitor the firewall and its logs.
22. Monitor your logs and search for suspicious activity (logwatch).
23. Scan your servers using a VAS such as Nessus or OpenVAS.
24. Make backups and test them.