Operating System Security Checklist (Linux & Windows)

1. User & Account Management

- Ensure strong password policy is enabled

- Disable unused user accounts

- Use least privilege principle

- Limit administrator/root access

2. File & Directory Permissions

- Set proper file permissions (chmod / NTFS)

- Avoid world-writable files

- Use ownership correctly (chown)

- Protect sensitive system files

3. Authentication & Authorization

- Enable account lockout policy

- Use multi-factor authentication where possible

- Disable guest accounts

4. Firewall Configuration

- Enable UFW (Linux) / Windows Firewall

- Allow only required ports

- Block unused inbound connections

- Monitor firewall logs

5. Services & Processes

- Identify running services

- Disable unnecessary services

- Monitor suspicious processes

6. System Updates & Patch Management

- Enable automatic updates

- Regularly apply security patches

- Verify update sources

7. Malware & Threat Protection

- Enable Windows Defender / Antivirus

- Perform regular scans

- Update virus definitions

8. Logging & Monitoring

- Enable system logs

- Review logs periodically

- Monitor login attempts

9. Backup & Recovery

- Perform regular system backups

- Test backup restoration

- Store backups securely

10. OS Hardening Best Practices

- Disable unused ports and protocols

- Secure boot enabled

- Encrypt disk where possible

- Use security benchmarks (CIS)