OS Security Checklist – Task 2

1. **User Accounts and Access Control**
   - Administrator and standard user accounts are identified.
   - Administrator account has full system access.
   - Standard user account has limited permissions.
   - Least privilege principle is followed

2. **Administrator vs Standard User**
   - Administrator can install software and modify system settings.
   - Standard user cannot make system-level changes.
   - Using standard user improves system security

3. **Firewall Configuration**
   - Windows Defender Firewall is enabled.
   - Firewall is active for private and public networks.
   - Firewall helps block unauthorized network access.

4. **Running Processes and Services**
   - Running processes are viewed using Task Manager.
   - Background services are identified.
   - Resource usage of processes is observed.

5. **Disabling Unnecessary Services**
   - Unnecessary services increase attack surface.
   - Identifying unused services improves security.
   - Disabling unused services reduces vulnerabilities.

6. **Antivirus Protection**
   - Windows Defender Antivirus is enabled
   - Real-time protection is active
   - Antivirus protects the system from malware and viruses

7. **File Permissions**

- File permissions control access to files and folders in the Windows operating system.
- Permissions are managed using the Security tab in file or folder properties.
- Users can access permissions by right-clicking a file/folder → Properties → Security.
- Common Windows permissions include:
- Read – allows viewing file contents
- Write – allows modifying file contents
- Modify – allows reading, writing, and deleting files
- Full Control – allows complete access, including changing permissions
- Proper file permission management prevents unauthorized access to sensitive data.
- Assigning permissions based on least privilege principle improves system security.

8. **OS Hardening Best Practice**
   - Firewall protection is enabled.
   - Strong passwords are used.
   - Regular system updates are applied.
   - Least privilege principle is followed.
   - Unused services are disabled.

Conclusion

This task helped in understanding operating system security fundamentals in Windows. By managing user privileges, file permissions, firewall, antivirus, and services, the operating system can be hardened against security threats.