## Objective:

To understand the concepts of software maintenance and apply patching strategies using different platforms. The lab focuses on identifying outdated software, applying patches, and verifying updates.

## Tools and Software Used:

• Windows 10 and Ubuntu 22.04

• Terminal / Command Prompt / Windows Update GUI

• Package managers: apt (Ubuntu), Windows Update

• Internet connection

## Lab Tasks & Results

### Task 1: Identify Outdated Software

Linux Command:

sudo apt list --upgradable

Output displayed a list of packages ready for upgrade (e.g., firefox, libssl, etc.).

Windows:

Opened 'Settings > Windows Update' and clicked 'Check for updates'. Several updates were listed.

### Task 2: Apply Security Updates

Linux Command:

sudo apt update && sudo apt upgrade -y

Packages updated successfully.

Windows:

Clicked on 'Download and install' for updates. Restarted the system after installation.

### Task 3: Automate Patching (Linux)

Commands:

sudo apt install unattended-upgrades  
sudo dpkg-reconfigure --priority=low unattended-upgrades

Auto updates configured successfully.

### Task 4: Validate Installed Updates

Linux:

Command used: apt list --installed | grep openssl

Verified openssl package updated to the latest version.

Windows:

Used 'winver' and 'systeminfo' to confirm updated OS build.

## Expected Outcomes Achieved

• Understood corrective, adaptive, perfective, and preventive maintenance

• Performed manual and automatic patching

• Verified software updates using both GUI and CLI tools

## Assessment Questions & Answers

1. What are the four types of software maintenance?  
➤ Corrective, Adaptive, Perfective, Preventive

2. Why is it important to test patches before deployment?  
➤ To ensure the patch doesn’t break functionality or cause instability.

3. Name two tools used for automated patching.  
➤ unattended-upgrades (Linux), Windows Update

4. How do you verify updates were installed successfully on Linux?  
➤ Using apt list --installed or checking system logs (/var/log/apt/).

5. What are the risks of not applying security patches?  
➤ Exposure to vulnerabilities, malware, and data breaches.