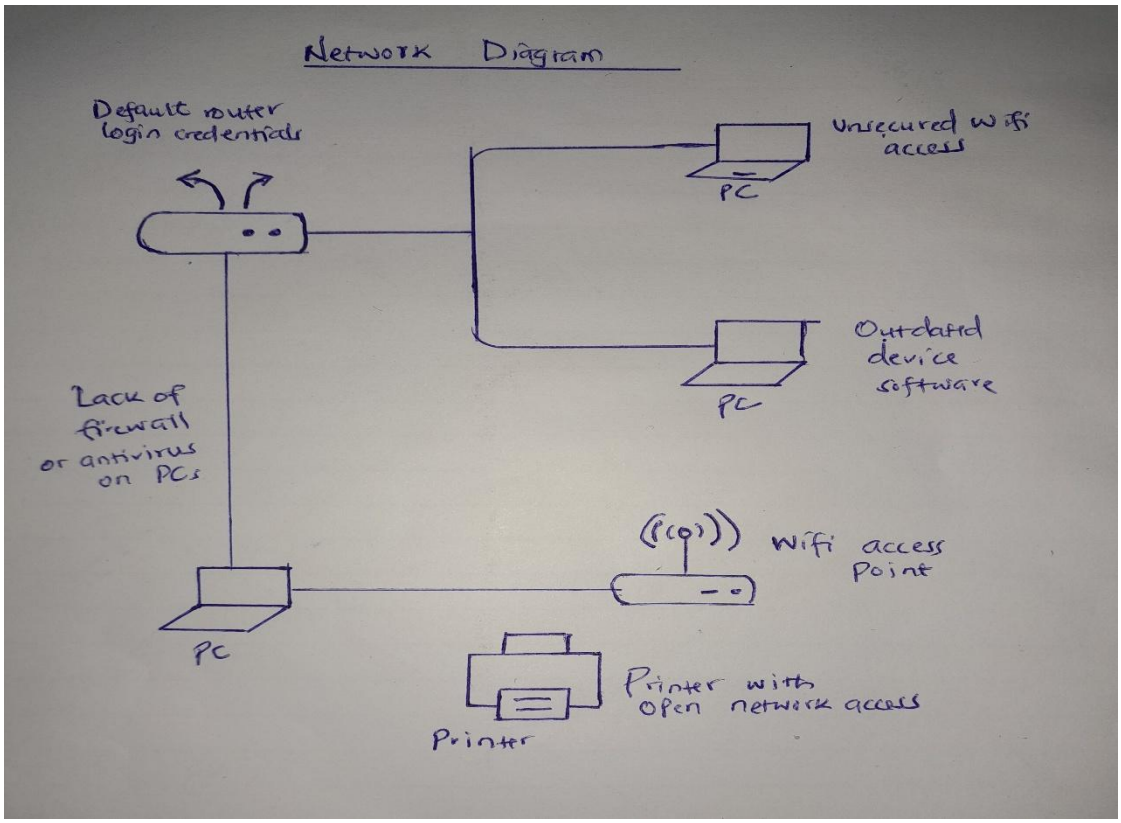
## A. Network Diagram Design




**Basic Components**

- Router
- 3 PCs
- Wi-Fi Access Point
- Network Printer

## B. Identify Five Security Vulnerabilities

1. **Default Router Login Credentials**
   Many users don't change default usernames and passwords.
2. **Unsecured Wi-Fi Access**
   Open Wi-Fi or weak encryption (e.g., WEP) makes it easy for outsiders to access.
3. **Outdated Device Software**
   PCs, router or printer running old firmware/OS are vulnerable to exploits.
4. **Lack of Firewall or Antivirus on PCs**
   Absence of endpoint protection can allow malware infection and propagation.
5. **Printer with Open Network Access:**
   A network printer can be used as a backdoor if unsecured.

## C. Mitigation Strategies

1. **Change Router Login Credentials**
    - Use strong, unique passwords
    - Disable remote admin access if not needed
2. **Secure Wi-Fi Configuration**
    - Use WPA3 (or at least WPA2)
    - Enable MAC address filtering
    - Hide SSID if feasible
3. **Regular Updates and Patch Management**
    - Schedule updates for all devices
    - Enable auto-update where possible
4. **Install and Maintain Security Software**
    - Use antivirus + personal firewall on each PC
    - Educate users on phishing and malware
5. **Secure Network Printer:**
    - Disable unused ports (FTP, Telnet)
    - Use password protection for admin access
    - Monitor logs for unusual access