Task 14: Linux Server Hardening & Secure Configuration

1. Review default Linux system settings

When a Linux server is installed, it comes with default users, services, and open network ports. First, we check which users are present, what services are running in the background, and which ports are open. This helps us understand the current system condition and identify possible security risks.

2. Remove unused user accounts and restrict sudo access

Unused or old user accounts can be misused by attackers. So, we delete unnecessary accounts. We also limit **sudo (administrator) access** only to trusted users. This follows the principle of **least privilege**, meaning users get only the permissions they really need.

3. Disable root login and configure SSH with key-based authentication

The root account has full control of the system, so it should not allow direct login. Instead, we disable root login and use SSH key-based authentication. SSH keys are more secure than passwords and protect against brute-force attacks.

4. Update system packages and enable automatic security updates

Outdated software may contain vulnerabilities. We regularly update system packages to fix security bugs. Enabling automatic updates ensures that important security patches are installed without delay.

5. Configure a firewall

A firewall controls incoming and outgoing network traffic. We configure it to allow only necessary ports (like SSH or web server ports) and block all others. This reduces the attack surface of the server.

6. Stop and disable unnecessary services

Some services may run automatically even if they are not needed. These extra services can create security risks. We stop and disable them so that only required services are active.

---

7. Secure file permissions

Sensitive files such as configuration files and password files must have strict permissions. Only authorized users should be able to read or modify them. Proper file permissions prevent unauthorized access or accidental changes.

---

8. Review system logs

System logs record important activities like login attempts, errors, and system changes. By checking logs regularly, we can detect suspicious activities such as failed login attempts or unusual behavior.
