Task 14: Linux Server Hardening & Secure Configuration

1. Introduction

Linux servers are widely used in production environments due to their stability and flexibility. However, default Linux installations often contain unnecessary services, open ports, and weak configurations. Server hardening is the process of securing a system by reducing its attack surface and applying security best practices.

2. Objectives

The objectives of this task are:

- To understand default Linux system settings
- To remove unnecessary users and services
- To apply the principle of least privilege
- To secure SSH access
- To configure firewall rules
- To protect sensitive system files
- To monitor system logs for suspicious activity

3. Tools Used

- **Ubuntu / Kali Linux (Primary)**
- **Lynis (Alternative)**
- **CIS Benchmarks (Reference)**

4. Review of Default System Settings

The default Linux configuration was reviewed to identify existing users, running services, and open ports. This step helps understand the initial security posture of the system.

---

5. User and Privilege Management

Unused user accounts were removed from the system. Sudo access was restricted to trusted users only, following the principle of least privilege to reduce the risk of privilege misuse.

---

6. Securing Root Access and SSH

Direct root login was disabled to prevent brute-force attacks. SSH was configured to use key-based authentication instead of password-based login, improving authentication security.

---

7. System Updates and Patch Management

System packages were updated to the latest versions. Automatic security updates were enabled to ensure that known vulnerabilities are patched regularly.

---

8. Firewall Configuration

A firewall was configured to allow only necessary inbound and outbound traffic. Unused ports were blocked to minimize exposure to external attacks.

---

9. Service Management

Unnecessary services running on the server were stopped and disabled. This reduces the attack surface and prevents exploitation of unused services.

---

10. File Permission Hardening

Sensitive system and configuration files were secured by applying proper file permissions. Access was limited to authorized users only.

---

11. Log Monitoring

System logs were reviewed to monitor authentication attempts and system activities. Log monitoring helps in early detection of suspicious behavior and security incidents.

---

12. Conclusion

This task provided hands-on experience in securing Linux servers using standard hardening techniques. It improved understanding of system security, access control, and server protection against common attacks.

RIFAH RESLIN MANIYODAN LATHEEF