Introduction

Linux Server Hardening is the process of securing a Linux system by reducing vulnerabilities, removing unnecessary components, and applying secure configurations. Since Linux servers are commonly used in production environments, proper hardening is essential to protect against unauthorized access, misconfigurations, and common cyberattacks.

This task focuses on reviewing system settings, applying security controls, and strengthening the Linux server configuration.

Review Default System Settings

The first step in hardening is reviewing the default system configuration.

Key review areas:

- Existing user accounts
- Running services
- Open network ports
- Installed packages

Understanding the system's baseline helps identify security gaps.

User Account Management

Unused or unnecessary user accounts increase security risk.

Hardening actions:

- Remove unused user accounts
- Disable inactive accounts
- Apply the principle of least privilege
- Restrict sudo access to trusted users only

Proper user management reduces insider and external threats.

Secure SSH Configuration

SSH is a common attack target and must be secured.

SSH hardening steps:

- Disable root login via SSH
- Enable key-based authentication
- Disable password-based login
- Change default SSH settings if required

Secure SSH reduces the risk of brute-force attacks.

System Updates & Patch Management

Outdated systems are vulnerable to known exploits.

Actions performed:

- Update all system packages
- Apply security patches
- Enable automatic security updates

Regular updates ensure protection against known vulnerabilities.

Firewall Configuration

A firewall controls incoming and outgoing network traffic.

Firewall hardening includes:

- Allow only required ports and services
- Block unused or unnecessary ports
- Enable firewall at system startup

Firewall configuration reduces network-based attacks.

Disable Unnecessary Services

Unneeded services increase the attack surface.

Actions taken:

- Identify running services
- Stop unused services

- Disable them from starting at boot

Only essential services should be running on the server.

Secure File Permissions

Incorrect file permissions can lead to privilege escalation.

Hardening actions:

- Restrict permissions on sensitive files
- Protect configuration files
- Ensure proper ownership of system files

File permission security prevents unauthorized access.

Log Monitoring

System logs help detect suspicious activity.

Log review includes:

- Authentication logs
- System activity logs
- Error and warning logs

Regular log monitoring helps identify security incidents early.

Linux Hardening Checklist

- Removed unused users
- Restricted sudo access
- Disabled root login
- Secured SSH access
- Updated system packages
- Enabled firewall
- Disabled unnecessary services
- Secured file permissions

- Reviewed system logs

Security Configuration Summary

The Linux server was hardened by applying secure configurations, minimizing exposed services, enforcing access controls, and enabling monitoring. These actions significantly reduce the risk of unauthorized access and system compromise.

Final Outcome

This task provides practical experience in securing Linux servers against common attacks. It builds the ability to apply system hardening techniques, enforce security best practices, and maintain a secure Linux environment.

Prepared by:

Megaraj S