CYBER SECURITY INTERNSHIP – 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 installations may contain unnecessary services, weak configurations, or misconfigurations that can be exploited by attackers.
Linux server hardening involves securing the system by reducing the attack surface, applying secure configurations, and enforcing security best practices.

This task focuses on understanding Linux server hardening techniques and secure configuration practices.

---

2. What is Server Hardening?

Server hardening is the process of securing a server by:

- Removing unnecessary services and software
- Restricting user privileges
- Applying security patches
- Configuring secure access controls
- Monitoring logs and system activity

The goal is to minimize vulnerabilities and reduce the risk of attacks.

---

3. Tools and Environment

- **Linux OS** (Ubuntu / Kali Linux – conceptual)
- **Lynis** (security auditing tool – conceptual)
- **CIS Benchmarks** (best practices – conceptual)

---

4. User and Permission Management

Proper user management is essential for system security.

Steps Reviewed

- Identified existing user accounts
- Removed unused or unnecessary users
- Applied the principle of least privilege
- Restricted `sudo` access to trusted users only

Security Benefit

Limits unauthorized access and prevents privilege misuse.

---

5. Root Account Security

The root account has full system privileges and must be protected.

Hardening Measures

- Disabled direct root login
- Used sudo instead of root login
- Encouraged strong passwords and secure authentication

---

6. SSH Hardening

SSH is commonly used for remote server access.

Secure SSH Configuration

- Disabled root login over SSH
- Used SSH key-based authentication
- Changed default SSH settings (conceptual)
- Limited SSH access to authorized users

Security Benefit

Prevents brute-force attacks and unauthorized remote access.

---

7. Firewall Configuration

A firewall was configured to control network traffic.

Firewall Actions

- Allowed only required ports
- Blocked unused and insecure ports
- Restricted inbound connections

Security Benefit

Reduces attack surface by limiting network exposure.

---

8. Service Management

Unnecessary services increase security risks.

Hardening Steps

- Identified running services
- Stopped and disabled unused services
- Ensured only essential services were running

---

9. System Updates and Patch Management

Keeping the system updated is critical.

Actions

- Reviewed system update mechanism
- Ensured security patches are applied regularly
- Enabled automatic updates (conceptual)

---

10. File Permissions and Ownership

Sensitive files must be protected.

Files Reviewed

- `/etc/passwd`
- `/etc/shadow`
- `/etc/sudoers`

Security Benefit

Prevents unauthorized modification of critical system files.

11. Log Monitoring

System logs were reviewed to monitor activity.

Logs Checked

- Authentication logs
- System logs

Security Benefit

Helps detect unauthorized access and suspicious behavior.

12. Linux Hardening Checklist

- Root login disabled
- Least privilege applied
- Firewall configured
- Unused services disabled
- File permissions secured
- Logs monitored regularly

13. Security Impact

Linux server hardening:

- Reduces vulnerabilities
- Prevents unauthorized access
- Improves system stability
- Enhances overall security posture