Cyber Security Internship
Task 14: Linux Server Hardening & Secure Configuration

Introduction

Server hardening is the process of securing a Linux server by reducing its attack surface. This task focuses on applying best security practices to protect the system from unauthorized access, misconfigurations, and common cyber attacks.

Linux Hardening Checklist

- Reviewed default system users, running services, and open network ports.
- Removed unused user accounts and restricted sudo access following least privilege principle.
- Disabled root login and configured SSH with key-based authentication.
- Updated all system packages and enabled automatic security updates.
- Configured firewall to allow only necessary inbound and outbound traffic.
- Stopped and disabled unnecessary services running on the server.
- Applied secure file permissions to sensitive system and configuration files.
- Reviewed system logs to monitor authentication attempts and system activities.

Security Configuration Summary

The Linux server was hardened by minimizing exposed services, enforcing strong authentication methods, and ensuring only authorized users have elevated privileges. Firewall rules were implemented to control network traffic, and regular updates were enabled to protect against known vulnerabilities.

Interview Questions & Answers

What is server hardening?
Server hardening is the process of securing a server by reducing vulnerabilities, disabling unnecessary services, and applying security best practices.

Why disable root login?
Disabling root login prevents attackers from directly accessing the most powerful account, reducing the risk of full system compromise.

What is least privilege?
Least privilege means giving users only the minimum permissions required to perform their tasks.

Purpose of firewall?
A firewall controls incoming and outgoing network traffic and blocks unauthorized access.

Risks of unused services?
Unused services increase the attack surface and may contain vulnerabilities that attackers can exploit.

Final Outcome

After completing this task, the ability to secure Linux systems against common attacks was achieved. The server is now more resilient, stable, and secure due to proper hardening techniques.