Cyber Security Internship Report

Task 14: Linux Server Hardening & Secure Configuration (With Security Audit Details)

Name: Mohammed Nihal
Environment: Kali Linux (VirtualBox) on Windows 11 Host
Objective: Implement structured Linux hardening controls and validate system security posture using automated audit tools.

Introduction

Linux server hardening reduces the attack surface of a system by enforcing strict access control, disabling unnecessary services, securing configurations, and applying regular security updates. In this task, both manual hardening techniques and automated auditing using Lynis were performed to validate the system's security posture.

Hardening Controls Implemented

- User account review and sudo privilege verification (Least Privilege principle).
- Root account locked and SSH root login disabled.
- SSH configuration hardened (PasswordAuthentication disabled).
- Firewall (UFW) enabled and restricted to required services only.
- Open ports reviewed using ss -tuln.
- Unnecessary services identified and disabled.
- System fully updated using apt update and full-upgrade.
- Automatic security updates configured.
- Sensitive file permissions verified for /etc/passwd and /etc/shadow.
- Authentication logs reviewed for suspicious login attempts.

Security Audit Tool: Lynis

Lynis is an open-source security auditing and compliance testing tool designed for Unix/Linux systems. It performs in-depth system analysis to detect security weaknesses, misconfigurations, and compliance gaps. Lynis is commonly used by system administrators, penetration testers, and security auditors.

Command Executed:
sudo lynis audit system

Key Audit Areas Reviewed by Lynis:
- Boot and system services configuration
- Kernel security parameters
- Authentication mechanisms and password policies
- Firewall and network security settings
- File permissions and ownership integrity
- Installed packages and patch status
- Malware scanning and suspicious binaries detection
- Logging and monitoring configuration
- Compliance checks aligned with CIS benchmarks

Lynis generates a security score and provides categorized warnings and suggestions. Warnings highlight misconfigurations that require immediate attention, while suggestions provide best-practice improvements. The audit results were reviewed and used to further strengthen system security configurations.

Risk Reduction & Audit Validation

Security Area	Hardening Action	Validated by Lynis
User Access Control	Restricted sudo & locked root	Yes
SSH Security	Disabled root login & password auth	Yes
Firewall Security	UFW enabled	Yes
System Updates	Full upgrade applied	Yes
File Permissions	Verified sensitive files	Yes
Service Hardening	Disabled unnecessary services	Yes

Conclusion

The Linux system was successfully hardened using structured security controls and validated using the Lynis security audit tool. Manual hardening steps reduced attack surface, while automated auditing ensured compliance with security best practices. This task demonstrates practical skills required for SOC Analysts, Linux Administrators, and Security Engineers.