CIS Benchmark Compliance Report

Ubuntu Linux 24.04 LTS Server Security Configuration Assessment

Date: December 15, 2025

Executive Summary

This report presents the findings from a Security Configuration Assessment (SCA) scan performed against an Ubuntu Linux 24.04 LTS Server using the CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0. The assessment was conducted using Wazuh SIEM to evaluate compliance with industry-standard security hardening guidelines.

Assessment Summary

Metric	Value
Total Checks Evaluated	**279**
Passed	122
Failed	115
Not Applicable	42
Compliance Score	**51%**

Findings by Category

Network Security (20 Failed Checks)

Network-related findings include firewall configuration, kernel module hardening, and network protocol settings.

ID	Finding	Status	Risk
35604	Ensure dccp kernel module is not available	Failed	Medium
35605	Ensure tipc kernel module is not available	Failed	Medium
35606	Ensure rds kernel module is not available	Failed	Medium
35607	Ensure sctp kernel module is not available	Failed	Medium
35613	Ensure secure ICMP redirects are not accepted	Failed	Medium
35619	Ensure a single firewall configuration utility is in use	Failed	Medium
35623	Ensure ufw loopback traffic is configured	Failed	Medium
35624	Ensure ufw default deny firewall policy	Failed	Medium
35626	Ensure ufw is uninstalled or disabled with nftables	Failed	Medium
35627	Ensure iptables are flushed with nftables	Failed	Medium

Authentication & Access Control (42 Failed Checks)

Authentication findings cover SSH configuration, password policies, cron permissions, and file system security.

ID	Finding	Status	Risk
35540	Ensure bootloader password is set	Failed	Medium
35594	Ensure permissions on /etc/crontab are configured	Failed	Medium
35595	Ensure permissions on /etc/cron.hourly are configured	Failed	Medium
35596	Ensure permissions on /etc/cron.daily are configured	Failed	Medium
35665	Ensure sshd PermitRootLogin is disabled	Failed	Medium
35671	Ensure sshd MaxAuthTries is configured	Failed	Medium
35677	Ensure sshd ClientAliveInterval and ClientAliveCountMax are configured	Failed	Medium
35700	Ensure password expiration is configured	Failed	Medium
35701	Ensure minimum password age is configured	Failed	Medium
35703	Ensure inactive password lock is configured	Failed	Medium

Logging & Auditing (25 Failed Checks)

Logging findings address audit configuration, log partitioning, and system event collection.

ID	Finding	Status	Risk
35528	Ensure separate partition exists for /var/log	Failed	Medium
35529	Ensure nodev option set on /var/log partition	Failed	Medium
35532	Ensure separate partition exists for /var/log/audit	Failed	Medium
35547	Ensure local login warning banner is configured properly	Failed	Medium
35548	Ensure remote login warning banner is configured properly	Failed	Medium
35640	Ensure audit log storage size is configured	Failed	Medium
35641	Ensure audit logs are not automatically deleted	Failed	Medium
35642	Ensure system is disabled when audit logs are full	Failed	Medium
35649	Ensure audit configuration is immutable	Failed	Medium
35683	Ensure sudo log file exists	Failed	Medium

Compliance Framework Mapping

The CIS Benchmark controls map to multiple compliance frameworks:

- **NIST 800-53:** AC (Access Control), AU (Audit), SI (System Integrity), CM (Configuration Management)
- **PCI DSS v4.0:** Requirements 1, 2, 5, 6, 7, 8, 10
- **HIPAA:** 164.308, 164.312 (Technical Safeguards)
- **SOC 2:** CC5.2, CC6.1, CC6.3, CC6.6, A1.1
- **CMMC v2.0:** AC.L1-3.1.1, CM.L2-3.4.7, AU.L2-3.3.1

Recommendations

Based on the assessment findings, the following prioritized remediation steps are recommended:

1. **High Priority:** Configure firewall default deny policies and enable a single firewall utility (ufw or nftables)
2. **High Priority:** Disable SSH root login and configure authentication timeouts
3. **High Priority:** Disable unnecessary kernel modules (dccp, sctp, rds, tipc)
4. **Medium Priority:** Enable auditd and configure comprehensive audit rules
5. **Medium Priority:** Implement password complexity and expiration policies
6. **Low Priority:** Configure separate partitions for /var/log and /var/log/audit

Methodology

This assessment was conducted using the following tools and methodology:

- **SIEM Platform:** Wazuh 4.14.1 with Security Configuration Assessment (SCA) module
- **Benchmark:** CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0
- **Target System:** Ubuntu Linux 24.04 LTS Server with Wazuh agent
- **Assessment Date:** December 15, 2025

— End of Report —