

System Security Report - PDF

System Security Compliance Report

Generated: **2025-12-19**
17:35:14



Executive Summary

97.5%

Overall Compliance Score

Excellent security posture - System meets most security requirements

2

Total Findings

Security issues identified

0

Critical Issues

Require immediate attention

0

High Priority

Address as soon as possible

1

Medium Priority

Plan for resolution

4

Rules Applied

Successfully hardened



Security Posture Improvement

Comparison of security status before and after hardening measures

Before Hardening

Critical:	1
High:	2
Medium:	1
Low:	1
Total:	5



After Hardening

Critical:	0
High:	0
Medium:	1
Low:	1
Total:	2

✓ 60.0% improvement in security posture
3 security issues successfully resolved

Compliance Score Progress

Before Hardening

77.5%



After Hardening

97.5%

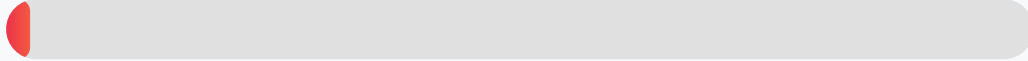




Security Findings Distribution

Critical

0 issues



High

0 issues



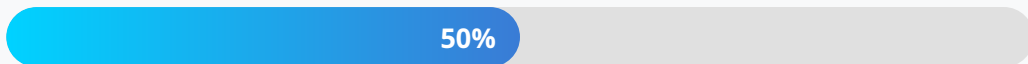
Medium

1 issues



Low

1 issues





Detailed Security Findings

Complete list of identified security issues and vulnerabilities

FINDING	SEVERITY	CATEGORY	DESCRIPTION & REMEDIATION
Outdated Packages	MEDIUM	System Updates	3 packages require security updates Remediation: Run apt update && apt upgrade
Unnecessary Services Running	LOW	Services	One unnecessary service is still running Remediation: Review and disable unnecessary service



Remediation Actions Taken

Security hardening measures applied to the system

Checkpoint Created: `checkpoint_xyz789`

System state saved for rollback capability

Disable SSH Root Login

SUCCESS

Changed configuration: `PermitRootLogin yes` →
`PermitRootLogin no`

Severity: **CRITICAL** Duration: 1.20s

Disable SSH Password Authentication

SUCCESS

Changed configuration: `PasswordAuthentication yes` →
`PasswordAuthentication no`

Severity: **CRITICAL** Duration: 0.80s

Configure Password Policy

SUCCESS

Changed configuration: `PASS_MAX_DAYS 99999` → `PASS_MAX_DAYS 90`

Severity: **HIGH** Duration: 0.50s

Enable Firewall

SUCCESS

Changed configuration: `inactive` → `active`

Severity: **HIGH** Duration: 2.30s

Disable Unnecessary Service

FAILED

Applied security rule

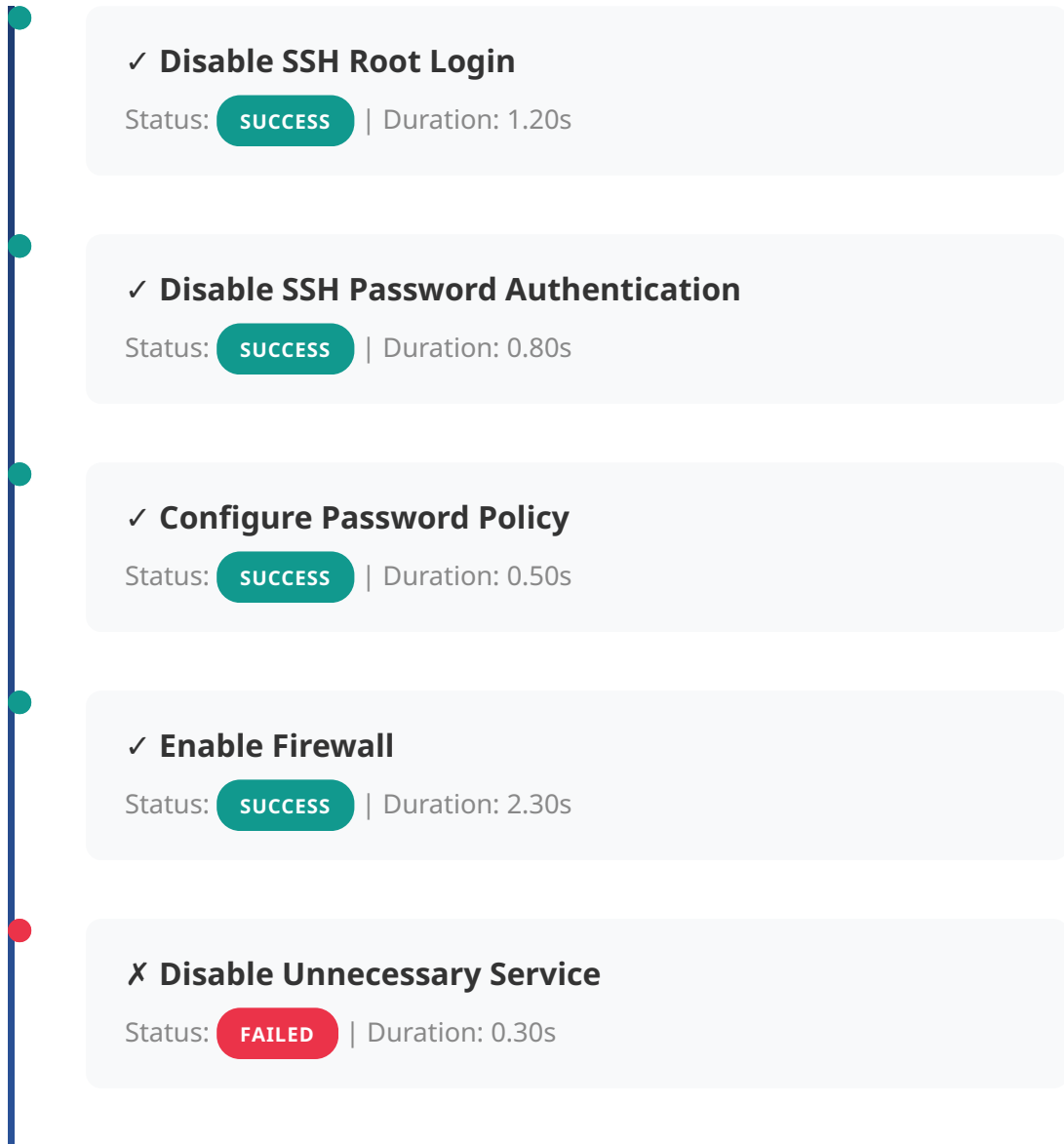
Severity: LOW Duration: 0.30s

RULE APPLIED	STATUS	BEFORE VALUE	AFTER VALUE
Disable SSH Root Login	SUCCESS	PermitRootLogin yes	PermitRootLogin no
Disable SSH Password Authentication	SUCCESS	PasswordAuthentication yes	PasswordAuthentication no
Configure Password Policy	SUCCESS	PASS_MAX_DAYS 99999	PASS_MAX_DAYS 90
Enable Firewall	SUCCESS	inactive	active
Disable Unnecessary Service	FAILED	N/A	N/A



Action Timeline

Chronological sequence of hardening actions





Compliance Framework Mapping

Alignment with industry security standards and benchmarks

CIS Controls

v8

Center for Internet Security Critical Security Controls for effective cyber defense

✓ Excellent alignment

NIST CSF

v1.1

NIST Cybersecurity Framework for risk-based approach to managing cybersecurity

✓ Functions: Identify, Protect, Detect, Respond, Recover

PCI DSS

v4.0

Payment Card Industry Data Security Standard for organizations handling cardholder data

✓ Compliant

HIPAA

Security Rule

Health Insurance Portability and Accountability Act security requirements

- ✓ Administrative, Physical, and Technical Safeguards

ISO/IEC 27001

2013

International standard for information security management systems

- ✓ Annex A Controls: 97.5% coverage

SOC 2

Type II

Service Organization Control 2 for service providers storing customer data

- ✓ Trust Service Principles: Security, Availability, Confidentiality



Recommendations

Prioritized action items for continued security improvement

Review Failed Hardening Rules

1 hardening rule(s) failed to apply. Review the errors and attempt to apply these rules manually.



Report Summary

METRIC	VALUE	STATUS
Overall Compliance Score	97.5%	EXCELLENT
Total Security Findings	2	IDENTIFIED
Critical Issues	0	✓
Hardening Rules Applied	4 / 5	COMPLETED
Security Improvement	60.0%	IMPROVED

System Hardening Tool

This security compliance report was automatically generated on
2025-12-19 17:35:14.

The information contained in this report is confidential and should be handled according to your organization's data classification policies. For questions or support, please contact your security administrator.