

Security Report

System Security Compliance Report

Generated: **2025-12-25**
18:54:59



Executive Summary

72.8%

Overall Compliance Score

Good security posture - Some improvements recommended

8

Total Findings

Security issues identified

1

Critical Issues

Require immediate attention

0

High Priority

Address as soon as possible

2

Medium Priority

Plan for resolution



Security Findings Distribution

Critical

1 issues



High

0 issues



Medium

2 issues



Low

1 issues



Detailed Security Findings

Complete list of identified security issues and vulnerabilities

FINDING	SEVERITY	CATEGORY	DESCRIPTION & REMEDIATION
SSH Configuration File Not Found	INFO	SSH Configuration	The SSH configuration file / etc/ssh/sshd_config was not found. SSH may not be installed or configured.
Password Maximum Age Too Long	MEDIUM	Password Policy	Password maximum age is set to 99999 days. Recommended: 90 days or less.
Password Minimum Age Too Short	LOW	Password Policy	Password minimum age is set to 0 days. Users can change passwords too frequently.
Password Minimum Length Not Set	MEDIUM	Password Policy	PASS_MIN_LEN is not configured in login.defs.

FINDING	SEVERITY	CATEGORY	DESCRIPTION & REMEDIATION
No Firewall Detected	CRITICAL	Firewall	Neither UFW nor iptables appears to be configured. A firewall is essential for system security.
/etc/passwd Permissions Correct	INFO	File Permissions	/etc/passwd has correct permissions (644).
/etc/shadow Permissions Correct	INFO	File Permissions	/etc/shadow has correct permissions (640).
No Unnecessary Services Found	INFO	Services	Common unnecessary services are not running.

Compliance Framework Mapping

Alignment with industry security standards and benchmarks

CIS Controls v8

Center for Internet Security Critical Security Controls for effective cyber defense

✓ Good 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

✗ Requires attention

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: 72.8% 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

Address Critical Security Issues

Found 1 critical security issue(s). These should be addressed immediately as they pose significant security risks.



Report Summary

METRIC	VALUE	STATUS
Overall Compliance Score	72.8%	GOOD
Total Security Findings	8	IDENTIFIED
Critical Issues	1	!

System Hardening Tool

This security compliance report was automatically generated on
2025-12-25 18:54:59.

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.