Test Security Report - PDF

System Security Compliance Report

Generated: **2025-11-23 16:27:56**

📊 Executive Summary

75.5%

Overall Compliance Score

Good security posture - Some improvements recommended

6

Total Findings

Security issues identified

1

Critical Issues

Require immediate attention

2

High Priority

Address as soon as possible

2

Medium Priority

Plan for resolution

4

Rules Applied

Successfully hardened

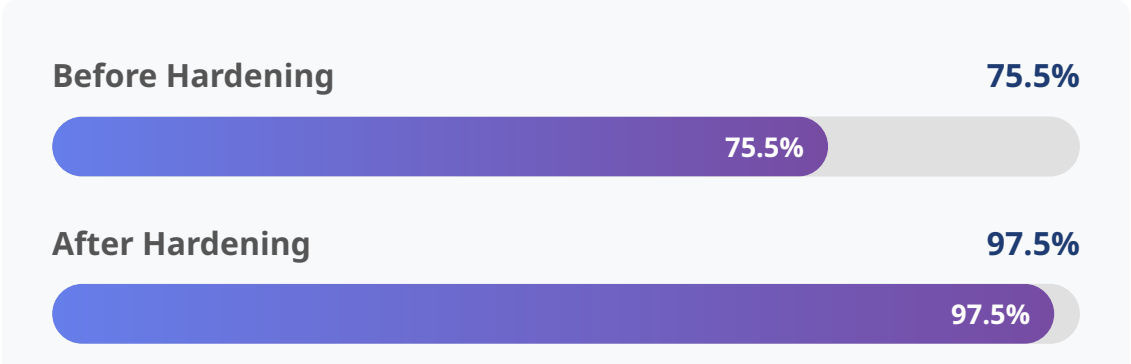
📈 Security Posture Improvement

Comparison of security status before and after hardening measures

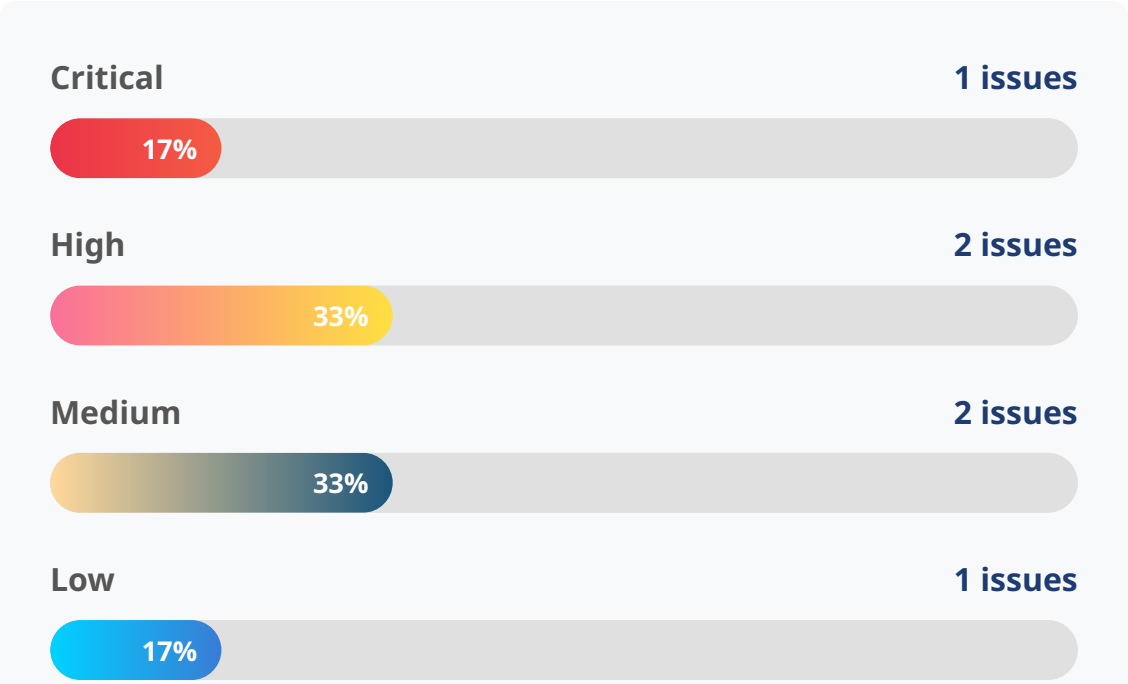
Before Hardening		After Hardening	
Critical:	1	Critical:	0
High:	2	High:	0
Medium:	2	Medium:	1
Low:	1	Low:	1
Total:	**6**	**Total:**	**2**

✓ 66.7% improvement in security posture
4 security issues successfully resolved

Compliance Score Progress



🔍 Security Findings Distribution



📋 Detailed Security Findings

Complete list of identified security issues and vulnerabilities

FINDING	SEVERITY	CATEGORY	DESCRIPTION & REMEDIATION
SSH Root Login Enabled	CRITICAL	Network Security	SSH server allows root user login which poses a security risk **Remediation:** Disable root login by setting 'PermitRootLogin no' in /etc/ssh/sshd_config
Weak Password Policy	HIGH	Authentication	Password minimum length is below recommended 12 characters **Remediation:** Update password policy to require minimum 12 characters
Firewall Not Configured	HIGH	Network Security	System firewall is not properly configured **Remediation:** Configure and enable firewall with appropriate rules

FINDING	SEVERITY	CATEGORY	DESCRIPTION & REMEDIATION
Missing Security Updates	MEDIUM	System Updates	15 security updates are available but not installed **Remediation:** Run system update to install security patches
World-Writable Files Found	MEDIUM	File System	Several files have overly permissive permissions **Remediation:** Review and restrict file permissions
Unnecessary Services Running	LOW	Services	Some unnecessary network services are enabled **Remediation:** Disable unused services to reduce attack surface

🛠️ Remediation Actions Taken

Security hardening measures applied to the system

Checkpoint Created: `checkpoint_abc123xyz`

System state saved for rollback capability

Disable SSH Root Login

SUCCESS

Changed configuration: `yes` → `no`

Severity: CRITICAL **Duration:** 1.20s

Enforce Strong Password Policy

SUCCESS

Changed configuration: `minlen=8` → `minlen=12`

Severity: HIGH **Duration:** 0.80s

Configure Firewall Rules

SUCCESS

Changed configuration: `disabled` → `enabled with rules`

Severity: HIGH **Duration:** 2.50s

Install Security Updates

SUCCESS

Changed configuration: `15 updates pending` → `all updates installed`

Severity: MEDIUM **Duration:** 45.00s

Disable Unnecessary Services

FAILED

Error: Service telnet not found on system

Severity: LOW **Duration:** 0.50s

RULE APPLIED	STATUS	BEFORE VALUE	AFTER VALUE	DURATION
Disable SSH Root Login	SUCCESS	`yes`	`no`	1.20s
Enforce Strong Password Policy	SUCCESS	`minlen=8`	`minlen=12`	0.80s
Configure Firewall Rules	SUCCESS	`disabled`	`enabled with rules`	2.50s
Install Security Updates	SUCCESS	`15 updates pending`	`all updates installed`	45.00s
Disable Unnecessary Services	FAILED	`N/A`	`N/A`	0.50s

⏱️ Action Timeline

Chronological sequence of hardening actions

✓ **Disable SSH Root Login**

Status: SUCCESS | Duration: 1.20s

✓ **Enforce Strong Password Policy**

Status: SUCCESS | Duration: 0.80s

✓ **Configure Firewall Rules**

Status: SUCCESS | Duration: 2.50s

✓ **Install Security Updates**

Status: SUCCESS | Duration: 45.00s

✗ **Disable Unnecessary Services**

Status: FAILED | Duration: 0.50s

✅ 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: 75.5% 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

Address Critical Security Issues

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

Resolve High Priority Issues

Found 2 high priority issue(s). Address these issues as soon as possible.

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	75.5%	GOOD
Total Security Findings	6	IDENTIFIED
Critical Issues	1	!
Hardening Rules Applied	4 / 5	COMPLETED
Security Improvement	66.7%	IMPROVED

System Hardening Tool

This security compliance report was automatically generated on 2025-11-23 16:27:56.

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.