Test Security Report

Report ID: APT-1754978218 | Generated: 2025-08-12 09:26:58

Target: test.example.com

Executive Summary

Overall Risk Level: Critical

Total Findings: 5

Scan Duration: 0:00:00

Scanners Used: test_scanner

Findings Breakdown

- Critical: 1
- High: 1
- Medium: 1
- Low: 1
- Informational: 1

Detailed Findings

Network Services

Open SSH Port

INFO

Description: SSH service is running on port 22

Details: SSH (Secure Shell) service detected on port 22. This is normal for servers that require remote administration.

Recommendation: Ensure SSH is properly configured with key-based authentication and disable password authentication.

Web Services

HTTP Service Detected

LOW

Description: Web server running on port 80

Details: HTTP web server detected. Consider redirecting HTTP traffic to HTTPS.

Recommendation: Configure HTTP to HTTPS redirect for better security.

Outdated Web Server

HIGH

Description: Web server version appears to be outdated

Details: The web server version contains known security vulnerabilities.

Recommendation: Update the web server to the latest stable version.

SSL/TLS

SSL Certificate Issue

MEDIUM

Description: SSL certificate is self-signed

Details: The SSL certificate is self-signed and not trusted by browsers.

Recommendation: Install a valid SSL certificate from a trusted Certificate Authority.

Web Application

Critical Security Flaw

CRITICAL

Description: Critical vulnerability in web application

Details: A critical security vulnerability that could allow remote code execution.

Recommendation: Apply security patches immediately and consider taking the service offline until fixed.

Generated by Auto-Pentest Framework v0.9.1