Network and Vulnerability Assessment – OpenVAS Web Server Scan

2025-09-29

Network and Vulnerability Assessment – OpenVAS Web Server Scan

Prepared for Applied Information Assurance Projects
Date: September 2025

---

1. Executive Summary

This report summarizes the results of a comprehensive **vulnerability assessment** performed on a web server using **Greenbone OpenVAS**.
The objective was to evaluate exposed services, identify potential security weaknesses, and provide mitigation recommendations aligned with **NIST CSF** and **OWASP** best practices.

> **Objective:** To demonstrate how automated vulnerability scanning supports risk-based assurance, compliance alignment, and proactive defense for web-facing systems.

---

2. Scan Overview

Parameter	Details
Scan Target	Internal Web Server (10.200.x.x)
Scan Profile	Full and Fast (Unauthenticated)
Feed Version	Greenbone Community Feed – October 2025
Duration	1 hour 17 minutes
Total Results	247 vulnerabilities detected
Severity Range	Low (2.0) → Critical (9.8)
CVSS Standard	CVSS v3.1

The scan covered HTTP/HTTPS, SSH, and supporting web application components.

---

3. Key Findings

Severity	Category	Example Vulnerability	CVSS Score
Critical	Outdated OpenSSL library	TLS 1.0 / 1.1 enabled; multiple CVEs (CVE-2023-3446)	9.8
High	Apache server misconfiguration	Directory listing and default test pages exposed	8.6
High	PHP version disclosure	PHP 7.4.x EOL – remote code execution risk	8.1
Medium	Weak HTTP response headers	Missing CSP and HSTS headers	6.5
Medium	Self-signed certificate	Untrusted root CA detected	6.1
Low	ICMP timestamp replies	Host fingerprinting information leak	3.4

> **Observation:** The server exposes several outdated components and protocol weaknesses.
> No active exploitation was detected, but the configuration state increases risk to data integrity and service availability.

---

4. Risk Analysis

Vulnerabilities were ranked using **CVSS v3.1** scoring and mapped to **NIST CSF functions** to support structured remediation.

Risk Level	Action Priority	NIST CSF Function
Critical (≥9.0)	Patch immediately; verify post-remediation scan	Protect (PR) / Respond (RS)
High (7.0–8.9)	Apply updates; disable insecure protocols	Protect (PR)
Medium (4.0–6.9)	Adjust configurations; improve headers and TLS policy	Detect (DE) / Protect (PR)
Low (<4.0)	Monitor and log for anomalous activity	Identify (ID) / Detect (DE)

---

5. Remediation Recommendations

1. **Patch Management:**
   - Upgrade OpenSSL ≥ 3.x and disable deprecated TLS versions.
   - Update Apache HTTP Server and PHP runtime to latest supported releases.
2. **Web Configuration Hardening:**
   - Disable directory indexing and remove test pages.
   - Enforce HTTPS only; apply strong cipher suites (AES-256-GCM).
3. **Security Headers:**
   - Implement HSTS, CSP, X-Frame-Options, and X-Content-Type-Options headers.
4. **Certificate Management:**
   - Replace self-signed certificates with CA-issued equivalents.
5. **Monitoring & Re-assessment:**
   - Integrate OpenVAS reports with SIEM or log analysis tools.
   - Schedule monthly scans to validate remediation progress.

---

6. Assurance Alignment

Framework	Relevant Controls / Domains
NIST CSF 2.0	Identify (ID.AM), Protect (PR.IP), Detect (DE.CM)
ISO 27001:2022	A.12 Operations Security, A.18 Compliance
OWASP Top 10	A05 Security Misconfiguration, A06 Vulnerable Components
NIST SP 800-115	Technical Testing and Vulnerability Management Lifecycle

> Mapping findings to standardized controls enables measurable improvement of system assurance posture.

---

7. Conclusion

The OpenVAS scan of the internal web server revealed multiple high-risk vulnerabilities related to outdated software and insecure defaults.
Addressing these issues through timely patching, configuration hardening, and continuous scanning will significantly improve confidentiality, integrity, and availability.
This assessment demonstrates how automated vulnerability management directly supports **risk reduction** and **compliance validation** within an **information assurance framework**.

---

8. References

1. Greenbone Networks. *Greenbone Community Edition Documentation.*
2. NIST SP 800-115: *Technical Guide to Information Security Testing and Assessment.*
3. OWASP Top 10 (2021) and ASVS v4.0.
4. ISO/IEC 27001:2022 – Information Security Management Systems.

□ Download Full Report (PDF)