Security Audit of a Cloud Application on OpenStack using OpenVAS

Auditing cloud applications hosted on OpenStack requires a structured approach given the platform's complexity. Using OpenVAS, an open-source vulnerability scanner, enables identification of critical weaknesses such as outdated Horizon dashboard components, weak TLS configurations, and exposed API endpoints. These vulnerabilities can facilitate remote code execution, privilege escalation, or man-in-the-middle attacks if unaddressed (Greenbone, 2023).

Mitigation strategies should align with ISO/IEC 27001, which emphasises systematic risk management and security controls. Relevant measures include enforcing patch management (A.12.6), applying strict access control and multi-factor authentication (A.9), and maintaining robust cryptographic configurations (A.10) (ISO, 2013). Hardening security groups, closing unnecessary ports, and implementing HTTP security headers further reduce attack surfaces (OpenStack Foundation, 2020).

Industry examples highlight these concerns. The BradStack project showed that applying hardening and penetration testing to OpenStack deployments significantly improved resilience (Mohammed et al., 2017). Earlier work on OpenStack Essex revealed flaws such as unencrypted dashboards and insecure credential handling, underscoring the importance of secure configuration (Jin et al., 2013). Broader guidance from the NIST Cybersecurity Framework and the Cloud Security Alliance Cloud Controls Matrix supports integration of vulnerability scanning with governance and compliance efforts (NIST, 2018; CSA, 2021).

In conclusion, OpenVAS provides actionable insight into technical vulnerabilities. However, true assurance requires embedding these findings into a compliance framework such as ISO/IEC 27001 and adopting continuous monitoring to sustain security posture across dynamic cloud environments.

References:

Mohammed, B. et.al. (2017) *Technical Report on Deploying a highly secured OpenStack Cloud Infrastructure using BradStack as a Case Study.* Available at: https://doi.org/10.48550/arXiv.1712.09152

Cloud Security Alliance (2021) *Cloud Controls Matrix*. Available at: https://cloudsecurityalliance.org/research/ccm/(Accessed: 9 September 2025).

Greenbone (2023) *OpenVAS Vulnerability Scanner*. Available at: https://www.greenbone.net (Accessed: 9 September 2025).

ISO (2013) *ISO/IEC 27001:2013 Information Security Management Systems – Requirements*. Geneva: International Organization for Standardization.

Jin, H., Ibrahim, S., Qi, Z. and Chen, H. (2013) *Cloud Penetration Testing on OpenStack Essex*. Available at: https://doi.org/10.5121/ijccsa.2012.2604

NIST (2018) *Framework for Improving Critical Infrastructure Cybersecurity*. Version 1.1. Gaithersburg: National Institute of Standards and Technology.

OpenStack Foundation (2020) *OpenStack Security Guide*. Available at: https://docs.openstack.org/security-guide/(Accessed: 9 September 2025).