Unit 7 – Formative Activity

This is an outline for a security audit report on a virtual instance within an OpenStack cloud environment. The audit was conducted using the OpenVAS vulnerability scanner. The process was challenging due to the limitations of my outdated lab hardware, which made it difficult to run the scans efficiently. The scan results (attached) were analysed, and mitigation strategies were developed based on industry standards, including ISO/IEC 27001.

Security Audit Report Outline

The primary objective was to identify and report on security risks present within the environment. The attached screenshot from the OpenVAS dashboard, taken after the scan completion, shows the results.

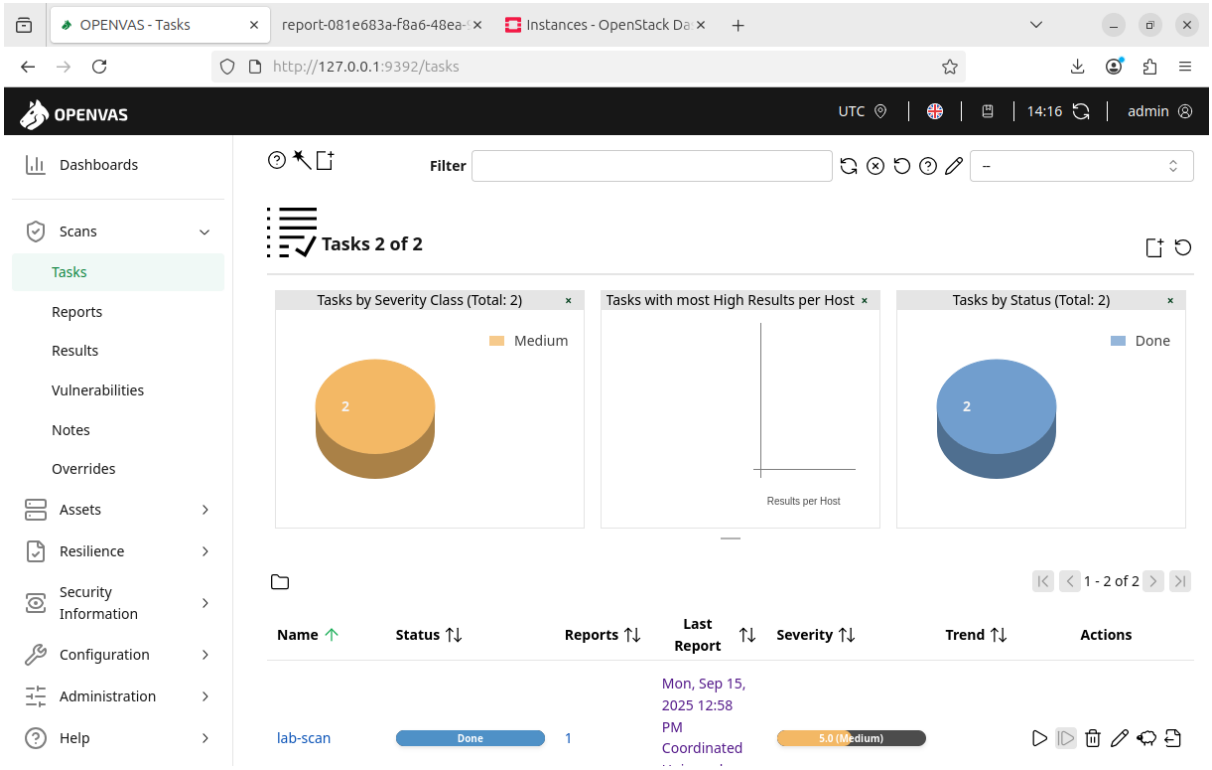

Figure 1: OpenVAS Dashboard with scanning result

Vulnerabilities Found

The scan, which ran from 12:58:56 UTC to 14:05:34 UTC on September 15, 2025, identified two medium-level vulnerabilities on the host 10.0.2.15. Prior to filtering, the scan detected 248 results; however, only two were included in the final report based on the filtering criteria, which required a minimum Quality of Detection (QoD) of 70% and excluded issues with threat levels such as "Log," "Debug," and "False Positive". The two vulnerabilities found were:

- **Mailserver VRFY/EXPN Requests:** The mail server on the host responds to VRFY and/or EXPN requests. A VRFY request for 'root' returned '252 2.0.0 root'. This is a medium-level threat with a CVSS score of 5.0 and a QoD of 99%.

- **Deprecated TLS Protocols:** The system was found to be using deprecated TLSv1.0 and TLSv1.1 protocols in addition to TLSv1.2+. This is a medium-level threat with a CVSS score of 1.3 and a QoD of 98%. These older protocols have known cryptographic flaws, such as
  BEAST (CVE-2011-3389) and FREAK (CVE-2015-0204), which could allow an attacker to eavesdrop on connections and access sensitive data (Stanek, 2017).

Mitigation Strategies

- **Mailserver:** The solution is to disable the VRFY and/or EXPN commands on the mail server. For Postfix, this can be done by adding 'disable_vrfy_command = yes' to the 'main.cf' file. For Sendmail, the option 'O PrivacyOptions=goaway' should be added. This aligns with ISO/IEC 27001 by reducing the amount of information an attacker can gather about user accounts, thereby protecting data from unauthorised access (Folorunso *et al*., 2024).
- **TLS Protocols:** It is recommended to disable the deprecated TLSv1.0 and TLSv1.1 protocols and use only TLSv1.2+. This mitigates the risk of known cryptographic attacks and ensures that the system is not vulnerable to future exploits targeting these outdated protocols. This recommendation supports the ISO/IEC 27001 standard by ensuring the confidentiality and integrity of data in transit through strong encryption protocols (Moriarty and Farrell, 2021).

Compliance Adherence
The identified vulnerabilities and their mitigations directly relate to ISO/IEC 27001 Annex A controls. By addressing these issues, the organisation improves its security posture and demonstrates a commitment to maintaining a secure environment. The fixes align with controls for access control (A.9) and cryptography (A.10), specifically in protecting information and ensuring secure communication (Kitsios, Chatzidimitriou and Kamariotou, 2023).

Word count: 457

References:
Folorunso, A., Mohammed, V., Wada, I. and Samuel, B. (2024) ‘The impact of ISO security standards on enhancing cybersecurity posture in organizations’, *World Journal of Advanced Research and Reviews*, 24(1), pp. 2582–2595. Available at: https://doi.org/10.30574/wjarr.2024.24.1.3169

Kitsios, F., Chatzidimitriou, E. and Kamariotou, M. (2023) ‘The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector’, *Sustainability*, 15(7). Available at: https://doi.org/10.3390/su15075828

Moriarty, K. and Farrell, S. (2021) ‘Deprecating TLS 1.0 and TLS 1.1’, *Internet Engineering Task Force (IETF)* [Preprint]. Available at: https://doi.org/10.17487/rfc8996

Stanek, M. (2017) ‘Secure by default - the case of TLS’, *arXiv (Cornell University)* [Preprint]. Available at: https://doi.org/10.48550/arxiv.1708.07569