Yuvin Perera

Summary of Nessus Findings

The Nessus scan conducted on the target system 10.137.0.149 identified a total of 42 vulnerabilities, categorized into three medium level and thirty nine low level findings. No critical or high level vulnerabilities were detected. The notable vulnerabilities revolve primarily around SSL certificate issues, which, while not immediately severe, pose a potential risk to the system's security posture.

The first notable finding is that the SSL certificate presented by the server cannot be trusted. This issue arises because the certificate cannot be verified, which could allow attackers to perform man in the middle (MITM) attacks. To mitigate this, the recommendation is to replace the certificate with one issued by a trusted Certificate Authority (CA). Another finding highlights the use of a self signed SSL certificate, which limits the trustworthiness of secure connections. The proposed solution is to replace the self-signed certificate with a CA signed SSL certificate to ensure proper verification and trust. Additionally, the scan flagged an SSL certificate nearing expiry, which could result in the loss of secure communication if not addressed. It is recommended to renew the certificate promptly.

While no high or critical vulnerabilities were discovered, the presence of medium level SSL vulnerabilities indicates a need for proactive management of encryption settings and certificates. The low level findings, although not urgent, represent potential entry points for attackers and should not be overlooked. Regular updates to server configurations, certificates, and software are essential to reducing exposure to common attack vectors.

In conclusion, the Nessus scan revealed manageable security issues that, if addressed, will significantly enhance the overall security posture of the system. Proper handling of SSL vulnerabilities and continuous auditing will ensure the system remains protected against common threats. For a comprehensive list of vulnerabilities, refer to the attached Nessus report.

Sprint 1 Nessus Report.pdf