Review Agent Report

Target: 192.168.49.141 | Generated: 2026-02-19 10:27:40

Review Summary

Total Reviewed	2
Approved	2
Rejected	0
Avg Security Score	9.0

Per-Finding Review Details

ID	Title	Approve	Optimal	Score	Feedback	Concerns	Improvements
openscap_001	Install AIDE	YES	No	9	Remediation successfully addressed the vulnerability; however, the script lacks comprehensive error handling and platform checks.	Script does not verify dnf install success beyond exit code It only checks for rpm query but does not handle other package managers No explicit check for root privileges or error handling for non-successful installs	Add verification of dnf install return code and output Include a check for supported OS families before using dnf Add logging or output to indicate actions taken Consider using yum or alternative package manager detection for broader compatibility
openscap_002	Build and Test AIDE Database	YES	No	9	The remediation successfully creates and installs the AIDE database, resolving the vulnerability. The approach works but could be improved for broader compatibility and cleanup.	Script assumes presence of kernel-core rpm and only runs when aide is missing, which may not be necessary for the database creation step. No verification that /var/lib/aide/aide.db.new.gz exists before copying. Does not clean up the temporary .new.gz file after successful copy. Limited to RPM-based systems; not portable to Debian-based platforms.	Check for existence of the .new.gz file before copying and handle missing case gracefully. Remove or archive aide.db.new.gz after successful database installation. Add support for Debian/Ubuntu by using apt instead of dnf. Include error handling and logging for auditability. Ensure file permissions and ownership are set correctly on the database file.