Review Agent Report

Target: 192.168.1.150 | Generated: 2026-02-19 03:12:11

Review Summary

Total Reviewed	6
Approved	6
Rejected	0
Avg Security Score	7.8

Per-Finding Review Details

ID	Title	Approve	Optimal	Score	Feedback	Concerns	Improvements
openscap_012	Ensure PAM Enforces Password Requirements - Minimum Different Characters	YES	No	8	Remediation successfully sets difok to 8, resolving the vulnerability, but the change is somewhat blunt and could be refined.	Hardcoded difok value of 8 may be overly strict or inappropriate for all environments sed replacement only targets exact string 'difok = 0' and may not handle comments or variations No check for other password policy parameters that should be aligned with complexity requirements No explicit reload of PAM modules to apply the change	Determine appropriate difok value through policy review or testing rather than defaulting to 8 Use a more robust configuration edit that matches the key regardless of surrounding whitespace or comments Validate the new password policy against existing policies and test password changes Include a step to reload or restart the relevant PAM services if required

ID	Title	Approve	Optimal	Score	Feedback	Concerns	Improvements
openscap_014	Ensure PAM Enforces Password Requirements - Maximum Consecutive Repeating Characters from Same Character Class	YES	No	8	The remediation successfully resolves the vulnerability by setting maxclassrepeat=1, but the approach lacks backup, validation, and handling of multiple config files.	Uses a single sed command without backing up the original configuration. Does not explicitly handle configuration files in /etc/security/pwquality.conf.d that may contain the directive. No verification after change beyond the scan pass. Hard■coded value may be too restrictive or not aligned with desired policy.	Create a backup of /etc/security/pwquality.conf and any files in /etc/security/pwquality.conf.d before modification. Use a more explicit pattern to target the directive only (e.g., ensure it matches the key exactly). Validate the resulting configuration syntax with pwquality-cracklib-test or similar. Consider making the value configurable rather than hard■coding to 1.
openscap_015	Ensure PAM Enforces Password Requirements - Minimum Different Categories	YES	No	8	The remediation successfully sets minclass to 4, resolving the OpenSCAP finding and passing verification.	Direct sed edit without creating a backup of the original file May not handle whitespace variations or comments reliably Does not verify the existence of the setting before replacement Lacks idempotent checks that could lead to unintended changes on re■run	Create a backup of /etc/security/pwquality.conf before modification Use a configuration management tool or package to enforce the setting consistently Employ a more specific regex that matches optional whitespace and comments Add a validation step to confirm the new value is applied correctly
openscap_017	Ensure PAM Enforces Password Requirements - Minimum Uppercase Characters	YES	No	6	The remediation correctly sets ucredit to -1, eliminating the openscap_017 finding, but the implementation is simplistic and could be improved for robustness and clarity.	Uses a broad sed pattern that may unintentionally modify commented lines or other settings Does not backup the original configuration file before modification Does not verify the resulting ucredit value after change Does not specifically target only the ucredit line with word boundaries May not handle multiple *.conf files correctly	Add a backup of /etc/security/pwquality.conf before modification Use a more precise regex such as '^ucredit[[:space:]]*' to match only the ucredit line Consider using a configuration management tool or pam_pwquality.d include files Validate the effective policy after change Document the change in change management system

ID	Title	Approve	Optimal	Score	Feedback	Concerns	Improvements
openscap_021	Configure Multiple DNS Servers in /etc/resolv.conf	YES	No	9	Fix successfully resolves the vulnerability.	Uses base64 encoding to write the file, which is unnecessary and obscure. Overwrites /etc/resolv.conf without preserving existing configuration. Does not verify that at least two distinct DNS server entries are present. Lacks idempotency; repeated runs may not behave predictably.	Directly edit /etc/resolv.conf to add 'nameserver' lines for at least two DNS servers. Check that the file already contains the required entries before modifying. Preserve any existing search or options directives. Validate the final content to ensure at least two unique nameserver entries exist. Use a configuration management tool or systemd-resolved for persistent, idempotent changes.
openscap_025	Ensure Chrony is only configured with the server directive	YES	No	8	The remediation successfully eliminates pool lines and adds a server directive, causing the OpenSCAP rule to pass.	The sed command only targets a specific pool line; other pool entries may remain. No backup of /etc/chrony.conf was made before modification. Appending a server line with echo may create duplicate entries. The service was not reloaded or validated after changes.	Create a backup of the configuration file before editing. Use a broader sed pattern to comment out any line starting with 'pool'. Verify the resulting configuration with 'chronyc sources' or 'systemctl reload chronyd'. Ensure only server directives remain and no unintended directives are present.