#Linux Hardening Audit Tool – Project ReportAnalysis

* This project focuses on the design and implementation of a Linux Hardening Audit Tool developed using Python.

* The primary objective of this tool is to evaluate the security posture of a Linux systemby performing a series of predefined security checks, identifying misconfigurations, and safelyapplying corrective actions wherever possible.

* The tool follows real-world security practices andavoids applying critical fixes automatically, ensuring system stability and administrator control.

* The audit process begins with baseline security checks that inspect key system configurations such as SSH hardening, firewall status, password policies, file permissions, and service configurations.

* Each check returns a structured result including the check name, pass or fail status, risk severity, score impact, and whether the issue is safe to auto-fix.

* This modular design allows easy extensionof the tool by adding new security checks without modifying the core logic.

* One of the key strengths of this tool is its Safe Auto-Fix mechanism. Only non-intrusive and low-risk fixes are applied automatically.

* Examples include enforcing password complexity rules or disabling unused services.

* High-risk configurations such as SSH root login or kernel-level parameters are flagged but left for manual intervention.

* After applying fixes, the tool re-runs the audit to verifychanges and recalculate the system hardening score.

Report Generation, Scoring, and Conclusion

* The tool generates comprehensive reports in both HTML and PDF formats.

* HTML reports provide avisually appealing and interactive view of audit results, while PDF reports are suitable fordocumentation, submission, and offline review.

* Both reports include an audit summary, detailedcheck results, risk categorization, auto-fix status, and final hardening score.

* The hardening score is calculated based on the cumulative impact of failed checks, providing a quantitative measure of system security.

* This scoring approach ensures transparency and avoids misleading results.

* Improvements in score are only reflected after verified fixes, reinforcing the reliability of the audit process.

* The terminal output mirrors the report content, offering real-time feedback during execution.

* From an academic and practical perspective, this project demonstrates core cybersecurity principles such as risk assessment, defense-in-depth, least privilege, and secure configuration management

* It also highlights the importance of automation with caution, ensuring that security tools do not introduce instability.

* Overall, the Linux Hardening Audit Tool serves as a practical andextensible solution for system security assessment and is well-suited for educational,demonstration, and entry-level professional use.