SMART INDIA HACKATHON 2025

TITLE PAGE

Problem Statement ID – SIH25237

Problem Statement Title – Multi-Platform System Hardening Tool

Theme – Blockchain & Cybersecurity

PS Category – Software

Team ID – 56394

Team Name – SentineIX

Multi-Platform System Hardening Tool

SMART INDIA HACKATHON 2025

Problem

Modern enterprise systems rely heavily on Windows and Linux servers and desktops. Out-of-the-box, these operating systems often have weak security defaults — like loose password policies, open services, or outdated configurations.

While frameworks like CIS Benchmarks exist, applying them is still:

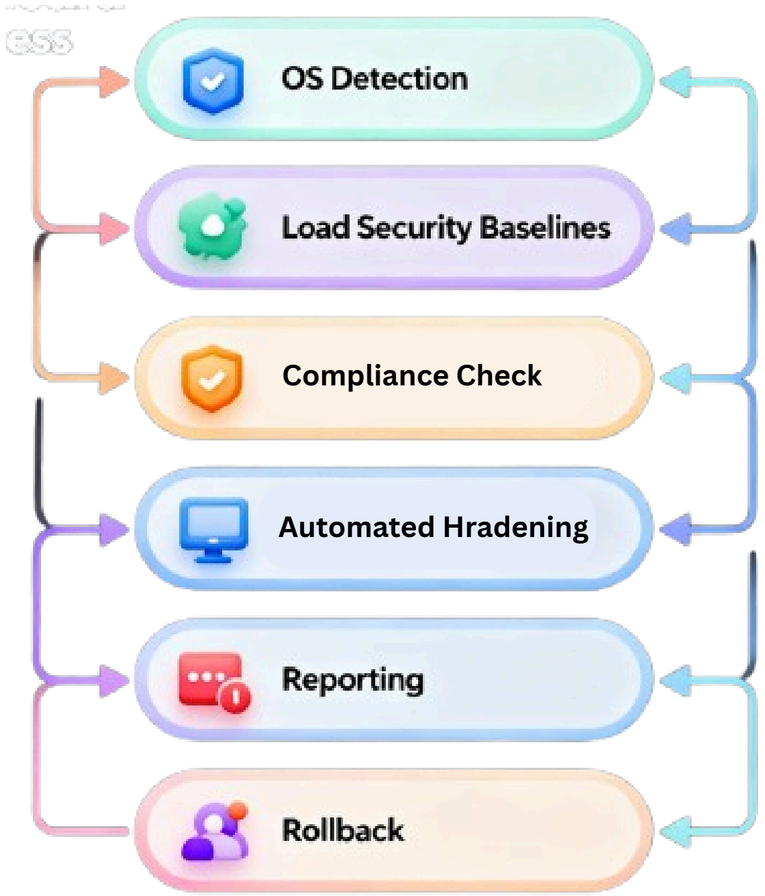
- **Manual and time-consuming (hundreds of checks per system)**
- **Error-prone and inconsistent (different admins apply different steps)**
- **Difficult to audit (no single source of truth for compliance)**
- **Hard to roll back (once a setting is changed, restoring is tricky)**

This leaves organizations exposed to misconfigurations, data breaches, and system compromises.

✨ **In short: The problem is the lack of a simple, automated, cross-platform way to harden and audit Windows & Linux systems consistently and safely.**

Instance of Approach

How we plan to achieve the solution step by step:



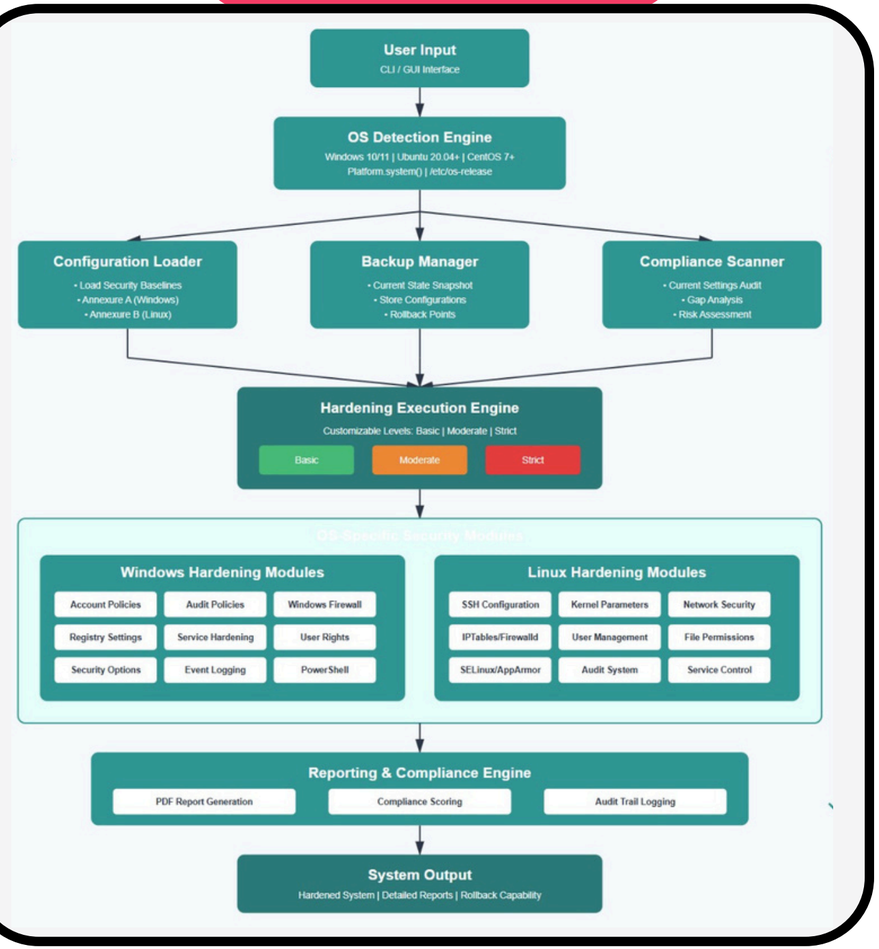
Solution

An **automated, cross-platform tool** for secure OS hardening:

- **Supports Windows, Ubuntu, CentOS**
- Detects OS & applies modular policies **(basic → strict)**
- **Enforces** Annexure A (Windows) & Annexure B (Linux) **parameters**
- **Generates compliance reports** (before/after, success/fail)
- **Offers CLI + optional GUI**
- **Provides rollback** to previous safe state

TECHNICAL APPROACH

WorkFlow Diagram



Working Principle

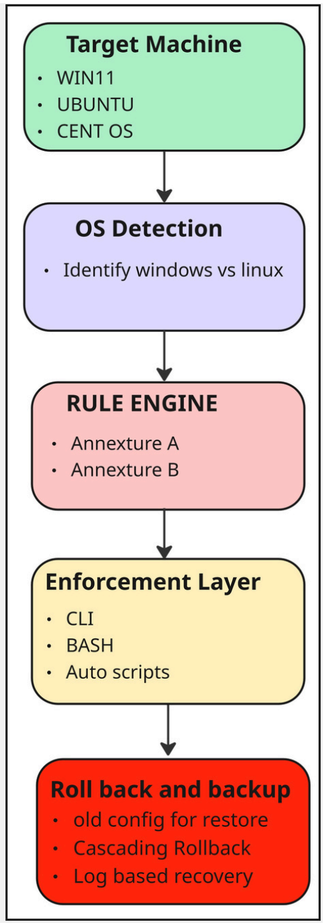
The proposed tool operates on the principle of detect, assess, enforce, verify, report, and rollback. It first identifies the underlying operating system—Windows 10/11, Ubuntu, or CentOS and loads the corresponding hardening policies.

It then assesses the current state of each security parameter, securely storing the original values to enable rollback if required. Based on the chosen hardening profile (basic, moderate, or strict), the tool enforces the appropriate configurations by applying system commands, registry edits, or configuration file updates.

Each change is immediately verified to ensure successful application, and detailed logs are maintained. The tool generates reports showing the previous and current states of each parameter, along with success or failure status and severity ratings.

If the administrator opts for rollback, the tool restores the system to its original configuration using the stored baseline.

System Architecture

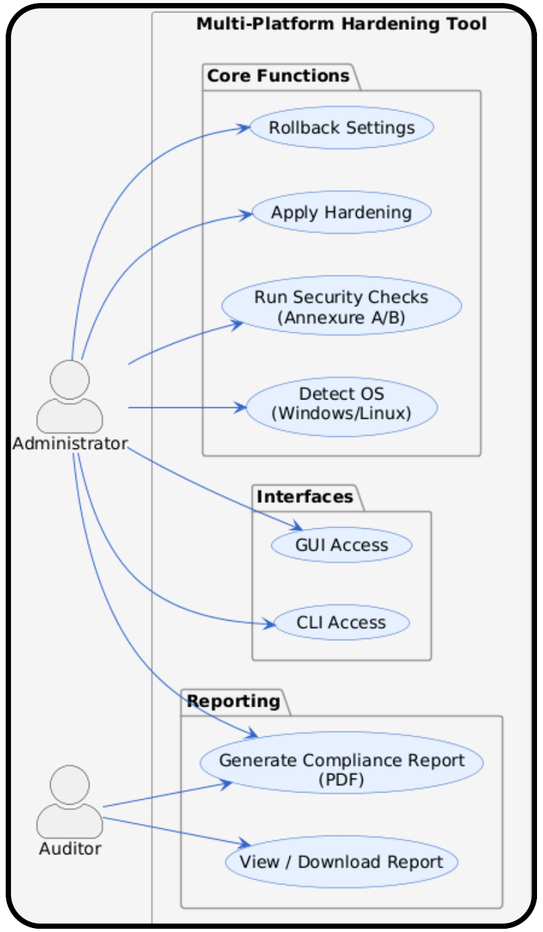


TECHNOLOGY STACK

CentOS · Windows 11 · GO · VirtualBox

FEASIBILITY AND VIABILITY

Feasible Use Case



Viability

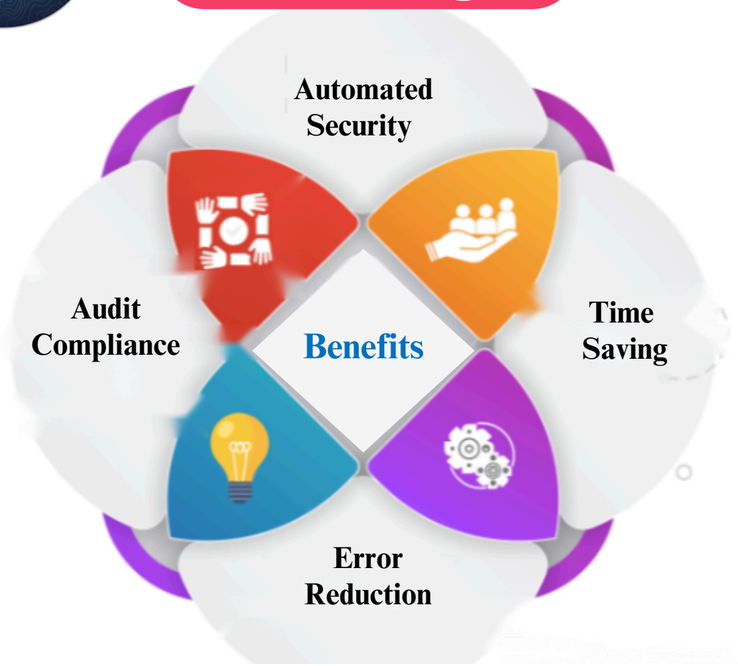
- Technical Feasibility
- Security Standard Availability
- Operational Viability
- Enterprise Relevance
- Administrator Impact

Challenges	Solution
Manual Security Configuration	Automated Hardening Engine
Platform Specific Difference	OS-Specific Modules
No Audit Tracking	Comprehensive Logging System
Risky Config Changes	Built Roll - Back Mechanism
Complex Compliance Checking	Automatic Report Generation

INFERENCE : https://sih.gov.in/dataset/Annexure_A_B_NTRO_SIH25237.pdf

IMPACT AND BENEFITS

Advantages



Uniqueness

- 01 Cross Platform Support
- 02 CIS Benchmark Integration
- 03 Automated Rollback
- 04 Real - time Reporting

Dependencies

- Administrator privileges on target system
- Network connectivity for distributed deployment
- Backup storage for configuration snapshot
- Trained personal for toll adoption
- Compliance Framework documentation

IMPACT

RESEARCH AND REFERENCES

SMART INDIA HACKATHON 2025

Link & Resources

https://sih.gov.in/dataset/Annexure_A_B_NTRO_SIH25237.pdf

https://docs.microsoft.com/security

https://ubuntu.com/security

https://wiki.centos.org/HowTos(2f)OS_Protection.html

https://www.cisecurity.org/cis-benchmarks

Prototype