**Software Requirements Specification (SRS)**

**Project Title:** Linux Hardening Audit Tool (L-HAT)

**Prepared by:** Nikhil Shakya  
**Domain:** Cybersecurity / System Administration  
**Platform:** Linux (Ubuntu, CentOS, Debian)

### 1. Introduction

#### 1.1 Purpose

This document outlines the software requirements for the Linux Hardening Audit Tool (L-HAT), a script-based auditing solution aimed at assessing and improving the security configuration of Linux systems. The tool evaluates compliance with CIS Benchmarks and provides actionable hardening recommendations.

#### 1.2 Scope

L-HAT will:

* Audit firewall rules, running services, SSH configuration, file permissions, and rootkit indicators.
* Generate a CIS Benchmark-based security score.
* Output reports in TXT, HTML, or JSON format.
* Provide structured, modular, and extensible functionality.
* Be fully Dockerized for portability and isolated execution.

#### 1.3 Intended Audience

* System Administrators
* Security Auditors
* DevSecOps Engineers
* Educational Institutions

#### 1.4 Definitions

* **CIS Benchmarks:** A set of industry best practices for securing systems.
* **Rootkit:** Malware designed to gain unauthorized root-level access.

### 2. Overall Description

#### 2.1 Product Perspective

L-HAT is a standalone command-line utility. It does not require a client-server model or GUI. It operates on any Linux distribution with Python or Bash installed. It is fully Dockerized to ensure consistent environments and easy deployment.

#### 2.2 Product Functions

* System auditing and benchmarking
* Logging and report generation
* Optional webhook-based alerting
* Optional live remediation prompts

#### 2.3 User Characteristics

* Users are expected to have root or sudo access.
* Users should understand basic Linux commands.

#### 2.4 Constraints

* Requires Python 3.x or Bash 5+
* Must run with elevated privileges
* Internet access required for auto-update and webhook features
* Must support containerization via Docker

### 3. Functional Requirements

#### 3.1 Firewall & Network Audit

* Check status of ufw, iptables, or firewalld
* List open ports via ss, netstat, or optional nmap
* Detect and log unused or insecure open ports

#### 3.2 Unused Services Audit

* List active services using systemctl
* Cross-check against an allowlist of essential services
* Flag legacy or insecure services (e.g., telnet, rsh)

#### 3.3 SSH Configuration Audit

* Parse /etc/ssh/sshd\_config for:
  + PermitRootLogin
  + PasswordAuthentication
  + MaxAuthTries
  + Protocol
  + Port
* Highlight insecure or default settings

#### 3.4 File Permission Check

* Validate permissions and ownership for:
  + /etc/passwd (should be 644)
  + /etc/shadow (should be 600)
* Log deviations from secure defaults

#### 3.5 Rootkit and Malware Checks

* Integrate or call chkrootkit or rkhunter
* Provide fallback manual checks for:
  + Suspicious binaries
  + Hidden processes
  + Kernel module anomalies

#### 3.6 CIS Benchmark Scoring

* Evaluate compliance with CIS Benchmark v1.0
* Assign weight and compute final score
* Breakdown by category: Network, User, Service, File System

#### 3.7 Report Generation

* Summarize all findings in structured format:
  + ✅ Passed Checks
  + ⚠️ Warnings
  + ❌ Critical Findings
* Export as .txt, .json, and optionally .html
* Include timestamp and host metadata

#### 3.8 Advanced Features

* **Auto-Update:** Fetch latest scripts, signatures, or CIS benchmark definitions
* **Webhook Integration:** Push alerts to Slack/Discord/Email
* **Live Hardening (Opt-in):** Offer in-place fixes after each failed check
* **HTML Dashboard (Optional):** Generate charts using Jinja2 + Plotly

### 4. Non-Functional Requirements

#### 4.1 Performance

* Should complete scans on a typical Linux system in under 3 minutes

#### 4.2 Portability

* Compatible with major Linux distributions
* Must be containerized using Docker for environment consistency

#### 4.3 Usability

* CLI-based, minimal learning curve
* Logs and reports are human-readable

#### 4.4 Security

* Must run with sudo/root
* No third-party data upload unless explicitly configured

### 5. System Design (Folder Structure)

linux-hardening-audit/  
├── src/  
│ ├── firewall\_audit.py  
│ ├── ssh\_config\_audit.py  
│ ├── file\_permissions.py  
│ ├── rootkit\_scan.py  
│ ├── cis\_score.py  
│ └── main.py  
├── reports/  
│ └── audit\_report\_TIMESTAMP.txt  
├── utils/  
│ └── logger.py  
├── Dockerfile  
├── requirements.txt  
├── README.md  
└── setup.sh

### 6. Appendix

* CIS Benchmark v1.0 Reference: <https://www.cisecurity.org/>
* chkrootkit: <http://www.chkrootkit.org/>
* psutil: <https://pypi.org/project/psutil/>
* Docker: <https://docs.docker.com/>

**End of Document**