**AutoSysGuard Documentation**

**Overview**

**AutoSysGuard** is a lightweight, automated system management tool designed for Linux-based systems. It aims to simplify system administration by automating tasks like system monitoring, backups, security audits, network monitoring, and more. It includes multiple functionalities that enhance system performance, security, and stability through an intuitive graphical interface powered by Python and Zenity, with backend logic written in Bash.

**Features**

**1. System Auditing (CIS Benchmarks Compliance)**

* Ensures that system settings align with CIS (Center for Internet Security) benchmarks.
* Audits the following areas:
  + Initial Setup
  + Filesystem Configuration
  + Service Clients
  + Network Configuration
  + Firewall Configuration
  + Access, Authentication, and Authorization
  + Time Synchronization
  + Special-purpose Services
* Provides recommendations and allows adjustments through a user-friendly interface.

**2. Network Monitoring**

* Monitors network traffic and detects anomalies using tools such as ARP Spoofing Detection, Brute Force Detection, and Intrusion Detection Systems.
* Key features include:
  + ARP Spoofing Detection
  + Network Traffic Monitor
  + Port Scan
  + SSH Hardening
  + VPN Configuration Check
  + DNS Spoofing Detection
  + Packet Sniffing Detection
  + SSL/TLS Configuration Analyzer for domain analysis
  + Rogue DHCP Server Detection
  + Wireless Network Security Check
  + IP Whitelisting Management
  + MAC Address Filtering

**3. System Monitoring**

* Monitors system resources like CPU usage, memory, and disk space in real time.
* Includes process monitoring and alerts for abnormal resource consumption.

**4. Performance Monitoring**

* Continuously tracks system performance metrics.
* Includes features for optimizing system health and identifying bottlenecks.

**5. Backup and Recovery**

* Allows automatic and scheduled backups of system data.
* Provides a simple, GUI-based backup configuration that allows users to select files, directories, or entire disk partitions for backup.
* Includes a stop button to pause or stop any ongoing backup processes.

**6. Antivirus & Threat Detection**

* Scans for malware and potential threats, ensuring a secure system environment.
* Designed to automatically detect, alert, and take corrective actions on identified threats.

**7. Additional Features**

* **Automation**: Tasks like software installation, system updates, and configurations can be automated.
* **Dependency Management**: Each script checks for required dependencies and prompts for installation if missing.
* **Error Handling**: Robust error handling to prevent conflicts or harm to the Linux kernel.
* **IP Scanning**: Allows users to scan IP ranges and provides detailed network information.

**Architecture**

AutoSysGuard is developed using a combination of Python and Zenity for the GUI and Bash scripting for backend logic:

* **Frontend (GUI)**:
  + The user interacts through a graphical interface built using Python and Zenity.
  + Provides simple dialogues and prompts for input (e.g., IP ranges, file paths, etc.).
* **Backend (Bash Scripts)**:
  + Handles the core functionality of system and network management tasks.
  + Scripts are modular and categorized based on tasks (e.g., backup, monitoring, security audits).
* **Integration**:
  + The frontend communicates with the backend to execute commands and display results to the user in real time.

**Usage Instructions**

**Installation**

1. Download the AutoSysGuard repository from the [GitHub link](https://github.com/Kunal8486).
2. Ensure Python, Zenity, and required dependencies are installed:

bash

Copy code

sudo apt install python3 zenity

**Running AutoSysGuard**

1. To start AutoSysGuard, navigate to the directory where it’s installed:

bash

cd /path/to/AutoSysGuard

1. Launch the main script:

bash

python3 main.py

**Backup Functionality**

1. Click on the "Backup" button from the GUI.
2. Select the files or directories to back up and specify the destination.
3. Choose backup frequency (automatic/scheduled).
4. Press "Start Backup."

**System Auditing**

1. Open the "System Audit" section.
2. Select audit categories (e.g., Network Configuration, Firewall Configuration).
3. Review the audit report and take corrective actions based on recommendations.

**Contributions**

Contributions to AutoSysGuard are welcome. If you wish to contribute:

1. Fork the repository from GitHub.
2. Create a new branch for your feature or fix.
3. Submit a pull request with a clear description of the changes.

**Contact Information**

For support or inquiries, contact **Kunal Kumar**:

* Email: kunalkumar8486@gmail.com
* LinkedIn: [Kunal Kumar](https://www.linkedin.com/in/kunalkumar8486/)
* GitHub: [Kunal8486](https://github.com/Kunal8486)

**Future Enhancements**

* **Virus Scanning**: An additional feature to automatically scan tar files for viruses.
* **Advanced Reporting**: More detailed insights on system performance and security threats.