Advanced Host-based IDS

Full Technical Documentation

1. Introduction

The Advanced Host-based IDS is a system designed to detect suspicious activity on a host machine by monitoring file changes, analyzing unexpected behavior, and optionally integrating ML-based anomaly models.

2. Features

- Real-time monitoring
- SHA-256 hashing & baseline tracking
- Smart quarantine logic
- Color-coded status indicators
- Logging & GUI controls
- Recursive scanning with adjustable intervals
- Auto baseline rebuilding

3. Technology Stack

Python — scanning, hashing, threading
Tkinter — GUI interface
hashlib — cryptographic SHA-256
JSON — metadata storage
OS / Shutil — file operations

4. System Overview

1. User selects a directory
2. Baseline hashes are generated
3. Monitoring detects new/modified/deleted files
4. Alerts are displayed in real time
5. Suspicious files can be quarantined
6. Baseline updates automatically

5. How to Use

Step 1: Run

```
python hbis.py
```

Step 2: Choose a directory
Step 3: Start monitoring
Step 4: Manage quarantine

Step 5: View logs

6. Paths Used

Baseline: ~/.simple_hids_baseline.json
Quarantine Folder: ~/.simple_hids_quarantine/
Quarantine Index: quarantine_index.json
Log File: ~/.simple_hids_log.txt

7. License

MIT License — fully open for modification and reuse.

8. Contact

GitHub Repository:
https://github.com/adarsht9555/Advanced-Host-based-IDS