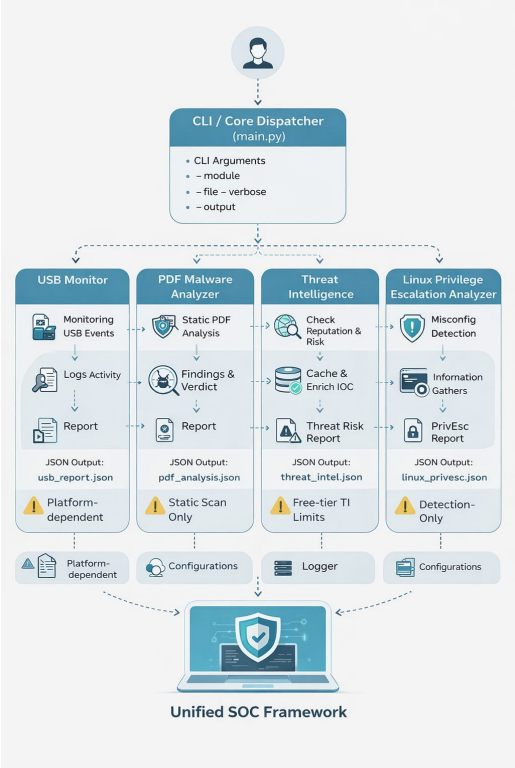
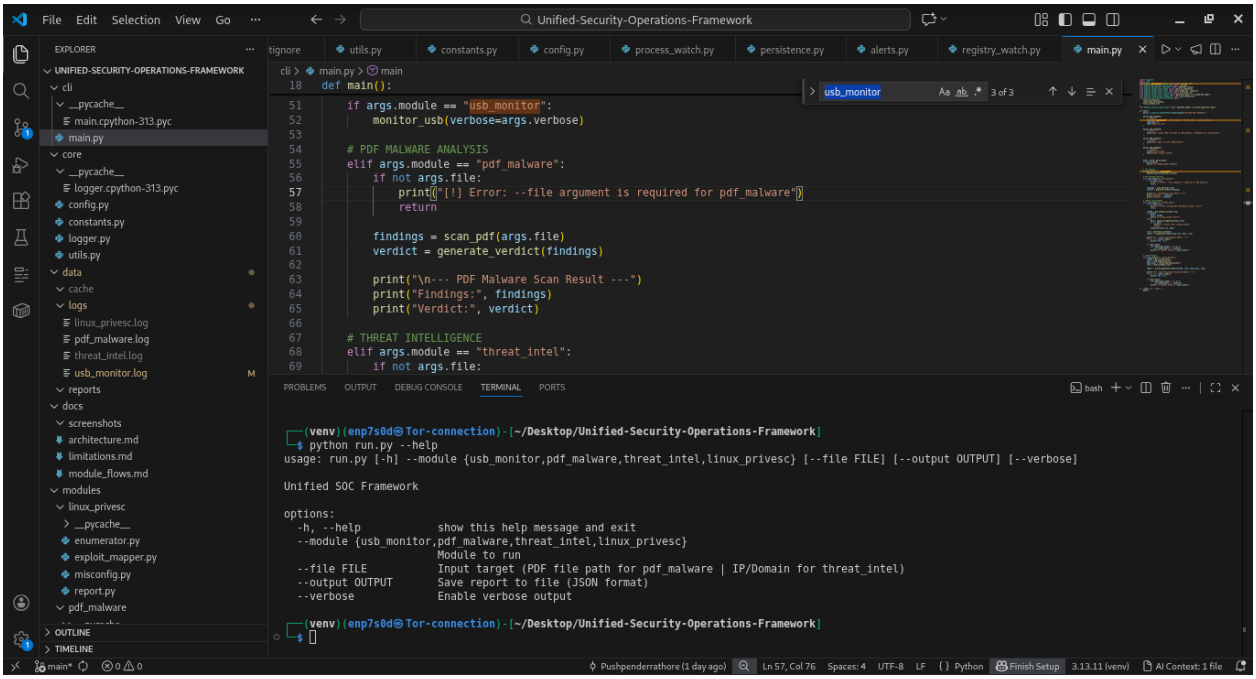
Unified Security Operations Framework – Project Submission

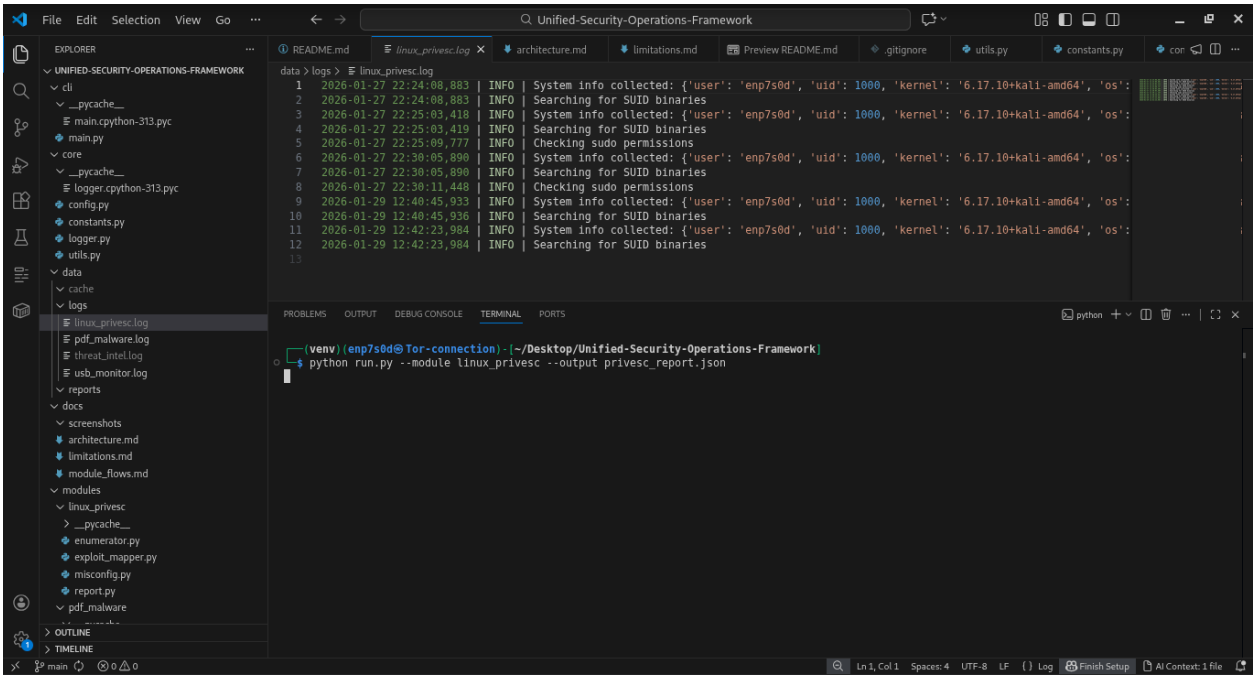
Overall Architecture Diagram



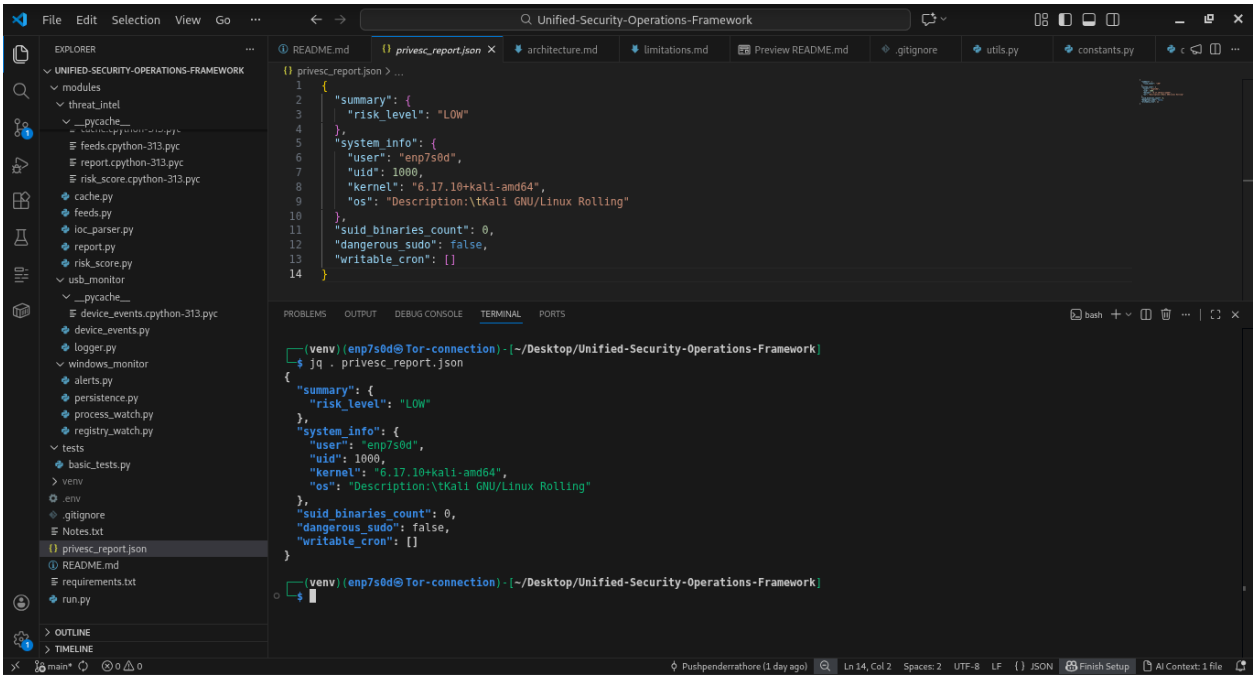
CLI Help & Module Execution



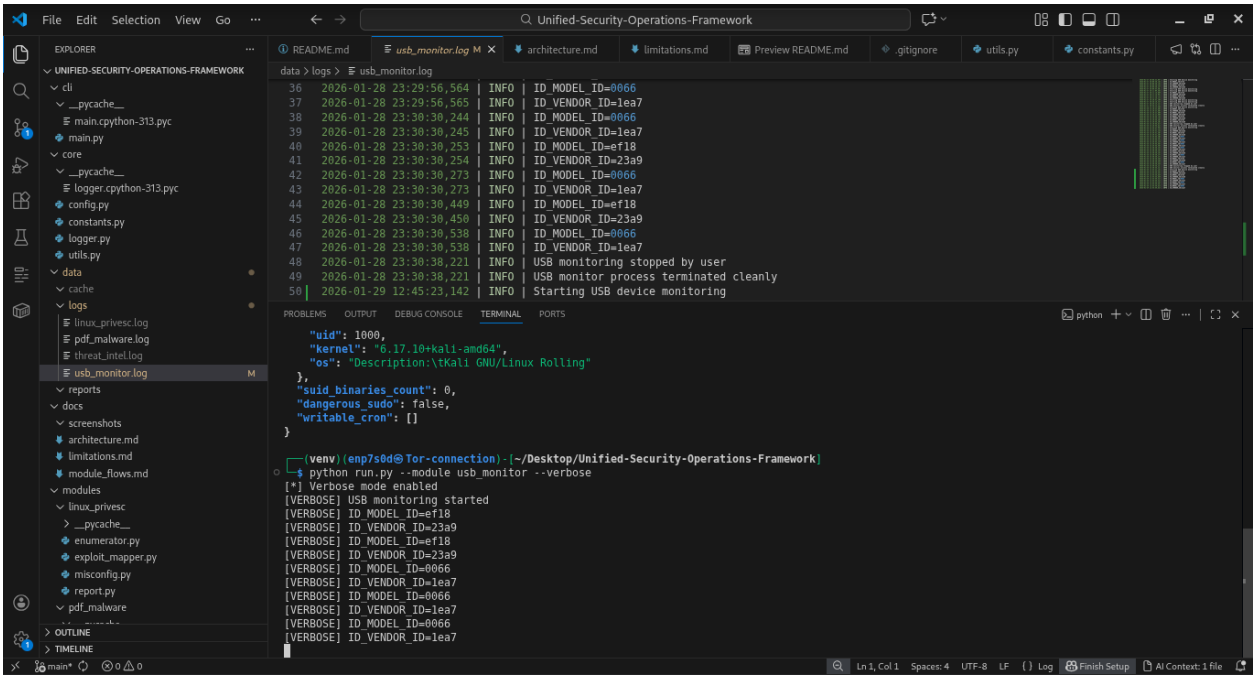
Linux Privilege Escalation Analyzer – Execution Output



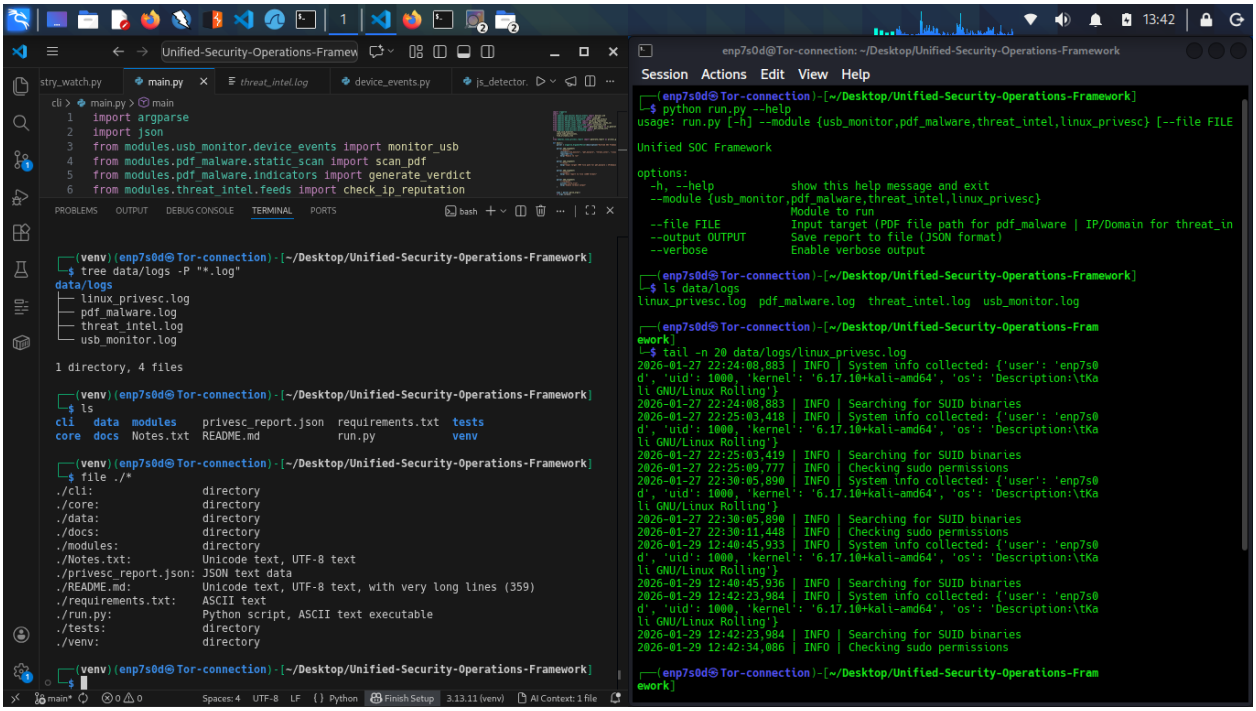
Privilege Escalation JSON Report



USB Monitoring Module – Verbose Mode



Generated Logs and Evidence


Unified-Security-Operations-Framew
stry_watch.py
main.py
threat_intel.log
device_events.py
js_detector.
cli > main.py > main
1 import argparse
2 import json
3 from modules.usb_monitor.device_events import monitor_usb
4 from modules.pdf_malware.static_scan import scan_pdf
5 from modules.pdf_malware.indicators import generate_verdict
6 from modules.threat_intel.feeds import check_ip_reputation
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS
bash
(venv)(enp7s0d㉿Tor-connection)-[~/Desktop/Unified-Security-Operations-Framework]
$ tree data/logs -P "*.log"
data/logs
├── linux_privesc.log
├── pdf_malware.log
├── threat_intel.log
└── usb_monitor.log
1 directory, 4 files
(venv)(enp7s0d㉿Tor-connection)-[~/Desktop/Unified-Security-Operations-Framework]
$ ls
cli data modules privesc_report.json requirements.txt tests
core docs Notes.txt README.md run.py venv
(venv)(enp7s0d㉿Tor-connection)-[~/Desktop/Unified-Security-Operations-Framework]
$ file ./*
./cli: directory
./core: directory
./data: directory
./docs: directory
./modules: directory
./Notes.txt: Unicode text, UTF-8 text
./privesc_report.json: JSON text data
./README.md: Unicode text, UTF-8 text, with very long lines (359)
./requirements.txt: ASCII text
./run.py: Python script, ASCII text executable
./tests: directory
./venv: directory
(venv)(enp7s0d㉿Tor-connection)-[~/Desktop/Unified-Security-Operations-Framework]
$
main*
0 0
Spaces: 4
UTF-8
LF
Python
Finish Setup
3.13.11 (venv)
AI Context: 1 file
13:42
enp7s0d@Tor-connection: ~/Desktop/Unified-Security-Operations-Framework
Session Actions Edit View Help
(enp7s0d㉿Tor-connection)-[~/Desktop/Unified-Security-Operations-Framework]
$ python run.py --help
usage: run.py [-h] --module {usb_monitor,pdf_malware,threat_intel,linux_privesc} [--file FILE
Unified SOC Framework
options:
-h, --help show this help message and exit
--module {usb_monitor,pdf_malware,threat_intel,linux_privesc}
Module to run
--file FILE Input target (PDF file path for pdf_malware | IP/Domain for threat_in
--output OUTPUT Save report to file (JSON format)
--verbose Enable verbose output
(enp7s0d㉿Tor-connection)-[~/Desktop/Unified-Security-Operations-Framework]
$ ls data/logs
linux_privesc.log pdf_malware.log threat_intel.log usb_monitor.log
(enp7s0d㉿Tor-connection)-[~/Desktop/Unified-Security-Operations-Framework]
$ tail -n 20 data/logs/linux_privesc.log
2026-01-27 22:24:08,883 | INFO | System info collected: {'user': 'enp7s0d', 'uid': 1000, 'kernel': '6.17.10+kali-amd64', 'os': 'Description:\tKali GNU/Linux Rolling'}
2026-01-27 22:24:08,883 | INFO | Searching for SUID binaries
2026-01-27 22:25:03,418 | INFO | System info collected: {'user': 'enp7s0d', 'uid': 1000, 'kernel': '6.17.10+kali-amd64', 'os': 'Description:\tKali GNU/Linux Rolling'}
2026-01-27 22:25:03,419 | INFO | Searching for SUID binaries
2026-01-27 22:25:09,777 | INFO | Checking sudo permissions
2026-01-27 22:30:05,890 | INFO | System info collected: {'user': 'enp7s0d', 'uid': 1000, 'kernel': '6.17.10+kali-amd64', 'os': 'Description:\tKali GNU/Linux Rolling'}
2026-01-27 22:30:05,890 | INFO | Searching for SUID binaries
2026-01-27 22:30:11,448 | INFO | Checking sudo permissions
2026-01-29 12:40:45,933 | INFO | System info collected: {'user': 'enp7s0d', 'uid': 1000, 'kernel': '6.17.10+kali-amd64', 'os': 'Description:\tKali GNU/Linux Rolling'}
2026-01-29 12:40:45,936 | INFO | Searching for SUID binaries
2026-01-29 12:42:23,984 | INFO | System info collected: {'user': 'enp7s0d', 'uid': 1000, 'kernel': '6.17.10+kali-amd64', 'os': 'Description:\tKali GNU/Linux Rolling'}
2026-01-29 12:42:23,984 | INFO | Searching for SUID binaries
2026-01-29 12:42:34,086 | INFO | Checking sudo permissions
(enp7s0d㉿Tor-connection)-[~/Desktop/Unified-Security-Operations-Framework]