KIRUBEL YONAS

SYSTEMS ENGINEER & SECURITY RESEARCHER

Addis Ababa, Ethiopia
Alias: **PicasoTheDealer**
GitHub: github.com/PicasoTheDeal
Portfolio: isitreallyme.pages.dev

PROFESSIONAL SUMMARY

I am a technical security researcher and software engineer with a deep focus on C/C++ development, vulnerability discovery, and systems architecture. My background involves building low-level software from scratch—ranging from ELF tracing engines to static analysis utilities—while executing advanced penetration testing in corporate environments. I thrive on bridging the gap between secure-by-design engineering and offensive security, bringing a self-directed and highly adaptable approach to solving complex technical challenges.

TECHNICAL SKILLS

Systems & Programming:	C++, Python, C, JavaScript, Bash/Zsh Scripting, Assembly (x86/ARM), PHP, SQL, Go, TypeScript.
Offensive Security:	AFL++ (Fuzzing), Burp Suite, Metasploit, Impacket, Mimikatz, Rubeus, Nmap, SQLmap, Ghidra, Wireshark.
Core Specializations:	Penetration Testing, Active Directory Lateral Movement, Reverse Engineering, Exploit Development, Zero-Day Fuzzing, Static Analysis (SAST).
Infrastructure & Ops:	Linux Administration (Arch/Debian), Windows Server (AD), Docker, Git, CI/CD, Scripted Automation, fscrypt.

PROFESSIONAL EXPERIENCE

LaloDev | *Software Engineer* **June 2025 – Nov 2025**

- Developed and optimized backend solutions within a professional SDLC, prioritizing both performance and security.
- Streamlined internal workflows by building custom Python automation for secure code deployment and CI/CD integrations.
- Collaborated with the engineering team to audit and harden application logic, effectively reducing attack surfaces across core systems.

KEY TECHNICAL PROJECTS

dSBOM-engine | *Runtime Software Bill of Materials Engine* **Core Developer**

- Architected a C++20 engine leveraging `ptrace(2)` and `PTRACE_SYSCALL` to intercept system boundaries and derive process components natively from the Linux kernel VFS.
- Implemented isolated namespace translation via `/proc/[pid]/root` to audit containerized targets (Docker, containerd) securely without performing `setns(2)` or compromising host isolation.
- Designed a page-aligned, allocation-free OpenSSL EVP SHA-256 cryptographic pipeline paired with dynamic ELF verification to output schema-validated CycloneDX 1.5 compliance records.

ZeroShadow | *Lightweight ELF Tracing Engine* **Systems Project**

- Built a high-performance C++ engine for tracing and instrumenting ELF binaries, providing granular, low-level execution visibility.
- Implemented features for function hooking and execution path tracing, specifically tailored for malware analysis and secure systems debugging.

AUR-scanner | *Offline Static Analysis Utility* **Security Utility**

- Developed a lightweight utility to scan local ALPM metadata and AUR helper build caches for security anomalies.
- Designed heuristic detection algorithms to identify compromised packages and malicious code patterns in open-source builds.

Project KASCVE | *Automated Security Auditing Ecosystem* **Platform Architect**

- Architected a platform to automate security audits for web applications and infrastructure.
- Integrated modules for detecting OWASP Top 10 vulnerabilities, including custom SQL Injection detection mechanisms.

Zero-Day Enumeration & Fuzzing | *Telegram Animation Engine* **Research Project**

- Engineered a fuzzing harness using AFL++ to stress-test the Telegram sticker media engine.
- Conducted systematic crash analysis to identify memory corruption vulnerabilities and input validation failures, documenting PoCs for identified memory leaks.

Active Directory Exploitation | *Corporate Labs Deployment* **Offensive Lab**

- Successfully compromised the "WingData" corporate lab environment, utilizing advanced Pass-the-Ticket (PtT) and Pass-the-Hash (PtH) techniques.
- Demonstrated domain dominance using Impacket, Mimikatz, and Rubeus, while managing complex Kerberos and AD CS protocols.

KiOS | *Secure Linux Architecture Deployment* **OS Distribution**

- Architected a custom, Arch-based Linux distribution optimized for a minimal attack surface and developer productivity.
- Developed Python and Bash automation for deep system localization and rapid provisioning.

EDUCATION & CREDENTIALS

EDUCATION & TRAINING

Radical Academy: High School Diploma (May 2026)
freeCodeCamp: DSA, Responsive Web Design
SoloLearn: Certified in C++, JS, SQL, PHP

CERTIFICATIONS & AWARDS

HTB Specialist: Password Attacks Specialist
Offensive Paths: CPTS Path (In Progress)
Hackathons: 2x Winner, ALX Engineering Hackathon