ALI MOHAMMAD MOHARRAMZADEH

Security Researcher · Red Team & Malware Development

Maragheh, East-Azerbaijan, Iran | +98 922 987 0544 | ali@neox1de.com | github.com/neox1de

PROFILE

Offensive security researcher specializing in Windows internals, kernel-mode development, and red team tooling. Builds anti-cheat and EDR-evasion engines, exploit tooling, and security research infrastructure across C++, Rust, and Python. Comfortable moving between low-level systems work and full-stack tooling to support security operations end to end.

TECHNICAL SKILLS

Languages: C++, Rust, Python, JavaScript / TypeScript

Red Team & Security Tools: Mythic, AdaptixC2, Metasploit, Mimikatz, BloodHound, Wireshark, Social-Engineer Toolkit, GoPhish, Bettercap, Aircrack-ng, tcpdump

Systems & Frameworks: Windows SDK / WDK, Arch Linux, ImGui, Express.js, NestJS, Next.js, Tauri

Tooling & Workflow: Git, Docker, CI/CD pipelines, n8n, Neovim / VS Code

Languages Spoken: English, Persian, Turkish

PROJECTS

Perca — Kernel-Mode Anti-Cheat Engine *perca.ir*

C++ · Lua · Windows SDK / WDK

- Designed and built a kernel-mode anti-cheat system detecting DLL injection, unauthorized memory access, and signature-based tampering in online games
- Implemented a Lua scripting layer enabling custom detection plugins without recompiling the core engine
- Actively developed across usermode and kernel-mode boundaries; currently in alpha

license-api — License Management & HWID Validation Platform *github.com/neox1de/license-api*

TypeScript · NestJS · PostgreSQL · Passport.js

- Built a license-validation backend with HWID locking and authentication flows for distributed security tooling
- Evolved from a single-purpose license checker into a reusable platform supporting multiple internal tools

img2ascii — Image-to-ASCII Rendering Engine *github.com/neox1de/img2ascii*

C · C++ · CMake

- Built a configurable rendering pipeline converting raster images into colorized ASCII art with multiple style modes

TRAINING & COURSEWORK

Red Team Operations *Ravin Academy, 2024*
Multi-stage simulated attacks emulating APT tactics, techniques, and procedures

Malware Development *Maldev Academy, 2024*
Process injection, API hooking, syscalls, reflective DLL injection, EDR evasion, anti-debugging

Advanced C++ *Anisa Group, 2022*
OOP, templates, operator overloading, smart pointers, exception handling

Python, Beginner to Advanced *Maktabkhooneh, 2025*
Core syntax through applied machine learning

EDUCATION

B.Eng. Computer Engineering — Azad University of Maragheh *2024 – Present*