Stefan Mladić

stefan@mladicstefan.com | Belgrade, Serbia | GitHub | Website

About

I like philosophy (ranting about stuff), programming (having no clue what I'm doing), and hacking. Currently working as a Security Engineer and Pentester at AlgoDev/ImpactLTD, where I break things on purpose. Outside of work, I play with new and old technologies occasionally building something, but usually breaking things by accident. It's a gift, really. I also blog about cybersecurity, compilers, and systems. Currently studying Computer Science and for the HTB CPTS certification.

Education

1st Year Computer Science Student — Aug 2025 — Present
Računarski Fakultet (RAF) — *Belgrade, Serbia*

Mathematics and Natural Sciences — 2021 — 2025
XIII Belgrade Gymnasium — *4.8/5 GPA*

Skills

Languages: Python, C (C11), Rust, React (TypeScript), Bash

Security: Malware RE (Ghidra, IDA Pro, gdb, strace, any.run, custom sandboxes), Pentesting (Burp Suite, ffuf, nmap, netcat, Wireshark, proxychains, WhatWeb), OSINT (Censys, crt.sh, VirusTotal, dig), SIEM/EDR (Elastic), Frameworks (MITRE ATT&CK, CIS Controls, NIST CSF 2.0)

Infrastructure: Linux (LFS), Docker (CIS-hardened, distroless, multi-stage), Ansible, AWS (S3, Lambda, DynamoDB), NGINX, Redis, SQL

AI/LLM: Prompt engineering, prompt injection attacks (offensive security), MCP servers, custom agent pipelines, API integrations, self-hosting local models

Professional Experience

Security Engineer & Pentester (Part-time) — May 2024 — Present
AlgoDev / ImpactLTD — *Belgrade, Serbia*

- **Offensive Security:** Performed web application penetration tests achieving SQL database exfiltration, admin credential extraction, SSRF via Next.js upstream GET, and CSRF exploit demonstration; delivered detailed reports and remediation. Conducted comprehensive security audits implementing XSS prevention, input validation hardening, and NGINX security configuration.
- **Incident Response:** Identified production server breach via a one-day vulnerability (disclosed 1 day prior). Isolated compromised host, located XMRig cryptominer, preserved forensic evidence. Traced attacker: Indonesian IP using MeshAgent RDP backdoor; recovered attacker's Monero wallet address.
- **Threat Intelligence:** Orchestrated takedown of spear phishing campaign by enumerating attacker infrastructure via Censys, crt.sh, VirusTotal; submitted Cloudflare abuse report. Monitor threat feeds (Mastodon, abuse.ch, C2Tracker, Malpedia) and darknet CTI sources via Tor. Developed custom AI-powered threat report automation with Typst templates—given a chain of evidence, generates full incident reports.
- **Defensive Security:** Designed Linux server hardening protocols: SSH key-only auth, fail2ban, Tor exit node blocking via automated UFW/iptables. Built custom Debian CIS IG2 compliant ISO with preseed; developed Ansible playbook for hardening (auditd, rsyslog, ufw, AppArmor). Implemented client privacy solutions: LUKS2, VeraCrypt hidden partitions, encrypted swap, YubiKey integration.
- **Development:** Developed React components with performance optimization (lazy loading, Next.js chunking, caching); reduced load times from 1.2s to 0.6s. Built CIS-hardened Docker images with distroless multi-stage builds for production deployments.

Co-Founder — Dec 2024 — May 2025
Redzlab — *Belgrade, Serbia*

- Founded algorithmic trading startup with 5-person engineering team
- Built high-frequency trading and backtesting system using Python (NumPy, Pandas)
- Designed AWS infrastructure (S3, Lambda, DynamoDB) and contributed to React TypeScript frontend

Projects

Jester C2 Framework
Rust

- C2 malware development proof-of-concept for Linux demonstrating EDR evasion: syscall spoofing, kernel API bypasses via async I/O, encrypted C2 communications with TLS mimicry, static analysis evasion through compiler flags and Rust memory allocation patterns. Tested against Elastic EDR in lab environment. *(Source private—happy to discuss implementation)*

Icepick
C — *GitHub*

- 802.11 Radiotap frame analyzer for deep packet inspection. Raw packet interception via libpcap with RTL8812AU monitor mode antenna.

Matrix
C++ — *GitHub*

- Multithreaded epoll-based web server handling 50k req/s on 8-core machine. Deployed via multi-stage Docker build on hardened Debian image.

CIS-Hardened Docker Deployments
Docker

- Production containers using distroless images with multi-stage builds. Security controls: read-only filesystems, tmpfs with noexec/nosuid/nodev, all capabilities dropped, no-new-privileges, non-root users, disabled IPC, resource limits, healthchecks, and isolated bridge networks with ICC disabled. Deployed Next.js apps and a Minecraft server.

DWG-JSON
Python — *GitHub*

- Geometry semantic engine inferring asset relationships from AutoCAD DWG files. Optimization via NumPy and Numba.

Other

Baltic Sea World Philosophy Event — 2x Finalist 2023 — 2024
Top 30 of 10,000+ participants

- Essays analyzing Kant, Dostoyevsky, Camus, Sartre

AIESEC Youth Entrepreneurship Competition — 2nd Place Jun 2022 — Jul 2022
Built ChatGPT-powered legal advisory app at age 16

- Led 5-person team through product development

Languages

English: Cambridge C2 Proficiency (native-level fluency)

French: B1 Intermediate (High School)