Ayush Kumar

scottastatine@gmail.com | linkedin.com/in/scottastatine | github.com/scott-astatine

ABOUT ME

Computer science student focused on cybersecurity and systems security. I build and test secure tooling in Linux environments using Rust and Python, applying authentication, networking, and risk management concepts through hands-on projects. Currently completing the Google Cybersecurity Professional Certificate to strengthen defensive foundations before transitioning into penetration testing.

SKILLS

- **Linux:** Arch Linux (daily driver), Hyprland WM, system hardening, service management, shell configuration
- **Networking:** TCP/IP, WebRTC (P2P), firewall rules, port analysis, Nmap, traffic monitoring
- **Security:** Argon2id authentication, zero-trust architecture, access controls, SIEM fundamentals, risk frameworks (NIST, OWASP)
- **Programming:** Rust, Python, SQL, C/C++, Bash/Shell, JavaScript
- **Systems:** D-Bus IPC, systemctl/loginctl, WebRTC data channels, chunked file transfer, SHA-256 integrity verification
- **Languages:** English (Fluent) · German (A2) · Hindi (Native)

CERTIFICATIONS

Google Cybersecurity Professional Certificate · Google / Coursera · *2026 — In Progress*

9-course industry certification by Google. Courses completed so far:

- **Foundations of Cybersecurity** — CIA triad, threat categories, and the security analyst role
- **Play It Safe: Manage Security Risks** — NIST & OWASP frameworks, threat modeling, security audits
- **Connect and Protect: Networks and Network Security** — TCP/IP, OSI model, DDoS/MITM/sniffing attacks, firewalls, VPNs
- **Tools of the Trade: Linux and SQL** — Bash, file permissions, process monitoring, SQL-based security queries

PROJECTS

Frankn — P2P Remote Operations Center · Personal Project · Rust + Flutter · *2025 – Present*

Rust (Host), Flutter (Client), WebRTC, Argon2id

- **Engineered a Zero-Trust Architecture:** Built a secure remote control system from scratch, assuming compromised network conditions to enforce strict host-client validation.
- **Implemented Cryptographic Authentication:** Secured access using Argon2id for robust password hashing, actively mitigating brute-force and dictionary attacks.
- **Architected Peer-to-Peer Networking:** Integrated WebRTC for encrypted, low-latency communication, bypassing the need for vulnerable port-forwarding on the host network.
- **Developed Low-Level System Integration:** Leveraged Rust for memory-safe, high-performance host operations, ensuring stable system control within a custom Arch Linux/Hyprland environment.
- **Designed Cross-Platform Client:** Built a responsive, secure mobile interface using Flutter, focusing on safe data handling and seamless remote command execution.

Home Network Security Lab · Personal Homelab · *Ongoing*

- Regularly audit firewall rules and port forwarding on personal network hardware to reduce attack surface.
- Use Nmap to check external exposure and close anything that shouldn't be visible from outside the network.
- Sandbox for applying what I'm learning — testing real configurations rather than just reading theory.

EDUCATION

Bachelor of Computer Applications (BCA) · Lovely Professional University · *Sep 2025 – Present*

- Coursework: computer networks, operating systems, data structures, software development.

12th Grade — Science Stream · SANS College Motihari · *Mar 2023*