

NOUMAN ALI KHAN

Security Engineer | Penetration Tester

 +358 442357924

 noumanalikhan328@gmail.com

 Tampere, Finland

 [in/nouman-ali-khan/](https://in.linkedin.com/in/nouman-ali-khan/)

 [numankhaan](https://github.com/numankhaan)

 [@noumankhaan](https://twitter.com/noumankhaan)

SUMMARY

Security researcher and penetration tester with 3+ years of experience in vulnerability assessment, secure software development, and post-quantum cryptography research. Experienced with Rust, Python, PKCS#11, and TLS security systems, with hands-on work integrating PQC into Mozilla NSS for the QUBIP project. Background in offensive security testing using Burp Suite, Metasploit, and Nessus. Interested in security engineering and applied cryptography roles.

SKILLS

Technical Skills:

Python, Rust, SQL, Bash, C
Backend systems, APIs
Data processing and analysis
Cryptography, TLS, PKI
Linux, networking, databases
Git, CI/CD, Docker
Cloud fundamentals

Core Competencies:

Problem solving
Analytical thinking
Debugging and troubleshooting
Technical documentation
Team collaboration
Fast learner, ownership mindset
Interest in AI and data systems

EDUCATION

2023 - 2025	Masters in Information Security Major Modules: Cryptography, Cloud technologies, Networking and Security	Tampere University, Finland
2019 - 2021	BS in Information Technology Major Modules: Data Structures, Algorithms, Database Systems, Operating Systems, Software Engineering	COMSATS University, Pakistan

EXPERIENCE

2024 – Present	Project Researcher - Developed a PKCS#11 loadable module in Rust to enable Post-Quantum Cryptography (PQC) key and signature operations within the Firefox browser via Mozilla NSS. - Implemented unit tests in Rust and interoperability testing with TLS 1.3 servers (OQS and Cloudflare) to validate PQC functionality and ensure compatibility with existing cryptographic infrastructure. - Improved development workflows by introducing structured logging, CI pipelines, and setup documentation using GitLab, making builds and testing easier for collaborators. - Collaborated with NISec and EU research partners on project deliverables and demonstrations, using Wireshark analysis and Python automation to support debugging and testing of cryptographic protocols. Tools: Rust, PKCS#11, Firefox, NSS, TLS 1.3, Python, Wireshark, Git/GitLab	Tampere University, Finland
2021 – 2023	Penetration Tester & Security Researcher - Conducted penetration tests across web and network environments using Burp Suite, Metasploit, and Nessus, identifying high-risk vulnerabilities and supporting remediation planning for enterprise clients. - Performed security assessments and risk analysis, helping organizations understand exposure to common attack vectors and improve their defensive posture. - Developed Python automation scripts on Linux to streamline reporting and routine security tasks, improving operational efficiency for the security team. - Worked with incident response teams during security investigations, using network traffic analysis with Wireshark to help contain and mitigate potential breaches. - Assisted in maintaining security documentation, policies, and procedures to support governance practices and regulatory compliance. Tools: Burp Suite, Metasploit, Nessus, Python, Linux, Wireshark	Trillium, Pakistan

PROJECTS

2024	Cryptotoken – PKCS#11 Software Token Developed a Rust-only software token integrating Post-Quantum Cryptography into NSS, enabling Firefox to use PQC keys and signatures. Implemented secure backend components and PKI support.	Research / Academic Project
------	---	-----------------------------

2023	<u>Scanix - Python Port Scanner</u> Personal Project Built a Python tool for port scanning and OS fingerprinting using TTL heuristics. Applied secure programming practices for safe network scanning.
2024	<u>OpenSSL Toy Provider</u> Personal Project Developed a minimal OpenSSL 3.x provider in C to experiment with custom cryptographic algorithms, provider lifecycle management, and logging for secure software design.

LANGUAGES			
	English - Fluent	Urdu - Native	Finnish - Learning