Neel Upadhyay

647-224-2484 • neelmu12@gmail.com • LinkedIn • GitHub • Brampton, Ontario

SUMMARY

Software Engineering student (Cybersecurity Stream) at York University with hands-on experience in penetration testing, SIEM deployment, cryptographic protocol implementation, and threat detection. Proven ability to build and attack real systems — from hardware-level AES encryption on FPGA to SQL injection assessments and network traffic analysis. Brings both the attacker and defender mindset needed for modern security roles.

TECHNICAL SKILLS

Languages: Python, Java, C/C++, SQL, Bash, Verilog
Security Tools: Wireshark, Nmap, Hydra, John the Ripper, Metasploit, SQLMap, Kali Linux, OpenSSL, GPG
SIEM & Detection: Splunk, ELK Stack, SOC Analysis, Threat Hunting, MITRE ATT&CK, Network Traffic Analysis
Cryptography: AES-128 (hardware), Double Ratchet / Signal protocol, KDF chains, OpenSSL, GPG
OS & Scripting: Linux / Unix, Kali Linux, WSL, Bash scripting, Shell scripting
Frameworks: NIST CSF, MITRE ATT&CK, Threat Intelligence, Malware Research
Certifications: Google Cybersecurity Certificate (2025), CompTIA Security+ (In Progress), Java HackerRank (2024)

WORK EXPERIENCE

TJX Companies — Mississauga, ON *Sept 2024 – Dec 2024*
Real Estate Market Analyst Co-op

- Automated repetitive reporting workflows using Python scripting, improving data accuracy by 15% and freeing analyst hours for higher-value work.
- Analyzed multi-source market data (population growth, competitor activity, demographics) to produce actionable trade area expansion recommendations.
- Built Excel-based performance dashboards synthesizing store-level data to drive retention and relocation strategy decisions.

Manefa Contracting Inc. — Brampton, ON *June 2021 – Aug 2022*
Software Developer Intern

- Engineered a Java application with a SQL backend to automate material cost tracking, cutting manual entry errors by 60% and improving data integrity across project records.
- Built real-time Excel dashboards for project tracking and forecasting, boosting operational efficiency by 30%.

PROJECTS

Cybersecurity Home Lab — SIEM & Threat Hunting | *Splunk, ELK Stack, Nmap, Hydra, MITRE ATT&CK* *2025 – 2026*

- Deployed Splunk and ELK Stack to ingest Windows and Linux logs for centralized monitoring; simulated Nmap scans, SSH brute-force, and Hydra credential attacks on controlled targets.
- Mapped attacker behavior to MITRE ATT&CK TTPs (Reconnaissance, Credential Access, Lateral Movement) using timeline correlation and custom detection rules — replicating a real SOC analyst workflow.

SQLMap Penetration Test — Full-Stack Web Application | *SQLMap, Python, SQL, Parameterized Queries* *2025 – 2026*

- Executed a full SQL injection assessment against a personal full-stack application using SQLMap, identifying blind and error-based injection vectors in live database queries.
- Remediated all findings with parameterized queries and input validation — documenting the complete attack-and-fix cycle as a structured penetration test report.

Double Ratchet Secure Messaging Protocol | *Python, Diffie-Hellman, KDF Chains, AES* *2025 – 2026*

- Implemented Signal's Double Ratchet protocol over email, combining DH ratchet key exchange with symmetric KDF chains to derive a unique ephemeral encryption key per message.
- Enforced forward secrecy and break-in recovery guarantees: past messages remain secure after key compromise; future messages recover automatically after each ratchet step.

AES-128 Hardware Encryption — FPGA | *Verilog, DE10-Lite FPGA, RTL Design* *2025 – 2026*

- Implemented AES-128 encryption/decryption in Verilog at the register-transfer level on a DE10-Lite FPGA, including all core cipher transformations: SubBytes, ShiftRows, MixColumns, and AddRoundKey.
- Built modular hardware components: ALU, key-expansion module, RAM storage, and FSM controller with switch-based I/O for plaintext input, key generation, and RAM addressing.

Wireshark Network Traffic Analysis | *Wireshark, TCP/IP, DNS, HTTP, ARP* *2025 – 2026*

- Captured and dissected live network traffic to identify unencrypted credentials, ARP spoofing indicators, and anomalous sessions through deep packet inspection across TCP, DNS, and HTTP layers.
- Built detection intuition for anomaly-based network analysis, directly supporting SIEM alert-tuning and threat hunting workflows.

EDUCATION

Lassonde School of Engineering — York University *Sept 2022 – Dec 2026*
Honours Bachelor of Engineering, Software Engineering | Cybersecurity Stream