Angeline Nicole Faina

in/lynfaina lynfaina.io

PROFESSIONAL SUMMARY

Dedicated **Cybersecurity and Threat Management** student at Seneca Polytechnic with a strong foundation in Computer Programming. Specialized in bridging the gap between software development and threat management, with hands-on experience in **Legacy Systems Security (COBOL)**, **Cloud Security (AWS)**, and **Offensive Security**. Proven ability to conduct full-scale penetration tests, secure IoT infrastructures, and analyze complex financial data to mitigate fraud and infrastructure vulnerabilities.

SKILLS

Technical Skills

Security Operations	Splunk Enterprise, Suricata IDS, ELK Stack (Kibana), Wireshark, Digital Forensics.
Offensive Security	Metasploit, Burp Suite, Nmap, SEToolkit, Privilege Escalation, SQL Injection.
Cloud & Infrastructure	AWS (VPC, IAM, S3, IoT Core), Active Directory, Linux (Bash/Kali), Windows Server.
Development & Data	COBOL, Python (Pandas/Flask), C/C++, JavaScript, HTML/CSS, Git/GitHub, PySpark.
Frameworks	NIST Cybersecurity Framework, OWASP Top 10, AWS Shared Responsibility Model.

Transferable Skills

Problem-Solving & Analytical Thinking	Identify security flaws, evaluate risks, and implement remediation strategies across complex network environments.
Communication & Technical Reporting	Experienced in authoring industry-standard Penetration Test Reports, detailing risk severity and impact analysis for non-technical stakeholders.
Collaboration & Teamwork	Experienced in working with technical teams during open-source workshops and security labs to achieve project goals.
Time Management & Adaptability	Efficiently manage multiple technical projects and certifications while maintaining academic excellence.

PROJECTS

Legacy Systems Security Lab (COBOL Financial Transaction Model) | *Personal Project* **January 2026 - present**

- Developed a **COBOL-based** financial transaction module to simulate legacy banking environments, targeting **input validation vulnerabilities** common in mainframe systems.
- Implemented **defensive programming** techniques to sanitize data inputs, successfully creating a proof-of-concept for hardening financial infrastructure against **buffer overflow attacks**.
- Demonstrated the critical application of modern security principles to legacy architecture, a key requirement for securing financial sector systems.

MITM (Man-in-the-Middle) Chat Application Simulation | *Personal Project* **December 2025 - present**

- Built a vulnerable-by-design **Python Flask** messaging platform to demonstrate unencrypted communication risks to non-technical stakeholders.
- Conducted deep-packet traffic analysis using **Wireshark** to capture **plaintext credentials** and subsequently remediated the vulnerability by implementing **TLS/SSL encryption**.
- Eliminated plaintext credential transmission and message interception vulnerabilities, validating the effectiveness of cryptographic controls.

Active Directory Exploitation & Lateral Movement | *Seneca Polytechnic* **December 2025**

- Simulated a red team engagement on a corporate Windows domain, exploiting the **MS17-010 (EternalBlue)** vulnerability to gain initial **System-level access**.
- Performed credential harvesting using **Mimikatz** to dump NTLM hashes for offline cracking and executed lateral movement via **Pass-the-Hash** attacks to compromise client machines.
- Authored a comprehensive **remediation report** detailing defensive configurations to mitigate unauthorized persistence and domain-wide escalation.

IoT Security Monitoring & Threat Analysis | *Seneca Polytechnic* **December 2025**

- Designed a secure IoT infrastructure using **Raspberry Pi** and **AWS IoT Core**, utilizing Python scripts to manage sensor data and **certificate-based authentication**.
- Deployed a virtualized Security Operations Center (SOC) using **Suricata** for intrusion detection and the **Elastic Stack (ELK)** to visualize real-time threats.
- Executed controlled **DDoS attacks** to test defense resilience and analyzed traffic patterns using **AWS VPC Flow Logs** stored in S3 to identify reconnaissance signatures.

Network & Web Application Penetration Test | *Seneca Polytechnic* **December 2025**

- Conducted a comprehensive penetration test on virtualized **Metasploitable2** environment to identify and exploit critical security flaws.
- Gained initial footholds by exploiting misconfigured VNC and Tomcat Apache services, followed by executing **privilege escalation** on SUID binaries to compromise system **root access**.
- Identified web application vulnerabilities including **Cross-Site Scripting (XSS)** and **SQL Injection**, producing an industry-standard report

with prioritized remediation strategies.

CERTIFICATIONS

Cloud & Operating Systems

- **AWS Cloud Security Foundations** | *AWS Academy*
  - Validated understanding of the AWS Shared Responsibility Model, IAM policies, and cloud security compliance.
- **Introduction to Linux** | *The Linux Foundation*
  - Demonstrated proficiency in Linux command line operations, file system navigation, and system administration.

Cybersecurity & Forensics

- **Foundations of Cybersecurity** | *Google Coursera*
  - Covered core security concepts including the NIST Cybersecurity Framework, SQL, Python, and intrusion detection.
- **Introduction to Digital Forensics** | *Cyber5W*
  - Acquired skills in digital evidence preservation, chain of custody, and forensic analysis methodologies.
- **Introduction to Cybersecurity** | *Cisco Networking Academy*
  - Acquired skills in digital evidence preservation, chain of custody, and forensic analysis methodologies.

Networking & Infrastructure

- **IPv6 Address Planning & Fundamentals** | *APNIC*
  - Mastered IPv6 addressing schemes, subnetting, and packet structure.
- **Introduction to Critical Infrastructure Protection** | *OPSWAT Academy*
  - Gained insight into securing critical infrastructure assets against cyber-physical threats.

EDUCATION

Cybersecurity and Threat Management (Ontario College Graduate Certificate)
Seneca Polytechnic - Toronto, ON | Expected October 2026

- **President's Honour List (Fall Term 2025)** - Awarded for outstanding academic achievement **(Term GPA 4.0)**.
- Executed phishing simulations with **SEToolkit**, performed OS fingerprinting with **Nmap**, and created payloads/trojans using **MSFVenom** for Windows exploitation.
- Configured **AWS VPCs**, Subnets, and **ACLs**, deployed **DVWA** on EC2, and monitored IoT traffic using **Suricata** and Kibana.
- Configured **Splunk Enterprise** for log collection, conducted risk assessments using Likelihood-Impact matrices, and performed system log analysis using **Pandas** and **PySpark**.
- Implemented **symmetric/asymmetric encryption (OpenGPG)**, analyzed email headers for malicious origins, and performed password cracking using **brute force** and dictionary attacks.
- Winter 2026 Coursework includes Threat Investigation, Mobile Application Security (OWASP Mobile Top 10), Digital Forensics, and Authentication and Access Control.

Computer Programming (Ontario College Diploma) | **GPA: 3.7 (with Honours)**
Seneca Polytechnic - Toronto, ON | 2023-2024

- Completed a comprehensive programming diploma focused on **software development, object-oriented design, and algorithms**.
- Gained strong proficiency in **C** and **C++**, developing complex systems including a Veterinary Clinic Management System with custom file I/O
- Developed responsive web applications using **HTML, CSS**, and **JavaScript**, building a deep understanding of client-side code structure.
- Strengthened algorithmic thinking through **Data Structures**, implementing custom Hash Tables and Minimax AI algorithms in **Python**.
- Applied structured testing techniques including **Black Box testing** and defect tracking during Software Quality Assurance courses.

PROFESSIONAL DEVELOPMENT

TASK (Toronto Area Security Klatch) - A Cognitive Kill Chain / The Future of Cyberwarfare | November 2025

- Engaged with industry experts on the intersection of **AI, psychology, and cybersecurity**, specifically analyzing **"cognitive offloading"** as a security risk.
- Explored concepts of **"Burnout as a Threat to National Security,"** understanding how personnel resilience directly impacts infrastructure defense.

SecTor 2025 (Security Education Conference Toronto) | October 2025

- Explored automated penetration testing workflows at the OWASP Arsenal, specifically analyzing the "Faction" framework for streamlined security assessments and team collaboration.
- Participated in the **"Safe Escape" lock-picking challenge**, gaining hands-on insight into physical access vulnerabilities and lock-bypass techniques.
- Contributed to the community **LEGO mosaic project** and networked with vendors and security engineers to gain insight into the Canadian cybersecurity job market.

EXPERIENCE

Google Developers Group (GDG) Cloud DevFest **Nov 2025, Toronto, ON**

- Supported the technical delivery of cloud workshops for a major developer conference by pre-validating labs for Gemini Enterprise and Cloud CLI tools.
- Provided direct troubleshooting assistance to attendees, ensuring a seamless learning experience and successful workshop completion.

Swiss Chalet **Jan 2023 – Present, Toronto, ON**

- Thrived in a high-pressure, fast-paced team environment, consistently meeting productivity targets while maintaining quality standards.
- Ensured strict compliance with operational policies and safety regulations, demonstrating professional accountability and attention to detail.
- Collaborated effectively with team members to coordinate efficient service flow and resolve immediate operational issues.