

Angeline Nicole Faina

in/lynfaina lynfaina.io

PROFESSIONAL SUMMARY

Cybersecurity and Threat Management Student seeking a Summer 2026 Work Term/Internship. Dedicated security analyst with a strong technical foundation in **Cloud Infrastructure (AWS)** and **Vulnerability Assessment**. Proven ability to bridge the gap between **Software Development** and **Threat Management**, leveraging code-level knowledge to secure web applications and cloud environments. Equipped with **several certifications** and hands-on experience in **Network Defense (Suricata/ELK)** and **Offensive Security**, ready to contribute immediately to security operations.

SKILLS

Technical Skills

Offensive Security	Penetration Testing, Metasploit Framework, Nmap, Burp Suite, Privilege Escalation (SUID/SGID), Lateral Movement, Social Engineering.
Web Application Security	OWASP Top 10, Cross-Site Scripting (XSS), SQL Injection (SQLi), Command Injection, HTML5/CSS3, JavaScript.
Cloud Security	AWS (IoT Core, VPC, S3, IAM), Cloud Misconfigurations, Log Analysis (CloudWatch/VPC Flow Logs), Azure.
Defensive Tools	Suricata IDS, ELK Stack (Elasticsearch, Logstash, Kibana), Wireshark, Splunk, Digital Forensics.
Operating Systems	Kali Linux, Linux Administration (Bash scripting), Windows, Ubuntu.

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

MITM (Man-in-the-Middle) Chat Application Simulation | *Personal Project (In Progress)*

- Designed and executed a comprehensive **multi-stage penetration test** simulating real-world attack scenarios from **initial reconnaissance through data exfiltration** documenting findings in professional security reports that demonstrated critical vulnerabilities in authentication, input validation, and encryption implementations.
- Built a vulnerable-by-design messaging platform using **Python Flask** to create controlled environments for **ethical hacking** demonstrations, showcasing proficiency in both **offensive security techniques and defensive strategies**.
- Performed network traffic analysis and man-in-the-middle demonstrations using **Wireshark** to capture and analyze unencrypted communications, then implemented **cryptographic controls** that eliminated plaintext credential transmission and message interception vulnerabilities.

Network & Web Application Penetration Test | *Seneca Polytechnic*

- Conducting a comprehensive penetration test on a virtualized network environment (**Metasploitable2**) to identify and exploit critical security flaws.
- Successfully gained **initial footholds** by exploiting misconfigurations in **VNC** and **Tomcat Apache** services, followed by executing **privilege escalation** techniques to compromise system root access.
- Identifying and exploiting **web application vulnerabilities** including **Cross-Site Scripting (XSS)** and **SQL Injection** on Port 80 web services.
- Producing a professional industry-standard Penetration Test Report detailing risk severity, impact analysis, and remediation strategies for the client.

Active Directory Exploitation & Lateral Movement | *Seneca Polytechnic*

- 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/Kiwi** to dump NTLM hashes and utilized **John the Ripper** for offline password cracking.
- Executed **Lateral Movement** via Pass-the-Hash attacks using **Impacket** to compromise client machines and establish persistence via **RDP**.

IoT Security Monitoring & Threat Analysis | *Seneca Polytechnic*

- Designed a secure IoT infrastructure using **Raspberry Pi** and **AWS IoT Core**, utilizing **Python** scripts to manage sensor data (Temperature).
- 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** against the IoT network to test defense resilience, analyzing traffic patterns using **AWS VPC Flow Logs** stored in **S3**.

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 August 2026

- **President's Honour List (Fall Term 2025)** - Awarded for outstanding academic achievement (**Term GPA 4.0**).
- Conducted comprehensive **penetration tests** on virtualized networks (**Metasploitable2**), identifying Critical flaws (CVSS 9.8) such as **Remote Code Execution (RCE)** and **weak authentication**.
- Gained hands-on experience in **Privilege Escalation** by identifying and exploiting misconfigured SUID binaries to gain root access.
- Architected secure cloud infrastructures using **AWS IoT Core**, implementing TLS/SSL certificate-based authentication to prevent MITM.
- Deployed and tuned a **Suricata IDS** and **ELK Stack (Kibana)** to detect and visualize real-time network threats and protocol anomalies.
- Analyzed network traffic patterns using **AWS VPC Flow Logs** to conduct forensics and identify unauthorized external reconnaissance.

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 **HTML5**, **CSS3**, 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

- Served as a **Tech volunteer** and focused on ensuring a seamless and valuable experience for all attendees.
- Provided direct technical assistance to participants covering **Gemini Enterprise**, **Gemini CLI**, **Apps Script**, and **Gmail add-ons**.
- Proactively prepared for the event by completing all the workshop labs beforehand to offer the highest level of support.
- Managed key logistics, including **participant check-in** and **assisting attendees** throughout the day.
- Collaborated with the **Creative Team** to produce and distribute event certificates.

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.