

## PROFESSIONAL SUMMARY

IT support professional with Bachelor of Computer Science and Information Technology; transitioning into cybersecurity, with hands-on experience in ethical hacking, intrusion detection, and cloud/IoT security. Currently in the **Cybersecurity and Threat Management Student seeking a Summer 2026 Work Term/CO-OP**, with projects in penetration testing, Suricata–ELK monitoring, and AWS IoT security using Metasploit, Nmap, and AWS services (WAF, GuardDuty, CloudWatch). 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

#### Penetration Testing & Analysis

Nmap, Metasploit, Enum4linux, SMBclient, Nikto, Nessus, OpenVAS; exploitation, post-exploitation, lateral movement, log analysis, OSINT.

#### Web Application Security

OWASP Top 10, Cross-Site Scripting (XSS), SQL Injection (SQLi), Command Injection, HTML5/CSS3, JavaScript.

#### Cloud Security

AWS IoT Core, AWS WAF, GuardDuty, CloudWatch, VPC Flow Logs, secure device-to-cloud communication.

#### Security Operations

Suricata IDS, Elasticsearch, Kibana, Filebeat, threat detection, dashboarding, vulnerability assessment, report writing.

#### Tools & Language

Kali Linux, VMware, Wireshark, Raspberry Pi, Python, Bash, MS Office, Teams, Outlook.

### Transferable Skills

#### Problem-Solving & Analytical Thinking

Diagnose security weaknesses, assess associated risks, and deploy effective remediation measures across diverse and complex network infrastructures.

#### Communication & Technical Reporting

Skilled in producing professional penetration testing documentation that clearly explains risk levels and impact assessments for audiences without technical backgrounds.

#### Collaboration & Teamwork

Work effectively with technical peers in open-source workshops and security lab environments to complete objectives and deliver shared project outcomes

#### Time Management & Adaptability

Consistently balance multiple technical projects and certification pursuits while sustaining strong academic performance.

## PROJECTS

### Network & Web Application Penetration Test | *Seneca Polytechnic*

- Performed an end-to-end penetration test against a virtualized network (**Metasploitable2**) to uncover and exploit high-impact security weaknesses.
- Achieved initial access by abusing misconfigurations in VNC and Apache Tomcat services, then leveraged **privilege escalation** techniques to obtain root-level control.
- Discovered and exploited web application flaws such as **Cross-Site Scripting (XSS)** and **SQL Injection** on HTTP services running on port 80.
- Authored a professional penetration testing report outlining risk severity, business impact, and prioritized remediation recommendations for the client.

### Active Directory Exploitation & Lateral Movement | *Seneca Polytechnic*

- Emulated a red-team operation against a corporate Windows domain by exploiting the **MS17-010 (EternalBlue)** vulnerability to secure initial System-level access.
- Conducted **credential harvesting** with **Mimikatz/Kiwi** to extract **NTLM hashes** and used **John the Ripper** for offline password cracking.
- Performed **lateral movement** using Pass-the-Hash attacks with **Impacket** to compromise additional hosts and maintain persistence over RDP.

### IoT Security Monitoring & Threat Analysis | *Seneca Polytechnic*

- Engineered a secure IoT setup with Raspberry Pi and AWS IoT Core, orchestrating temperature sensor data using Python-based automation.
- Built a virtualized Security Operations Center (SOC) leveraging **Suricata** for intrusion detection and the Elastic Stack (ELK) for real-time threat visualization.
- Launched controlled **DDoS simulations** against the IoT environment to validate defensive robustness, inspecting traffic behavior through **AWS VPC Flow Logs stored in S3**.

## Security Case Studies & IR Analysis | *Seneca Polytechnic*

- Completed multiple written security case studies covering large-scale breaches, supply-chain attacks, and identity data exposures, focusing on incident timelines, root cause, and impact.
- Developed incident response and communication plans, including executive summaries, stakeholder notifications, and vendor-related risk handling for real-world style scenarios.
- Produced legal and governance-oriented recommendations (policies, contracts, and preventative controls) to strengthen organizational preparedness and third-party risk management.

## CERTIFICATIONS

### Cloud & Operating Systems

- **AWS Cloud Security Foundations** | *AWS Academy*
- **Introduction to Linux** | *The Linux Foundation*

### Cybersecurity & Forensics

- **Introduction to Digital Forensics** | *Cyber5W*
- **Introduction to Cybersecurity** | *Cisco Networking Academy*

### Networking & Infrastructure

- **IPv6 Address Planning & Fundamentals** | *APNIC*
- **Introduction to Critical Infrastructure Protection** | *OPSWAT Academy*
- CompTIA A+

## EDUCATION

- **Cybersecurity and Threat Management** (Ontario College Graduate Certificate)  
*Seneca Polytechnic - Toronto, ON* | (Term GPA 4.0) Expected August 2026
- **Bachelor of Computer Science and Information Technology**  
*Deerwalk Institute of Technology – Kathmandu, Nepal* | Mar 2013 – Mar 2017

## WORK EXPERIENCE

### IT - User Service Representative (Part-Time)

#### George Brown College Library – Toronto, ON

Sep 2023 – Present

- Support 70+ users per day across Windows, macOS, and ChromeOS for login, printing, connectivity, and software issues.
- Handle Identity Management (IDM) tasks: account verification, temporary passwords, coordination with ITS for-account issues.
- Assist with MFA setup and security-related access issues while maintaining positive user experience.
- Use Banner, PaperCut, Helix, Waitwell, MS Office, Teams, and Outlook in daily operations.

### DevOps | Cedar gate Technologies | Kathmandu, Nepal

May 2018 – Mar 2020

- Lead release management for Cedar gate products, scripting application builds, and automating routine operational tasks.
- Managed Agile support and sprint work through ticketing platforms (Redmine, Jira) while administering Git branching and tagging for clean version control.
- Deployed and maintained application servers and services using Jenkins pipelines and systemctl scripts to improve reliability and reduce manual work.
- Implemented ELK and CloudWatch (plus tools like PagerDuty and Nagios) for centralized logging and proactive monitoring of application and server performance.