Neel Soni

Guelph, ON N1L 0J2 | sonineelp@gmail.com | 6479198283 | linkedin.com/in/sonineelp | github.com/neelsoni26

Professional Summary

Master's student in Cybersecurity with practical experience in penetration testing, malware analysis, and threat intelligence. Proven ability to lead technical initiatives and participate in real-world attack simulations. Committed to protecting systems and applying AI for proactive threat mitigation.

EDUCATION

Master of Cybersecurity & Threat Intelligence Expected Jan 2026
University of Guelph
Guelph, ON

Graduate Certificate in Information Security Management Dec 2024
Fanshawe College, GPA: 3.59
London, ON

Bachelor of Computer Science and Engineering Jun 2021
Navrachana University, CGPA: 7.25
Vadodara, Gujarat, India

PROJECTS & RESEARCH

ArXiv Paper Summarizer (Multi-Agent AI System) Jun 2025 – Jul 2025

- Tasked with automating literature reviews from arXiv by developing a multi-agent research assistant using Microsoft's AutoGen framework, leveraging Python libraries like autogen, arxiv, openai, and asyncio.
- Designed and implemented two specialized agents (search and summarizer) that communicate through a RoundRobinGroupChat to efficiently divide tasks and generate structured Markdown reviews.
- Delivered a modular AI system demonstrating effective coordination and scalability for autonomous research tools, improving the efficiency and quality of literature summarization.

Hybrid Malware Detection with Explainable AI (SHAP) May 2025 – Jun 2025

- Led development of a hybrid malware classification system by merging static (EMBER) and dynamic (CIC-MalMem) features, managing a dataset of approximately $850,000$ samples with $2,400+$ dimensions.
- Applied Principal Component Analysis (PCA) to reduce dimensionality while maintaining 98% variance and used Synthetic Minority Over-sampling Technique (SMOTE) to fix class imbalance. Then trained XGBoost, LightGBM, and Multi-Layer Perceptron (MLP) models, with XGBoost reaching 96.1% accuracy and 0.991 ROC AUC after tuning.
- Employed SHapley Additive exPlanations (SHAP) for explainability to pinpoint key features and interpret model decisions, producing visualizations that enhanced transparency and trust in detection results.

Exploit Development and Vulnerability Assessment Jan 2025 – Apr 2025

- Identified and exploited buffer overflow vulnerabilities in user programs by crafting custom payloads to achieve local privilege escalation.
- Utilized GDB for detailed memory and call stack analysis, developing return-to-libc and shellcode attacks to validate exploitability.

- Performed comprehensive vulnerability scanning with OpenVAS and Nessus, automated fingerprinting via Nmap NSE, and leveraged Metasploit for post-exploitation tasks like credential dumping and persistence.

APT Analysis and AI-Based Detection for Cyber Threat Intelligence Jan 2025 – Apr 2025

- Collaborated in a team to research 40+ state-sponsored APT groups and develop structured TTP profiles using OpenCTI for detailed threat modeling.
- Reverse-engineered malware samples with GHIDRA to extract opcode-level features, then engineered Machine Learning (ML) models (Support Vector Machines (SVM), K-Nearest Neighbors (KNN), Decision Trees) on n-gram opcode sequences for detection.
- Implemented and benchmarked a Convolutional Neural Network (CNN) model against traditional classifiers, evaluating performance via accuracy, precision, recall, F1-score, and visual analytics to optimize threat identification.

Web Application Security Testing (SEED Labs) Jan 2025 – Apr 2025

- Conducted black-box and white-box testing to exploit XSS, CSRF, and SQL injection vulnerabilities in lab-built web apps.
- Built PoC payloads using curl, Burp Suite, and in-browser JavaScript to demonstrate real-world attack vectors.
- Recommended mitigations including Content Security Policy (CSP) headers, Cross-Site Request Forgery (CSRF) tokens, and input sanitization to improve app security posture.

PUBLICATIONS

OpCode-Based Malware Classification Using Machine Learning and Deep Learning Techniques

- *arXiv preprint arXiv:2504.13408*, April 2025

VOLUNTEER LEADERSHIP

Chapter Leader, OWASP WWW Chapter – University of Guelph

- Co-leading the university's OWASP chapter, organizing security workshops, CTFs, and promoting secure development practices on campus.

SKILLS SUMMARY

- **Technical Security Skills:** Network security, penetration testing, vulnerability assessment, SIEM (Splunk, Elastic), incident response, threat intelligence, malware analysis, reverse engineering (GHIDRA)
- **Programming & Scripting:** Python, Bash, JavaScript, regex, automation, secure coding practices, data science libraries (Keras, TensorFlow), Git, prompt engineering (LLMs)
- **Systems & Network Administration:** Linux/Unix, Windows, macOS, TCP/IP, DNS, DHCP, VPNs, cloud platforms (AWS, Azure, GCP), virtualization (VMware), containerization (Docker)
- **Cybersecurity Frameworks & Compliance:** NIST, GDPR, risk assessment, security auditing
- **Tools & Technologies:** Nessus, OpenVAS, Wireshark, Nmap, Burp Suite, Splunk, Elastic, Metasploit, Suricata

EXPERIENCE

Sales Associate, Sai Krupa Jewellers, Vadodara, India Jul 2021 – Mar 2024

- Delivered customer service to 2,000+ clients in a high-value retail setting, managed daily POS transactions exceeding rupees 2 lakh, and improved display efficiency by 15% through organized inventory handling and presentation.