Shayaan Rashedin

Mississauga, ON • 647-877-1449 • shayaan.rashedin@torontomu.com
linkedin.com/in/shayaanrashedin • github.com/shayaanrashedin • Portfolio: shayaanrashedin.github.io

Summary of Qualifications

- Third-year Computer Engineering student with strong foundations in programming, circuit analysis, and systems design, combined with hands-on cybersecurity experience.
- Developed applied cybersecurity skills through a home lab: performed vulnerability scanning, SIEM detection, and incident reporting using tools like Splunk, Nmap, OpenVAS, Hydra.
- Strong problem-solving, teamwork, and technical communication skills, demonstrated in robotics competitions, engineering courses, and instructional roles.
- **Technical Skills:** SIEM (Splunk), OpenVAS/GVM, Nmap, Linux (Kali, Ubuntu), VirtualBox, Bash, Java, SQL, Digital Systems, Embedded Systems, Computer Architecture, Circuit Analysis, Algorithms & Data Structures

Education

Bachelor of Engineering – Computer Engineering Sept. 2023 – Exp. 2028
Toronto Metropolitan University, Toronto, ON
• Relevant Coursework: Computer Programming Fundamentals, Electric Circuit Analysis, Digital Systems, Software Systems, Algorithms & Data Structures

Certifications
• Google Cybersecurity Professional Certificate — *Jun 2025*
• Google IT Support Professional Certificate — *Feb 2025*

Projects

Cybersecurity Home Lab (VirtualBox – Kali Linux, Metasploitable2, Ubuntu, Splunk):
Built a virtualized security lab to practice offensive and defensive techniques, focusing on scanning, exploitation, and SIEM detection. Full technical write-ups and screenshots available on portfolio: shayaanrashedin.github.io

- **Brute-Force Detection with Splunk:** Simulated SSH brute-force attacks from Kali Linux against Metasploitable2, configured Splunk SIEM to detect SSH brute-force attempts, reducing detection time by 75% (MITRE ATT&CK T1110).
- **Network Scanning & Reconnaissance:** Conducted Nmap service/version scans and an OpenVAS vulnerability assessment on Metasploitable2, enumerating 30+ services and identifying critical exposures including vsftpd 2.3.4 backdoor, UnrealIRCd, and distcc.
- **Vulnerability Exploitation:** Validated and exploited vulnerabilities from the reconnaissance phase to gain root shells (vsftpd, UnrealIRCd, distcc), documenting procedures and findings on personal portfolio site.

Experience

Youth Engineering Instructor – Toronto High Park Young Engineers, Toronto, ON
Sept 2024 – Present
• Delivered engineering curriculum with hands-on LEGO projects; mentored 20+ students in teamwork and problem-solving.
• Simplified technical concepts (transmissions, gear ratios) into engaging lessons; received positive parent feedback.

Lead Builder & Programmer – VEX Robotics World Championship Team, Mississauga, ON
2022 – 2023
• Designed and programmed competition robots; represented Canada internationally.
• Trained teammates on programming and debugging, improving reliability and performance.