# AMAN SHARMA

+1 (226) 886-5762 || North York, Ontario || aman.s14199@gmail.com || linkedin.com/in/aman-sharma-1a79ba1b6

## PROFESSIONAL SUMMARY:

Aspiring Cyber Security Analyst with a solid foundation in vulnerability management, threat detection, and compliance frameworks. Skilled in identifying, investigating, and remediating network vulnerabilities using industry-standard tools. Proven ability to support awareness training, internal audits, and policy development in fast-paced environments. Dedicated to protecting organizational assets while supporting broader ESG (environmental, social, governance) goals.

## TECHNICAL SKILLS:

| | |
|---|---|
| **Operating Systems** | MS-DOS, Windows XP/7/8/10, Windows Server 2008/20012/2016, Linux – Debian, Kali, Ubuntu. |
| **Tools** | Wireshark, NMAP, Metasploit, Splunk, Snort, Autopsy, OSSEC, Tcpdump,Tshark, Zeek, Brim, Yara, Misp. |
| **Programming Skills** | Shell Scripting – Python, C#, WordPress. |
| **Additional Skills** | SIEM, VirusTotal, Awareness Training Content (Newsletters, Presentations), project documentation, endpoint management, vulnerability management. |
| **Frameworks** | Familiarity with ISO 27001, SOC 2, NIST CSF |
| **Soft Skills** | Communication skills, Team Collaboration, problem-solving, analytical. |

## WORK EXPERIENCE:

**Intern – Infowiz, Chandigarh, India**                                    **Jan 2022 – May 2022**

- Conducted asset inventory and managed secure deployment of IT hardware/software
- Developed secure systems for complaint and hospital management with integrated access controls
- Assisted in troubleshooting and patch management for networked environments
- Supported policy and awareness initiatives related to security best practices

## PROJECTS (Volunteered):

**Network Traffic Analysis using Wireshark**
- Captured and analyzed packet data (PCAP files) from simulated attacks including port scans, brute force attempts, and DDoS scenarios.
- Identified patterns of malicious activity and classified alerts as true/false positives.
- Used filters and TCP stream reassembly to trace attacker behavior and pinpoint compromised endpoints.
- Documented all findings with detailed logs and recommended mitigation steps.

**Host-Based Intrusion Detection System with OSSEC**
- Deployed OSSEC on a Linux virtual machine to actively monitor system logs and detect security anomalies.
- Configured real-time alerts for unauthorized access attempts, file integrity changes, and privilege escalations.
- Implemented custom rule sets to enhance detection accuracy and reduce false positives.
- Integrated alerts with email notifications for real-time response simulation.

## EDUCATION:

**Post-Graduate Diploma in Business Administration**                    May 2024 – Jan  2025
York University, Toronto, ON

**Post-Graduate Diploma in Cybersecurity Operations**                    Sept 2023 –Apr 2024
York University, Toronto, ON

**Bachelor's in Computer Engineering and Technology**                    June2018 – May 2022
Guru Nanak Dev University, Amritsar, PB

## WEBSITE AND PORTFOLIO:

- **https://aman-sharma-portfolio.framer.website**
- **https://github.com/aman14199**

## CERTIFICATIONS & LABS:

- TryHackMe Labs (hands-on labs in exploitation, scanning, traffic analysis)
- Ongoing preparation for CompTIA Security+ and CEH