Dhrumil Rupakar

Information Technology Student | Specializing in Cybersecurity, Cloud & Networking
Toronto, Ontario • (437) 858-4650 • dhrumilrupakar04@gmail.com • https://www.linkedin.com/in/dhrumilrupakar/

SUMMARY

Cybersecurity student with hands-on experience in threat detection, incident response, vulnerability management, and cloud infrastructure. Skilled in technical support, system troubleshooting, and network security. Proficient in configuring secure Linux, Windows, and macOS systems, deploying Azure and AWS services, and automating tasks using Bash and PowerShell.

PROFESSIONAL EXPERIENCE

Warehouse Associate **Nov 2024 – Present**

Amazon, Toronto

- Processed 1,200+ packages per shift with 98% accuracy using automated systems, improving speed and efficiency.
- Diagnosed and resolved 15+ device issues weekly (RF scanners), sharpening troubleshooting and tech support skills.
- Ranked in top 5% of team for productivity during high-volume periods.
- Contributed to a 20% improvement in workflow by identifying and suggesting layout optimizations.

Cybersecurity Virtual Experience - Remote **Aug 2024**

Mastercard, Toronto

- Analyzed 5+ phishing simulations and proposed mitigations to reduce human risk factors.
- Designed a security awareness module that enhanced user resilience against phishing by 30% in case scenarios.
- Evaluated breach response documentation and mapped incident response steps in simulated SOC tasks.
- Applied vulnerability assessment techniques and threat detection workflows in cloud-based case studies.

PROJECT EXPERIENCE

Cybersecurity Homelab Project

Personal Project, Toronto

- Created an enterprise-like environment using Windows Server, Kali Linux, and Ubuntu to simulate real-world threats and defensive strategies.
- Deployed pfSense firewall, VPN, and ACLs across 5+ segmented networks to simulate multi-layered defense.
- Integrated Splunk to monitor 10K+ logs daily and ran 50+ Nessus scans, identifying and remediating critical vulnerabilities with 90% closure rate.

Remote File Inclusion to Remote Code Execution Attack Simulation

Seneca Polytechnic, Toronto

- Exploited RFI vulnerability in DVWA to achieve full remote code execution in a sandboxed Linux-Windows environment.
- Used Suricata IDS to detect and log attack signatures, demonstrating real-time threat monitoring.
- Reduced simulated attack surface by 60% through hardening strategies and documented remediation workflows.

SKILLS

- **Networking:** TCP/IP (HTTP, HTTPS, UDP, ICMP, FTP, SSH, ARP, DNS, DHCP), OSI, Routing & Switching (Cisco), Firewalls (pfSense, iptables, windows), VPNs, ACLs, VLANs, SDN/OpenFlow.
- **Cybersecurity:** Threat Detection, Incident Response, Vulnerability Management, Digital Forensics.
- **Cloud:** Azure, AWS (EC2, S3, IAM, VPC), Azure SQL, VM Provisioning, Cost Management, Backup Policies, Governance, Compliance, Security Automation.
- **Systems & Tools:** System Administration - Windows, Linux (Ubuntu, Kali, Debian, CentOS), macOS, Active Directory, Bash, PowerShell, Python, Nmap, Wireshark, IDS/IPS, Suricata, Splunk, Nessus, Virtualization (VMware, VirtualBox)
- **Soft Skills:** Communication, Troubleshooting, Technical Documentation, Teamwork, Problem Solving, Multitasking.

CERTIFICATIONS

CISSP Foundation | Introduction to Cybersecurity & Cybercrime | Foundational Online Security Awareness | Packet Tracer – Cisco Networking | Programming with Python 3.x | Pursuing CompTIA Security+

EDUCATION

Seneca Polytechnic **Toronto, Canada**

Advanced Diploma in Computer Systems Technology (CGPA: 3.9/4.0) May 2024 – Dec 2026

Award: President’s Honor List x2 (Summer 2024, Winter 2025)