Monarch Giri

monarchgiri19@gmail.com | 647-897-3638 | Toronto, ON | LinkedIn | Portfolio

Professional Summary

Cybersecurity Analyst with a solid foundation in security concepts, frameworks, and technologies. Adept at utilizing tools like Wireshark, Nmap, Snort, Python, and Splunk for monitoring, analysis, and threat detection. Proficient in implementing and optimizing SIEM systems, deploying real-time threat detection solutions, and designing comprehensive network infrastructures. Committed to safeguarding assets through innovative solutions and fostering a culture of security awareness.

Key Skills

- Network Security: Firewall, VPNs, IDS/IPS, Zero Trust, Port Security
- Cybersecurity Tools: Splunk, Wireshark, Nmap, Burp Suit, Nessus, Wazuh
- Threat and Risk Management: Vulnerability Management, Threat Detection, Incident Response
- Security Frameworks: NIST Cybersecurity Framework, ISO 27001, 27002, 31000, PCI DSS
- Operating Systems: Linux, Windows, MacOS
- Programming Languages: Python, Bash

Education

Ontario College Graduate Certificate in Cyber Security **January 2023 – August 2024**
Loyalist College, Toronto

BSc (Hons) Computer Networking and IT Security **August 2018 – December 2021**
Islington College, affiliated to London Metropolitan University, London

Work Experience

Project Lead **May 2024 – August 2024**
Vulnerability Vanguards

- Led a team of 6 to develop a vulnerability scanner, meet 100% of project milestones within a strict 4-month deadline, and improved endpoint/network security capabilities.
- Increased threat detection accuracy by 35% by integrating Nmap for accurate scanning with SearchSploit for exploit analysis, resulting in trustworthy security insights for client's networks.
- Developed a TOTP-based authentication system and a user-friendly interface in PyQt6, streamlining access control and reducing login security risks by 50%.
- Collaborated with the marketing team to create a professional website and promotional video demos, which boosted client engagement and increased project visibility by 60%.
- Presented project deliverables to clients and stakeholders in a final showcase, achieving 90% positive feedback and securing interest in future deployments.

IT Intern **January 2022 – August 2022**
Hospital and rehabilitation center for disabled children (HRDC)

- Developed and implemented network infrastructure and security standards in collaboration with the CTO, IT manager, and senior network architect, improving network reliability and reducing downtime by 20%.
- Monitored and maintained network systems, including routers, switches, and firewalls, ensuring smooth operation and timely updates, resulting in a 10% increase in network uptime.
- Managed network security incidents, including user access control, firewall breaches, and VPN configurations, reducing network-related security risks.
- Troubleshooted and resolved network connectivity issues, ensuring minimal service disruption and reducing resolution time by 15% through effective coordination with the network operations team.

Cybersecurity Intern **September 2020 – May 2021**

Vairav Technology

- In the Security Operations Center (SOC), real-time network activity tracking and analysis was carried out. Potential security threats were recognized and addressed, resulting in a 15% reduction in incident detection time.
- Implemented and monitored security measures, such as firewalls, antivirus programs, and intrusion detection systems (IDS), increasing the effectiveness of threat detection and response.
- Used Splunk capabilities for monitoring and analyzing active logs, configuring automated alerts to identify questionable activity, and promptly notifying the lead analyst of key alerts for immediate incident response.
- Developed and implemented security awareness training programs, which helped the company create a culture of cybersecurity awareness and reduce security incidents linked to human error by 25%.

Projects

IDS, IPS with Snort and Log analysis using Splunk

- Developed a home lab environment with 4 virtual machines, integrating Snort for packet detection and Splunk for log analysis, to simulate real-world SOC (Security Operations Center) scenarios.
- Wrote custom IDS and IPS detection rules, and triggered those rules to generate logs, demonstrating real-time threat detection and rule-based incident response.
- Used Wireshark to further analyze the Snort logs, drilling down into specific log files to identify the nature of network activity and potential security events.
- Analysed logs using Splunk to find patterns in network activity and any security risks. Alongside performing practical Splunk tasks on the TryHackMe platform.

Smart room temperature controller and smart light with Google Assistant

- Developed a voice-activated smart home system with integrated Google Assistant for temperature monitoring and lighting control, streamlining household administration.
- Used NodeMCU as the primary microcontroller for communication and parts such as temperature sensors, relays, and an LCD screen that displayed the temperature and time in real-time.
- Used the Arduino IDE for programming which allowed for smooth device control and real-time data monitoring, resulting in an easy-to-use and intuitive interface.
- Addressed the need for smart home automation by streamlining light and temperature control, improving convenience, and showcasing the integration of IoT technologies into everyday tasks.

Certifications and Achievements

- CompTIA Security+ (Expected 12/2025)
- SOC level 1 | TryHackMe
- Cyber Defense | TryHackMe