KRIPESH ACHARYA

kripeshacharya2025@gmail.com | (475) 221-3321 | Virginia, VA 23901 | LinkedIn Profile | Portfolio

OBJECTIVE: Aspiring cybersecurity expert dedicated to bridging the gap between emerging threats and robust security solutions, eager to embrace new challenges and drive impactful results.

EDUCATION

Mercy University, Dobbs Ferry, NY — August 2023 - December 2024

Master of Science in Cybersecurity

- **GPA:** 4.0

***Specialization**:* C/C++, Python, Networking & Data Communication, Database Security, Information Assurance & Management, Firewall & Intrusion Detection, Digital Forensics, Applied Cryptography, Wireless Network Security

Leeds Beckett University, UK — January 2021 - April 2022

Bachelor of Science in Computing

- **GRADE:** First Class Honors

***Specialization**:* Intelligent Systems, Digital Security, Advanced Database System, Advanced Web Engineering

International School of Management and Technology, Kathmandu, Nepal — January 2018 - March 2020

Associate of Science in Computing

***Specialization*:** Java, Networking, Cloud Computing, Network Security, SDLC, Project Management, Web Development, Client/Server Computing, Network Management

TECHNICAL SKILLS

***Languages**:* C, C++, Python, PowerShell, SQL, HTML

Tools & Technologies: Linux, Vulnerability Management, Threat Analysis, Open-Source Intelligence, Network Analysis, Cryptography, Forensic Analysis, Microsoft Tools, Splunk, SIEM, SOAR, GitHub, IAM, Encryption, Hashing, AWS security EDR, Log Analysis and Management, Firewalls, Intrusion Detection Systems, Security Monitoring, Zero Trust, Network Protocols

Other Skills*:* Time Management, Problem-Solving, Leadership, Project Management, Communication, Teamwork, Attention to Detail

Certification: CompTIA Security+ (Ongoing), ISC2 Certified in Cybersecurity, CISCO Ethical Hacker, Security Blue Team Junior Analyst Training, NIST Risk Management Framework (RMF), CNSS Certified Network Security Specialist

WORK EXPERIENCE

Vianet Communications, Lalitpur, Nepal — March 2020 - September 2022

Network Security Analyst

- Monitored network traffic and security alerts for real-time threat detection and response.
- Configured and maintained security devices such as firewalls, intrusion detection/prevention systems, VPNs, and endpoint protection solutions to protect the organization's network.
- Provided training and support to staff on best practices and protocols, fostering a culture of security awareness throughout the organization.

Visva Technikos, Kathmandu, Nepal — January 2019 - November 2019

System Administrator

- Configured Windows Server 2012 R2 and Red Hat Enterprise Linux, including Active Directory, FTP, VPN, User Accounts, and File Permissions.
- Troubleshot system/network issues and monitored performance for seamless operations.

PROJECTS GitHub Link

- **Investigating Compounding Threat Trends on National Critical Infrastructure**
  Sandia National Laboratories — August 2024 – December 2024
  Cybersecurity Researcher
  - Analyzed compounded threats to national critical infrastructure across sectors.
  - Developed and validated a comprehensive Threat Assessment Framework addressing Digital, Physical, and Human threat factors.
- **Home Lab Setup & SIEM Implementation using Splunk** — September 2024
  - Built and configured a home lab environment to implement Splunk for SIEM.
  - Integrated, monitored, and analyzed logs, creating dashboards and alerts for enhanced threat visibility.
- **Firewall Configuration and Rule Implementation** — May 2024
  - Configured and managed PfSense and Palo Alto firewall, implementing various security rules to control traffic and enhance network protection.
- **Configuring Snort and Creating Detection Rules for Network Traffic and Attack Patterns** — June 2024
  - Configured Snort on Ubuntu to monitor network traffic and developed custom detection rules, utilizing a Kali Linux attacker environment to simulate and analyze attack patterns.
- **Developing Red Team Reports** — December 2023
  - Performed red team assessment on Windows systems using Kali Linux, utilizing tools like Nmap for information gathering and Metasploit for exploitation, followed by post-exploitation tasks.
  - Provided security recommendations, detailed risk ratings, and mitigation strategies for identified vulnerabilities.
- **Cybersecurity Awareness Training Delivery** — July 2022
  - Delivered training on social engineering attacks, educating students on recognizing tactics like phishing, pretexting, and baiting to prevent security breaches.