Subodh Shrestha

| shresthasubodh73@gmail.com| +977-9868836822 | LinkedIn: Subodh Shrestha| GitHub: subodhstha |

Cybersecurity professional with practical experience across threat detection, incident response and network security. Skilled in ELK Stack, ElastAlert, TheHive, Snort and Suricata for monitoring and defensive operations. Strong understanding of network infrastructure and secure system design, enabling a comprehensive approach to identifying and mitigating cyber threats. Passionate about proactive defense, continuous improvement and maintaining confidentiality in all operations.

EDUCATION

College of Applied Business & Technology **Chabahil, Kathmandu**
B.S. in Computer Science and Information Technology *Graduated, 2025*
Tribhuvan University

- **Key Courses: -** Cryptography, Network Security, Computer Networks, Operating Systems, Machine Learning, Design & Analysis of Algorithms

CERTIFICATIONS

CyberOps Associate (Cisco)

- Security monitoring, threat detection and incident response

CSI Linux Certified Investigator (CSI Linux)

- *Digital forensics and evidence acquisition*

Junior Cybersecurity Analyst (Cisco)

- *Threat detection, incident response, and network defense tools (Wireshark, Snort, Nmap)*

PROFESSIONAL EXPERIENCE

Green Tick Nepal Pvt. Ltd. **Gyaneshwor, Kathmandu**
Cybersecurity Associate *August 2025 – Present*

- Developed and tuned detection rules in ELK Stack and ElastAlert to identify malicious behavior.
- Built KQL detection queries in Kibana for SQL injection, XSS and command injection attacks across web traffic.
- Created threat dashboards in Kibana showing attack trends, MITRE ATT&CK coverage and alert metrics.
- Implemented RSPAN traffic mirroring and centralized syslog aggregation from network devices.
- Performed packet analysis with Wireshark to validate alerts and reconstruct attack chains.
- Supported digital forensics using Autopsy and FTK Imager for disk imaging and artifact recovery.
- Managed Snort and Suricata IDS/IPS deployments with custom signature development.
- Investigated phishing campaigns analyzing email headers, DMARC/SPF, attachments and URLs.
- Collaborated on SOC reports and security documentation for enterprise clients.
- Conducted Network assessments.

Cybersecurity Intern April 2025 – July 2025

- Performed security hardening for firewalls, switches and wireless infrastructure.
- Resolved Elasticsearch cluster issues optimizing SIEM performance.
- Deployed network monitoring infrastructure for SOC operations.

College of Applied Business & Technology **Chabahil, Kathmandu**
Software Development and Computer Network *May 2023 – Jan 2025*

- Designed, configured and maintained LAN/WAN infrastructure.
- Configured pfSense firewalls, VLANs, and VPNs for secure communication and segmentation.
- Conducted network troubleshooting, performance optimization and technical documentation.
- Developed and secured web applications using Django and Laravel frameworks.
- Applied encryption and authentication mechanisms to protect sensitive data.

SKILLS

Cybersecurity & Forensics: - ELK Stack, ElastAlert, TheHive, CSI Linux, FTK Imager, Autopsy, Wireshark, MITRE ATT&CK
Network Security: - Snort, Suricata, pfSense, Nmap, RSPAN, NetFlow, SNMP, IDS/IPS
Programming & Tools: - Python, Bash, SQL, Django, Laravel, Git, Docker, Linux
Development: - Python, Bash, SQL, Django, Laravel, Git, Docker, Linux
Core Strengths: - Threat Detection, Forensic Analysis, Incident Response, Log Correlation, Network Defense

PROJECTS

Image Forgery Detection **Chabahil, Kathmandu**

Team Project *Aug 2024*

- Designing a system to detect image forgery using digital signatures (ed25519) and perceptual hashing.

Robo-Soccer Bots **Chabahil, Kathmandu**

Team project *Jul 2023*

- Built Arduino-based robotics platform for competitive event (Hex-Himalaya)

TRAFFIC SIGN CLASSIFICATION **Chabahil, Kathmandu**

Team Project *Mar 2023 – April 2023*

- Built a CNN-based traffic sign recognition system using Keras.

ACTIVITIES AND LEADERSHIP

Hex-Himalaya **Chyasal, Lalitpur**

Showcased technical skills in robotics and teamwork during the Robo-Soccer event. *Jul 2023*

Code Brisk Hackathon **Naxal, Kathmandu**

Participated in a Hackathon on problem-solving and innovation. *Feb. 2023*

KU HackFest 2022 **Dhulikhel, Kavrepalanchok**

Participated in a hackathon, developing innovative solutions to real-world challenges. *Aug. 2022*