

Saksham Sharma

Cybersecurity Analyst / SOC (Blue Team)

sharma@saksham.info.np | contactsaksham52@gmail.com | +977 9764777592 | Lalitpur, Nepal
LinkedIn: sakshamsharma52 | GitHub: unexplainablefish52

Summary

Self-driven IT undergraduate (TU IOST) focused on **Security Operations (SOC)** and defensive cybersecurity. Built hands-on fundamentals through **home lab** practice and scenario-based training, including **traffic capture/analysis**, **firewall configuration**, and **log analysis** with SIEM concepts. Strong interest in applying skills in **alert triage**, **threat detection**, and **risk-aware security operations**.

Skills

Operating Systems	Linux (Kali), Windows
Networking	TCP/IP, DNS, HTTP/S; packet capture and analysis
SOC / Blue Team	Log analysis fundamentals, alert triage mindset, incident response basics
Tools	Wireshark, tcpdump, Splunk (SPL), pfSense, Burp Suite, Nmap (lab/defensive)

Hands-on Practice & Home Lab

- Performed **packet capture and analysis** using **Wireshark** and **tcpdump**, identifying common patterns in **DNS** resolution and **TCP** connection setup.
- Configured a virtual **pfSense** firewall lab, implemented basic **allow/deny rules**, and reviewed **firewall logs** to validate allowed vs. blocked traffic.
- Practiced **security monitoring** concepts using **Splunk** and **SPL** to explore ingested events and perform basic investigation-style searches (top sources, spikes, and anomalies).
- Completed SOC-style investigation scenarios on **LetsDefend** (phishing, brute force, and firewall-related alerts) and documented key indicators and next-step checks.
- Used **Burp Suite** for **web traffic interception** and basic testing on intentionally vulnerable applications (e.g., **OWASP Juice Shop**) to understand web request/response flows.
- Used **Nmap** in a controlled lab environment for **asset discovery** and service enumeration to support defensive visibility and hardening.

Certifications

- ISC2 Certified in Cybersecurity (CC)** — 2026
- Google Cybersecurity Professional Certificate** — 2026
- Certified Ethical Hacker (course/certificate)** — Packt via Coursera — 2025

Education

Bachelor in Information Technology (BIT), TU IOST Nov 2024 – Present

Patan Multiple Campus, Lalitpur, Nepal

High School (Science Stream), GPA: 3.43 Aug 2022 – Jun 2024

Madhyabindu Multiple Campus, Gandaki Province, Nepal

Languages

Nepali (Native) | English (Certified + Professional)