Swapnil Katuwal

SOC INTERN | CYBERSECURITY INTERN

Kapan, Kathmandu • 9818221348 • swopnilkatwal@gmail.com

@ https://www.linkedin.com/in/swapnil-katuwal-bb7529309/ @ https://github.com/swapnilbrrr

Motivated and detail-oriented cybersecurity learner transitioning from software testing into security operations. Experienced in Kali Linux home-lab setup and SOC-style alert triage. Solid foundation in structured documentation and procedural accuracy. Seeking a SOC Internship to strengthen incident response capabilities and contribute to real-world monitoring environments.

KEY COMPETENCIES

- Security & SOC Skills: Kali Linux, Alert Triage, Network Traffic Analysis (Wireshark), Incident Response (Conceptual), Vulnerability Scanning (Conceptual), Threat Intelligence, Endpoint Detection and Response (Conceptual)
- Systems & Tools: Linux (CLI & GUI), Windows, VMware, VirtualBox, Postman
- Programming & Scripting: Python (Basic), Shell Scripting, JavaScript (Basic), R (Basic)
- Professional Skills: Technical Documentation, Procedural Diligence, Analytical Problem Solving, Manual QA Testing, Web Development

EXPERIENCE

QA INTERN Kathmandu

Midas Health Services Feb, 2025 - May, 2025

- Executed multi-step test procedures with high precision, demonstrating SOC-level procedural accuracy.
- Identified, analyzed, and prioritized defects in a workflow similar to triaging security alerts.
- Produced clear documentation with exact reproduction steps and environment details.
- Collaborated with developers to validate fixes and maintain product stability.

EDUCATION

BSc.IT Kathmandu

Lord Buddha Educational Foundation Nov, 2024 - Present

PROJECTS

Port Scan Detector (Python)

Built a custom network enumeration tool designed to simulate real-world reconnaissance techniques and measure defensive visibility. The system performs raw socket-level banner grabbing to detect vulnerable service versions (including SSH, HTTP, and RPC) without relying on external libraries. It also includes a forensic logging module that generates timestamped audit trails (scan.log) for post-scan analysis. The project is developed using Python with a strong focus on TCP/IP networking and low-level socket programming and is available on GitHub.

LetsDefend – Security Alert Triage Simulations

Completed multiple incident simulations including Web Shell Detection, Brute Force Attempts, and Malware Infection. Performed evidence collection and wrote incident summaries.

TRAINING /CERTIFICATIONS

Introduction to CyberSecurity 2025

CISCO NetAcademy

SOC Beginner 2025

LetsDefend