Sumit Gyawali

Aspiring Cybersecurity/SOC Analyst

+4917615416064 | sumitgyawali85@gmail.com |

Prinzenstraße 64, Kamp-Lintfort, North Rhine-Westphalia, 47475, Germany | LinkedIn | Portfolio

SUMMARY

Driven cybersecurity professional with around one year of network support experience and hands-on expertise from Cisco training, CTF challenges, and TryHackMe labs. Skilled in Security Operations, with practical SOC exposure and knowledge of ISO 27001 and NIST frameworks. Proficient in tools like Splunk and Wireshark, and experienced in penetration testing, vulnerability assessments, cryptography, network traffic monitoring, and threat analysis. Committed to continuous learning and applying cybersecurity best practices to protect digital environments.

CORE SKILLS

Technical Skills	:	Network Security & Monitoring, Threat Intelligence & Malware Analysis, Operating Systems & Cloud Security, Log Analysis & Incident Response, Cryptography & Password Testing, Scripting & Version Control, AI Technology, Penetration Testing & Vulnerability Scanning, peripheral configuration
Tools & Technologies	:	SecureCRT, Nagios, Wireshark, Splunk, Nmap, IDS/IPS (Snort, Zeek), Burp Suite, Nessus, Kali Linux, AWS, VirtualBox, Active Directory, ChatGPT
Programming & Scripting	:	PowerShell, Bash, Python, GitHub
Soft Skills	:	Adaptability, Analytical Thinking, Teamwork, Strong Communication, Time Management, Problem-Solving
Languages	:	English (Fluent), Nepali (Native), Hindi (Fluent), German (Conversational-Improving)

WORK EXPERIENCES

Cybersecurity Trainee (Self-Initiated Learning), TryHackMe, United Kingdom **Jul 2024 — Present**

Key Learnings:

- Solved Capture The Flag (CTF) challenges and completed over 100 labs simulating real-world cyber threats, enhancing problem-solving skills and applying learned concepts to threat detection, incident response, and vulnerability mitigation.
- Developed SPL queries in Splunk to detect unauthorized access, privilege escalations, and failed logins. Created SIEM use cases for threat detection, integrating Burp Suite, Nessus, and Metasploit for vulnerability scanning and penetration testing. Enhanced monitoring with Splunk dashboards for real-time alerts and incident response.
- Conducted threat hunting exercises leveraging the MITRE ATT&CK framework to identify adversarial TTPs, mitigate risks, and improve detection capabilities while collaborating in Purple Team exercises to refine detection logic and enhance response strategies.
- Monitored and analyzed network traffic with tools like Wireshark and Nmap, identifying vulnerabilities and automating security tasks using PowerShell and shell scripting to improve operational efficiency.
- Acquired hands-on experience in identifying and mitigating common web vulnerabilities from the OWASP Top 10, such as SQL injection and cross-site scripting (XSS).
- Explored cryptographic operations such as hashing, encryption, decryption, and digital signatures using tools like OpenSSL and Hashcat.
- Enhanced cybersecurity expertise in cloud security, web security, and penetration testing through practical labs, and tool based exercises.

Network Monitoring and Troubleshoot Support,
Websurfer Nepal Communication System Pvt. Ltd., Kathmandu, Nepal **Dec 2020 — Aug 2021**

Roles and Responsibilities:

- Managed incoming tickets, provided incident support, and oversaw management tasks.
- Engagement in monitoring, diagnosing, and resolving technical issues both remotely and on-site user support.
- Supervised network operations via Nagios, configured EPON and GPON OLTs.
- Leveraged Whois and macvendor websites to track domain ownership, IP addresses, and identify devices by MAC address, improving network troubleshooting and security.
- Aid L3 engineers with setting up, diagnosing, and validating new network systems.
- Optimized router configurations, verified optical signal integrity, and registered MAC addresses in the OLT to ensure efficient network performance and high-quality connectivity.
- Updated data to accommodate changes in OLT SFP power and client PON power reception.

INTERNSHIP, iSewa Pvt. Ltd, Kathmandu, Nepal **Sep 2019 — Dec 2019**

Roles and Responsibilities:

- Developed and maintained web applications using PHP, MySQL, HTML, CSS, and JavaScript, ensuring both functionality and performance.
- Executed front-end and back-end development tasks, working with a team to integrate new features and optimize user experience.
- Collaborated with team members to design, develop, and implement innovative solutions to meet client requirements.
- Researched and evaluated new technologies to improve development workflows and enhance project delivery.

- Assisted in documenting technical specifications and procedures, ensuring streamlined processes for future development work.

EDUCATION

Hochschule Rhein-Waal, **Kamp-Lintfort, Germany** - *Bachelor, Infotronics System Engineering* **Sep 2022 — Present**

NIST College, **Banepa, Nepal** - *Bachelor, Computer Science and Information Technology* **Dec 2015 — Dec 2019**

CERTIFICATIONS

SOC Level 1 & 2, **TryHackMe** **Oct 2024**

Junior Cybersecurity Analyst Career Path, **CISCO** **Jul 2024**

Google Cybersecurity, **Coursera** **Apr 2024**

AWS Certified Cloud Practitioner CLF-C02, **Udemy** **Dec 2023**

PROJECTS/LABS

Credit Card Fraud Detection , Link
- Developed a credit card fraud detection system using RandomForest on Kaggle data, with a Streamlit dashboard for batch and single-transaction fraud probability predictions.

Network Intrusion Detection System (NIDS) , Link
- Developed using Python, Streamlit, Scapy, and Scikit-Learn, the tool captures network traffic, extracts source/destination IPs and packet sizes, applies K-Means clustering to detect anomalies, and presents the results through an interactive Streamlit dashboard.

Web Security Vulnerability Identification and Remediation, TryHackMe, Link
- Identified and mitigated web application vulnerabilities using tools like Burp Suite and OWASP ZAP.

Integrated Phishing Analysis and Data Security Toolkit, TryHackMe, Link
- Developed a toolkit integrating CyberChef, VirusTotal, and John the Ripper for phishing analysis and secure data handling.

Log Analysis and Threat Detection with Splunk, TryHackMe, Link
- Utilized Splunk to analyze security logs, detect threats, and enhance SOC operations with custom dashboards and alerts.

Network Scanning with Nmap, TryHackMe, Link
- Conducted network scanning and vulnerability assessments using Nmap to identify open ports and security risks.