KRISH SHRESTHA

SYSTEMS AND NETWORK

Gokarna, Kathmandu • 9763231786 • Krishshrestha768@gmail.com • LinkedIn • GitHub

Shresthakrish.com.np

PROFESSIONAL OVERVIEW

Driven by a strong interest in networking, system administration, and security, I have hands-on experience working with Linux servers, virtualization, web hosting, containerization, and infrastructure monitoring. I am currently developing a network automation and management tool, Luminet, designed for multi-vendor enterprise environments using Django and Ansible, while expanding my cloud knowledge through AWS certifications in Cloud Foundations, Architecture, Operations, and Security. My goal is to grow into a Network or Systems Administrator role where I can contribute to reliable, secure, and scalable IT environments.

WORK EXPERIENCE

Systems and Network Intern – DataHub Pvt. Ltd. **Jan 2026 - Present**

- Designed and deployed a multi-service virtualized lab environment using VirtualBox on Fedora Linux, provisioning Ubuntu and Rocky Linux servers with static IP addressing, SSH access, and system hardening
- Implemented a LAMP stack and deployed a production-grade WordPress site; managed full database lifecycle including scheduled backups and restoration via mysqldump
- Managed FortiGate firewall configuration including firewall rules, NAT policies, and traffic filtering to enforce network security standards
- Monitored system health across multiple hosts using Zabbix; configured alert triggers and dashboards for proactive incident detection
- Configured NFS file sharing, LVM storage management, and Linux file permissions across a multi-server environment

Offensive Security Intern - inRed Labs Pvt. Ltd. **Jul 2025 - Oct 2025**

- Performed vulnerability scanning and exploitation in a controlled lab environment covering SMB, RDP, and SUID privilege escalation scenarios
- Practiced the full VAPT process from information gathering and scanning through exploitation and professional reporting
- Applied OSINT and reconnaissance techniques including Google dorking and DNS enumeration to identify potential attack surfaces
- Explored web application vulnerabilities, CVE identification, and CVSS scoring to assess and prioritize security risks

Networking and IT support Intern - Dusit Princess Nepal **Aug 2024 - Nov 2024**

- Gained hands-on experience in VLAN configuration, network segmentation, and resolving Layer 1 and Layer 2 issues
- Used Cisco Packet Tracer to simulate and plan network changes prior to live deployment, reducing implementation risk
- Provided day-to-day IT and network support across hotel departments to ensure uninterrupted operations

SKILLS

Technical skills:

Networking: TCP/IP, DNS, DHCP, VLAN, Subnetting, VPN, NAT, FortiGate Firewall, Network Automation, Network Monitoring, Layer 1 & 2 Troubleshooting

Systems & Infrastructure: Linux, Windows, VirtualBox, VMware Workstation, Apache, Nginx, LAMP Stack, LVM, NFS, SSH, Docker

Automation & Cloud: Ansible, Python, Django, Git, AWS (Foundations, Architecture, Operations, Security)

Security: Nmap, Wireshark, Burp Suite, Metasploit, Bettercap, Volatility 3, MITRE ATT&CK, VAPT, DVWA

Monitoring: Zabbix

PROJECTS

FINAL YEAR PROJECT

Luminet – Network Automation and Management Tool

- Developed a web-based network automation platform supporting multi-vendor enterprise environments including Cisco, Arista, and MikroTik
- Engineered multi-vendor compatibility using Ansible as the automation engine to standardize tasks across different CLI syntaxes and workflows
- Implemented core automation features including VLAN management, port configuration, and dynamic interface discovery via a unified web GUI
- Built role-based access control (Admin, Operator, Viewer) with job tracking and audit logging for operational accountability
- Integrated encrypted device configuration backups with Git-based version control and one-click rollback to stable configuration

ACADEMIC PROJECTS

Memory Forensic Analysis of Fileless Malware and Anti-Forensic Techniques

Volatility 3, Metasploit, Wireshark, Autopsy, DumpIt

- Simulated a process hollowing attack injecting a Meterpreter payload into spoolsv.exe, escalating privileges to NT AUTHORITY\SYSTEM in a controlled Windows 10 lab
- Performed memory forensics using Volatility 3; identified suspicious memory regions, anomalous parent-child process relationships, and an active C2 channel over TCP/443
- Uncovered anti-forensic artifacts including NTFS timestamp manipulation, registry hive exfiltration, event log clearing, and deleted file recovery via Autopsy

ARP Spoofing Simulation (Security Lab)

Ettercap, Bettercap, Wireshark, Metasploitable

- Simulated ARP spoofing and Man-in-the-Middle attacks to capture unencrypted credentials; tested mitigations including Dynamic ARP Inspection (DAI) and Snort IDS

EDUCATION

BSc (Hons) Computer Networking and IT Security **2023-Present**

Islington College
London Metropolitan University
Kamaladi, Kamalpokhari, Kathmandu

CERTIFICATIONS AND TRAININGS

AWS Academy Cloud Architecting (2025)
AWS Academy Cloud Foundations (2025)
AWS Academy Cloud Operations (2025)
AWS Academy Cloud Security Foundations (2025)
DevOps Foundations: Bridging Development and Operations (2025)

REFERENCES

Raman Pradhananga
Networking Lecturer and Tutor, Islington College
ramanpradhananga@islingtoncollege.edu.np

Ganesh Subedi
Networking Lecturer and Tutor, Islington College
ganeshsubedi@islingtoncollege.edu.np