AAYUSH SHRESTHA

www.aayushng@gmail.com +977-9848445119 Kathmandu, Bagmati 44600

linkedin.com/in/aayush-shrestha-3379aa165

OBJECTIVE

Cybersecurity student with hands-on experience in offensive security, malware analysis, and secure network design. Highly motivated individuals with a proven track record in CTFs and hackathons, committed to continuous learning and staying updated in the cybersecurity domain.

EXPERIENCE

IT Auditor 05/2026 – Present

Himalayan Integrated Cloud Technologies

- Conducting ISO 27001 Annex A compliance audits for SEBON-licensed brokerage firms, assessing all 93 controls against implemented policies, vendor agreements, and IT infrastructure evidence.
- Reviewing internal information security policies, vendor contracts, and technical documentation to evaluate control maturity and identify compliance gaps.
- Drafting formal audit observations, gap analyses, and missing policy documents aligned with NEPSE-approved compliance formats.
- Mapping vendor SLA and third-party evidence to relevant ISO 27001 controls and coordinating with client stakeholders to validate audit findings.
- Producing consolidated audit reports and compliance checklists for client submission and internal review.

Penetration Tester 06/2025 – Present

Himalayan Integrated Cloud Technologies

- Conducting Vulnerability Assessment and Penetration Testing (VAPT) on web applications, network infrastructure, firewalls, antivirus systems, and databases.
- Identifying security vulnerabilities and providing remediation recommendations.
- Assisting in security audits and risk assessment processes.
- Preparing detailed technical reports for clients and internal teams.

CTF Player 2022 – Present

Attack On Hash Function

- My focus is on reverse engineering and PWN challenges.
- Coordinate with team members to solve complex challenges.

EDUCATION

BSc (Hons) Ethical Hacking and Cybersecurity 2023 – 2026

Softwarica College of IT and E-Commerce Kathmandu, Bagmati

Cambridge A-levels 2020 – 2022

Saipal Academy Dhumbaharai, Kathmandu

TECHNICAL SKILLS

Networking (CCNA 1 & 2), Python, Bash Scripting, Reverse Engineering, Cryptography, Linux Environments, Docker, Wazuh (SIEM), IT Audit (ISO 27001)

ACHIEVEMENTS

HackAstra CTF 01/12/2025
Herald College
1st Runner-Up

Softwarica Hackfest 01/12/2024
Softwarica
2nd Runner-Up

OWASP Nepal Cybersecurity Challenge 01/12/2024
OWASP Nepal
1st Runner-Up

IEEE LogPoint CTF TU 01/12/2024
IEEE LogPoint
Top 10

Softwarica CTF Competition 01/12/2023
Softwarica
Winner

COMMUNITY ENGAGEMENT

- TechX Softwarica 2024: Wazuh SIEM and Evilginx phishing demonstration.
- TechX Softwarica 2025: C2 (Command and Control) and real time CTF platform demonstration

PROJECTS

Command and Control
- Designed a custom C2 system for remote command execution simulation
- Demonstrates attacker infrastructure and post-exploitation concepts

Cryptography-based E-Voting System
- Implemented PKI, RSA encryption, and certificate validation
- Ensured integrity, confidentiality, and secure vote verification

Intrusion Detection System
- Built hybrid IDS using signature + anomaly detection techniques
- Integrated traffic monitoring and suspicious behavior detection

Web Enumeration Tool
- Developed automated tool for web reconnaissance and vulnerability discovery
- Performs endpoint discovery and misconfiguration detection

Networking Architecture
- Designed enterprise-grade architecture with network segmentation, firewall rules, and isolation
- Applied defense-in-depth security principles

Wazuh SIEM
- actual detection engine. It receives logs/events from enrolled endpoints (agents)
- handles agent enrollment, active response, vulnerability detection, File Integrity Monitoring, and SCA scans.

Ajax-Security-Team (MITRE-ATT-CK-G0130)
- academic red-team case study that emulates the tactics, techniques, and procedures (TTPs)
- simulated corporate endpoint, executed inside a fully isolated virtual lab and mapped end-to-end to the MITRE ATT&CK framework